kaspersky

Kaspersky Unified Monitoring and Analysis Platform

Руководство по эксплуатации

Версия программы: 2.1

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Внимание! Права на этот документ являются собственностью АО «Лаборатории Касперского» (далее также «Лаборатория Касперского»). Все права защищены законодательством Российской Федерации об авторском праве и международными договорами. За незаконное копирование и распространение документа и его отдельных частей нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с применимым законодательством.

Копирование в любой форме, распространение, в том числе в переводе, любых материалов возможны только с письменного разрешения «Лаборатории Касперского».

Документ и связанные с ним графические изображения могут быть использованы только в информационных, некоммерческих или личных целях.

Документ может быть изменен без предварительного уведомления.

За содержание, качество, актуальность и достоверность используемых в документе материалов, права на которые принадлежат другим правообладателям, а также за возможный ущерб, связанный с использованием этих материалов, «Лаборатория Касперского» ответственности не несет.

Зарегистрированные товарные знаки и знаки обслуживания, используемых в документе, являются собственностью их правообладателей.

Дата редакции документа: 01.04.2023

© 2023 АО «Лаборатория Касперского»

https://www.kaspersky.ru
https://support.kaspersky.ru

О «Лаборатории Касперского» (https://www.kaspersky.ru/about/company)

Содержание

О программе Kaspersky Unified Monitoring and Analysis Platform
- Что нового
- Комплект поставки
- Аппаратные и программные требования
- Интерфейс KUMA
- Совместимость с другими программами

Архитектура программы
- Ядро
- Коллектор
- Коррелятор
- Хранилище
- Основные сущности
  - О тенантах
  - О событиях
  - Об алертах
  - Об инцидентах
  - Об активах
  - О ресурсах
  - О сервисах
  - Об агентах
  - Об уровне важности

Установка и удаление KUMA
- Требования к установке программы
- Установка для демонстрации
  - Подготовка файла инвентаря для демонстрационной установки
  - Демонстрационная установка программы
  - Расширение демонстрационной установки
- Установка KUMA в производственной среде
  - Настройка сетевого доступа
  - Подготовка контрольной машины
  - Подготовка целевой машины
  - Подготовка файла инвентаря
    - О файле инвентаря

Установка KUMA без использования кластера Kubernetes
Установка KUMA с размещением Ядра в кластере Kubernetes
Обновление KUMA с версии 2.0.X
Перенос Ядра KUMA в новый кластер Kubernetes
Установка программы
Изменение самоподписанного сертификата веб-консоли
Добавление коллектора в сетевую инфраструктуру
Установка KUMA в отказоустойчивом варианте
Об отказоустойчивости KUMA
Аппаратные требования к узлам Kubernetes
Дополнительные требования к установке программы
Управление Kubernetes и доступ к KUMA
Часовой пояс в кластере Kubernetes
Удаление KUMA
Обновление предыдущих версий KUMA
Устранение ошибок при обновлении
Лицензирование программы
О Лицензионном соглашении
О лицензии
О Лицензионном сертификате
О лицензионном ключе
О файле ключа
Добавление лицензионного ключа в веб-интерфейс программы
Просмотр информации о добавленном лицензионном ключе в веб-интерфейсе программы
Удаление лицензионного ключа в веб-интерфейсе программы
Интеграция с другими решениями
Интеграция с Kaspersky Security Center
Настройка параметров интеграции с Kaspersky Security Center
Добавление тенанта в список тенантов для интеграции с Kaspersky Security Center
Создание подключения к Kaspersky Security Center
Изменение подключения к Kaspersky Security Center
Удаление подключения к Kaspersky Security Center
Импорт событий из базы Kaspersky Security Center
Интеграция с Kaspersky Endpoint Detection and Response
Импорт событий Kaspersky Endpoint Detection and Response
Настройка отображения ссылки на обнаружение Kaspersky Endpoint Detection and Response в информации о событии KUMA
Интеграция с Kaspersky CyberTrace

Интеграция поиска по индикаторам CyberTrace
Настройка CyberTrace для приема и обработки запросов
Создание правил обогащения событий
Интеграция интерфейса CyberTrace
Интеграция с Kaspersky Threat Intelligence Portal
Инициализация интеграции
Запрос данных от Kaspersky Threat Intelligence Portal
Просмотр данных от Kaspersky Threat Intelligence Portal
Обновление данных от Kaspersky Threat Intelligence Portal
Интеграция с R-Vision Incident Response Platform
Настройка интеграции в KUMA
Настройка интеграции в R-Vision IRP
Добавление полей инцидента ALERT_ID и ALERT_URL
Создание коллектора в R-Vision IRP
Создание коннектора в R-Vision IRP
Создание правила на закрытие алерта в KUMA при закрытии инцидента в R-Vision IRP
Работа с алертами с помощью R-Vision IRP
Интеграция с Active Directory, Active Directory Federation Services и FreeIPA
Подключение по протоколу LDAP
Включение и выключение LDAP-интеграции
Добавление тенанта в список тенантов для интеграции с LDAP-сервером
Создание подключения к LDAP-серверу
Создание копии подключения к LDAP-серверу
Изменение подключения к LDAP-серверу
Изменение частоты обновления данных
Изменение срока хранения данных
Запуск задач на обновление данных об учетных записях
Удаление подключения к LDAP-серверу
Аутентификация с помощью доменных учетных записей
Включение и выключение доменной аутентификации
Настройка соединения KUMA с FreeIPA
Настройка соединения KUMA с Active Directory
Настройка соединения KUMA с Active Directory Federation Services
Настройка подключения на стороне Active Directory Federation Services
Действия при ошибке Da
Интеграция с НКЦКИ
Интеграция с Security Vision Incident Response Platform
Настройка интеграции в KUMA

- Настройка интеграции в Security Vision IRP
  - Импорт и настройка коннектора
  - Настройка обработчика, расписания и рабочего процесса
- Интеграция с Kaspersky Industrial CyberSecurity for Networks
  - Настройка интеграции в KICS for Networks
  - Настройка интеграции в KUMA
  - Включение и выключение интеграции с KICS for Networks
  - Изменение частоты обновления данных
  - Особенности импорта информации об активах из KICS for Networks
  - Изменение статуса актива KICS for Networks
- Интеграция с Kaspersky Automated Security Awareness Platform
  - Создание токена в ASAP и получение ссылки для API-запросов
  - Настройка интеграции в KUMA
  - Просмотр данных о пользователях ASAP и изменение учебных групп
- Ресурсы KUMA
  - Операции с ресурсами
    - Создание, переименование, перемещение и удаление папок ресурсов
    - Создание, дублирование, перемещение, редактирование и удаление ресурсов
    - Обновление ресурсов
      - Настройка пользовательского источника с использованием Kaspersky Update Utility
    - Экспорт ресурсов
    - Импорт ресурсов
  - Правила корреляции
    - Правила корреляции типа standard
    - Правила корреляции типа simple
    - Правила корреляции типа operational
    - Переменные в корреляторах
      - Свойства переменных
      - Требования к переменным
      - Функции переменных
      - Объявление переменных
  - Нормализаторы
    - Параметры парсинга событий
    - Обогащение в нормализаторе
    - Условия передачи данных в дополнительный парсер
    - Предустановленные нормализаторы
  - Коннекторы
    - Просмотр параметров коннектора

- Добавление коннектора
- Параметры коннекторов
  - Тип internal
  - Тип tcp
  - Тип udp
  - Тип netflow
  - Тип sflow
  - Тип nats
  - Тип kafka
  - Тип http
  - Тип sql
  - Тип file
  - Тип 1c-xml
  - Тип 1c-log
  - Тип diode
  - Тип ftp
  - Тип nfs
  - Тип wmi
  - Тип wec
  - Тип snmp
  - Тип snmp-trap
    - Настройка источника SNMP-trap сообщений для Windows
      - Настройка и запуск служб SNMP и SNMP Trap
      - Настройка службы Event to Trap Translator
- Правила агрегации
- Правила обогащения
- Точки назначения
  - Тип nats
  - Тип tcp
  - Тип http
  - Тип diode
  - Тип kafka
  - Тип file
  - Тип storage
  - Тип correlator
- Фильтры
- Правила реагирования
  - Правила реагирования для Kaspersky Security Center

- Правила реагирования для пользовательского скрипта
- Правила реагирования для KICS for Networks
- Правила реагирования для Kaspersky Endpoint Detection and Response
- Правила реагирования через Active Directory
- Шаблоны уведомлений
- Активные листы
  - Просмотр таблицы активных листов
  - Добавление активного листа
  - Просмотр параметров активного листа
  - Изменение параметров активного листа
  - Дублирование параметров активного листа
  - Удаление активного листа
  - Просмотр записей в активном листе
  - Поиск записей в активном листе
  - Добавление записи в активный лист
  - Дублирование записей в активном листе
  - Изменение записи в активном листе
  - Удаление записей в активном листе
  - Импорт данных в активный лист
  - Экспорт данных из активного листа
- Словари
- Прокси-серверы
- Секреты
- Правила сегментации
  - Параметры правил сегментации
  - Привязка правил сегментации к правилам корреляции
- Сервисы KUMA
  - Инструменты сервисов
    - Получение идентификатора 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
- Создание набора ресурсов для хранилища
- Создание сервиса хранилища в веб-интерфейсе KUMA
- Установка хранилища в сетевой инфраструктуре KUMA
- Создание коррелятора
- Запуск мастера установки коррелятора
- Шаг 1. Общие параметры коррелятора
- Шаг 2. Глобальные переменные
- Шаг 3. Корреляция
- Шаг 4. Обогащение
- Шаг 5. Правила реагирования
- Шаг 6. Маршрутизация
- Шаг 7. Проверка параметров
- Установка коррелятора в сетевой инфраструктуре KUMA
- Проверка правильности установки коррелятора
- Создание коллектора
- Запуск мастера установки коллектора
- Шаг 1. Подключение источников событий
- Шаг 2. Транспорт
- Шаг 3. Парсинг событий
- Шаг 4. Фильтрация событий
- Шаг 5. Агрегация событий
- Шаг 6. Обогащение событий
- Шаг 7. Маршрутизация
- Шаг 8. Проверка параметров
- Установка коллектора в сетевой инфраструктуре KUMA
- Проверка правильности установки коллектора
- Обеспечение бесперебойной работы коллекторов
- Управление потоком событий с помощью rsyslog
- Управление потоком событий с помощью nginx
- Создание агента
- Создание набора ресурсов для агента
- Создание сервиса агента в веб-интерфейсе KUMA
- Установка агента в сетевой инфраструктуре KUMA
- Установка агента KUMA на устройствах Linux
- Установка агента KUMA на устройствах Windows
- Автоматически созданные агенты
- Обновление агентов

- Передача в KUMA событий из изолированных сегментов сети
  - Конфигурационный файл diode-агента
  - Описание полей секретов
  - Установка Linux-агента в изолированном сегменте сети
  - Установка Windows-агента в изолированном сегменте сети
- Передача в KUMA событий с машин Windows

Аналитика
- Панель мониторинга
  - Создание макета панели мониторинга
  - Выбор макета панели мониторинга
  - Выбор макета панели мониторинга в качестве макета по умолчанию
  - Редактирование макета панели мониторинга
  - Удаление макета панели мониторинга
  - Преднастроенные виджеты
  - Включение и отключение режима ТВ
- Отчеты
  - Шаблон отчета
    - Создание шаблона отчета
    - Настройка расписания отчетов
    - Изменение шаблона отчета
    - Копирование шаблона отчета
    - Удаление шаблона отчета
  - Сформированные отчеты
    - Просмотр отчетов
    - Создание отчетов
    - Сохранение отчетов
    - Удаление отчетов
- Состояние источников
  - Список источников событий
  - Политики мониторинга
- Виджеты
  - Стандартные виджеты
  - Настраиваемая аналитика по событиям
  - Настраиваемая аналитика по активным листам
  - Особенности отображения данных в виджетах

Работа с тенантами
- Выбор тенанта
- Правила принадлежности к тенантам

Работа с инцидентами
- О таблице инцидентов
- Сохранение и выбор конфигураций фильтра инцидентов
- Удаление конфигураций фильтра инцидентов
- Просмотр информации об инциденте
- Создание инцидента
- Обработка инцидентов
- Изменение инцидентов
- Автоматическая привязка алертов к инцидентам
- Категории и типы инцидентов
- Взаимодействие с НКЦКИ
  - Особенности экспорта в НКЦКИ из иерархической структуры KUMA
  - Экспорт данных в НКЦКИ
  - Дополнение данных об инциденте по запросу
  - Отправка файлов в НКЦКИ
  - Обмен сообщениями с сотрудниками НКЦКИ
  - Допустимые категории и типы инцидентов НКЦКИ
  - Уведомления об изменении статуса инцидента в НКЦКИ

Работа в режиме иерархии
- Первое включение режима иерархии
- Создание сертификата узла
- Соединение узлов в иерархическую структуру
  - Подключение к родительскому узлу
  - Подключение дочернего узла
  - Отключение от узла
  - Изменение узла
  - Ошибки при подключении узлов
- Просмотр своей ветви иерархии и доступных узлов
- Изменение профиля узла
- Просмотр инцидентов от дочерних узлов
- Включение и выключение режима иерархии

Работа с алертами
- Настройка таблицы алертов
  - Фильтрация алертов
  - Сохранение и выбор конфигураций фильтра алертов
  - Удаление конфигураций фильтра алертов
- Просмотр информации об алерте
- Изменение название алертов

- Обработка алертов
- Детализированный анализ
- Срок хранения алертов и инцидентов
- Уведомления об алертах

Работа с событиями

- Фильтрация и поиск событий
  - Формирование SQL-запроса с помощью конструктора
  - Создание SQL-запроса вручную
  - Создание пресета
    - Применение пресета
  - Ограничение сложности запросов в режиме детализированного анализа
  - Фильтрация событий по периоду
  - Сохранение и выбор конфигураций фильтра событий
  - Удаление конфигураций фильтра событий
  - Поддерживаемые функции ClickHouse
- Просмотр информации о событии
- Экспорт событий
- Выбор хранилища
- Получение статистики по событиям в таблице
- Настройка таблицы событий
- Обновление таблицы событий
- Открытие окна корреляционного события

Ретроспективная проверка

Работа с геоданными

- Формат геоданных
- Конвертация геоданных из MaxMind и IP2Location
- Импорт и экспорт геоданных
- Сопоставление геоданных по умолчанию

Управление активами

- Категории активов
- Добавление категории активов
- Настройка таблицы активов
- Поиск активов
- Экспорт данных об активах
- Просмотр информации об активе
- Добавление активов
  - Добавление информации об активах в веб-интерфейсе KUMA
  - Импорт информации об активах из Kaspersky Security Center

- Импорт информации об активах из MaxPatrol
- Импорт информации об активах из KICS for Networks
- Примеры сравнения полей активов при импорте
- Назначение активу категории
- Изменение параметров активов
- Удаление активов
- Обновление программ сторонних производителей и закрытие уязвимостей на активах Kaspersky Security Center
- Перемещение активов в выбранную группу администрирования
- Аудит активов
- Настройка аудита активов
- Хранение и поиск событий аудита активов
- Включение и выключение аудита активов
- Настраиваемые поля активов
- Активы, относящиеся к критический информационной инфраструктуре

Управление пользователями

- Роли пользователей
- Создание пользователя
- Редактирование пользователя
- Редактирование своей учетной записи

Управление KUMA

- Вход в веб-интерфейс программы
- Просмотр метрик KUMA
- Работа с задачами KUMA
- Просмотр таблицы задач
- Настройка отображения таблицы задач
- Просмотр результата выполнения задачи
- Повторный запуск задачи
- Работа с задачами Kaspersky Security Center
- О создании задач KUMA в Kaspersky Security Center
- Запуск задач Kaspersky Security Center вручную
- Автоматический запуск задач Kaspersky Security Center
- Проверка статуса задач Kaspersky Security Center
- Подключение к SMTP-серверу
- Онлайн-справка KUMA
- Журналы KUMA
- Резервное копирование KUMA
- Резервное копирование KUMA с помощью файла kuma

- Уведомления KUMA
- Обращение в службу технической поддержки
- REST API
  - Создание токена
  - Настройка прав доступа к API
  - Авторизация API-запросов
  - Стандартная ошибка
  - Операции
    - Просмотр списка активных листов на корреляторе
    - Импорт записей в активный лист
    - Поиск алертов
    - Закрытие алертов
    - Поиск активов
    - Импорт активов
    - Удаление активов
    - Поиск событий
    - Просмотр информации о кластере
    - Поиск ресурсов
    - Загрузка файла с ресурсами
    - Просмотр содержимого файла с ресурсами
    - Импорт ресурсов
    - Экспорт ресурсов
    - Скачивание файла с ресурсами
    - Поиск сервисов
    - Поиск тенантов
    - Просмотр информации о предъявителе токена
    - Обновление словаря в сервисах
    - Получение словаря
    - Просмотр пользовательских полей активов
    - Создание резервной копии Ядра KUMA
    - Восстановление Ядра KUMA из резервной копии
- Приложения
  - Команды для запуска и установки компонентов вручную
  - Проверка целостности файлов KUMA
  - Модель данных нормализованного события
  - Модель данных алерта
  - Модель данных актива
  - Модель данных учетной записи

Поля событий аудита

- Поля событий с общей информацией
- Пользователь успешно вошел в систему или не смог войти
- Логин пользователя успешно изменен
- Роль пользователя успешно изменена
- Другие данные пользователя успешно изменены
- Пользователь успешно вышел из системы
- Пароль пользователя успешно изменен
- Пользователь успешно создан
- Пользователю успешно назначена роль
- Роль пользователя успешно отозвана
- Токен доступа пользователя успешно изменен
- Сервис успешно создан
- Сервис успешно удален
- Сервис успешно перезагружен
- Сервис успешно перезапущен
- Сервис успешно запущен
- Сервис успешно сопряжен
- Статус сервиса изменен
- Раздел хранилища удален пользователем
- Раздел хранилища автоматически удален в связи с истечением срока действия
- Активный лист успешно очищен или операция завершилась с ошибкой
- Элемент активного листа успешно изменен или операция завершилась с ошибкой
- Элемент активного листа успешно удален или операция завершилась с ошибкой
- Активный лист успешно импортирован или операция завершилась с ошибкой
- Активный лист успешно экспортирован
- Ресурс успешно добавлен
- Ресурс успешно удален
- Ресурс успешно обновлен
- Актив успешно создан
- Актив успешно удален
- Категория актива успешно добавлена
- Категория актива успешно удалена
- Параметры успешно обновлены
- Тенант успешно создан
- Тенант успешно включен
- Тенант успешно выключен
- Другие данные тенанта успешно изменены

Изменена политика хранения данных после изменения дисков
Словарь успешно обновлен на сервисе или операция завершилась ошибкой
Ответ в Active Directory
Реагирование через KICS for Networks
Реагирование через Kaspersky Automated Security Awareness Platform
Реагирование через KEDR
Настройка получения событий Auditd с помощью rsyslog
Установка коллектора KUMA для получения событий Auditd
Настройка сервера источника событий
Проверка поступления событий Auditd в коллектор
Настройка получения событий KATA/EDR с помощью Syslog
Настройка передачи событий KATA/EDR в KUMA
Создание коллектора KUMA для получения событий KATA/EDR
Установка коллектора KUMA для получения событий KATA/EDR
Проверка поступления событий KATA/EDR в KUMA
Настройка получения событий Kaspersky Security Center в формате CEF
Настройка передачи событий Kaspersky Security Center в формате CEF
Настройка коллектора KUMA для сбора событий Kaspersky Security Center
Установка коллектора KUMA для сбора событий Kaspersky Security Center
Проверка поступления событий Kaspersky Security Center в KUMA
Настройка получения событий Kaspersky Security Center из БД MS SQL
Создание учетной записи в БД MS SQL
Настройка службы SQL Server Browser
Создание секрета в KUMA
Настройка коннектора
Настройка коллектора KUMA для получения событий Kaspersky Security Center из БД MS SQL
Установка коллектора KUMA для сбора событий Kaspersky Security Center из БД MS SQL
Проверка поступления событий Kaspersky Security Center из БД MS SQL
Информация о стороннем коде
Уведомления о товарных знаках
Глоссарий
SELinux (Security-Enhanced Linux)
SIEM
STARTTLS
userPrincipalName
Агрегация
Веб-интерфейс KUMA
Кластер

Коллектор

Коннектор

Нормализация

Обогащение

Парсинг

Роль

Сетевой порт

Событие

Фильтр

О программе Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Unified Monitoring and Analysis Platform (далее KUMA или "программа") – это комплексное программное решение, сочетающее в себе следующие функциональные возможности:

- получение, обработка и хранение событий информационной безопасности;
- анализ и корреляция поступающих данных;
- поиск по полученным событиям;
- создание уведомлений о выявлении признаков угроз информационной безопасности.

Программа построена на микросервисной архитектуре. Это означает, что вы можете создавать и настраивать только необходимые микросервисы (далее также "сервисы"), что позволяет использовать KUMA и как систему управления журналами, и как полноценную SIEM-систему. Кроме того, благодаря гибкой маршрутизации потоков данных вы можете использовать сторонние сервисы для дополнительной обработки событий.

Что нового

- Реализована возможность автоматического и ручного обновления репозитория для получения пакетов с новыми правилами корреляции и коннекторами к источникам логов.
- Реализована возможность холодного хранения событий.
- Добавлены новые коннекторы: SNMP traps, 1C log, 1C xml.
- Добавлена интеграция с платформой онлайн-обучения Kaspersky Automated Security Awareness Platform.
- Добавлен новый тип реагирования: правило реагирования через Active Directory.

- Расширен перечень форматов для генерации отчетов. Теперь доступны следующие форматы: HTML, PDF, CSV, раздельный CSV, Excel.

- Расширена интеграция с НКЦКИ.

- Добавлена возможность создавать единые для всех тенантов (универсальные) макеты панели мониторинга и наполнять их данными по доступным текущему пользователю тенантам. Таким образом количество используемых в системе макетов можно значительно сократить и не создавать отдельные типовые макеты для каждого тенанта.

- Добавлена интеграция с Active Directory Federation Services для входа в систему без ввода логина и пароля (сценарий Single Sign On - SSO).

- Добавлена поддержка домена FreeIPA для входа в систему.

- Добавлена возможность получать из LDAP пользовательские атрибуты учетных записей Active Directory и обогащать события по **пользовательским атрибутам учетных записей AD**.

  Перед настройкой обогащения событий с помощью пользовательских атрибутов убедитесь, что пользовательские атрибуты настроены в AD.

  Чтобы обогащать события учетными записями с помощью пользовательских атрибутов:

  1. Добавьте **Пользовательские атрибуты учетных записей AD** в Параметрах подключения к LDAP.

     Невозможно добавить стандартные **Импортируемые атрибуты из AD** в качестве пользовательских. Например, если вы захотите добавить стандартны й атрибут

     accountExpires в качестве пользовательского атрибута, при сохранении параметров подключения KUMA вернет ошибку.

     Из Active Directory можно запросить следующие атрибуты учетных записей:

     - `accountExpires`
     - `badPasswordTime`
     - `cn`
     - `co`

- `company`
- `department`
- `description`
- `displayName` (по этому атрибуту события можно искать при корреляции)
- `distinguishedName` (по этому атрибуту события можно искать при корреляции)
- `division`
- `employeeID`
- `givenName`
- `l`
- `lastLogon`
- `lastLogonTimestamp`
- `mail` (по этому атрибуту события можно искать при корреляции)
- `mailNickname`
- `managedObjects`
- `manager`
- `memberOf` (по этому атрибуту события можно искать при корреляции)
- `mobile`
- `name`
- `objectCategory`
- `objectGUID` (этот атрибут запрашивается из Active Directory всегда)
- `objectSid`
- `physicalDeliveryOfficeName`

- `pwdLastSet`
- `sAMAccountName` (по этому атрибуту события можно искать при корреляции)
- `sAMAccountType`
- `sn` (по этому атрибуту события можно искать при корреляции)
- `streetAddress`
- `telephoneNumber`
- `title`
- `userAccountControl` (по этому атрибуту события можно искать при корреляции)
- `userPrincipalName` (по этому атрибуту события можно искать при корреляции)
- `whenChanged`
- `whenCreated`

После того, как вы добавите пользовательские атрибуты в Параметрах подключения к LDAP, раскрывающийся список **LDAP-атрибуты** в коллекторе будет автоматически дополнен. Пользовательские атрибуты можно отличить по знаку вопроса рядом с именем атрибута. Если для нескольких доменов вы добавили один и тот же атрибут, в раскрывающемся списке атрибут будет указан один раз, а домены можно просмотреть, если навести курсор на знак вопроса. Названия доменов отображаются в виде ссылок: если вы нажмете на ссылку, домен автоматически добавится в **Сопоставление с учетными записями LDAP**, если прежде он не был добавлен.

Если вы удалили пользовательский атрибут в Параметрах подключения к LDAP, удалите вручную строку с атрибутом из таблицы сопоставления в коллекторе. Информация об атрибутах учетных записей в KUMA обновляется каждый раз после того, как вы выполните импорт учетных записей.

2. Импортируйте учетные записи.
3. В коллекторе в таблице **Обогащение полей KUMA** задайте правила сопоставления полей KUMA с атрибутами LDAP.
4. Перезапустите коллектор.

После перезапуска коллектора KUMA начнет обогащать события учётными записями.

- Расширены возможности работы с активами: появилась возможность добавлять активам настраиваемые поля, добавлена возможность поиска по активам с учетом названий полей, а также возможность экспорта результатов поиска в файл.
- В разделе с поиском по событиям добавлены пресеты полей событий, позволяющие быстро настраивать колонки таблицы поиска в зависимости от анализируемых логов.
- Расширена отказоустойчивость системы.
- В информации об активах теперь отображаются дополнительные сведения о защите хостов с KES for Windows и KES for Linux. Отображении информации доступно, если вы импортировали актив из KSC.
- Для событий о срабатываниях KATA/EDR добавлена ссылка, позволяющая перейти на карточку соответствующего алерта в интерфейс консоли управления KATA/EDR.
- На этапе получения событий появилась возможность использовать преобразования **hex**, **base64**, **base64url** для обработки бинарных значений в журналах.
- Расширены возможности корреляции:
  - Дополнен список функций переменных. С их помощью теперь можно преобразовывать ключи или формулировать условия.
  - Добавлена возможность управлять последовательностью применения правил корреляции в корреляторе.
- Добавлены правила сегментации алертов.
- Добавлены нормализаторы для источников событий.
- Добавлена новая роль Аналитик первой линии: такие пользователи смогут создавать собственный контент в системе, но не смогут изменять ресурсы, созданные другими пользователями.
- Расширено протоколирование системы и возможность экспортировать журналы компонентов программы в файлы.

Комплект поставки

В комплект поставки входят следующие файлы:

- kuma-ansible-installer-<номер сборки>.tar.gz – используется для установки компонентов KUMA без возможности развертывания в отказоустойчивой конфигурации;
- kuma-ansible-installer-ha-<номер сборки>.tar.gz – используется для установки компонентов KUMA с возможностью развертывания в отказоустойчивой конфигурации;
- файлы с информацией о версии (примечания к выпуску) на русском и английском языках.

Аппаратные и программные требования

Рекомендуемые требования к оборудованию

На перечисленном ниже оборудовании могут обрабатываться до 40 000 событий в секунду. Этот показатель зависит от типа анализируемых событий и от эффективности парсера. Следует также учитывать, что большее количество ядер будет эффективнее, чем их меньшее количество, но с более высокой частотой процессора.

- Серверы для установки коллекторов:
  - Процессор: Intel или AMD от 4 ядер (8 потоков) с поддержкой набора инструкций SSE 4.2 или 8 vCPU (виртуальных процессоров).
  - ОЗУ: 16 ГБ.

    Каждому коллектору, на котором используется обогащения событий геоданными, требуется дополнительный объем оперативной памяти, равный размеру базы геоданных.
  - Диск: 500 ГБ доступного места на диске, смонтированного в разделе /opt.
- Серверы для установки корреляторов:
  - Процессор: Intel или AMD от 4 ядер (8 потоков) с поддержкой набора инструкций SSE 4.2 или 8 vCPU (виртуальных процессоров).
  - ОЗУ: 16 ГБ.
  - Диск: 500 ГБ доступного места на диске, смонтированного в разделе /opt.
- Серверы для установки Ядра:
  - Процессор: Intel или AMD от 4 ядер (8 потоков) с поддержкой набора инструкций SSE 4.2 или 4 vCPU (виртуальных процессоров).
  - ОЗУ: 16 ГБ.

При импорте геоданных серверу требуется дополнительный объем оперативной памяти, равный размеру базы геоданных.

- Диск: 500 ГБ доступного места на диске, смонтированного в разделе /opt.

- Серверы для установки хранилищ:

  - Процессор: Intel или AMD от 12 ядер (24 потока) с поддержкой набора инструкций SSE 4.2 или 24 vCPU (виртуальных процессоров).

    Требуется поддержка команд SSE4.2.

  - ОЗУ: 48 ГБ.

  - Диск: 500 ГБ доступного места на диске, смонтированного в разделе /opt.

  Для подключения системы хранения данных (далее также СХД) к серверам хранилища требуется использовать высокоскоростные протоколы (например, Fiber Channel или iSCSI 10G). Мы не рекомендуем подключать СХД с использованием протоколов прикладного уровня (например, NFS, SMB).

  Использование твердотельных накопителей позволяет улучшить индексирование кластерных узлов и повысить эффективность поиска.

  Смонтированные локально жесткие диски или твердотельные накопители эффективнее внешних дисковых массивов (JBOD). Рекомендуется использовать RAID 0 для скорости, а RAID 10 для избыточности.

  Для повышения надежности не рекомендуется развертывать все кластерные узлы на одном JBOD-массиве или одном физическом сервере (если используются виртуальные серверы).

  Для повышения эффективности рекомендуется держать все серверы в одном центре данных.

  > В качестве файловой системы на серверах кластера ClickHouse рекомендуется использовать ext4.

- Машины для установки агентов Windows:

  - Процессор: одноядерный, 1.4 ГГц или выше.

  - ОЗУ: 512 МБ.

  - Диск: 1 ГБ.

  - ОС:

    - Microsoft Windows 2012.
    - Microsoft Windows Server 2012 R2.
    - Microsoft Windows Server 2016.
    - Microsoft Windows Server 2019.
    - Microsoft Windows 10 (20H2, 21H1).
- Машины для установки агентов Linux:
    - Процессор: одноядерный, 1.4 ГГц или выше.
    - ОЗУ: 512 МБ.
    - Диск: 1 ГБ.
    - ОС:
        - Ubuntu 20.04 LTS, 21.04.
        - Oracle Linux версии 8.6.
        - Astra Linux Special Edition РУСБ.10015-01 (2021-1126SE17 оперативное обновление 1.7.1).
- Поддерживается установка в виртуальных средах:
    - VMWare 6.5 и выше.
    - Hyper-V для Windows Server 2012 R2 и выше.
    - KVM Qemu version 4.2 и выше.
    - ПК СВ "Брест" РДЦП.10001-02.

Требования к программному обеспечению

Для развертывания компонентов Коллектор, Коррелятор, Ядро и Хранилище поддерживается использование операционных систем Oracle Linux 8.6 и Astra Linux Special Edition (исполнение РУСБ.10015-01, 2021-1126SE17 оперативное обновление 1.7.1).

Требования к сети

Пропускная способность сетевого интерфейса должна быть не менее 100 Мбит/с.

Чтобы программа KUMA обрабатывала более 20 000 событий в секунду, необходимо обеспечить скорость передачи данных между узлами ClickHouse не менее 10 Гбит/с.

Дополнительные требования

Компьютеры, используемые для веб-интерфейса KUMA:

- Процессор: Intel Core i3 8-го поколения.
- ОЗУ: 8 ГБ.
- Установленный браузер Google Chrome 102 или более поздней версии либо Mozilla Firefox 103 или более поздней версии.

Интерфейс KUMA

Работа с программой осуществляется через веб-интерфейс.

Окно веб-интерфейса программы содержит следующие элементы:

- разделы в левой части окна веб-интерфейса программы;
- закладки 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 закладках 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 KUMA и программы Kaspersky Endpoint Security для Linux каталог report.db может достигать больших размеров и занимать все дисковое пространство. Чтобы избежать этой проблемы, рекомендуется обновить программу Kaspersky Endpoint Security для Linux до версии 11.2 или выше.

Архитектура программы

Стандартная установка программы включает следующие компоненты:

- *Ядро*, включающее графический интерфейс для мониторинга и управления настройками компонентов системы.
- Один или несколько *коллекторов*, которые получают сообщения из источников событий и осуществляют их парсинг, нормализацию и, если требуется, фильтрацию и/или агрегацию.
- *Коррелятор*, который анализирует полученные из коллекторов нормализованные события, выполняет необходимые действия с активными листами и создает алерты в соответствии с правилами корреляции.
- *Хранилище*, в котором содержатся нормализованные события и зарегистрированные алерты.

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

Архитектура KUMA

Ядро

Ядро – это центральный компонент KUMA, на основе которого строятся все прочие сервисы и компоненты. Предоставляемый Ядром графический пользовательский интерфейс веб-интерфейса предназначен как для повседневного использования операторами и аналитиками, 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;
- расследовать угрозы безопасности на основе полученных событий.

Коллектор

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

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

Алгоритм работы коллектора состоит из следующих этапов:

1. **Получение сообщений из источников событий**

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

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

   В программе доступны следующие типы коннекторов:

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

- wec;
- snmp.

2. **Парсинг и нормализация событий**

   События, полученные коннектором, обрабатываются с помощью парсера 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.
   - NetFlow v5.
   - NetFlow v9.
   - IPFIX (v10).

3. **Фильтрация нормализованных событий**

   Вы можете настроить фильтры, которые позволяют отсеивать события, удовлетворяющие заданным условиям. События, не удовлетворяющие условиям фильтрации, будут отправляться на 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;
   - cybertrace;

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

Правила преобразования позволяют преобразовать содержимое 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 – выбор текстовых строк по заданным номерам 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 сообщений, передаваемых в хранилище и/или коррелятор. Например, можно агрегировать в одно событие все сообщения о сетевых подключениях, выполненных по одному и тому же протоколу (транспортного и прикладного уровней) между двумя IP-адресами и полученных в течение заданного интервала времени. Если настроены правила агрегации, несколько сообщений могут обрабатываться и сохраняться как одно событие. Это помогает снизить нагрузку на сервисы, которые отвечают за дальнейшую обработку событий, экономит место для хранения и экономит частоту обработки событий (EPS).

6 Передача нормализованных событий

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

Коррелятор

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

Полученные в ходе анализа данные применяются для выполнения следующих задач:

- выявление алертов;
- уведомление о выявленных алертах;
- управление содержимым активных листов;
- отправка корреляционных событий в настроенные точки назначения.

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

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

Алгоритм работы коррелятора состоит из следующих этапов:

1. **Получение события**

   Коррелятор получает нормализованное событие из коллектора или другого сервиса.

2. **Применение правил корреляции**

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

3. **Реагирование на алерт**

Вы можете задать действия, которые программа будет выполнять при выявлении алерта. В программе доступны следующие действия:

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

4 **Отправка корреляционного события**

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

Хранилище

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

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

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

Основные сущности

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

О тенантах

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

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

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

По умолчанию в KUMA созданы два тенанта:

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

- Общий – в этот тенант главный администратор может поместить ресурсы, категории активов и политики мониторинга, которые смогут задействовать пользователи всех тенантов.

О событиях

События – это случаи активности сетевых устройств и служб, связанных с безопасностью, которые можно обнаружить и записать. Например, события включают попытки входа в систему, взаимодействия с базой данных и рассылку информации с датчиков. Каждое отдельное событие может показаться бессмысленным, но если рассматривать их вместе, они формируют более широкую картину сетевой активности, помогающую идентифицировать угрозы безопасности. Это основная функциональность KUMA.

KUMA получает события из журналов и реструктурирует их, приводя данные из разнородных источников к единому формату (этот процесс называется нормализацией). После этого события фильтруются, агрегируются и отправляются в сервис коррелятора для анализа и в сервис хранилища для хранения. Когда KUMA распознает заданное событие или последовательность событий, создаются *корреляционные события*, которые также анализируются и сохраняются. Если событие или последовательность событий указывают на возможную угрозу безопасности, KUMA создает алерт: это оповещение об угрозе, к которому привязываются все относящиеся к нему данные и которое требует внимания специалиста по безопасности.

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

Первые шаги выполняются в коллекторе.

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

2. Нормализованное событие. Нормализатор – это набор парсеров, которые преобразуют данные "сырого" события так, чтобы они соответствовали модели данных KUMA. После этой трансформации исходное сообщение становится *нормализованным событием* и может быть проанализировано в KUMA. С этого момента KUMA работает только с

нормализованными событиями. Необработанные, "сырые" события больше не используются, но их можно сохранить как часть нормализованных событий внутри поля `Raw`.

В программе представлены следующие нормализаторы:

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

По завершении этого этапа нормализованные события можно использовать для анализа.

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

Следующие этапы жизненного цикла события проходят в корреляторе.

Типы событий:

1. Базовое событие. Событие, которое было нормализовано.

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

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

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

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

Об алертах

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

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

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

На основании алертов можно создать инциденты.

Работа с алертами в KUMA описана в этом разделе.

Об инцидентах

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

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

Инциденты можно экспортировать в НКЦКИ.

Об активах

Активы – это сетевые устройства, зарегистрированные в KUMA. Активы генерируют сетевой трафик при отправке и получении данных. Программа KUMA 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).

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

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

Работа с активами в KUMA описана в этом разделе.

О ресурсах

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

О сервисах

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

- Одна часть сервиса создается внутри веб-интерфейса KUMA на основе набора ресурсов для сервисов.

- Вторая часть сервиса устанавливается в сетевой инфраструктуре, где развернута система KUMA, в качестве одного из ее компонентов. Серверная часть сервиса может состоять из нескольких экземпляров: например, сервисы одного и того же агента или хранилища могут быть установлены сразу на нескольких машинах.

Между собой части сервисов соединены с помощью идентификатора сервисов.

Об агентах

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

Типы агентов:

- wmi – используются для получения данных с удаленных машин Windows с помощью Windows Management Instrumentation. Устанавливается на устройства Windows.
- wec – используются для получения журналов Windows с локальной машины 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 – 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.
- 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.

Об уровне важности

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

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

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

Возможные значения уровня важности:

- Низкий
- Средний
- Высокий
- Критический

Установка и удаление KUMA

В этом разделе описана установка KUMA. Установка программы возможна в следующих вариантах:

- Установка на одном сервере для ознакомления с возможностями программы.
- Установка программы в производственной среде.
- Установка программы в производственной среде в отказоустойчивой конфигурации.

Требования к установке программы

Требования при установке на операционной системе Oracle Linux

- Образ диска для установки доступен на официальном сайте Oracle.

- Убедиться, что в операционной системе установлен Python версии 3.6 или выше.
- Убедиться, что в операционной системе НЕ включен модуль SELinux. Работа KUMA и установщика KUMA совместно с включенным SELinux не поддерживается.
- Убедиться, что в операционной системе установлена система управления пакетами pip3.
- Убедиться, что в операционной системе установлены следующие пакеты:
  - netaddr
  - firewalld

  Эти пакеты можно установить с помощью следующих команд:

  - `pip3 install netaddr`
  - `yum install firewalld`
- Для корректного формирования отчетов в форматах HTML и PDF и возможности их скачивания необходимо установить на машине с Ядром KUMA следующие пакеты:
  - nss
  - gtk2
  - atk
  - libxkbcommon
  - libdrm
  - at-spi2-atk
  - mesa-libgbm
  - alsa-lib

Требования при установке на операционной системе Astra Linux Special Edition

- Убедиться, что в операционной системе установлен Python версии 3.6 или выше.
- Убедиться, что в операционной системе установлена система управления пакетами pip3.

- Убедиться, что в операционной системе установлены следующие пакеты:
  - python3-apt
  - curl
  - libcurl4

  Эти пакеты можно установить с помощью команды `apt install python3-apt curl libcurl4`.

- Убедиться, что в операционной системе установлены следующие зависимые пакеты:
  - netaddr
  - python3-cffi-backend

  Эти пакеты можно установить с помощью следующих команд:

  - `apt install python3-cffi-backend`
  - `pip3 install netaddr`

  > Если вы собираетесь из KUMA обращаться к базам данных Oracle DB, необходимо установить пакет libaio1.

- Пользователю, под которым вы собираетесь устанавливать программу, требуется присвоить необходимый уровень прав с помощью команды `sudo pdpl-user -i 63 <имя пользователя>`.

- Для корректного формирования отчетов в форматах HTML и PDF и возможности их скачивания необходимо установить на машине с Ядром KUMA следующие пакеты:
  - libgtk2.0.0
  - libnss3
  - libatk-adaptor
  - libdrm-common
  - libgbm1
  - libxkbcommon0

- libasound2

Общие требования к установке

- Имя сервера, на котором запускается установщик, должно отличаться от `localhost` или `localhost.<домен>`. Установщик можно запустить из любой директории.
- Перед развертыванием программы требуется убедиться, что серверы, предназначенные для установки ее компонентов, соответствуют аппаратным и программным требованиям.
- Адресация компонентов KUMA осуществляется по полному доменному имени (FQDN) хоста. Перед установкой программы убедитесь, что команда `hostnamectl status` возвращает правильное имя FQDN хоста в поле `Static hostname`.
- Для синхронизации времени на всех серверах с сервисами KUMA рекомендуется использовать протокол Network Time Protocol (NTP).
- В качестве файловой системы на серверах кластера ClickHouse рекомендуется использовать ext4.

Установка для демонстрации

Для демонстрации вы можете развернуть компоненты KUMA на одном сервере. Перед установкой программы ознакомьтесь с требованиями к установке KUMA, а также аппаратными и системными требованиями.

Установка KUMA происходит в несколько этапов:

1. **Подготовка контрольной машины**

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

2. **Подготовка целевой машины**

   На целевые машины устанавливаются компоненты программы. Контрольную машину можно использовать в качестве целевой.

3. **Подготовка файла инвентаря для демонстрационной установки**

   Создайте файл инвентаря с описанием сетевой структуры компонентов программы, с помощью которого установщик сможет развернуть KUMA.

4. **Установка программы для демонстрации**

   Установите программу и получите URL и учетные данные для входа в веб-интерфейс.

При необходимости установленную на демонстрации программу можно разнести на разные серверы для полноценной работы.

Подготовка файла инвентаря для демонстрационной установки

Установка, обновление и удаление компонентов KUMA производится из папки с распакованным установщиком с помощью инструмента Ansible и созданного пользователем *файла инвентаря* с перечнем хостов компонентов KUMA и других параметров. В случае демонстрационной установке хост для всех компонентов будет указан один и тот же. Файл инвентаря имеет формат YAML.

Чтобы создать файл инвентаря для демонстрационной установки:

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

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

2. Создайте файл инвентаря, скопировав шаблон single.inventory.yml.template:

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

3. Отредактируйте параметры файла инвентаря single.inventory.yml:

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

     ```
     deploy_example_services: true
     ```

     Демонстрационные сервисы можно создать только при первичной установке KUMA – при обновлении системы с помощью того же файла инвентаря демонстрационные сервисы созданы не будут.

   - Если вы устанавливаете KUMA для демонстрации и хотите разместить все компоненты программы на одной машине, присвойте параметру ansible_connection значение local:

     ```
     ansible_connection: local
     ```

4. Замените в файле инвентаря все строки `kuma.example.com` на хост целевой машины, на которую следует установить компоненты KUMA.

Файл инвентаря создан. С его помощью можно установить KUMA для демонстрации.

Рекомендуется не удалять файл инвентаря после установки KUMA:

- Если этот файл изменить (например, дополнить данными о новом сервере для коллектора), его можно использовать повторно для обновления системы новым

компонентом.

- Этот же файл инвентаря можно использовать для удаления KUMA.

Демонстрационная установка программы

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

Чтобы установить KUMA для демонстрации:

1. На контрольной машине войдите в папку с распакованным установщиком.
2. Подложите в папку <папка установщика>/roles/kuma/files/ файл с лицензионным ключом.

   Файл ключа должен иметь название license.key.
3. Запустите установщик, выполнив следующую команду:

   ```
   sudo ./install.sh single.inventory.yml
   ```
4. Примите условия Лицензионного соглашения.

   > Если вы не примите условия Лицензионного соглашения, программа не будет установлена.

   Компоненты KUMA установлены на целевой машине. На экране будет отображен URL веб-интерфейса KUMA и указано имя пользователя и пароль, которые необходимо использовать для доступа к веб-интерфейса.

   > По умолчанию адрес веб-интерфейса KUMA – `https://kuma.example.com:7220`.

   > Учетные данные, используемые для входа по умолчанию (после первого входа требуется изменить пароль учетной записи admin):
   > - логин – `admin`
   > - пароль – `mustB3Ch@ng3d!`

Рекомендуется сохранить файл инвентаря, использованный для установки программы. С его помощью можно дополнить систему компонентами или удалить KUMA.

Демонстрационную установку можно расширить до полноценной.

Расширение демонстрационной установки

Расширение демонстрационной установки производится путем установки программы по шаблону distributed.inventory.yml поверх установленной KUMA.

Расширение демонстрационной установки производится в несколько этапов:

1. **Установка программы**

   На этапе подготовке файла инвентаря укажите хост демонстрационного сервера поместите в группе `kuma_core`.

2. **Удаление демонстрационных сервисов**

   В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** скопируйте идентификаторы существующих сервисов и удалите их.

   Затем удалите сервисы с машины, где они были установлены, с помощью команды `sudo /opt/kaspersky/kuma/kuma <collector/correlator/storage> --id <идентификатор сервиса> --uninstall`. Повторите команду удаления для каждого сервиса.

3. **Пересоздание сервисов на нужных машинах**

Если демонстрационная установка KUMA производилась в отказоустойчивом варианте и при этом использовались совмещенные узлы Kubernetes, являющиеся контроллерами и рабочими узлами, то при расширении установки рекомендуется перенести данные в новый кластер путем резервного копирования данных Ядра KUMA и последующего восстановления из резервной копии на новой установке.

Установка KUMA в производственной среде

Перед установкой программы ознакомьтесь с требованиями к установке KUMA, а также аппаратными и системными требованиями. Установка KUMA происходит в несколько этапов:

1. **Настройка сетевого доступа**

   Убедитесь, что все необходимые порты открыты для взаимодействия между компонентами KUMA с учетом структуры безопасности на вашем предприятии.

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**

   Создайте файл инвентаря с описанием сетевой структуры компонентов программы, с помощью которого установщик сможет развернуть KUMA.

5. **Установка программы**

   Установите программу и получите URL и учетные данные для входа в веб-интерфейс.

6. **Создание сервисов**

   Создайте сервисы в веб-интерфейсе KUMA и установите их на предназначенных для них целевых машинах.

   Сервисы KUMA следует устанавливать только после завершения установки KUMA. Сервисы можно устанавливать в любом порядке.

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

При необходимости вы можете изменить корневой сертификат KUMA на сертификат своей компании.

Настройка сетевого доступа

Для правильной работы программы нужно убедиться, что компоненты KUMA могут взаимодействовать с другими компонентами и программами по сети через протоколы и порты, указанные во время установки компонентов KUMA. В таблице ниже показаны значения сетевых портов по умолчанию.

Сетевые порты, используемые для взаимодействия компонентов KUMA друг с другом

Протокол	Порт	Направление	Назначение подключения
HTTPS	7222	От клиента KUMA к серверу с компонентом Ядро KUMA.	Реверс-прокси к системе CyberTrace.

HTTPS	8123	От сервиса хранилища к узлу кластера ClickHouse.	Запись и получение нормализованных событий в кластере ClickHouse.
HTTPS	9009	Между репликами кластера ClickHouse.	Внутренняя коммуникация между репликами кластера ClickHouse для передачи данных кластера.
TCP	2181	От узлов кластера ClickHouse к сервису координации репликации ClickHouse keeper.	Получение и запись репликами серверов ClickHouse метаинформации о реплицировании.
TCP	2182	От сервисов координации репликации ClickHouse keeper друг к другу.	Внутренняя коммуникация между сервисами координации репликации, используемая для достижения кворума.
TCP	7210	От всех компонентов KUMA на сервер Ядра KUMA.	Получение конфигурации KUMA от сервера Ядра KUMA
TCP	7215	От коллектора KUMA к коррелятору KUMA.	Отправка данных коллектором в коррелятор KUMA
TCP	7220	• От клиента KUMA к серверу с компонентом Ядро KUMA. • От хостов хранилищ к серверу с компонентом Ядро KUMA.	• Доступ пользователей к веб-интерфейсу KUMA. • Взаимодействие хостов хранилищ с Ядром KUMA при установке или обновлении.

TCP	7221 и другие порты, используемые для установки сервисов в качестве значения параметра --api.port <порт>	От Ядра KUMA к сервисам KUMA.	Администрирование сервисов из веб-интерфейса KUMA
TCP	7223	К серверу Ядра KUMA.	Порт, используемый по умолчанию для API-запросов.
TCP	8001	От Victoria Metrics к серверу ClickHouse.	Получение метрик работы сервера ClickHouse.
TCP	9000	От клиента ClickHouse к узлу кластера ClickHouse.	Запись и получение данных в кластере ClickHouse.

Автоматически открываемые порты

Ниже перечислены порты, которые открываются установщиком автоматически при установке KUMA в варианте без использования кластера Kubernetes:

- Порты, используемые для функционирования Ядра KUMA:
  - 7209/tcp
  - 7210/tcp
  - 7220/tcp
  - 7222/tcp
  - 7223/tcp
- Порты, используемые для функционирования хранилища KUMA:
  - 2181/tcp
  - 2182/tcp
  - 8001/tcp

    - 9000/tcp
    - 9009/tcp
- Порты, используемые демонстрационными ресурсами из состава OOTB:
    - 7230/tcp
    - 7231/tcp
    - 7232/tcp
    - 7233/tcp
    - 7234/tcp
    - 7235/tcp
    - 5140/tcp
    - 5140/udp
    - 5141/tcp
    - 5144/udp

Ниже перечислены порты, которые открываются установщиком автоматически при установке KUMA в варианте с использованием кластера Kubernetes в дополнение к портам, перечисленным выше:

- Порты, используемые балансировщиком нагрузки:
    - 6443/tcp
    - 8132/tcp
    - 9443/tcp
    - 7209/tcp
    - 7210/tcp
    - 7220/tcp
    - 7222/tcp
    - 7223/tcp

- Порты управляющих узлов:
  - 2380/tcp
  - 6443/tcp
  - 8132/tcp
  - 9443/tcp
  - 10250/tcp
- Порты рабочих узлов:
  - 179/tcp
  - 10250/tcp
  - 9500/tcp
  - 51820/udp
  - 51821/udp
  - 7209/tcp
  - 7210/tcp
  - 7220/tcp
  - 7222/tcp
  - 7223/tcp

Подготовка контрольной машины

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

Чтобы подготовить контрольную машину для установки KUMA:

1. Установите на контрольную машину операционную систему и установите на нее необходимые пакеты.
2. Настройте сетевой интерфейс.

   Для удобства можно воспользоваться утилитой с графическим интерфейсом nmtui.

3. Настройте синхронизацию системного времени с NTP-сервером:

   a. Если машина не имеет прямого доступа в интернет, 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. Выждите несколько секунд и выполните следующую команду:

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

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

4. 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
   > ```

   ```
   sudo 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.

5. 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 контрольной 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:

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

6. Скопируйте архив с установщиком KUMA на контрольную машину и распакуйте его с помощью следующей команды (потребуется около 2 ГБ дискового пространства):

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

Контрольная машина готова для установки KUMA.

Подготовка целевой машины

На целевые машины устанавливаются компоненты программы.

Чтобы подготовить целевую машину для установки компонентов KUMA:

1. Установите на контрольную машину операционную систему и установите на нее необходимые пакеты.

2. Настройте сетевой интерфейс.

   Для удобства можно воспользоваться утилитой с графическим интерфейсом nmtui.

3. Настройте синхронизацию системного времени с NTP-сервером:

   a. Если машина не имеет прямого доступа в интернет, 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. Выждите несколько секунд и выполните следующую команду:

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

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

4. Установите имя хоста. Настоятельно рекомендуется использовать FQDN. Например: kuma-1.mydomain.com.

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

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

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

6. Выполните следующую команду и запишите результат:

   ```
   hostname -f
   ```

   Данное имя хоста потребуется указать при установке KUMA. Целевая машина должна быть доступна по этому имени для контрольной машины.

Целевая машина готова для установки компонентов KUMA.

> Контрольную машину можно использовать в качестве целевой. Для этого подготовьте контрольную машину, а затем выполните на ней шаги 4–6 из инструкции по подготовке целевой машины.

Подготовка файла инвентаря

Установка, обновление и удаление компонентов KUMA производится из папки с распакованным установщиком с помощью инструмента Ansible и созданного пользователем *файла инвентаря* с перечнем хостов компонентов KUMA и других параметров. Файл инвентаря имеет формат YAML.

Чтобы создать файл инвентаря:

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

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

2. Создайте файл инвентаря, скопировав необходимый шаблон:

   ```
   cp <название шаблона>.template <название шаблона>
   ```

   Пример: `cp distributed.inventory.yml.template distributed.inventory.yml`

   Доступные шаблоны:

   - single.inventory.yml – используется для демонстрационной установки KUMA.
   - distributed.inventory.yml – используется для установки KUMA в производственных средах, расширения демонстрационных установок KUMA и обновления KUMA с версий 2.0.x.
   - k0s.inventory.yml – используется для установки KUMA в отказоустойчивом варианте и переносе Ядра ранее установленной KUMA в кластер Kubernetes.

3. Отредактируйте параметры файла инвентаря в зависимости от варианта установки программы:

   - Установка KUMA без использования кластера Kubernetes.
   - Установка KUMA с размещением Ядра в кластере Kubernetes.
   - Обновление KUMA с версии 2.0.X.
   - Перенос Ядра KUMA в новый кластер Kubernetes.

   Файл инвентаря создан. С его помощью можно установить KUMA.

Рекомендуется не удалять файл инвентаря после установки KUMA:

- Если этот файл изменить (например, дополнить данными о новом сервере для коллектора), его можно использовать повторно для обновления системы новым компонентом.
- Этот же файл инвентаря можно использовать для удаления KUMA.

О файле инвентаря

Вы можете указать значения параметров конфигурации KUMA в файле инвентаря. Эти значения будут использованы при развертывании, обновлении и удалении программы.

Вы можете создать файл инвентаря на основе шаблонов, включенных в установщик. Доступные шаблоны:

- single.inventory.yml.template – используется для демонстрационной установки KUMA. Содержит минимальный набор параметров, оптимизированный для установки на одной машине, без использования кластера Kubernetes.
- distributed.inventory.yml.template – используется для установки KUMA в производственных средах без использования кластера Kubernetes.
- k0s.inventory.yml.template – используется для установки или переноса KUMA в кластер Kubernetes.

Файл инвентаря может включать следующие блоки:

- `all`
- `kuma`
- `kuma_k0s`

Для каждого хоста должен быть указан FQDN в формате <имя хоста>.<домен> или IP-адрес.

Пример:

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

Блок all

В этом блоке указываются переменные, которые распространяются на все хосты, указанные в инвентаре, включая неявно заданный localhost, на котором запущена установка. Переменные можно переопределять на уровне групп хостов или даже 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	Возможные значения
`ansible_connection`	Способ подключения к целевым машинам.	• `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, то нужно использовать имя пользователя, имеющего право на подключение по SSH и повышение привилегий через su или sudo.
`ansible_become`	Признак необходимости повышения привилегий пользователя, от имени которого осуществляется установка компонентов KUMA.	`true`, если значение ansible_user – не `root`.

`ansible_become_method`	Способ повышения привилегий пользователя, от имени которого осуществляется установка компонентов KUMA .	`su` или `sudo`, если значение ansible_user – не `root`.
`ansible_ssh_private_key_file`	Путь к закрытому ключу в формате /<путь>/.ssh/id_rsa. Эту переменную необходимо задать, если требуется указать файл ключа, отличный от используемого по умолчанию: ~/.ssh/id_rsa.	
`deploy_to_k8s`	Признак разворачивания компонент KUMA в кластере Kubernetes.	• `false` – значение по умолчанию для шаблонов single.inventory.yml и distributed.inventory.yml. • `true` – значение по умолчанию для шаблона k0s.inventory.yml.
`need_transfer`	Признак перемещения компонент KUMA в кластере Kubernetes.	• `false` – значение по умолчанию для шаблонов single.inventory.yml и distributed.inventory.yml. • `true`

		– значение по умолчанию для шаблона k0s.inventory.yml.
`airgap`	Признак отсутствия подключения к интернету.	`true` – значение по умолчанию для шаблона k0s.inventory.yml.
`generate_etc_hosts`	Признак регистрации машин в DNS-зоне вашей организации. В этом случае установщик автоматически дополнит файлы /etc/hosts на машинах, куда устанавливаются компоненты KUMA, IP-адресами машин из файла инвентаря. Указанные IP-адреса должны быть уникальными.	• `false`. • `true`.
`deploy_example_services`	Признак создания демонстрационных сервисов при установке.	• `false` – сервисы не нужны. Значение по умолчанию для шаблонов distributed.inventory.yml и k0s.inventory.yml. • `true` – сервисы нужно создать. Значение по умолчанию для

		шаблона single.inventory.yml.
`low_resources`	Признак установки KUMA в тестовых и демонстрационных окружениях с ограниченными вычислительными ресурсами. В этом случае Ядро может быть установлено на хосте с 4 ГБ свободного дискового пространства. По умолчанию переменная отсутствует.	

Блок kuma

В этом блоке перечисляются параметры компонентов KUMA, развернутых вне кластера Kubernetes.

В блоке доступны следующие разделы:

- `vars` – в этом разделе можно указать переменные, которые распространяются на все хосты, указанные в блоке `kuma`.
- `children` – в этом разделе можно перечислить группы параметров компонентов:
  - `kuma_core` – параметры Ядра KUMA. Может содержать только один хост.
  - `kuma_collector` – параметры коллекторов KUMA. Может содержать один и более хостов.
  - `kuma_correlator` – параметры корреляторов KUMA. Может содержать один и более хостов.
  - `kuma_storage` – параметры узлов хранилища KUMA. Может содержать один и более хостов.

В разделе `storage` вы можете указать параметры узлов, которые определяют роль узлов в хранилище и его структуру. **Подробнее о компонентах хранилища.**

Кластер ClickHouse – логическая группа машин, обладающих всеми накопленными нормализованными событиями KUMA. Подразумевает наличие одного или нескольких логических *шардов*.

*Шард (*параметр `shard` *)* – логическая группа машин, 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 машинами.

*Реплика (*параметр `replica` *)* – машина, являющаяся членом логического шарда и обладающая 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 (параметр `keeper`) – машина, участвующая в **координации** репликации данных на уровне **всего** кластера. На весь кластер требуется хотя бы одна машина с этой ролью. Рекомендуемое количество машин с такой ролью – 3. Число машин, участвующих в координации репликации, должно быть **нечетным**. Роль *кипера* и *реплики* можно совмещать.

Каждая машина может иметь следующие комбинации параметров:

- `shard + replica + keeper`
- `shard + replica`
- `keeper`

Если указаны параметры `shard` и `replica`, машина является частью кластера и принимает участие в накоплении и поиске нормализованных событий KUMA. Если дополнительно указан параметр `keeper`, машина также принимает участие в координации репликации данных на уровне всего кластера.

Если указан только параметр `keeper`, машина **не** будет накапливать нормализованные события, но будет участвовать в координации репликации данных на уровне всего кластера. Значения параметра keeper должны быть уникальными.

Если в рамках одного шарда определено несколько реплик, значение параметра replica должно быть уникальным **в рамках этого шарда**.

Если для кипера выделена отдельная машина, при развертывании демонстрационных сервисов или при обновлении с версии KUMA 2.0.x в конфигурации с несколькими узлами кластера хранилища первым хостом в группе должен идти хост с ненулевым значением параметра `keeper`.

Блок kuma_k0s

В этом блоке задаются параметры кластера Kubernetes, использование которого обеспечивает отказоустойчивость KUMA.

Минимальная конфигурация, на которую можно произвести установку – один контроллер, совмещенный с рабочим узлом. Данная конфигурация не обеспечивает отказоустойчивости Ядра и служит для демонстрации возможностей или проверки программной среды.

Для реализации отказоустойчивости необходимы 2 выделенных контроллера кластера и балансировщик нагрузки. Для промышленной эксплуатации рекомендуется использовать выделенные рабочие узлы и контроллеры. Если контроллер кластера находится под рабочей нагрузкой и под (англ. pod) с Ядром KUMA размещается на нем, его отключение приведет к полной потере доступа к Ядру.

В блоке доступны следующие разделы:

- `vars` – в этом разделе можно указать переменные, которые распространяются на все хосты, указанные в блоке `kuma`.
- `children` – в этом разделе задаются параметры кластера Kubernetes, использование которого обеспечивает отказоустойчивость KUMA.

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

Группа переменных	Описание	
`kuma_lb`	FQDN балансировщика нагрузки. Балансировщик пользователь устанавливает самостоятельно. Если внутри группы указать параметр `kuma_managed_lb = true`, во время установки KUMA балансировщик будет автоматически настроен, на его хосте будут открыты необходимые сетевые TCP-порты (6443, 8132, 9443, 7209, 7210, 7220, 7222, 7223), а также будет выполнена перезагрузка для применения изменений.	
`kuma_control_plane_master`	Хост, выполняющий роль выделенного главного контроллера кластера.	Группы для указания главного контроллера. Хост необходимо задать только в одной из них.
`kuma_control_plane_master_worker`	Хост, совмещающий роль главного контроллера и рабочего узла кластера.	
`kuma_control_plane`	Хосты, выполняющие роль выделенного контроллера кластера.	Группы для указания второстепенных контроллеров.
`kuma_control_plane_worker`	Хосты, совмещающие роль контроллера и рабочего узла кластера.	
`kuma_worker`	Рабочие узлы кластера.	

Для каждого хоста в этом блоке должен быть указан его уникальный FQDN и IP-адрес в параметре `ansible_host`, кроме хоста в разделе `kuma_lb` – для него должен быть указан FQDN. Хосты в группах не должны повторяться.

Для каждого рабочего узла кластера и для контроллера кластера, совмещенного с рабочим узлом, должен быть указан параметр `extra_args: "--labels=kaspersky.com/kuma-core=true,kaspersky.com/kuma-ingress=true,node.longhorn.io/create-default-disk=true"`.

Установка KUMA без использования кластера Kubernetes

При установке KUMA в производственной среде без использования функций отказоустойчивости в файле инвентаря необходимо или не указывать параметры `deploy_to_k8s` и `need_transfer`, или присвоить им значение `false`.

Пример файла инвентаря

```
all:
  vars:
    ansible_connection: ssh
    ansible_user: root
    deploy_to_k8s: False
    need_transfer: False
    airgap: True
    deploy_example_services: True
kuma:
  children:
    kuma_core:
      hosts:
        kuma.example.com:
          mongo_log_archives_number: 14
          mongo_log_frequency_rotation: daily
          mongo_log_file_size: 1G
```

```
  kuma_collector:
    hosts:
      kuma2.example.com:
  kuma_correlator:
    hosts:
      kuma2.example.com:
  kuma_storage:
    hosts:
      kuma3.example.com:
        shard: 1
        replica: 1
        keeper: 1
```

Установка KUMA с размещением Ядра в кластере Kubernetes

Минимальная конфигурация, на которую можно произвести установку – один контроллер, совмещенный с рабочим узлом. Данная конфигурация не обеспечивает отказоустойчивости Ядра и служит для демонстрации возможностей или проверки программной среды.

Для реализации отказоустойчивости необходим 1 выделенный главный контроллер кластера и минимум 2 рабочих узла. Для промышленной эксплуатации рекомендуется использовать выделенные рабочие узлы и контроллеры. Если контроллер кластера находится под рабочей нагрузкой и под с Ядром KUMA размещается на нем, его отключение приведет к полной потере доступа к Ядру.

Пример файла инвентаря с 1 выделенным контроллером и 2 рабочими узлами

```
all:
  vars:
    ansible_connection: ssh
```

```
    ansible_user: root
    deploy_to_k8s: True
    need_transfer: false
    generate_etc_hosts: false
    airgap: True
    deploy_example_services: False
kuma:
  children:
    kuma_core:
      hosts:
        kuma.example.com:
          mongo_log_archives_number: 14
          mongo_log_frequency_rotation: daily
          mongo_log_file_size: 1G
    kuma_collector:
      hosts:
        kuma.example.com:
    kuma_correlator:
      hosts:
        kuma.example.com:
    kuma_storage:
      hosts:
        kuma.example.com:
```

```
          shard: 1

          replica: 1

          keeper: 1

kuma_k0s:

  children:

    kuma_control_plane_master:

      hosts:

        kuma2.example.com:

          ansible_host: 10.0.1.10

    kuma_control_plane_master_worker:

    kuma_control_plane:

    kuma_control_plane_worker:

    kuma_worker:

      hosts:

        kuma.example.com:

          ansible_host: 10.0.1.11

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

        kuma3.example.com:

          ansible_host: 10.0.1.12

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

Пример файла инвентаря с управляемым балансировщиком трафика, 3 выделенными контроллерами и 2 рабочими узлами

```
all:
  vars:
    ansible_connection: ssh
    ansible_user: root
    deploy_to_k8s: True
  need_transfer: false
    generate_etc_hosts: false
    airgap: True
    deploy_example_services: False
kuma:
  children:
    kuma_core:
      hosts:
        kuma.example.com:
          mongo_log_archives_number: 14
          mongo_log_frequency_rotation: daily
          mongo_log_file_size: 1G
    kuma_collector:
      hosts:
        kuma.example.com:
    kuma_correlator:
```

```
      hosts:
        kuma.example.com:
    kuma_storage:
      hosts:
        kuma.example.com:
          shard: 1
          replica: 1
          keeper: 1
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"
```

Обновление KUMA с версии 2.0.X

При обновлении KUMA в файле инвентаря необходимо или не указывать параметры `deploy_to_k8s` и `need_transfer`, или присвоить им значение `false`. Параметру `deploy_example_services` необходимо присвоить значение `false`.

Файл инвентаря должен содержать те же хосты, которые использовались при установке KUMA версии 2.0.X.

При работе установщика по такому файлу инвентаря обновляются все компоненты KUMA до версии 2.1.0. 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.

- 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.

Пример файла инвентаря

```
all:

  vars:

    ansible_connection: ssh

    ansible_user: root

    deploy_to_k8s: False

    need_transfer: False

    airgap: True

    deploy_example_services: False

kuma:

  children:

    kuma_core:

      hosts:

        kuma.example.com:

          mongo_log_archives_number: 14

          mongo_log_frequency_rotation: daily
```

```
          mongo_log_file_size: 1G
    kuma_collector:
      hosts:
        kuma2.example.com:
kuma_correlator:
      hosts:
        kuma2.example.com:
    kuma_storage:
      hosts:
        kuma3.example.com:
          shard: 1
          replica: 1
          keeper: 1
```

Перенос Ядра KUMA в новый кластер Kubernetes

Подготовка файла инвентаря

При переносе Ядра KUMA в кластер Kubernetes при создании файла инвентаря рекомендуется использовать файл шаблона k0s.inventory.yml.template.

Используемый файл инвентаря в секциях `kuma_core`, `kuma_ collector`, `kuma_correlator`, `kuma_storage` должен содержать те же хосты, которые использовались при обновлении KUMA с версии 2.0.x до версии 2.1 или при новой установке программы. В файле инвентаря необходимо присвоить параметрам `deploy_to_k8s`, `need_transfer` и `airgap` значение `true`. Параметру `deploy_example_services` необходимо присвоить значение `false`.

Пример файла инвентаря с 1 выделенным контроллером и 2 рабочими узлами

```
all:
```

```
    vars:
      ansible_connection: ssh
      ansible_user: root
      deploy_to_k8s: True
      need_transfer: True
      airgap: True
      deploy_example_services: False
  kuma:
    children:
      kuma_core:
        hosts:
          kuma.example.com:
            mongo_log_archives_number: 14
            mongo_log_frequency_rotation: daily
            mongo_log_file_size: 1G
      kuma_collector:
        hosts:
          kuma.example.com:
      kuma_correlator:
        hosts:
          kuma.example.com:
      kuma_storage:
        hosts:
```

```
        kuma.example.com:

          shard: 1

          replica: 1

          keeper: 1

kuma_k0s:

  children:

    kuma_control_plane_master:

      hosts:

        kuma2.example.com:

          ansible_host: 10.0.1.10

    kuma_control_plane_master_worker:

    kuma_control_plane:

    kuma_control_plane_worker:

    kuma_worker:

      hosts:

        kuma.example.com:

          ansible_host: 10.0.1.11

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

        kuma3.example.com:

          ansible_host: 10.0.1.12
```

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

Процесс переноса Ядра KUMA в новый кластер Kubernetes

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

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

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

На хосте с Ядром установщик выполняет следующие действия:

- Удаляет с хоста systemd-сервисы: kuma-core, kuma-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/log
  - /opt/kaspersky/kuma/core/logs
  - /opt/kaspersky/kuma/grafana/bin
  - /opt/kaspersky/kuma/mongodb/bin
  - /opt/kaspersky/kuma/mongodb/log

    - /opt/kaspersky/kuma/victoria-metrics/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/grafana

    - /opt/kaspersky/kuma/mongodb

    - /opt/kaspersky/kuma/victoria-metrics

    в директории:

    - /opt/kaspersky/kuma/core.moved

    - /opt/kaspersky/kuma/grafana.moved

    - /opt/kaspersky/kuma/mongodb.moved

    - /opt/kaspersky/kuma/victoria-metrics.moved

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

В случае возникновения проблем с переносом нужно проанализировать логи задания переноса core-transfer в пространстве имен kuma на кластере (задание доступно 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, то при переносе Ядра в кластер Kubernetes содержимое файла /etc/hosts с хоста с Ядром заносится в ConfigMap coredns. Если переноса Ядра не происходит, то в ConfigMap заносится содержимое /etc/hosts с хоста, на котором разворачивается главный контроллер.

Установка программы

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

Чтобы установить KUMA:

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

   Установщик поставляется в двух вариантах:

   - kuma-ansible-installer-2.1.0.XXX.tar.gz содержит все необходимое для установки KUMA без поддержки отказоустойчивых конфигураций.
   - kuma-ansible-installer-ha-2.1.0.XXX.tar.gz содержит все необходимое для установки KUMA, включая поддержку отказоустойчивых конфигураций.

2. Подложите в папку <папка установщика>/roles/kuma/files/ файл с лицензионным ключом.

   Файл ключа должен иметь название license.key.

3. Запустите установщик, выполнив следующую команду:

   ```
   sudo ./install.sh <название файла инвентаря>
   ```

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

4. Примите условия Лицензионного соглашения.

   > Если вы не примите условия Лицензионного соглашения, программа не будет установлена.

Компоненты KUMA установлены. На экране будет отображен URL веб-интерфейса KUMA и указано имя пользователя и пароль, которые необходимо использовать для доступа к веб-интерфейса.

По умолчанию адрес веб-интерфейса KUMA – `https://kuma.example.com:7220`.

Учетные данные, используемые для входа по умолчанию (после первого входа требуется изменить пароль учетной записи admin):
- логин – `admin`
- пароль – `mustB3Ch@ng3d!`

Рекомендуется сохранить файл инвентаря, использованный для установки программы. С его помощью можно дополнить систему компонентами или удалить KUMA.

Особенности установки в отказоустойчивом варианте

Если KUMA устанавливалась 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.

Изменение самоподписанного сертификата веб-консоли

Перед изменением сертификата KUMA сделайте резервную копию действующего сертификата и ключа с именами external.cert.old и external.key.old.

После установки Ядра KUMA установщик создает следующие сертификаты в папке /opt/kaspersky/kuma/core/certificates:

- Самоподписанный корневой сертификат ca.cert с ключом ca.key.

  Подписывает все другие сертификаты, которые используются для внутренней связи между компонентами KUMA.

- Сертификат internal.cert, подписанный корневым сертификатом, и ключ internal.key сервера Ядра.

  Используется для внутренней связи между компонентами KUMA.

- Сертификат веб-консоли KUMA external.cert и ключ external.key.

  Используется в веб-консоли KUMA и для запросов REST API.

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

  В следующем примере показано, как заменить самоподписанный CA Core с помощью корпоративного сертификата в формате PFX. Вы можете использовать инструкцию в качестве примера и адаптировать шаги в соответствии со своими потребностями.

Чтобы заменить сертификат веб-консоли KUMA на сертификат external:

1. Переключитесь на работу под пользователем с правами root:

   ```
   sudo -i
   ```

2. Перейдите в директорию с сертификатами:

   ```
   cd /opt/kaspersky/kuma/core/certificates
   ```

3. Сделайте резервную копию действующего сертификата и ключа:

   ```
   mv external.cert external.cert.old && mv external.key external.key.old
   ```

4. 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.

5. Поместите полученные файлы сертификата external.cert и ключа external.key в директорию /opt/kaspersky/kuma/core/certificates.

6. Смените владельца файлов ключа:

   ```
   chown kuma:kuma external.cert external.key
   ```

7. Перезапустите KUMA:

   ```
   systemctl restart kuma-core
   ```

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

Сертификат и ключ вашей компании заменены.

Добавление коллектора в сетевую инфраструктуру

Коллектор состоит из двух частей: одна часть создается внутри веб-интерфейса KUMA, а другая устанавливается в сетевой инфраструктуре, куда будут поступать события. В сетевой инфраструктуре устанавливается вторая часть коллектора.

Способ добавления сервиса в сетевую инфраструктуру зависит от варианта установки KUMA:

- Если программа устанавливалась без функций отказоустойчивости и не внедрялась в кластер Kubernetes, сервис коллектора необходимо установить на сервере, который будет принимать события.

- Если программа устанавливалась в отказоустойчивом варианте, сервис необходимо добавить в кластер Kubernetes.

Установка KUMA в отказоустойчивом варианте

Отказоустойчивость KUMA обеспечивается путем внедрения Ядра KUMA в кластер Kubernetes, развернутый установщиком KUMA.

Конфигурация кластера Kubernetes задается в файле инвентаря. Она должна включать один контроллер (выделенный или совмещенный с рабочим узлом), как минимум один рабочий узел (выделенный или совмещенный с контроллером), 0 и более выделенных рабочих узлов.

Для установки KUMA в отказоустойчивом исполнении используется установщик kuma-ansible-installer-ha-2.1.0.XXX.tar.gz.

При установке программы в отказоустойчивом исполнении Ядро KUMA помещается в кластер Kubernetes с помощью установщика и файла инвентаря. Поместить Ядро KUMA в кластер Kubernetes можно следующими способами:

- Установить KUMA в кластере Kubernetes.

- Перенести Ядро существующей установки KUMA в кластер Kubernetes.

Об отказоустойчивости KUMA

Отказоустойчивость KUMA обеспечивается путем внедрения Ядра KUMA в кластер Kubernetes, развернутый установщиком KUMA, а также использования внешнего балансировщика TCP-трафика.

В Kubernetes существует 2 роли узлов:

- контроллеры (control-plane) – узлы с данной ролью управляют кластером, хранят метаданные, распределяют рабочую нагрузку.

- рабочие (worker) – узлы с этой ролью несут полезную рабочую нагрузку, то есть размещают процессы KUMA.

Подробнее о требованиях к узлам кластера.

Для продуктивных инсталляций Ядра KUMA на Kubernetes критически важно выделить 3 обособленных узла с единственной ролью контроллера. Это позволит обеспечить отказоустойчивость самого кластера Kubernetes и гарантировать, что рабочая нагрузка (процессы KUMA и другие) не повлияет на задачи, связанные с управлением кластером Kubernetes. При этом, в случае использования средств виртуализации, следует убедиться, что данные узлы размещены на разных физических серверах и что на тех же физических серверах не присутствуют рабочие узлы.

В тех случаях, когда KUMA установлена для демонстрации, допускается использование узлов, которые совмещают роли контроллера и рабочего узла. Однако при расширении демонстрационной установки до промышленной необходимо переустановить кластер Kubernetes целиком, выделив 3 отдельных узла с ролью контроллера и, как минимум, 2 узла с ролью рабочего узла. Обновление KUMA до следующих версий при наличии узлов, совмещающих роли контроллера и рабочего узла, недоступно.

> Совмещайте разные роли на одном узле кластера только при демонстрационном развертывании программы.

Доступность Ядра KUMA при различных сценариях:

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

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

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

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

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

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

- **Потеря доступности одного или нескольких контроллеров кластера (кроме одного).**

  Рабочие узлы работают в обычном режиме. Перерыва в доступе к KUMA не возникает.

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

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

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

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

Аппаратные требования к узлам Kubernetes

Минимальные требования к узлам, составляющим кластер Kubernetes:

- Узел балансировщика:
  - Процессор: 2 ядра (потока).
  - ОЗУ: 2 ГБ.
  - Диск: 30 ГБ.
- Узел контроллера:
  - Процессор: 2 ядра (потока).
  - ОЗУ: 2 ГБ.
  - Диск: 30 ГБ.
- Рабочие узлы:
  - Процессор: 12 ядер (потоков).
  - ОЗУ: 12 ГБ.
  - Диск: 500 ГБ.
- Скорость передачи данных внутри кластера (между узлами, а также между узлами и балансировщиком): 10 гбит/с.

Кластер Kubernetes для развертывания KUMA в отказоустойчивом варианте включает (минимальная конфигурация):

- 1 узел балансировщика (не входит непосредственно в кластер).
- 3 узла-контроллера.

- 2 рабочих узла.

Дополнительные требования к установке программы

Если вы планируете защитить сетевую инфраструктуру KUMA с помощью программы Kaspersky Endpoint Security for Linux, необходимо сначала установить KUMA в кластере Kubernetes и только потом разворачивать Kaspersky Endpoint Security for Linux.

При установке KUMA 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

  Также для адресов этих блоков исключен трафик на прокси-серверы.
- Установлен и настроен балансировщик нагрузки nginx (подробнее о настройке nginx). Для установки можно воспользоваться, например, командой `sudo yum install nginx`.

  Если вы хотите, чтобы nginx был настроен автоматически в процессе установки KUMA, установите 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.

  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;
    }
}
```

- На сервере балансировщика добавлен ключ доступа с машины, с которой осуществляется установка KUMA.
- На сервере балансировщика в операционной системе НЕ включен модуль SELinux.
- На хостах установлены пакеты tar, systemctl, setfacl.

При установке KUMA автоматически проверяется соответствие хостов указанным ниже аппаратным требованиям. Если эти условия не выполняются, установка прерывается.

> Проверку этих условий при установке для демонстрации можно отключить, указав в файле инвентаря переменную `low_resources: true`.

- 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, то в /var/lib/ должно быть не менее 32GB свободного места. Если установка кластера на данный узел ранее уже проводилась, то размер требуемого свободного пространства уменьшается на размер директории /var/lib/k0s.

Дополнительные требования при установке на операционной системе Astra Linux Special Edition

- Установка KUMA в отказоустойчивом варианте поддерживается на операционной системе Astra Linux Special Edition РУСБ.10015-01 (2022-1011SE17MD, оперативное обновление 1.7.2.UU.1). Требуется версия ядра 5.15.0.33 или выше.
- На машинах, предназначенных для развертывания кластера Kubernetes, установлены следующие пакеты:
  - open-iscsi
  - wireguard
  - wireguard-tools

  Пакеты можно установить с помощью следующей команды:

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

Дополнительные требования при установке на операционной системе Oracle Linux

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

- iscsi-initiator-utils
- wireguard-tools

> Перед установкой пакетов необходимо добавить репозиторий EPEL в качестве источника: `sudo yum install oracle-epel-release-el8`

Пакеты можно установить с помощью следующей команды:

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

Управление Kubernetes и доступ к KUMA

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

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

Управление кластером Kubernetes

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

Доступ к Ядру KUMA

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

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

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

Часовой пояс в кластере Kubernetes

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

- В событиях аудита в поле `DeviceTimeZone` будет указан часовой пояс UTC+0.
- В сформированных отчетах пользователь будет видеть разницу между временем формирования отчета и временем браузера.

Удаление KUMA

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

Чтобы удалить KUMA:

1. На контрольной машине войдите в директорию установщика:

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

2. Выполните следующую команду:

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

   KUMA и все данные программы удалены с серверов.

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

Особенности удаления KUMA, установленной в отказоустойчивом варианте

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

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

Помимо установленных вне кластера компонентов KUMA на узлах кластера удаляются следующие директории и файлы:

- /usr/bin/k0s
- /etc/k0s/
- /var/lib/k0s/
- /usr/libexec/k0s/
- ~/k0s/ (для пользователя ansible_user)
- /opt/longhorn/
- /opt/cni/
- /opt/containerd

При удалении кластера возможен вывод на экран сообщений об ошибках, при котором работа установщика не прерывается.

- Для задач **Delete KUMA transfer job** и **Delete KUMA pod** такие сообщения можно игнорировать.
- Для задач **Reset k0s** (при сообщении об ошибке, содержащем текст "To ensure a full reset, a node reboot is recommended.") и Delete k0s Directories and files (при сообщении об ошибке, содержащем текст "Ошибка ввода/вывода: '/var/lib/k0s/kubelet/plugins/kubernetes.io/csi/driver.longhorn.io/") рекомендуется перезагрузить хост, к которому относится ошибка и выполнить повторное удаление KUMA с тем же файлом инвентаря.

После удаления KUMA необходимо перезагрузить хосты, на которых были установлены компоненты KUMA или Kubernetes.

Обновление предыдущих версий KUMA

Обновление выполняется одинаково на всех хостах с использованием установщика и файла инвентаря. Если вы используете версию 1.5 или 1.6 и хотите обновить KUMA до версии 2.1.x, сначала выполните обновление до 2.0.x, а затем с 2.0.x до 2.1.x.

Чтобы установить KUMA версии 2.1.x поверх версии 2.0.x, выполните шаги предварительной подготовки, а затем выполните обновление.

Предварительная подготовка

1. Создайте резервную копию Ядра KUMA.

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

3. Убедитесь в совместимости версий MongoDB, выполнив на машине с Ядром KUMA следующую последовательность команд:

   ```
   cd /opt/kaspersky/kuma/mongodb/bin/
   ./mongo
   use kuma
   db.adminCommand({getParameter: 1, featureCompatibilityVersion: 1})
   ```

   Если версия компонента отличается от 4.4, задайте значение 4.4 с помощью следующей команды:

   ```
   db.adminCommand({ setFeatureCompatibilityVersion: "4.4" })
   ```

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

5. Если в кластере ClickHouse у вас есть кипер, развернутый на отдельной машине, перед обновлением установить сервис хранилища на той же машине:

   - Создайте набор ресурсов сервиса.
   - Добавьте сервис в активные сервисы.
   - Установите сервис на машине с выделенным кипером ClickHouse.

6. 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.

7. Чтобы выполнить обновление, вам понадобится действительный пароль от пользователя admin. Если вы забыли пароль от пользователя admin, обратитесь в Службу технической поддержки, чтобы сбросить действующий пароль и воспользуйтесь новым паролем, чтобы выполнить обновление на следующем этапе.

Обновление KUMA

1. Если у вас есть готовый файл инвентаря, следуйте инструкции по установке программы в производственной среде.

   Если файл инвентаря для действующей версии недоступен, воспользуйтесь шаблоном файла инвентаря в поставке и заполните соответствующие параметры. Чтобы посмотреть список хостов и роли хостов в действующей системе KUMA, в веб-интерфейсе перейдите в раздел **Ресурсы** - **Активные сервисы**.

2. При обновлении с версии 2.0.x на системах, которые содержат большие данные и при этом работают на предельных ресурсах, после того, как вы введете пароль администратора, система может вернуть сообщение об ошибке Wrong admin password. Если вы указываете верный пароль, KUMA может все равно возвращать ошибку, потому что KUMA не удалось запустить сервис Ядра из-за ошибки по таймауту и предельных ресурсов. Если вы введете пароль администратора трижды, не дожидаясь завершения установки, обновление может завершиться фатальной ошибкой. Устраните ошибку по таймауту, чтобы продолжить обновление.

Финальный этап подготовки KUMA к работе

1. После обновления KUMA очистите кеш браузера.

2. Создайте заново правила правила сегментации алертов.

3. Вручную обновить агенты KUMA.

Обновление KUMA успешно выполнено.

Устранение ошибок при обновлении

При обновлении KUMA 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, KUMA может все равно возвращать ошибку, потому что из-за предельных ресурсов и ошибки по таймауту KUMA 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.

   KUMA продолжит установку. В условиях предельных ресурсов установка может занять до часа.

5. После успешного завершения установки верните параметр `TimeoutSec` к значению 300 в файле /usr/lib/systemd/system/kuma-core.service.

6. После изменения файла сервиса выполните следующие команды во втором терминале:

   ```
   systemctl daemon-reload
   ```

   ```
   service kuma-core restart
   ```

После выполнения команд обновление будет успешно выполнено.

- Неверный пароль администратора

Пароль к пользователю admin нужен для автоматического заполнения параметров хранилища при обновлении. Если при выполнении задачи TASK [Prompt for admin password] вы указали неверный пароль к пользователю admin девять раз, установщик все равно выполнит обновление и веб-интерфейс будет доступен, но 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 KUMA 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 KUMA:

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

Устраните ошибки, чтобы успешно завершить обновление.

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:

- Во время установки KUMA.
- Прочитав документ LICENSE. Этот документ включен в комплект поставки программы и находится внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

  После развертывания программы документ доступен директории /opt/kaspersky/kuma/LICENSE.

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. По истечении срока действия лицензии программа продолжает работу, но с ограниченной функциональностью (например, недоступно создание новых ресурсов). Чтобы продолжить использование KUMA в режиме полной функциональности, вам нужно продлить срок действия лицензии.

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

О Лицензионном сертификате

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

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- лицензионный ключ 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 KUMA.

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.

Добавление лицензионного ключа в веб-интерфейс программы

В веб-интерфейсе KUMA можно добавить лицензионный ключ программы.

Только пользователи с ролью администратора могут добавлять лицензионные ключи.

Чтобы добавить лицензионный ключ в веб-интерфейс KUMA:

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

   Откроется окно с условиями лицензии KUMA.

2. Выберите ключ, который хотите добавить:

   - Если необходимо добавить активный ключ, нажмите на кнопку **Добавить активный лицензионный ключ**.

     Эта кнопка не отображается, если в программу уже был добавлен лицензионный ключ. Если вы хотите добавить активный лицензионный ключ вместо уже добавленного ключа, текущий лицензионный ключ необходимо удалить.

   - Если вы хотите добавить резервный ключ, нажмите на кнопку **Добавить резервный лицензионный ключ**.

     Эта кнопка неактивна, пока не будет добавлен активный ключ. Если вы хотите добавить резервный лицензионный ключ вместо уже добавленного ключа, текущий резервный лицензионный ключ необходимо удалить.

   Откроется окно выбора файла лицензионного ключа.

3. Выберите файл лицензии, указав путь к папке и имя лицензионного ключа (файла с расширением KEY).

Лицензионный ключ из выбранного файла загружен в программу. Информация о лицензионном ключе отображается в разделе **Параметры** → **Лицензия**.

Просмотр информации о добавленном лицензионном ключе в веб-интерфейсе программы

В веб-интерфейсе KUMA 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 закладки **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 EPS** – текущее среднее количество событий в секунду, которое обрабатывает KUMA.
- **Лицензионный ключ** – уникальная буквенно-цифровая последовательность.
- **Компания** – название компании, купившей лицензию.
- **Имя клиента** – имя клиента, купившего лицензию.
- **Модули** – модули, доступные для лицензии.

Удаление лицензионного ключа в веб-интерфейсе программы

Вы можете удалить добавленный лицензионный ключ из KUMA (например, если вам нужно заменить текущий лицензионный ключ другим). После удаления лицензионного ключа программа перестает получать и обрабатывать события. Эта работа возобновится при добавлении лицензионного ключа.

Только пользователи с ролью администратора могут удалять лицензионные ключи.

Чтобы удалить лицензионный ключ:

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

   Откроется окно с условиями лицензии KUMA.

2. Нажмите на значок на лицензии, которую требуется удалить.

   Откроется окно подтверждения.

3. Подтвердите удаление лицензионного ключа.

Лицензионный ключ удален из программы.

Интеграция с другими решениями

В этом разделе описано, как интегрировать KUMA с другими приложениями для расширения возможностей программы.

Интеграция с Kaspersky Security Center

Вы можете настроить интеграцию с выбранными серверами Kaspersky Security Center для одного, нескольких или всех тенантов KUMA. Если интеграция с Kaspersky Security Center включена, вы можете импортировать информацию об активах, защищаемых этой программой, управлять активами с помощью задач, а также импортировать события из базы событий Kaspersky Security Center.

> Предварительно вам требуется убедиться, что на требуемом сервере Kaspersky Security Center разрешено входящее соединение для сервера с KUMA.

Настройка интеграции KUMA с Kaspersky Security Center включает следующие этапы:

1. **Создание в Консоли администрирования Kaspersky Security Center учетной записи пользователя**

   Данные этой учетной записи используются при создании секрета для установки соединения с Kaspersky Security Center. Учетной записи должны быть назначены права главного администратора.

   Подробнее о создании учетной записи и назначении прав пользователю см. в *справке Kaspersky Security Center*.

2. **Создание секрета с типом credentials для соединения с Kaspersky Security Center**

3. **Настройка параметров интеграции с Kaspersky Security Center**

4. **Создание подключения к серверу Kaspersky Security Center для импорта информации об активах**

   Если вы хотите импортировать в KUMA информацию об активах, зарегистрированных на серверах Kaspersky Security Center, вам требуется создать отдельное подключение к каждому серверу Kaspersky Security Center для каждого выбранного тенанта.

   > Если для тенанта выключена интеграция или отсутствует подключение к Kaspersky Security Center, при попытке импорта информации об активах в веб-интерфейсе KUMA отобразится ошибка. Процесс импорта при этом не запускается.

Настройка параметров интеграции с Kaspersky Security Center

Чтобы настроить параметры интеграции с Kaspersky Security Center:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center по тенантам**.

2. Выберите тенант, для которого вы хотите настроить параметры интеграции с Kaspersky Security Center.

   Откроется окно **Интеграция с Kaspersky Security Center**.

3. Для флажка **Выключено** выполните одно из следующих действий:

   - Снимите флажок, если вы хотите включить интеграцию с Kaspersky Security Center для этого тенанта.

   - Установите флажок, если хотите выключить интеграцию с Kaspersky Security Center для этого тенанта.

   По умолчанию флажок снят.

4. В поле **Период обновления данных** укажите период времени, по истечении которого KUMA обновляет данные об устройствах Kaspersky Security Center.

   Интервал указывается в часах. Вы можете указать только целое число.

   По умолчанию временной интервал составляет 12 часов.

5. Нажмите на кнопку **Сохранить**.

Параметры интеграции с Kaspersky Security Center для выбранного тенанта будут настроены.

Если в списке тенантов отсутствует нужный вам тенант, вам требуется добавить его в список.

Добавление тенанта в список тенантов для интеграции с Kaspersky Security Center

Чтобы добавить тенант в список тенантов для интеграции с Kaspersky Security Center:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center по тенантам**.

2. Нажмите на кнопку **Добавить тенант**.

   Откроется окно **Интеграция с Kaspersky Security Center**.

3. В раскрывающемся списке **Тенант** выберите тенант, который вам требуется добавить.

4. Нажмите на кнопку **Сохранить**.

Выбранный тенант будет добавлен в список тенантов для интеграции с Kaspersky Security Center.

Создание подключения к Kaspersky Security Center

Чтобы создать подключение к Kaspersky Security Center:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center по тенантам**.

2. Выберите тенант, для которого вы хотите создать подключение к Kaspersky Security Center.

3. Нажмите на кнопку **Добавить подключение** и укажите значения для следующих параметров:

   - **Название** (обязательно) – имя подключения. Имя может включать от 1 до 128 символов Юникода.

   - **URL** (обязательно) – URL сервера Kaspersky Security Center в формате hostname:port или IPv4:port.

   - В раскрывающемся списке **Секрет** выберите ресурс секрета с учетными данными Kaspersky Security Center или **создайте новый ресурс секрета**.

     1. Нажмите на кнопку +.

        Откроется окно секрета.

     2. Введите данные секрета:

        a. В поле **Название** выберите имя для добавляемого секрета.

        b. В раскрывающемся списке **Тенант** выберите тенант, которому будут принадлежать учетные данные Kaspersky Security Center.

        c. В раскрывающемся списке **Тип** выберите **credentials**.

        d. В полях **Пользователь** и **Пароль** введите учетные данные вашего сервера Kaspersky Security Center.

        e. В поле **Описание** можно добавить описание секрета.

3. Нажмите **Сохранить**.

Выбранный секрет можно изменить, нажав на кнопку .

- **Выключено** – состояние подключения к выбранному серверу Kaspersky Security Center. Если флажок установлен, подключение к выбранному серверу неактивно. В этом случае вы не можете использовать это подключение для соединения с сервером Kaspersky Security Center.

  По умолчанию флажок снят.

4. Если вы хотите, чтобы программа KUMA импортировала только активы, которые подключены к подчиненным серверам или включены в группы:

   a. Нажмите на кнопку **Загрузить иерархию**.

   b. Установите флажки рядом с именами подчиненных серверов и групп, из которых вы хотите импортировать информацию об активах.

   c. Если вы хотите импортировать активы только из новых групп, установите флажок **Импортировать активы из новых групп**.

   Если ни один флажок не установлен, при импорте выгружается информация обо всех активах выбранного сервера Kaspersky Security Center.

5. Нажмите на кнопку **Сохранить**.

Подключение к серверу Kaspersky Security Center будет создано. Его можно использовать для импорта информации об активах из Kaspersky Security Center в KUMA и для создания задач, связанных с активами, в Kaspersky Security Center из KUMA.

Изменение подключения к Kaspersky Security Center

Чтобы изменить подключение к Kaspersky Security Center:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center по тенантам**.

2. Выберите тенант, для которого вы хотите настроить параметры интеграции с Kaspersky Security Center.

   Откроется окно **Интеграция с Kaspersky Security Center**.

3. Нажмите на подключение с Kaspersky Security Center, которое вы хотите изменить.

   Откроется окно с параметрами выбранного подключения к Kaspersky Security Center.

4. Измените значения необходимых параметров.

5. Нажмите на кнопку **Сохранить**.

Подключение к Kaspersky Security Center будет изменено.

Удаление подключения к Kaspersky Security Center

Чтобы удалить подключение к Kaspersky Security Center:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center по тенантам**.

2. Выберите тенант, для которого вы хотите настроить параметры интеграции с Kaspersky Security Center.

   Откроется окно **Интеграция с Kaspersky Security Center**.

3. Выберите подключение Kaspersky Security Center, которое вы хотите удалить.

4. Нажмите на кнопку **Удалить**.

Подключение к Kaspersky Security Center будет удалено.

Импорт событий из базы Kaspersky Security Center

В KUMA можно получать события непосредственно из SQL-базы Kaspersky Security Center. Получение событий производится с помощью коллектора, в котором используются доступные в поставке ресурсы коннектора [OOTB] KSC SQL и нормализатора [OOTB] KSC from SQL.

Чтобы создать коллектор для получения событий Kaspersky Security Center:

1. Запустите мастер установки коллектора одним из следующих способов:

   - В веб-интерфейсе KUMA в разделе **Ресурсы** нажмите **Подключить источник**.

   - В веб-интерфейсе KUMA в разделе **Ресурсы** → **Коллекторы** нажмите **Добавить коллектор**.

2. На шаге 2 мастера установки выберите коннектор [OOTB] KSC SQL:

   - В поле **URL** укажите адрес для подключения к серверу в следующем формате:

     ```
     sqlserver://user:password@kscdb.example.com:1433/KAV
     ```

где:

- `user` – учетная запись с правами public и db_datareader к нужной базе данных;
- `password` – пароль учетной записи;
- `kscdb.example.com:1433` – адрес и порт сервера базы данных;
- `KAV` – название базы данных.

- В поле **Запрос** укажите запрос к базе данных, исходя из потребности получать определенные события.

  Пример запроса к SQL-базе Kaspersky Security Center

```
SELECT ev.event_id AS externalId, ev.severity AS severity, ev.task_display_name AS taskDisplayName,

      ev.product_name AS product_name, ev.product_version AS product_version,

       ev.event_type As deviceEventClassId, ev.event_type_display_name As event_subcode, ev.descr As msg,

CASE

      WHEN ev.rise_time is not NULL THEN DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),ev.rise_time )

         ELSE ev.rise_time

      END

   AS endTime,

   CASE

      WHEN ev.registration_time is not NULL

         THEN DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),ev.registration_time )

         ELSE ev.registration_time

      END

   AS kscRegistrationTime,
```

```
    cast(ev.par7 as varchar(4000)) as sourceUserName,

    hs.wstrWinName as dHost,

    hs.wstrWinDomain as strNtDom, serv.wstrWinName As kscName,

        CAST(hs.nlp / 256 / 256 / 256 % 256 AS VARCHAR) + '.' +

    CAST(hs.nlp / 256 / 256 % 256 AS VARCHAR) + '.' +

    CAST(hs.nlp / 256 % 256 AS VARCHAR) + '.' +

    CAST(hs.nlp % 256 AS VARCHAR) AS sourceAddress,

    serv.wstrWinDomain as kscNtDomain,

        CAST(serv.nlp / 256 / 256 / 256 % 256 AS VARCHAR) + '.' +

    CAST(serv.nlp / 256 / 256 % 256 AS VARCHAR) + '.' +

    CAST(serv.nlp / 256 % 256 AS VARCHAR) + '.' +

    CAST(serv.nlp % 256 AS VARCHAR) AS kscIP,

    CASE

    WHEN virus.tmVirusFoundTime is not NULL

            THEN
DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),virus.tmVirusFoundTime
)

            ELSE ev.registration_time

        END

    AS virusTime,

    virus.wstrObject As filePath,

    virus.wstrVirusName as virusName,

    virus.result_ev as result

FROM KAV.dbo.ev_event as ev
```

```
LEFT JOIN KAV.dbo.v_akpub_host as hs ON ev.nHostId = hs.nId

INNER JOIN KAV.dbo.v_akpub_host As serv ON serv.nId = 1

Left Join KAV.dbo.rpt_viract_index as Virus on ev.event_id = virus.nEventVirus

where registration_time >= DATEADD(minute, -191, GetDate())
```

3. На шаге 3 мастера установки выберите нормализатор [OOTB] KSC from SQL.

4. Остальные параметры укажите в соответствии вашими требованиями к коллектору.

В результате выполнения шагов мастера в веб-интерфейсе KUMA создается сервис коллектора, с помощью которого вы можете импортировать события из SQL-базы Kaspersky Security Center.

Интеграция с Kaspersky Endpoint Detection and Response

Kaspersky Endpoint Detection and Response (далее также KEDR) – функциональный блок программы Kaspersky Anti Targeted Attack Platform, обеспечивающий защиту активов локальной сети организации.

Вы можете настроить интеграцию KUMA с Kaspersky Endpoint Detection and Response версий 4.1 и 5.0, чтобы управлять действиями по реагированию на угрозы на активах, подключенных к серверам Kaspersky Endpoint Detection and Response, и активах Kaspersky Security Center. Команды на выполнение операций поступают на сервер Kaspersky Endpoint Detection and Response, после чего она передает их программе Kaspersky Endpoint Agent, установленной на активах.

Также вы можете импортировать события в KUMA и получать информацию об обнаружениях Kaspersky Endpoint Detection and Response (подробнее о получении информации об обнаружениях см. в разделе *Настройка интеграции с SIEM-системой* в справке Kaspersky Anti Targeted Attack Platform).

При интеграции KUMA с Kaspersky Endpoint Detection and Response вы можете выполнять следующие операции на активах Kaspersky Endpoint Detection and Response с Kaspersky Endpoint Agent:

- Управлять сетевой изоляцией активов.
- Управлять правилами запрета.
- Запускать программы.

За инструкцией по настройке интеграции для управления действиями по реагированию вам требуется обратиться к вашему аккаунт-менеджеру или в службу технической поддержки.

Импорт событий Kaspersky Endpoint Detection and Response

> При импорте событий из Kaspersky Endpoint Detection and Response телеметрия передается открытым текстом и может быть перехвачена злоумышленником.

Вы можете импортировать в KUMA события Kaspersky Endpoint Detection and Response 4.1 и 5.0 с помощью коннектора Kafka.

Для импорта событий вам потребуется выполнить действия на стороне Kaspersky Endpoint Detection and Response и на стороне KUMA.

Импорт событий Kaspersky Endpoint Detection and Response 4.1

Чтобы импортировать в KUMA события Kaspersky Endpoint Detection and Response 4.1, выполните следующие действия:

На стороне Kaspersky Endpoint Detection and Response:

1. Войдите в консоль управления того сервера Central Node, с которого вы хотите экспортировать события, по протоколу SSH или через терминал.

2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке Kaspersky Endpoint Detection and Response.

   Отобразится меню администратора компонента программы.

3. В меню администратора компонента программы выберите режим **Technical Support Mode**.

4. Нажмите на клавишу **Enter**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.

5. Подтвердите, что хотите выполнять действия с программой в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **Enter**.

6. Выполните команду `sudo -i`.

7. В конфигурационном файле `/etc/sysconfig/apt-services` в поле `KAFKA_PORTS` удалите значение `10000`.

Если к серверу Central Node подключены серверы Secondary Central Node или компонент Sensor, установленный на отдельном сервере, вам требуется разрешить соединение с сервером, на котором вы изменили конфигурационный файл, по порту 10000.

Настоятельно не рекомендуется использовать этот порт для каких-либо внешних подключений, кроме KUMA. Чтобы ограничить подключение по порту 10000 только для KUMA, выполните команду `iptables -I INPUT -p tcp ! -s KUMA_IP_address --dport 10000 -j DROP`.

8. Выполните команду `systemctl restart apt_ipsec.service`.

9. В конфигурационном файле `/usr/bin/apt-start-sedr-iptables` в поле `WEB_PORTS` добавьте значение `10000` через запятую без пробела.

10. Выполните команду `sudo sh /usr/bin/apt-start-sedr-iptables`.

Подготовка к экспорту событий на стороне Kaspersky Endpoint Detection and Response будет завершена.

На стороне KUMA:

1. На сервере KUMA добавьте IP-адрес сервера Central Node в формате `<IP-адрес> centralnode` в один из следующих файлов:

   - `%WINDIR%\System32\drivers\etc\hosts` – для Windows.

   - `/etc/hosts file` – для Linux.

2. В веб-интерфейсе KUMA создайте коннектор типа Kafka.

   При создании коннектора укажите следующие параметры:

   - В поле **URL** укажите `<IP-адрес сервера Central Node>:10000`.

   - В поле **Topic** укажите `EndpointEnrichedEventsTopic`.

   - В поле **Consumer group** укажите любое уникальное имя.

3. В веб-интерфейсе KUMA создайте коллектор.

   В качестве транспорта для коллектора используйте коннектор, созданный на предыдущем шаге.

При успешном завершении создания и установки коллектора события Kaspersky Endpoint Detection and Response будут импортированы в KUMA. Вы можете найти и просмотреть эти события в таблице событий.

Импорт событий Kaspersky Endpoint Detection and Response 5.0

При импорте событий из Kaspersky Endpoint Detection and Response 5.0 действует ряд ограничений:

- Импорт событий доступен только для неотказоустойчивой версии Kaspersky Endpoint Detection and Response.
- Импорт событий доступен, если в программе Kaspersky Endpoint Detection and Response используются лицензионные ключи KATA и KEDR.
- Импорт событий **не** доступен, если в составе программы Kaspersky Endpoint Detection and Response используется компонент Sensor, установленный на отдельном сервере.

Чтобы импортировать в KUMA события Kaspersky Endpoint Detection and Response 5.0, выполните следующие действия:

На стороне Kaspersky Endpoint Detection and Response:

1. Войдите в консоль управления того сервера Central Node, с которого вы хотите экспортировать события, по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке Kaspersky Endpoint Detection and Response.

   Отобразится меню администратора компонента программы.
3. В меню администратора компонента программы выберите режим **Technical Support Mode**.
4. Нажмите на клавишу **Enter**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.
5. Подтвердите, что хотите выполнять действия с программой в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **Enter**.
6. В конфигурационном файле `/usr/local/lib/python3.8/dist-packages/firewall/create_iptables_rules.ru` укажите дополнительный порт `10000` для константы `WEB_PORTS`:

   ```
   WEB_PORTS = f'10000,80,{AppPort.APT_AGENT_PORT},{AppPort.APT_GUI_PORT}'
   ```

7. Выполните команды:

   ```
   kata-firewall stop
   ```

   ```
   kata-firewall start --cluster-subnet <маска сети для адресации серверов кластера>
   ```

   Подготовка к экспорту событий на стороне Kaspersky Endpoint Detection and Response будет завершена.

На стороне KUMA:

1. На сервере KUMA добавьте IP-адрес сервера Central Node в формате `<IP-адрес> kafka.services.external.dyn.kata` в один из следующих файлов:

   - `%WINDIR%\System32\drivers\etc\hosts` – для Windows.
   - `/etc/hosts file` – для Linux.

2. В веб-интерфейсе KUMA создайте коннектор типа Kafka.

   При создании коннектора укажите следующие параметры:

   - В поле **URL** укажите `<IP-адрес сервера Central Node>:10000`.
   - В поле **Topic** укажите `EndpointEnrichedEventsTopic`.
   - В поле **Consumer group** укажите любое уникальное имя.

3. В веб-интерфейсе KUMA создайте коллектор.

   В качестве транспорта для коллектора используйте коннектор, созданный на предыдущем шаге. В качестве нормализатора для коллектора рекомендуется использовать нормализатор *[OOTB] KATA telemetry*.

   При успешном завершении создания и установки коллектора события Kaspersky Endpoint Detection and Response будут импортированы в KUMA. Вы можете найти и просмотреть эти события в таблице событий.

Настройка отображения ссылки на обнаружение Kaspersky Endpoint Detection and Response в информации о событии KUMA

При получении обнаружений Kaspersky Endpoint Detection and Response в KUMA создается алерт для каждого обнаружения. Вы можете настроить отображение ссылки на обнаружение Kaspersky Endpoint Detection and Response в информации об алерте KUMA.

Вы можете настроить отображение ссылки на обнаружение, если используете только один сервер Central Node Kaspersky Endpoint Detection and Response. Если Kaspersky Endpoint Detection and Response используется в режиме распределенного решения, настроить отображение ссылок в KUMA на обнаружения Kaspersky Endpoint Detection and Response невозможно.

Для настройки отображения ссылки на обнаружение в информации об алерте KUMA вам требуется выполнить действия в веб-интерфейсе Kaspersky Endpoint Detection and Response и KUMA.

В веб-интерфейсе Kaspersky Endpoint Detection and Response вам нужно настроить интеграцию программы с KUMA в качестве SIEM-системы. Подробнее о том, как настроить интеграцию, см. в справке *Kaspersky Anti Targeted Attack Platform* в разделе *Настройка интеграции с SIEM-системой*.

Настройка отображения ссылки в веб-интерфейсе KUMA включает следующие этапы:

1. Добавление актива, содержащего информацию о сервере Central Node Kaspersky Endpoint Detection and Response, с которого вы хотите получать обнаружения, и назначение этому активу категории.

2. Создание правила корреляции.

3. Создание коррелятора.

Вы можете использовать преднастроенное корреляционное правило. В этом случае настройка отображения ссылки в веб-интерфейсе KUMA включает следующие этапы:

1. Создание коррелятора.

   В качестве правила корреляции вам нужно выбрать правило `[OOTB] KATA Alert`.

2. Добавление актива, содержащего информацию о сервере Central Node Kaspersky Endpoint Detection and Response, с которого вы хотите получать обнаружения, и назначение этому активу категории `KATA standAlone`.

Шаг 1. Добавление актива и назначение ему категории

Предварительно вам нужно создать категорию, которая будет назначена добавляемому активу.

Чтобы добавить категорию:

1. В веб-интерфейсе KUMA выберите раздел **Активы**.

2. На закладке **Все активы** разверните список категорий тенанта, нажав на кнопку + рядом с его названием.

3. Выберите требуемую категорию или подкатегорию и нажмите на кнопку **Добавить категорию**.

   В правой части окна веб-интерфейса отобразится область деталей **Добавить категорию**.

4. Укажите параметры категории:

   a. В поле **Название** введите название категории.

   b. В поле **Родительская категория** укажите место категории в дереве категорий. Для этого нажмите на кнопку и выберите родительскую категорию для создаваемой вами категории.

      Выбранная категория отобразится в поле **Родительская категория**.

   c. При необходимости укажите значения для следующих параметров:

      - Назначьте уровень важности категории в раскрывающемся списке **Уровень важности**.

        Указанный уровень важности присваивается корреляционным событиям и алертам, связанным с этим активом.

      - При необходимости в поле **Описание** добавьте описание категории.

      - В раскрывающемся списке **Способ категоризации** выберите, как категория будет пополняться активами. В зависимости от выбора может потребоваться указать дополнительные параметры:

        - **Вручную** – активы можно привязать к категории только вручную.

        - **Активно** – активы будут с определенной периодичностью привязываться к категории, если удовлетворяют заданному фильтру.

          1. В раскрывающемся списке **Регулярность категоризации** укажите периодичность, с которой активы будут привязываться к категории. Можно выбрать значения от одного раза в час до одного раза в сутки.

             Категоризацию можно запустить принудительно, выбрав в контекстном меню категории **Начать категоризацию**.

          2. В блоке параметров **Условия** укажите фильтр, которому должны соответствовать активы для привязывания к категории.

Условия можно добавлять с помощью кнопок **Добавить условие**. Группы условий можно добавлять с помощью кнопок **Добавить группу**. Групповые операторы можно переключать между значениями **И**, **ИЛИ**, **НЕ**.

Операнды и операторы фильтра категоризации

Операнд	Операторы	Комментарий
Номер сборки	>, >=, =, <=, <	
ОС	=, like	Оператор like обеспечивает регистронезависимый поиск.
IP-адрес	inSubnet, inRange	IP-адрес указывается в нотации CIDR (например: 192.168.0.0/24). При выборе оператора inRange допускается указывать только адреса из частных диапазонов IP-адресов (например: 10.0.0.0-10.255.255.255). Оба адреса должны быть из одного диапазона.
Полное доменной имя	=, like	Оператор like обеспечивает регистронезависимый поиск.
CVE	=, in	Оператор in позволяет указать массив значений.

3. С помощью кнопки **Проверить условия** убедитесь, что указанный фильтр верен: при нажатии на кнопку отображается окно **Активы, найденные по заданным условиям** с перечнем активов, удовлетворяющих условиям поиска.

- **Реактивно** – категория будет наполняться активами с помощью правил корреляции.

5. Нажмите на кнопку **Сохранить**.

Чтобы добавить актив:

1. В веб-интерфейсе KUMA выберите раздел **Активы**.

2. Нажмите на кнопку **Добавить актив**.

   В правой части окна откроется область деталей **Добавить актив**.

3. Укажите следующие параметры актива:

   a. В поле **Название актива** введите имя актива.

   b. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать актив.

   c. В поле **IP-адрес** укажите IP-адрес сервера Central Node Kaspersky Endpoint Detection and Response, с которого вы хотите получать обнаружения.

   d. В поле **Категории** выберите категорию, которую добавили на предыдущем этапе.

   > Если вы используете предустановленное корреляционное правило, вам нужно выбрать категорию `KATA standAlone`.

   e. При необходимости укажите значения для следующих полей:

      - В поле **Полное доменное имя** укажите FQDN сервера Central Node Kaspersky Endpoint Detection and Response.

      - В поле **MAC-адрес** укажите MAC-адрес сервера Central Node Kaspersky Endpoint Detection and Response.

      - В поле **Владелец** укажите имя владельца актива.

4. Нажмите на кнопку **Сохранить**.

Шаг 2. Добавление правила корреляции

Чтобы добавить правило корреляции:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.

2. Выберите **Правила корреляции** и нажмите на кнопку **Создать правило корреляции**.

3. На закладке **Общие** укажите следующие параметры:

a. В поле **Название** укажите название правила.

b. В раскрывающемся списке **Тип** выберите **simple**.

c. В поле **Наследуемые поля** добавьте следующие поля: DeviceProduct, DeviceAddress, EventOutcome, SourceAssetID, DeviceAssetID.

d. При необходимости укажите значения для следующих полей:

- В поле **Частота срабатывания** укажите максимальное количество срабатываний правила в секунду.
- В поле **Уровень важности** укажите уровень важности алертов и корреляционных событий, которые будут созданы в результате срабатывания правила.
- В поле **Описание** укажите любую дополнительную информацию.

4. На закладке **Селекторы** → **Параметры** укажите следующие параметры:

a. В раскрывающемся списке **Фильтр** выберите **Создать**.

b. В поле **Условия** нажмите на кнопку **Добавить группу**.

c. В поле с оператором для добавленной группы выберите **И**.

d. Добавьте условие для фильтрации по значению KATA:

1. В поле **Условия** нажмите на кнопку **Добавить условие**.
2. В поле с условием выберите **Если**.
3. В поле **Левый операнд** выберите **поле события**.
4. В поле **поле события** выберите **DeviceProduct**.
5. В поле **оператор** выберите =.
6. В поле **Правый операнд** выберите **константа**.
7. В поле **значение** введите KATA.

e. Добавьте условие для фильтрации по категории:

1. В поле **Условия** нажмите на кнопку **Добавить условие**.
2. В поле с условием выберите **Если**.

3. В поле **Левый операнд** выберите **поле события**.

4. В поле **поле события** выберите **DeviceAssetID**.

5. В поле **оператор** выберите **inCategory**.

6. В поле **Правый операнд** выберите **константа**.

7. Нажмите на кнопку .

8. Выберите категорию, в которую вы поместили актив сервера Central Node Kaspersky Endpoint Detection and Response.

9. Нажмите на кнопку **Сохранить**.

f. В поле **Условия** нажмите на кнопку **Добавить группу**.

g. В поле с оператором для добавленной группы выберите **ИЛИ**.

h. Добавьте условие для фильтрации по идентификатору класса события:

1. В поле **Условия** нажмите на кнопку **Добавить условие**.

2. В поле с условием выберите **Если**.

3. В поле **Левый операнд** выберите **поле события**.

4. В поле **поле события** выберите **DeviceEventClassID**.

5. В поле **оператор** выберите =.

6. В поле **Правый операнд** выберите **константа**.

7. В поле **значение** введите **taaScanning**.

i. Повторите шаги 1–7 пункта f для каждого из следующих идентификаторов классов событий:

- file_web.
- file_mail.
- file_endpoint.
- file_external.

- ids.
- url_web.
- url_mail.
- dns.
- iocScanningEP.
- yaraScanningEP.

5. На закладке **Действия** укажите следующие параметры:

   a. В разделе **Действия** откройте раскрывающийся список **На каждом событии**.

   b. Установите флажок **Отправить на дальнейшую обработку**.

   c. В разделе **Обогащение** нажмите на кнопку **Добавить обогащение**.

   d. В раскрывающемся списке **Тип источника данных** выберите **шаблон**.

   e. В поле **Шаблон** введите *https://{{.DeviceAddress}}:8443/katap/#/alerts?id={{.EventOutcome}}*.

   f. В раскрывающемся списке **Целевое поле** выберите **DeviceExternalID**.

   g. При необходимости в раскрывающемся списке **Отладка** выберите одно из следующих значений:

      - **Включено**.

        В этом случае программа регистрирует информацию, связанную с работой ресурса, в журнал.

      - **Выключено**.

        В этом случае информация, связанная с работой ресурса, не регистрируется.

6. Нажмите на кнопку **Сохранить**.

Шаг 3. Создание коррелятора

Вам нужно запустить мастер установки коррелятора. На шаге 3 мастера вам требуется выбрать правило корреляции, добавленное при выполнении этой инструкции.

После завершения создания коррелятора в информации об алертах, созданных при получении обнаружений из Kaspersky Endpoint Detection and Response, будет отображаться ссылка на эти обнаружения. Ссылка отображается в информации о корреляционном событии (раздел **Связанные события**), в поле **DeviceExternalID**.

> Если вы хотите, чтобы в поле DeviceHostName в информации об обнаружении отображался FQDN сервера Central Node Kaspersky Endpoint Detection and Response, вам нужно создать запись для этого сервера в системе DNS и на шаге 4 мастера создать правило обогащения с помощью DNS.

Интеграция с Kaspersky CyberTrace

Kaspersky CyberTrace (далее CyberTrace) – это инструмент, который объединяет потоки данных об угрозах с решениями SIEM. Он обеспечивает пользователям мгновенный доступ к данным аналитики, повышая их осведомленность при принятии решений, связанных с безопасностью.

Вы можете интегрировать CyberTrace с KUMA одним из следующих способов:

- Интегрировать функцию поиска индикаторов CyberTrace для обогащения событий KUMA информацией потоков данных CyberTrace.
- Интегрировать в KUMA веб-интерфейс CyberTrace целиком, чтобы обеспечить полный доступ к CyberTrace.

  > Интеграция с веб-интерфейсом CyberTrace доступна только в том случае, если ваша лицензия CyberTrace включает многопользовательскую функцию.

Интеграция поиска по индикаторам CyberTrace

Интеграция функции поиска по индикаторам CyberTrace состоит из следующих этапов:

1. **Настройка CyberTrace для приема и обработки запросов от KUMA**

   Вы можете настроить интеграцию с KUMA сразу после установки CyberTrace в мастере первоначальной настройки или позднее в веб-интерфейсе CyberTrace.

2. **Создание правила обогащения событий в KUMA**

После завершения всех этапов интеграции требуется перезапустить коллектор, отвечающий за получение событий, которые вы хотите обогатить информацией из CyberTrace.

Настройка CyberTrace для приема и обработки запросов

Вы можете настроить CyberTrace для приема и обработки запросов от KUMA сразу после установки в мастере первоначальной настройки или позднее в веб-интерфейсе программы.

Чтобы настроить CyberTrace для приема и обработки запросов в мастере первоначальной настройки:

1. Дождитесь запуска мастера первоначальной настройки CyberTrace после установки программы.

   Откроется окно **Welcome to Kaspersky CyberTrace**.

2. В раскрывающемся списке **<select SIEM>** выберите тип SIEM-системы, от которой вы хотите получать данные, и нажмите на кнопку **Next**.

   Откроется окно **Connection Settings**.

3. Выполните следующие действия:

   a. В блоке параметров **Service listens on** выберите вариант **IP and port**.

   b. В поле **IP address** введите `0.0.0.0`.

   c. В поле **Port** введите `9999`.

   d. В нижнем поле **IP address or hostname** укажите `127.0.0.1`.

      Остальные значения оставьте по умолчанию.

   e. Нажмите на кнопку **Next**.

   Откроется окно **Proxy Settings**.

4. Если в вашей организации используется прокси-сервер, укажите параметры соединения с ним. Если нет, оставьте все поля незаполненными и нажмите на кнопку **Next**.

   Откроется окно **Licensing Settings**.

5. В поле **Kaspersky CyberTrace license key** добавьте лицензионный ключ для программы CyberTrace.

6. В поле **Kaspersky Threat Data Feeds certificate** добавьте сертификат, позволяющий скачивать с серверов обновлений списки данных (data feeds), и нажмите на кнопку **Next**.

CyberTrace будет настроен.

Чтобы настроить CyberTrace для приема и обработки запросов в веб-интерфейсе программы:

1. В окне веб-интерфейса программы CyberTrace выберите раздел **Settings** – **Service**.
2. В блоке параметров **Connection Settings** выполните следующие действия:
   a. Выберите вариант **IP and port**.
   b. В поле **IP address** введите `0.0.0.0`.
   c. В поле **Port** введите `9999`.
3. В блоке параметров **Web interface** в поле **IP address or hostname** введите `127.0.0.1`.
4. В верхней панели инструментов нажмите на кнопку **Restart Feed Service**.
5. Выберите раздел **Settings** – **Events format**.
6. В поле **Alert events format** введите `%Date% alert=%Alert%%RecordContext%`.
7. В поле **Detection events format** введите `Category=%Category%|MatchedIndicator=%MatchedIndicator%%RecordContext%`.
8. В поле **Records context format** введите `|%ParamName%=%ParamValue%`.
9. В поле **Actionable fields context format** введите `%ParamName%:%ParamValue%`.

CyberTrace будет настроен.

После обновления конфигурации CyberTrace требуется перезапустить сервер CyberTrace.

Создание правил обогащения событий

Чтобы создать правила обогащения событий:

1. Откройте раздел веб-интерфейса KUMA **Ресурсы** → **Правила обогащения** и в левой части окна выберите или создайте папку, в которую требуется поместить новый ресурс.

   Отобразится список доступных правил обогащения.

2. Нажмите на кнопку **Добавить правило обогащения**, чтобы создать новый ресурс.

   Откроется окно правила обогащения.

3. Укажите параметры правила обогащения:

   a. В поле **Название** введите уникальное имя ресурса. Название должно содержать от 1 до 128 символов Юникода.

   b. В раскрывающемся списке **Тенант** выберите, к какому тенанту относится этот ресурс.

   c. В раскрывающемся списке **Тип источника** выберите **cybertrace**.

   d. Укажите **URL** сервера CyberTrace, к которому вы хотите подключиться. Например, *example.domain.com:9999*.

   e. При необходимости укажите в поле **Количество подключений** максимальное количество подключений к серверу CyberTrace, которые может одновременно установить KUMA. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

   f. В поле **Запросов в секунду** введите количество запросов к серверу CyberTrace, которое сможет выполнять KUMA в секунду. Значение по умолчанию: `1000`.

   g. В поле **Время ожидания** укажите время в секундах, в течение которого KUMA должна ожидать ответа от сервера CyberTrace. Событие не будет отправлено в коррелятор, пока не истечет время ожидания или не будет получен ответ. Если ответ получен до истечения времени ожидания, он добавляется в поле события `TI`, и обработка события продолжается. Значение по умолчанию: `30`.

   h. В блоке параметров **Сопоставление** требуется указать поля событий, которые следует отправить в CyberTrace на проверку, а также задать правила сопоставления полей событий KUMA с типами индикаторов CyberTrace:

      - В столбце **Поле KUMA** выберите поле, значение которого требуется отправить в CyberTrace.

      - В столбце **Индикатор CyberTrace** выберите тип индикатора CyberTrace для каждого выбранного поля:

        - **ip**

- **url**
- **hash**

В таблице требуется указать как минимум одну строку. С помощью кнопки **Добавить строку** можно добавить строку, а с помощью кнопки ✕ – удалить.

i. С помощью раскрывающегося списка **Отладка** укажите, следует ли включить логирование операций сервиса. По умолчанию логирование выключено.

j. При необходимости в поле **Описание** добавьте до 256 символов Юникода, описывающих ресурс.

k. В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом правила обогащения. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

Создание фильтра в ресурсах

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. Название должно содержать от 1 до 128 символов Юникода.
4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

c. В раскрывающемся списке **оператор** выберите нужный вам 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).
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

4. Нажмите **Сохранить**.

Создано правило обогащения.

Интеграция поиска по индикаторам CyberTrace настроена. Созданное правило обогащения можно добавить к коллектору. Требуется перезапустить коллекторы KUMA, чтобы применить новые параметры.

Если какие-либо из полей CyberTrace в области деталей события содержат " [{ " или " }] ", это означает, что информация из потока данных об угрозах из CyberTrace была обработана некорректно и некоторые данные, возможно, не отображаются. Информацию из потока данных об угрозах можно получить, скопировав из события KUMA значение поля **TI indicator** событий и выполнив поиск по этому значению на портале CyberTrace в разделе индикаторов. Вся информация будет отображаться в разделе CyberTrace **Indicator context**.

Интеграция интерфейса CyberTrace

Вы можете интегрировать веб-интерфейс CyberTrace в веб-интерфейс KUMA. Когда эта интеграция включена, в веб-интерфейсе KUMA появляется раздел **CyberTrace**, в котором предоставляется доступ к веб-интерфейсу CyberTrace. Интеграция настраивается в разделе **Параметры** → **Kaspersky CyberTrace** веб-интерфейса KUMA.

Чтобы интегрировать веб-интерфейс CyberTrace в KUMA:

1. Откройте раздел веб-интерфейса KUMA **Ресурсы** → **Секреты**.

   Отобразится список доступных секретов.

2. Нажмите на кнопку **Добавить секрет**, чтобы создать новый секрет. Этот ресурс используется для хранения учетных данных для подключения к серверу CyberTrace.

   Откроется окно секрета.

3. Введите данные секрета:

   a. В поле **Название** выберите имя для добавляемого секрета. Название должно содержать от 1 до 128 символов Юникода.

   b. В раскрывающемся списке **Тенант** выберите, к какому тенанту относится этот ресурс.

   c. В раскрывающемся списке **Тип** выберите **credentials**.

   d. В полях **Пользователь** и **Пароль** введите учетные данные для вашего сервера CyberTrace.

   e. При необходимости в поле **Описание** добавьте до 256 символов Юникода, описывающих ресурс.

4. Нажмите **Сохранить**.

   Учетные данные сервера CyberTrace сохранены и могут использоваться в других ресурсах KUMA.

5. Откройте раздел веб-интерфейс KUMA **Параметры** → **Kaspersky CyberTrace**.

   Откроется окно с параметрами интеграции CyberTrace.

6. Измените необходимые параметры:

   - **Выключено** – снимите этот флажок, если хотите включить интеграцию веб-интерфейса CyberTrace в веб-интерфейс KUMA.
   - **Адрес сервера** (обязательно) – введите адрес сервера CyberTrace в формате `hostname:port`.
   - **Порт** (обязательно) – введите порт сервера CyberTrace.

7. В раскрывающемся списке **Секрет** выберите ресурс секрета, который вы создали ранее.

8. Нажмите **Сохранить**.

   CyberTrace теперь интегрирован с KUMA: раздел **CyberTrace** отображается в веб-интерфейсе KUMA.

Если для работы в веб-интерфейсе программы вы используете браузер Mozilla Firefox, данные в разделе **CyberTrace** могут не отображаться. В таком случае очистите кеш браузера и настройте отображение данных (см. ниже).

Чтобы настроить отображение данных в разделе **CyberTrace**:

1. В строке браузера введите FQDN веб-интерфейса KUMA с номером порта 7222: https://kuma.example.com:7222. Не рекомендуется в качестве адреса сервера указывать IP-адрес.

   Отобразится окно с предупреждением о вероятной угрозе безопасности.

2. Нажмите на кнопку **Подробнее**.

3. В нижней части окна нажмите на кнопку **Принять риск и продолжить**.

   Для URL-адреса веб-интерфейса KUMA будет создано исключение.

4. В строке браузера введите URL-адрес веб-интерфейса KUMA с номером порта 7220.

5. Перейдите в раздел **CyberTrace**.

   Данные отобразятся в разделе.

Обновление списка запрещенных объектов CyberTrace (Internal TI)

Если веб-интерфейс CyberTrace интегрирован в веб-интерфейс KUMA, можно обновлять список запрещенных объектов CyberTrace или **Internal TI** данными из событий KUMA.

Чтобы обновить Internal TI в CyberTrace:

1. Откройте область деталей события в таблице событий, окне алертов или окне корреляционного события и нажмите ссылку на домене, веб-адресе, IP-адресе или хеш-коде файла.

   Откроется контекстное меню.

2. Выберите **Добавить в Internal TI CyberTrace**.

Выбранный объект добавлен в список запрещенных объектов в CyberTrace.

Интеграция с Kaspersky Threat Intelligence Portal

Портал Kaspersky Threat Intelligence Portal объединяет все знания Лаборатории Касперского о киберугрозах и их взаимосвязи в единую мощную веб-службу. При интеграции с KUMA он помогает пользователям KUMA быстрее принимать обоснованные решения, предоставляя им данные о веб-адресах, доменах, IP-адресах, данных WHOIS / DNS.

> Доступ к Kaspersky Threat Intelligence Portal предоставляется на платной основе. Лицензионные сертификаты создаются специалистами Лаборатории Касперского. Чтобы получить сертификат для Kaspersky Threat Intelligence Portal, вашему персональному техническому менеджеру Лаборатории Касперского.

Инициализация интеграции

Чтобы интегрировать Kaspersky Threat Intelligence Portal в KUMA:

1. Откройте раздел веб-интерфейса KUMA **Ресурсы** → **Секреты**.

   Отобразится список доступных секретов.

2. Нажмите на кнопку **Добавить секрет**, чтобы создать новый секрет. Этот ресурс используется для хранения данных вашей учетной записи Kaspersky Threat Intelligence Portal.

   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 **ktl**.

d. В полях **Пользователь** и **Пароль** введите данные своей учетной записи Kaspersky Threat Intelligence Portal.

e. В поле **Описание** можно добавить описание секрета.

4. 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.

5. Нажмите **Сохранить**.

   Ваши учетные данные Kaspersky Threat Intelligence Portal сохранены и могут использоваться в других ресурсах KUMA.

6. В разделе **Параметры** веб-интерфейса KUMA откройте закладку **Kaspersky Threat Lookup**.

   Отобразится список доступных подключений.

7. Убедитесь, что флажок **Выключено** снят.

8. В раскрывающемся списке **Секрет** выберите ресурс секрета, который вы создали ранее.

   Можно создать новый секрет, нажав на кнопку со значком плюса. Созданный секрет будет сохранен в разделе **Ресурсы** → **Секреты**.

9. При необходимости в раскрывающемся списке **Прокси-сервер** выберите ресурс прокси-сервера.

10. Нажмите **Сохранить**.

11. После того, как вы сохраните настройки, выполните вход в веб-интерфейс и примите **Условия использования**, иначе в API будет возвращаться ошибка.

Процесс интеграции Kaspersky Threat Intelligence Portal с KUMA завершен.

После интеграции Kaspersky Threat Intelligence Portal и KUMA в области деталей события можно запрашивать сведения о хостах, доменах, URL-адресах, IP-адресах и хешах файлов (MD5, SHA1, SHA256).

Запрос данных от Kaspersky Threat Intelligence Portal

Чтобы запросить данные от Kaspersky Threat Intelligence Portal:

1. Откройте область деталей события в таблице событий, окне алертов или окне корреляционного события и нажмите ссылку на домене, веб-адресе, IP-адресе или хеш-коде файла.

   В правой части экрана откроется область **Обогащение Threat Lookup**.

2. Установите флажки рядом с типами данных, которые нужно запросить.

   Если ни один из флажков не установлен, запрашиваются все данные.

3. В поле **Максимальное количество записей в каждой группе данных** введите количество записей для выбранного типа данных, которое вы хотите получить. Значение по умолчанию: `10`.

4. Нажмите **Запрос**.

Задача *ktl* создана. По ее завершении события дополняются данными из Kaspersky Threat Intelligence Portal, которые можно просмотреть в таблице событий, окне алерта или окне корреляционного события.

Просмотр данных от Kaspersky Threat Intelligence Portal

Чтобы просмотреть данные из Kaspersky Threat Intelligence Portal,

Откройте область деталей события в таблице событий, окне алертов или окне корреляционного события и нажмите ссылку на домене, веб-адресе, IP-адресе или хеш-коде файла, для которого вы ранее запрашивали данные от Kaspersky Threat Intelligence Portal.

В правой части экрана откроется область деталей с данными из Kaspersky Threat Intelligence Portal с указанием времени последнего обновления этих данных.

Информация, полученная от Kaspersky Threat Intelligence Portal, кешируется. Если нажать на домен, веб-адрес, IP-адрес или хеш файла в области деталей события, для которого у KUMA уже есть доступная информация, вместо окна **Обогащение Threat Lookup** отобразятся данные из Kaspersky Threat Intelligence Portal с указанием времени их получения. Эти данные можно обновить.

Обновление данных от Kaspersky Threat Intelligence Portal

Чтобы обновить данные, полученные от Kaspersky Threat Intelligence Portal:

1. Откройте область деталей события в таблице событий, окне алертов или окне корреляционного события и нажмите ссылку на домене, веб-адресе, IP-адресе или хеш-коде файла, для которого вы ранее запрашивали данные от Kaspersky Threat Intelligence Portal.

2. Нажмите **Обновить** в области деталей события с данными, полученными с портала Kaspersky Threat Intelligence Portal.

   В правой части экрана откроется область **Обогащение Threat Lookup**.

3. Установите флажки рядом с типами данных, которые вы хотите запросить.

   Если ни один из флажков не установлен, запрашиваются все данные.

4. В поле **Максимальное количество записей в каждой группе данных** введите количество записей для выбранного типа данных, которое вы хотите получить. Значение по умолчанию: `10`.

5. Нажмите **Обновить**.

   Создается задача *KTL* и запрашиваются новые данные, полученные из Kaspersky Threat Intelligence Portal.

6. Закройте окно **Обогащение Threat Lookup** и область подробной информации о KTL.

7. Откройте область подробной информации о событии из таблицы событий, окна алертов или окна корреляционных событий и перейдите по ссылке, соответствующей домену, веб-адресу, IP-адресу или хешу файла, для которого вы обновили информацию на Kaspersky Threat Intelligence Portal, и выберите **Показать информацию из Threat Lookup**.

В правой части экрана откроется область деталей с данными из Kaspersky Threat Intelligence Portal с указанием времени.

Интеграция с R-Vision Incident Response Platform

R-Vision Incident Response Platform (далее R-Vision IRP) – это программная платформа для автоматизации мониторинга, обработки и реагирования на инциденты информационной безопасности. Она объединяет данные о киберугрозах из различных источников в единую базу данных для дальнейшего анализа и расследования, что позволяет облегчить реагирование на инциденты.

R-Vision IRP можно интегрировать с KUMA. Когда интеграция включена, создание алерта в KUMA приводит к созданию инцидента в R-Vision IRP. Алерт KUMA и инцидент R-Vision IRP взаимосвязаны: при обновлении статуса инцидента в R-Vision IRP статус соответствующего алерта KUMA также меняется.

Интеграция R-Vision IRP и KUMA настраивается в обоих приложениях. На стороне KUMA настройка интеграции доступна только для главных администраторов.

Сопоставление полей алерта KUMA и инцидента R-Vision IRP при передаче данных по API

Поле алерта KUMA	Поле инцидента R-Vision IRP
`firstSeen`	`detection`
`priority`	`level`
`correlationRuleName`	`description`
`events` (в виде json-файла)	`files`

Настройка интеграции в KUMA

В этом разделе описывается интеграция KUMA с R-Vision IRP на стороне KUMA.

Интеграция в KUMA настраивается в разделе веб-интерфейса KUMA **Параметры** → **IRP / SOAR**.

Чтобы настроить интеграцию с R-Vision IRP:

1. Откройте раздел веб-интерфейса KUMA **Ресурсы** → **Секреты**.

   Отобразится список доступных секретов.

2. Нажмите на кнопку **Добавить секрет**, чтобы создать новый секрет. Этот ресурс будет использоваться для хранения токена для API-запросов в R-Vision IRP.

   Откроется окно секрета.

3. Введите данные секрета:

   a. В поле **Название** укажите имя для добавляемого секрета. Длина названия должна быть от 1 до 128 символов Юникода.

   b. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать создаваемый ресурс.

c. В раскрывающемся списке **Тип** выберите **token**.

d. В поле **Токен** введите свой API-токен для R-Vision IRP.

   Токен можно узнать в веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Общие** → **API**.

e. При необходимости в поле **Описание** добавьте описание секрета. Длина описания должна быть от 1 до 256 символов Юникода.

4. Нажмите **Сохранить**.

   API-токен для R-Vision IRP сохранен и теперь может использоваться в других ресурсах KUMA.

5. Откройте раздел веб-интерфейса KUMA **Параметры** → **IRP / SOAR**.

   Откроется окно с параметрами интеграции R-Vision IRP.

6. Измените необходимые параметры:

   - **Выключено** – установите этот флажок, если хотите выключить интеграцию R-Vision IRP с KUMA.
   - В раскрывающемся списке **Секрет** выберите ресурс секрета, созданный ранее.

     Можно создать новый секрет, нажав на кнопку со значком плюса. Созданный секрет будет сохранен в разделе **Ресурсы** → **Секреты**.
   - **URL** (обязательно) – URL хоста сервера R-Vision IRP.
   - **Название поля для размещения идентификаторов алертов KUMA** (обязательно) – имя поля R-Vision IRP, в которое будет записываться идентификатор алерта KUMA.
   - **Название поля для размещения URL алертов KUMA** (обязательно) – имя поля R-Vision IRP, в которое будет помещаться ссылка на алерт KUMA.
   - **Категория** (обязательно) – категория алерта R-Vision IRP, который создается при получении данных об алерте от KUMA.
   - **Поля событий KUMA для отправки в IRP / SOAR** (обязательно) – раскрывающийся список для выбора полей событий KUMA, которые следует отправлять в R-Vision IRP.
   - Группа настроек **Уровень важности** (обязательно) – используется для сопоставления значений уровня важности KUMA со значениями уровня важности R-Vision IRP.

7. Нажмите **Сохранить**.

В KUMA теперь настроена интеграция с R-Vision IRP. Если интеграция также настроена в R-Vision IRP, при появлении алертов в KUMA информация о них будет отправляться в R-Vision IRP для создания инцидента. В разделе **Информация об алерте** в веб-интерфейсе KUMA отображается ссылка в R-Vision IRP.

Если вы работаете с несколькими тенантами и хотите интегрироваться с R-Vision IRP, названия тенантов должны соответствовать коротким названиям компаний в R-Vision IRP.

Настройка интеграции в R-Vision IRP

В этом разделе описывается интеграция KUMA с R-Vision IRP на стороне R-Vision IRP.

Интеграция в R-Vision IRP настраивается в разделе **Настройки** веб-интерфейса R-Vision IRP. Подробнее о настройке R-Vision IRP см. в документации этой программы.

Настройка интеграции с KUMA состоит из следующих этапов:

- **Настройка роли пользователя R-Vision IRP**

  1. Присвойте используемому для интеграции пользователю R-Vision IRP системную роль **Менеджер по управлению инцидентами**. Роль можно присвоить в веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Общие** → **Пользователи системы**, выбрав нужного пользователя. Роль добавляется в блоке параметров **Системные роли**.

     Пользователь R-Vision IRP версии 4.0 с ролью Менеджер по управлению инцидентами

     Пользователь R-Vision IRP версии 5.0 с ролью Менеджер по управлению инцидентами

2. Убедитесь, что API-токен используемого для интеграции пользователя R-Vision IRP указан в секрете в веб-интерфейсе KUMA. Токен отображается в веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Общие** → **API**.

API-токен в R-Vision IRP версии 4.0

API-токен в R-Vision IRP версии 5.0

- **Настройка полей инцидентов R-Vision IRP и алертов KUMA**

  1. Добавьте поля инцидента ALERT_ID и ALERT_URL.

  2. Настройте категорию инцидентов R-Vision IRP, создаваемых по алертам KUMA. Это можно сделать в веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Управление инцидентами** → **Категории инцидентов**. Добавьте новую или измените существующую категорию инцидентов, указав в блоке параметров **Поля категорий** созданные ранее поля инцидентов `Alert ID` и `Alert URL`. Поле `Alert ID` можно сделать скрытым.

     Категории инцидентов с данными из алертов KUMA в R-Vision IRP версии 4.0

     Категории инцидентов с данными из алертов KUMA в R-Vision IRP версии 5.0

3. Запретите редактирование ранее созданных полей инцидентов `Alert ID` и `Alert URL`. В веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Управление инцидентами** → **Представления** выберите категорию инцидентов R-Vision IRP, которые будут создаваться по алертам KUMA, и установите рядом с полями `Alert ID` и `Alert URL` значок замка.

[Поле Alert URL недоступно для редактирования в R-Vision IRP версии 4.0]

[Поле Alert URL недоступно для редактирования в R-Vision IRP версии 5.0]

- **Создание коллектора и коннектора в R-Vision IRP**

  1. Создайте коллектор R-Vision IRP для взаимодействия с KUMA.

  2. Создайте и настройте коннектор R-Vision IRP для отправки в KUMA API-запросов на закрытие алертов.

- **Создание правила на закрытие алерта в KUMA**

  Создайте правило на отправку в KUMA запроса на закрытие алерта при закрытии инцидента в R-Vision IRP.

В R-Vision IRP теперь настроена интеграция с KUMA. Если интеграция также настроена в KUMA, при появлении алертов в KUMA информация о них будет отправляться в R-Vision IRP для создания инцидента. В разделе **Информация об алерте** в веб-интерфейсе KUMA отображается ссылка в R-Vision IRP.

Добавление полей инцидента ALERT_ID и ALERT_URL

Чтобы добавить в R-Vision IRP поле инцидента ALERT_ID:

1. В веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Управление инцидентами** → **Поля инцидентов** выберите группу полей **Без группы**.

2. Нажмите на значок плюса в правой части экрана.

   В правой части экрана отобразится область параметров создаваемого поля инцидента.

3. В поле **Наименование** введите название поля, например `Alert ID`.

4. В раскрывающемся списке **Тип** выберите **Текстовое поле**.

5. В поле **Тег для распознавания** введите `ALERT_ID`.

Поле ALERT_ID добавлено в инцидент R-Vision IRP.

Поле ALERT_ID в R-Vision IRP версии 4.0

Поле ALERT_ID в R-Vision IRP версии 5.0

Чтобы добавить в R-Vision IRP поле инцидента ALERT_URL:

1. В веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Управление инцидентами** → **Поля инцидентов** выберите группу полей **Без группы**.

2. Нажмите на значок плюса в правой части экрана.

   В правой части экрана отобразится область параметров создаваемого поля инцидента.

3. В поле **Наименование** введите название поля, например `Alert URL`.

4. В раскрывающемся списке **Тип** выберите **Текстовое поле**.

5. В поле **Тег для распознавания** введите `ALERT_URL`.

6. Установите флажки **Отображение ссылок** и **Отображать URL как ссылки**.

Поле ALERT_URL добавлено в инцидент R-Vision IRP.

[Поле ALERT_URL в R-Vision IRP версии 4.0]

[Поле ALERT_URL в R-Vision IRP версии 5.0]

При необходимости аналогичным образом можно настроить отображение других данных из алерта KUMA в инциденте R-Vision IRP.

Создание коллектора в R-Vision IRP

Чтобы создать коллектор в R-Vision IRP:

1. В веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Общие** → **Коллекторы** нажмите на значок плюса.

2. В поле **Название** укажите название коллектора (например, `Main collector`).

3. В поле **Адрес коллектора** введите IP-адрес или название хоста, где установлена R-Vision IRP (например, `127.0.0.1`).

4. В поле **Порт** введите значение `3001`.

5. Нажмите **Добавить**.

6. На закладке **Организации** выберите организацию, для которой вы хотите добавить интеграцию с KUMA и установите флажки **Коллектор по умолчанию** и **Коллектор реагирования**.

Коллектор R-Vision IRP создан.

Создание коннектора в R-Vision IRP

Чтобы создать коннектор в R-Vision IRP:

1. В веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Управление инцидентами** → **Коннекторы** нажмите на значок плюса.

2. В раскрывающемся списке **Тип** выберите **REST**.

3. В поле **Название** укажите название коннектора, например, `KUMA`.

4. В поле **URL** введите API-запрос на закрытие алерта в формате `<FDQN сервера Ядра KUMA>:<Порт, используемый для API-запросов (по умолчанию 7223)>/api/v1/alerts/close`.

   Пример: `https://kuma-example.com:7223/api/v1/alerts/close`

5. В раскрывающемся списке **Тип авторизации** выберите **Токен**.

6. В поле **Auth header** введите значение `Authorization`.

7. В поле **Auth value** введите токен главного администратора KUMA в следующем формате:

   ```
   Bearer <токен главного администратора KUMA>
   ```

8. В раскрывающемся списке **Коллектор** выберите ранее созданный коллектор.

9. Нажмите **Сохранить**.

Коннектор создан.

Коннектор в R-Vision IRP версии 4.0

Коннектор в R-Vision IRP версии 5.0

После того как коннектор создан, требуется настроить отправку API-запросов на закрытие алертов в KUMA.

Чтобы настроить отправку API-запросов в R-Vision IRP:

1. В веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Управление инцидентами** → **Коннекторы** откройте созданный коннектор для редактирования.

2. В раскрывающемся списке типа запросов выберите **POST**.

3. В поле **Params** введите API-запрос на закрытие алерта в формате `<FDQN сервера Ядра KUMA>:<Порт, используемый для API-запросов (по умолчанию 7223)>/api/v1/alerts/close`.

   Пример, `https://kuma-example.com:7223/api/v1/alerts/close`

4. На закладке **HEADERS** добавьте следующие ключи и их значения:

   - Ключ `Content-Type`; значение: `application/json`.
   - Ключ `Authorization`; значение: `Bearer <токен главного администратора KUMA>`.

     Токен главного администратора KUMA можно получить в веб-интерфейсе KUMA в разделе **Параметры** → **Пользователи**.

5. На закладке **BODY** → **Raw** введите содержание тела API-запроса:

```
{
    "id":"{{tag.ALERT_ID}}",
    "reason":"<причина закрытия алерта. Доступные значения: "Incorrect Correlation Rule", "Incorrect Data", "Responded".>"
}
```

6. Нажмите **Сохранить**.

Коннектор настроен.

Коннектор в R-Vision IRP версии 4.0

Заголовок API-запроса

Тело API-запроса

[Коннектор в R-Vision IRP версии 5.0](#)

Создание правила на закрытие алерта в KUMA при закрытии инцидента в R-Vision IRP

Чтобы создать правило на отправку в KUMA запроса на закрытие алерта при закрытии инцидента в R-Vision IRP:

1. В веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Управление инцидентами** → **Сценарии реагирования** нажмите на значок плюса.

2. В поле **Название** введите название создаваемого правила, например `Close alert`.

3. В раскрывающемся списке **Группа** выберите **Все сценарии**.

4. В блоке параметров **Критерии автоматического запуска** нажмите **Добавить** и в открывшемся окне введите условия срабатывания правила:

a. В раскрывающемся списке **Тип** выберите **Значение поля**.

b. В раскрывающемся списке **Поле** выберите **Статус инцидента**.

c. Установите флажок напротив статуса **Закрыт**.

d. Нажмите **Добавить**.

Условия срабатывания правила добавлены. Правило будет срабатывать при закрытии инцидента.

5. В блоке параметров **Действия по инциденту** нажмите **Добавить** → **Запуск коннектора** и в открывшемся окне выберите коннектор, который следует выполнить при срабатывании правила:

   a. В раскрывающемся списке **Коннектор** выберите ранее созданный коннектор.

   b. Нажмите **Добавить**.

   Коннектор добавлен в правило.

6. Нажмите **Добавить**.

Правило на отправку в KUMA запроса на закрытие алерта при закрытии инцидента в R-Vision IRP создано.

Правило сценария R-Vision IRP версии 4.0

Правило сценария R-Vision IRP версии 5.0

Работа с алертами с помощью R-Vision IRP

После того как интеграция KUMA и R-Vision IRP настроена, данные об алертах KUMA поступают в R-Vision IRP. Изменение параметров алертов в KUMA отражается в R-Vision IRP. Изменение статусов алертов в KUMA или R-Vision IRP, кроме закрытия, также отражается в другой системе.

Если настроена интеграция KUMA и R-Vision IRP, вы можете выполнять следующее:

- **Передавать сведения о киберугрозах из KUMA в R-Vision IRP**

  Из KUMA в R-Vision IRP автоматически передаются сведения об обнаруженных алертах. При этом в R-Vision IRP создается инцидент.

  В R-Vision IRP передаются следующие сведения об алерте KUMA:

  - идентификатор;
  - название;
  - статус;
  - дата первого события, относящегося к алерту;
  - дата последнего обнаружения, относящегося к алерту;
  - имя учетной записи или адрес электронной почты специалиста по безопасности, назначенного для обработки алерта;

- уровень важности алерта;
- категория инцидента R-Vision IRP, соответствующего алерту KUMA;
- иерархический список событий, связанных с алертом;
- список активов, как внутренних, так и внешних, связанных с алертом;
- список пользователей, связанных с алертом;
- журнал изменений алерта;
- ссылка на алерт в KUMA.

- **Расследовать киберугрозы в KUMA**

  Первоначальная обработка алерта производится в KUMA. Специалист по безопасности может уточнять и менять любые параметры алерта, кроме идентификатора и названия. Внесенные изменения отражаются в карточке инцидента R-Vision IRP.

  Если киберугроза признается ложной и алерт закрывается в KUMA, соответствующий ему инцидент R-Vision IRP также автоматически закрывается.

- **Закрывать инциденты в R-Vision IRP**

  После необходимых работ по инциденту и фиксации хода расследования в R-Vision IRP инцидент закрывается. Соответствующий алерт KUMA также автоматически закрывается.

- **Открывать ранее закрытые инциденты**

  Если в процессе мониторинга обнаруживается, что инцидент не был решен полностью или обнаруживаются дополнительные сведения, такой инцидент снова открывается в R-Vision IRP. При этом в KUMA алерт остается закрытым.

  Специалист по безопасности с помощью ссылки может перейти из инцидента R-Vision IRP в соответствующий алерт в KUMA и изменить его параметры, кроме идентификатора, названия и статуса. Внесенные изменения отражаются в карточке инцидента R-Vision IRP.

  Дальнейший анализ происходит в R-Vision IRP. Когда расследование завершено и инцидент в R-Vision IRP снова закрыт, статус соответствующего алерта в KUMA не меняется: алерт остается закрытым.

- **Запрашивать дополнительные сведения из системы-источника в рамках сценария реагирования или вручную**

  Если в процессе анализа в R-Vision IRP возникает необходимость получить дополнительные сведения из KUMA, в R-Vision IRP можно сформировать требуемый поисковый запрос (например, запрос телеметрии, репутации, сведений о хосте) к KUMA. Запрос передается с помощью REST API KUMA, ответ фиксируется в карточке инцидента R-Vision IRP для дальнейшего анализа и вывода в отчет.

Действия выполняются в такой же последовательности на этапе автоматической обработки, если нет возможности сразу сохранить всю информацию по инциденту при импорте.

Интеграция с Active Directory, Active Directory Federation Services и FreeIPA

KUMA можно интегрировать с используемыми в вашей организации службами Active Directory, Active Directory Federation Services и FreeIPA.

Вы можете настроить подключение к службе каталогов Active Directory по протоколу LDAP. Это позволит использовать информацию из Active Directory в правилах корреляции для обогащения событий и алертов, а также для аналитики.

Если вы настроите соединение с сервером контроллера домена, это позволит использовать доменную авторизацию. В этом случае вы сможете привязать группы пользователей из домена к фильтрам ролей KUMA. Пользователи, принадлежащие к этим группам, смогут войти в веб-интерфейс KUMA, используя свои доменные учетные данные, и получат доступ к разделам программы в соответствии с назначенной ролью.

Рекомендуется предварительно создать в Active Directory, Active Directory Federation Services или FreeIPA группы пользователей, которым вы хотите предоставить возможность проходить авторизацию с помощью доменной учетной записи в веб-интерфейсе KUMA. В свойствах учетной записи пользователя в Active Directory обязательно должен быть указан адрес электронной почты.

Подключение по протоколу LDAP

Подключения по протоколу LDAP создаются и управляются в разделе **Параметры** → **LDAP-сервер** веб-интерфейса KUMA. В разделе **Интеграция с LDAP-сервером по тенантам** отображаются тенанты, для которых созданы подключения по протоколу LDAP. Тенанты можно создать или удалить.

Если выбрать тенант, откроется окно **Интеграция с LDAP-сервером**, в котором отображается таблица с существующими LDAP-подключениями. Подключения можно создать или изменить. В этом же окне можно изменить частоту обращения к LDAP-серверам и установить срок хранения устаревших данных.

После включения интеграции информация об учетных записях Active Directory становится доступной в окне алертов, в окне с подробной информацией о корреляционных событиях, а также окне инцидентов. При выборе имени учетной записи в разделе **Связанные пользователи** откроется окно **Информация об учетной записи** с данными, импортированными из Active Directory.

Данные из LDAP можно также использовать при обогащении событий в коллекторах и в аналитике.

Импортируемые атрибуты Active Directory

Из Active Directory можно запросить следующие атрибуты учетных записей:

- `accountExpires`
- `badPasswordTime`
- `cn`
- `co`
- `company`
- `department`
- `description`
- `displayName` (по этому атрибуту события можно искать при корреляции)
- `distinguishedName` (по этому атрибуту события можно искать при корреляции)
- `division`
- `employeeID`
- `givenName`
- `l`
- `lastLogon`
- `lastLogonTimestamp`
- `mail` (по этому атрибуту события можно искать при корреляции)
- `mailNickname`
- `managedObjects`
- `manager`

- `memberOf` (по этому атрибуту события можно искать при корреляции)
- `mobile`
- `name`
- `objectCategory`
- `objectGUID` (этот атрибут запрашивается из Active Directory всегда)
- `objectSid`
- `physicalDeliveryOfficeName`
- `pwdLastSet`
- `sAMAccountName` (по этому атрибуту события можно искать при корреляции)
- `sAMAccountType`
- `sn` (по этому атрибуту события можно искать при корреляции)
- `streetAddress`
- `telephoneNumber`
- `title`
- `userAccountControl` (по этому атрибуту события можно искать при корреляции)
- `userPrincipalName` (по этому атрибуту события можно искать при корреляции)
- `whenChanged`
- `whenCreated`

Включение и выключение LDAP-интеграции

Можно включить или выключить сразу все LDAP-подключения тенанта, а можно включить или выключить только определенное LDAP-подключение.

Чтобы включить или отключить все LDAP-подключения тенанта:

1. Откройте раздел **Параметры** → **LDAP-сервер** веб-интерфейса KUMA и выберите тенант, у которого вы хотите включить или выключить все подключения к LDAP.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.

2. Установите или снимите флажок **Выключено**.

3. Нажмите **Сохранить**.

Чтобы включить или отключить определенное LDAP-подключение:

1. Откройте раздел **Параметры** → **LDAP-сервер** веб-интерфейса KUMA и выберите тенант, у которого вы хотите включить или выключить подключение к LDAP.

   Откроется окно **Интеграция с LDAP-сервером**.

2. Выберите нужное подключение и в открывшемся окне установите или снимите флажок **Выключено**.

3. Нажмите **Сохранить**.

Добавление тенанта в список тенантов для интеграции с LDAP-сервером

Чтобы добавить тенант в список тенантов для интеграции с LDAP-сервером:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **LDAP-сервер**.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.

2. Нажмите на кнопку **Добавить тенант**.

   Отобразится окно **Интеграция с LDAP-сервером**.

3. В раскрывающемся списке **Тенант** выберите тенант, который вам требуется добавить.

4. Нажмите **Сохранить**.

Выбранный тенант добавлен в список тенантов для интеграции с LDAP-сервером.

Чтобы добавить тенант из списка тенантов для интеграции с LDAP-сервером:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **LDAP-сервер**.

   Отобразится таблица **Интеграция с LDAP-сервером по тенантам**.

2. Установите флажок рядом с тенантом, который необходимо удалить, и нажмите на кнопку **Удалить**.

3. Подтвердите удаление тенанта.

Выбранный тенант удален из списка тенантов для интеграции с LDAP-сервером.

Создание подключения к LDAP-серверу

Чтобы создать LDAP-подключение к Active Directory:

1. Откройте раздел **Параметры** → **LDAP-сервер** веб-интерфейса KUMA.

2. Выберите или создайте тенант, для которого хотите создать подключение к LDAP.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.

3. Нажмите на кнопку **Добавить подключение**.

   Откроется окно **Параметры подключения**.

4. Добавьте секрет с учетными данными для подключения к серверу Active Directory. Для этого выполните следующие действия:

   a. Если вы добавили секрет ранее, в раскрывающемся списке **Секрет** выберите существующий ресурс секрета (тип **credentials**).

      Выбранный секрет можно изменить, нажав на кнопку .

   b. Если вы хотите создать новый секрет, нажмите на кнопку .

      Откроется окно **Секрет**.

   c. В поле **Название** (обязательно) введите название ресурса: от 1 до 128 символов Юникода.

   d. В полях **Пользователь** и **Пароль** (обязательно) введите учетные данные для подключения к серверу Active Directory.

      Вы можете указать имя пользователя в одном из следующих форматов: <имя пользователя>@<домен> или <домен><имя пользователя>.

   e. В поле **Описание** введите описание ресурса: до 256 символов Юникода.

   f. Нажмите на кнопку **Сохранить**.

5. В поле **Название** (обязательно) введите уникальное имя LDAP-подключения.

   Длина должна быть от 1 до 128 символов Юникода.

6. В поле **URL** (обязательно) введите адрес контроллера домена в формате `<hostname или IP-адрес сервера>:<порт>`.

Вы можете указать через запятую адреса нескольких серверов с контроллерами домена на случай, если один из них будет недоступен. Все указанные серверы должны находиться в одном домене.

7. Если вы хотите использовать TLS-шифрование для соединения с контроллером домена, в раскрывающемся списке **Тип** выберите один из следующих вариантов:

   - **startTLS**.

     При использовании метода startTLS сначала устанавливается незащищенное соединение по порту 389, а затем отправляется запрос на шифрование. Если команда STARTTLS завершается с ошибкой, соединение обрывается.

     Убедитесь, что порт 389 открыт. В противном случае соединение с контроллером домена будет невозможно.

   - **ssl**.

     При использовании SSL сразу устанавливается шифрованное соединение по порту 636.

   - **незащищенный**.

   При использовании шифрованного соединения невозможно указать IP-адрес в качестве URL.

8. Если на предыдущем шаге вы включили TLS-шифрование, добавьте TLS-сертификат. Для этого выполните следующие действия:

   a. Если вы загрузили сертификат ранее, выберите его в раскрывающемся списке **Сертификат**.

      Если ранее не было добавлено ни одного сертификата, в раскрывающемся списке отобразится **Нет данных**.

   b. Если вы хотите загрузить новый сертификат, справа от списка **Сертификат** нажмите на кнопку +.

      Откроется окно **Секрет**.

   c. В поле **Название** введите название, которое будет отображаться в списке сертификатов после его добавления.

   d. По кнопке **Загрузить файл сертификата** добавьте файл с сертификатом Active Directory. Поддерживаются открытые ключи сертификата X.509 в Base64.

e. Если требуется, укажите любую информацию о сертификате в поле **Описание**.

f. Нажмите на кнопку **Сохранить**.

Сертификат будет загружен и отобразится в списке **Сертификат**.

9. В поле **Время ожидания в секундах** укажите, сколько времени требуется ожидать ответа от сервера контроллера домена.

   Если в поле **URL** указано несколько адресов, то KUMA будет ждать ответа от первого сервера указанное количество секунд. Если за это время ответ не будет получен, программа обратится к следующему указанному серверу и т.д. Если ни один из указанных серверов не ответит в течение заданного времени, подключение будет прервано с ошибкой.

10. В поле **База поиска (Base DN)** введите базовое отличительное имя каталога, в котором должен выполняться поисковый запрос.

11. В поле **Пользовательские атрибуты учетных записей AD** укажите **дополнительные атрибуты, с использованием которых вы хотите обогащать события**.

    Перед настройкой обогащения событий с помощью пользовательских атрибутов убедитесь, что пользовательские атрибуты настроены в AD.

    Чтобы обогащать события учетными записями с помощью пользовательских атрибутов:

    1. Добавьте **Пользовательские атрибуты учетных записей AD** в Параметрах подключения к LDAP.

       Невозможно добавить стандартные **Импортируемые атрибуты из AD** в качестве пользовательских. Например, если вы захотите добавить стандартны й атрибут

       accountExpires в качестве пользовательского атрибута, при сохранении параметров подключения KUMA вернет ошибку.

       Из Active Directory можно запросить следующие атрибуты учетных записей:

       - `accountExpires`
       - `badPasswordTime`
       - `cn`
       - `co`

- `company`
- `department`
- `description`
- `displayName` (по этому атрибуту события можно искать при корреляции)
- `distinguishedName` (по этому атрибуту события можно искать при корреляции)
- `division`
- `employeeID`
- `givenName`
- `l`
- `lastLogon`
- `lastLogonTimestamp`
- `mail` (по этому атрибуту события можно искать при корреляции)
- `mailNickname`
- `managedObjects`
- `manager`
- `memberOf` (по этому атрибуту события можно искать при корреляции)
- `mobile`
- `name`
- `objectCategory`
- `objectGUID` (этот атрибут запрашивается из Active Directory всегда)
- `objectSid`
- `physicalDeliveryOfficeName`

- `pwdLastSet`
- `sAMAccountName` (по этому атрибуту события можно искать при корреляции)
- `sAMAccountType`
- `sn` (по этому атрибуту события можно искать при корреляции)
- `streetAddress`
- `telephoneNumber`
- `title`
- `userAccountControl` (по этому атрибуту события можно искать при корреляции)
- `userPrincipalName` (по этому атрибуту события можно искать при корреляции)
- `whenChanged`
- `whenCreated`

После того, как вы добавите пользовательские атрибуты в Параметрах подключения к LDAP, раскрывающийся список **LDAP-атрибуты** в коллекторе будет автоматически дополнен. Пользовательские атрибуты можно отличить по знаку вопроса рядом с именем атрибута. Если для нескольких доменов вы добавили один и тот же атрибут, в раскрывающемся списке атрибут будет указан один раз, а домены можно просмотреть, если навести курсор на знак вопроса. Названия доменов отображаются в виде ссылок: если вы нажмете на ссылку, домен автоматически добавится в **Сопоставление с учетными записями LDAP**, если прежде он не был добавлен.

Если вы удалили пользовательский атрибут в Параметрах подключения к LDAP, удалите вручную строку с атрибутом из таблицы сопоставления в коллекторе. Информация об атрибутах учетных записей в KUMA обновляется каждый раз после того, как вы выполните импорт учетных записей.

2. Импортируйте учетные записи.
3. В коллекторе в таблице **Обогащение полей KUMA** задайте правила сопоставления полей KUMA с атрибутами LDAP.
4. Перезапустите коллектор.

После перезапуска коллектора KUMA начнет обогащать события учётными записями.

12. Установите флажок **Выключено**, если не хотите использовать это LDAP-подключение.

    По умолчанию флажок снят.

13. Нажмите на кнопку **Сохранить**.

LDAP-подключение к Active Directory создано и отображается в окне **Интеграция с LDAP-сервером**.

Информация об учетных записях из Active Directory будет запрошена сразу после сохранения подключения, а затем будет обновляться с указанной периодичностью.

Если вы хотите использовать одновременно несколько LDAP-подключений для одного тенанта, вам нужно убедиться, что адрес контроллера домена, указанный в каждом из этих подключений, является уникальным. В противном случае KUMA позволяет включить только одно из этих подключений. Порт при проверке адреса контроллера домена на уникальность не проверяется.

Создание копии подключения к LDAP-серверу

Вы можете создать LDAP-подключение, скопировав уже существующее подключение. В этом случае в созданное подключение дублируются все параметры исходного подключения.

Чтобы скопировать LDAP-подключение:

1. Откройте раздел **Параметры** → **LDAP-сервер** веб-интерфейса KUMA и выберите тенант, для которого вы хотите скопировать подключение к LDAP.

   Откроется окно **Интеграция с LDAP-сервером**.

2. Выберите нужное подключение.

3. В открывшемся окне **Параметры подключения** нажмите на кнопку **Дублировать подключение**.

   Отобразится окно создания нового подключения. К названию подключения будет добавлено слово `копия`.

4. Если требуется, измените нужные параметры.

5. Нажмите на кнопку **Сохранить**.

Создано новое подключение.

Если вы хотите использовать одновременно несколько LDAP-подключений для одного тенанта, вам нужно убедиться, что адрес контроллера домена, указанный в каждом из этих подключений, является уникальным. В противном случае KUMA позволяет включить только одно из этих подключений. Порт при проверке адреса контроллера домена на уникальность не проверяется.

Изменение подключения к LDAP-серверу

Чтобы изменить подключение к LDAP-серверу:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **LDAP-сервер**.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.

2. Выберите тенант, для которого вы хотите изменить подключение к LDAP-серверу.

   Откроется окно **Интеграция с LDAP-сервером**.

3. Нажмите на подключение с LDAP-серверу, которое вы хотите изменить.

   Откроется окно с параметрами выбранного подключения к LDAP-серверу.

4. Измените значения необходимых параметров.

5. Нажмите на кнопку **Сохранить**.

Подключение к LDAP-серверу изменено. Перезапустите сервисы KUMA, использующие обогащение данными LDAP-серверов, чтобы изменения вступили в силу.

Изменение частоты обновления данных

KUMA обращается к LDAP-серверу для обновления данных об учетных записях. Это происходит в следующих случаях:

- Сразу после создания нового подключения.
- Сразу после изменения параметров существующего подключения.
- Регулярно по расписанию каждые несколько часов. По умолчанию каждые 12 часов.
- При создании пользователем задачи на обновление данных об учетных записях.

При обращении к LDAP-серверам создается задача в разделе **Диспетчер задач** веб-интерфейса KUMA.

Чтобы изменить расписание обращений KUMA к LDAP-серверам:

1. Откройте в веб-интерфейсе KUMA раздел **Параметры** → **LDAP-сервер** → **Интеграция с LDAP-сервером по тенантам**.

2. Выберите нужный тенант.

   Откроется окно **Интеграция с LDAP-сервером**.

3. В поле **Период обновления данных** укажите требуемую частоту в часах. Значение по умолчанию – 12.

Расписание обращений изменено.

Изменение срока хранения данных

Полученные данные об учетных записях, если сведения о них перестают поступать от сервера Active Directory, по умолчанию хранятся в KUMA в течение 90 дней. По прошествии этого срока данные удаляются.

После удаления данных об учетных записях в KUMA новые и существующие события не обогащаются этой информацией. Информация об учетных записях также будет недоступна в алертах. Если вы хотите просматривать информацию об учетных записях на протяжении всего времени хранения алерта, требуется установить срок хранения данных об учетных записях больше, чем срок хранения алерта.

Чтобы изменить срок хранения данных об учетных записях:

1. Откройте в веб-интерфейсе KUMA раздел **Параметры** → **LDAP-сервер** → **Интеграция с LDAP-сервером по тенантам**.

2. Выберите нужный тенант.

   Откроется окно **Интеграция с LDAP-сервером**.

3. В поле **Время хранения данных** укажите количество дней, в течение которого требуется хранить полученные от LDAP-сервера данные.

Срок хранения данных об учетных записях изменен.

Запуск задач на обновление данных об учетных записях

После создания подключения к серверу Active Directory задачи на получение данных об учетных записях создаются автоматически. Это происходит в следующих случаях:

- Сразу после создания нового подключения.
- Сразу после изменения параметров существующего подключения.
- Регулярно по расписанию каждые несколько часов. По умолчанию каждые 12 часов. Расписание можно изменить.

Задачи на обновление данных об учетных записях можно создать вручную. Загрузить данные можно для всех подключений требуемого тенанта, так и для одного подключения.

Чтобы запустить задачу на обновление данных об учетных записях для всех LDAP-подключений тенанта:

1. Откройте в веб-интерфейсе KUMA разделе **Параметры** → **LDAP-сервер** → **Интеграция с LDAP-сервером по тенантам**.
2. Выберите требуемый тенант.

   Откроется окно **Интеграция с LDAP-сервером**.
3. Нажмите на кнопку **Импортировать учетные записи**.

В разделе **Диспетчер задач** веб-интерфейса KUMA добавлена задача на получение данных об учетных записях выбранного тенанта.

Чтобы запустить задачу на обновление данных об учетных записях для одного LDAP-подключения тенанта:

1. Откройте в веб-интерфейсе KUMA разделе **Параметры** → **LDAP-сервер** → **Интеграция с LDAP-сервером по тенантам**.
2. Выберите требуемый тенант.

   Откроется окно **Интеграция с LDAP-сервером**.
3. Выберите требуемое подключение к LDAP-серверу.

   Откроется окно **Параметры подключения**.
4. Нажмите на кнопку **Импортировать учетные записи**.

В разделе **Диспетчер задач** веб-интерфейса KUMA добавлена задача на получение данных об учетных записях из выбранного подключения тенанта.

Удаление подключения к LDAP-серверу

Чтобы удалить LDAP-подключения к Active Directory:

1. Откройте раздел **Параметры** → **LDAP-сервер** веб-интерфейса KUMA и выберите тенант, которому принадлежит нужное подключение к LDAP.

   Откроется окно **Интеграция с LDAP-сервером**.

2. Нажмите на подключение LDAP, которое вы хотите удалить, а затем нажмите на кнопку **Удалить**.

3. Подтвердите удаление подключения.

LDAP-подключение к Active Directory удалено.

Аутентификация с помощью доменных учетных записей

Чтобы пользователи могли проходить аутентификацию в веб-интерфейсе KUMA с помощью своих доменных учетных данных, требуется выполнить следующие этапы настройки.

1. **Включить доменную аутентификацией, если она отключена**

   По умолчанию доменная аутентификация включена, но подключение к домену не настроено.

2. **Настроить соединение с контроллером домена**

   Доступны следующие соединения:

   - Active Directory (AD)
   - Active Directory Federation Services (ADFS)
   - FreeIPA

   Одновременно могут быть настроены параметры подключения к AD и ADFS.

   Подключение возможно только к одному домену.

3. **Добавить группы ролей пользователей**

   Вы можете указать для каждой роли KUMA группу домена. Пользователи из этой группы, пройдя аутентификацию с помощью своих доменных учетных данных, будут получать доступ к веб-интерфейсу KUMA в соответствии с указанной ролью.

При этом программа проверяет соответствие группы пользователя указанному фильтру в порядке следования ролей в веб-интерфейсе KUMA: оператор → аналитик первой линии → аналитик → 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 наименьшими правами. Если указано несколько групп для разных тенантов, то в каждом тенанте пользователю будет присвоена указанная роль.

Особенности входа в систему после настройки доменной аутентификации

Для успешной аутентификации необходимо соблюдать следующие условия:

- **FreeIPA**: при входе в систему пользователю следует указывать в логине домен заглавными буквами. Пример: user@FREEIPA.COM
- **AD/ADFS**: при входе в систему пользователю следует указывать в логине UserPrincipalName. Пример: user@domain.ru.

Если вы выполнили все этапы настройки, но пользователь не может пройти аутентификацию в веб-интерфейсе KUMA с помощью своей доменной учетной записи, мы рекомендуем проверить конфигурацию на наличие следующих проблем:

- В свойствах учетной записи пользователя в Active Directory не указан адрес электронной почты. В этом случае при первой аутентификации пользователя отобразится сообщение об ошибке и учетная запись KUMA не будет создана.
- Локальная учетная запись KUMA с адресом электронной почты, указанным в свойствах доменной учетной записи, уже существует. В этом случае при попытке аутентификации с помощью доменной учетной записи пользователь получит сообщение об ошибке.
- Доменная аутентификация отключена в параметрах KUMA.
- Допущена ошибка при вводе группы ролей.
- Доменное имя пользователя содержит пробел.

Включение и выключение доменной аутентификации

По умолчанию доменная аутентификация включена, но подключение к домену не настроено. Если после настройки подключения вы хотите временно приостановить доменную аутентификацию, вы можете отключить ее в веб-интерфейсе KUMA, 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 KUMA:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Доменная аутентификация**.

2. В раскрывающемся списке **Тип аутентификации** выберите один из вариантов:

   - FreeIPA

   - AD/ADFS

3. Выполните одно из следующих действий:

   - Если вы хотите выключить доменную аутентификацию, в верхней части рабочей области установите флажок **Выключено**.

   - Если вы хотите включить доменную аутентификацию, в верхней части рабочей области снимите флажок **Выключено**.

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** → **Доменная аутентификация**.

2. В раскрывающемся списке **Тип аутентификации** выберите **FreeIPA**.

3. В блоке параметров **FreeIPA** в поле **База поиска (Base DN)** введите DistinguishedName корневой записи для поиска групп доступа в службе каталогов FreeIPA. Формат записи: dc=example,dc=com.

4. 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.

5. 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.

   - **ssl**.

     При использовании SSL сразу устанавливается шифрованное соединение по порту 636.

   - **незащищенный**.

   При использовании шифрованного соединения невозможно указать IP-адрес в качестве URL.

6. Если на предыдущем шаге вы включили TLS-шифрование, добавьте секрет с типом Credentials:

   - Если вы загрузили секрет ранее, выберите его в раскрывающемся списке **Секрет**.

     Если ранее не было добавлено ни одного секрета, в раскрывающемся списке отобразится **Нет данных**.

   - Если вы хотите загрузить новый секрет с типом Credentials, справа от списка **Секрет** нажмите на кнопку +. В открывшемся окне 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 отобразится в списке **Секрет**.

7. В поле **Время ожидания в секундах** укажите, сколько времени требуется ожидать ответа от сервера контроллера домена. По умолчанию указано значение 0.

Если в поле **URL** указано несколько адресов, то KUMA будет ждать ответа от первого сервера указанное количество секунд. Если за это время ответ не будет получен, программа будет обращаться к следующему указанному серверу. Если ни один из указанных серверов не ответит в течение заданного времени, подключение будет прервано с ошибкой.

8. Если вы хотите настроить доменную аутентификацию для пользователя с ролью главного администратора KUMA, в поле **Группа главных администраторов** укажите DistinguishedName группы FreeIPA, в которой состоит пользователь.

   > Если для пользователя указано несколько групп в одном тенанте, то будет использована роль с наименьшими правами.

   Пример ввода фильтра: `CN=KUMA team,OU=Groups,OU=Clients,DC=test,DC=domain`

9. 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** → **Доменная аутентификация**.

2. В раскрывающемся списке **Тип аутентификации** выберите **FreeIPA**.

3. В блоке параметров **FreeIPA** выберите нужный секрет в поле **Данные аутентификации**.

   При необходимости вы можете создать новый секрет, нажав на кнопку +, или изменить параметры существующего секрета, нажав на кнопку . Если интеграция с FreeIPA включена, выбор секрета всегда сбрасывается при загрузке страницы, даже

4. Нажмите на кнопку **Тест**.

   После нажатия на кнопку **Тест** система выполнит проверку соединения с доменом и вернет всплывающее уведомление с результатами теста. Система не выполняет проверку возможности входа в систему и правильность настройки группы пользователей.

Для работы доменной аутентификации требуется также добавить группы для ролей пользователей KUMA.

Вы можете указать группы только для тех ролей, для которых требуется настроить доменную аутентификацию. Остальные поля можно оставить пустыми.

Чтобы добавить группы ролей пользователей:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Доменная аутентификация**.

2. В блоке параметров **Группы ролей** нажмите на кнопку **Добавить группы ролей**.

3. В раскрывающемся списке **Тенант** выберите, для пользователей какого тенанта вы хотите настроить доменную аутентификацию.

4. Укажите DistinguishedName группы домена, пользователи которого должны иметь возможность пройти аутентификацию со своими доменными учетными данными, в полях для следующих ролей:

   - **Оператор**.
   - **Аналитик первой линии**.
   - **Аналитик**.
   - **Администратор**.

   Пример ввода группы: `CN=KUMA team,OU=Groups,OU=Clients,DC=test,DC=domain`.

   Вы можете указать для каждой роли только одну группу домена. Если вам нужно указать несколько групп, то 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 оператор, аналитик первой линии, аналитик или администратор тенанта.

6. Нажмите на кнопку **Сохранить**.

Группы ролей пользователей будут добавлены. Заданные параметры будут применены после следующего входа пользователя в веб-интерфейс KUMA.

После первой аутентификации пользователя информация о нем отобразится в разделе **Параметры** → **Пользователи**. Поля **Логин** и **Пароль**, полученные из домена, недоступны для редактирования. Роль пользователя также будет недоступна для редактирования: для изменения роли потребуется изменить группы ролей пользователей. Изменения роли применяются после повторной аутентификации пользователя. До истечения текущей сессии пользователь продолжает работу с действующей ролью.

Если в свойствах доменной учетной записи изменяется имя или адрес электронной почты пользователя, требуется вручную внести эти изменения в учетную запись KUMA.

Настройка соединения KUMA с Active Directory

После настройки на странице входа в KUMA появится кнопка **Вход через AD**.

Кнопка **Вход через AD** 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 отсутствуют или установлен флажок **Выключено** для настроек AD.

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** → **Доменная аутентификация**.
2. В раскрывающемся списке **Тип аутентификации** выберите **AD/ADFS**.
3. В блоке параметров **Active Directory** в поле **База поиска (Base DN)** введите DistinguishedName корневой записи для поиска групп доступа в службе каталогов Active Directory.
4. 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.

5. 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.

- **ssl**.

  При использовании SSL сразу устанавливается шифрованное соединение по порту 636.

- **незащищенный**.

При использовании шифрованного соединения невозможно указать IP-адрес в качестве URL.

6. 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**.

7. В поле **Время ожидания в секундах** укажите, сколько времени требуется ожидать ответа от сервера контроллера домена.

   Если в поле **URL** указано несколько адресов, то KUMA будет ждать ответа от первого сервера указанное количество секунд. Если за это время ответ не будет получен, программа будет обращаться к следующему указанному серверу. Если ни один из указанных серверов не ответит в течение заданного времени, подключение будет прервано с ошибкой.

8. Если вы хотите настроить доменную аутентификацию для пользователя с ролью главного администратора KUMA, в поле **Группа главных администраторов** укажите

DistinguishedName группы Active Directory, в которой состоит пользователь.

> Если для пользователя указано несколько групп в одном тенанте, то будет использована роль с наименьшими правами.

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 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** → **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 user/domain.

4. Нажмите на кнопку **Тест**.

   После нажатия на кнопку **Тест** система выполнит проверку соединения с доменом и вернет всплывающее уведомление с результатами теста. Система не выполняет проверку возможности входа в систему и правильность настройки группы пользователей.

Для работы доменной аутентификации требуется также добавить группы для ролей пользователей KUMA.

> Вы можете указать группы только для тех ролей, для которых требуется настроить доменную аутентификацию. Остальные поля можно оставить пустыми.

Чтобы добавить группы ролей пользователей:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Доменная аутентификация**.

2. В блоке параметров **Группы ролей** нажмите на кнопку **Добавить группы ролей**.

3. В раскрывающемся списке **Тенант** выберите, для пользователей какого тенанта вы хотите настроить доменную аутентификацию.

4. Укажите DistinguishedName группы домена, пользователи которого должны иметь возможность пройти аутентификацию со своими доменными учетными данными, в полях для следующих ролей:

   - **Оператор**.
   - **Аналитик первой линии**.
   - **Аналитик**.
   - **Администратор**.

   Пример ввода группы: `CN=KUMA team,OU=Groups,OU=Clients,DC=test,DC=domain`.

   > Вы можете указать для каждой роли только одну группу домена. Если вам нужно указать несколько групп, то 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 оператор, аналитик первой линии, аналитик или администратор тенанта.

6. Нажмите на кнопку **Сохранить**.

   Группы ролей пользователей будут добавлены. Заданные параметры будут применены после следующего входа пользователя в веб-интерфейс KUMA.

После первой аутентификации пользователя информация о нем отобразится в разделе **Параметры** → **Пользователи**. Поля **Логин** и **Пароль**, полученные из домена, недоступны для редактирования. Роль пользователя также будет недоступна для редактирования: для изменения роли потребуется изменить группы ролей пользователей. Изменения роли применяются после повторной аутентификации пользователя. До истечения текущей сессии пользователь продолжает работу с действующей ролью.

Если в свойствах доменной учетной записи изменяется имя или адрес электронной почты пользователя, требуется вручную внести эти изменения в учетную запись KUMA.

Настройка соединения KUMA с Active Directory Federation Services

Чтобы настроить доменную аутентификацию в KUMA и обеспечить для пользователей возможность входа в KUMA под учетной записью без указания логина и пароля, необходимо предварительно создать группу подключения и настроить правила на стороне ADFS или убедиться, что необходимые группы подключения и правила уже существуют.

После настройки на странице входа в KUMA появится кнопка **Вход через ADFS**.

Кнопка **Вход через ADFS** будет скрыта на странице входа в KUMA при следующих условиях:

- Если в раскрывающемся списке **Тип аутентификации** выбран пункт **FreeIPA**.
- Если в раскрывающемся списке **Тип аутентификации** выбран пункт **AD/ADFS** и настройки для ADFS отсутствуют или установлен флажок **Выключено** для настроек ADFS.

Вы можете подключиться только к одному домену ADFS. Для этого требуется настроить соединение с контроллером домена.

Чтобы настроить соединение с контроллером домена ADFS:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Доменная аутентификация**.
2. В раскрывающемся списке **Тип аутентификации** выберите **AD/ADFS**.
3. В блоке параметров **Active Directory Federation Services** в поле **Идентификатор клиента** укажите идентификатор KUMA из поля **Client ID** в ADFS.
4. В поле **Идентификатор доверенной стороны** укажите идентификатор KUMA из поля **Relying party identifiers** в ADFS.
5. Укажите **URI для получения метаданных Connect** из поля **Connect Metadata URI**. Параметр состоит из хоста, на котором расположен ADFS (https://adfs.example.com), и настройки endpoint (/adfs/.well-known/openid-configuration).

   Например, https://adfs.example.com/adfs/.well-known/openid-configuration).
6. Укажите **URL для перенаправления из ADFS** из поля **Redirect URL** в ADFS. Значение поля **Redirect URL** в ADFS указывается при настройке Application group. В ADFS необходимо указать FQDN KUMA и подстроку </sso-callback>. В KUMA URL необходимо указать без подстроки, например, https://kuma-example:7220

7. Если вы хотите настроить доменную аутентификацию для пользователя с ролью главного администратора KUMA, в поле **Группа главных администраторов** укажите DistinguishedName группы Active Directory Federation Services, в которой состоит пользователь.

   > Если для пользователя указано несколько групп в одном тенанте, то будет использована роль с наименьшими правами.

   Пример ввода фильтра: `CN=KUMA team,OU=Groups,OU=Clients,DC=test,DC=domain`

8. Нажмите на кнопку **Сохранить**.

Соединение с контроллером домена Active Directory Federation Services будет настроено.

Для работы доменной аутентификации требуется также добавить группы для ролей пользователей KUMA.

> Вы можете указать группы только для тех ролей, для которых требуется настроить доменную аутентификацию. Остальные поля можно оставить пустыми.

Чтобы добавить группы ролей пользователей:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Доменная аутентификация**.

2. В блоке параметров **Группы ролей** нажмите на кнопку **Добавить группы ролей**.

3. В раскрывающемся списке **Тенант** выберите, для пользователей какого тенанта вы хотите настроить доменную аутентификацию.

4. Укажите DistinguishedName группы домена, пользователи которого должны иметь возможность пройти аутентификацию со своими доменными учетными данными, в полях для следующих ролей:

   - **Оператор**.
   - **Аналитик первой линии**.
   - **Аналитик**.
   - **Администратор**.

Пример ввода группы: `CN=KUMA team,OU=Groups,OU=Clients,DC=test,DC=domain`.

> Вы можете указать для каждой роли только одну группу домена. Если вам нужно указать несколько групп, то 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 оператор, аналитик первой линии, аналитик или администратор тенанта.

6. Нажмите на кнопку **Сохранить**.

Группы ролей пользователей будут добавлены. Заданные параметры будут применены после следующего входа пользователя в веб-интерфейс KUMA.

После первой аутентификации пользователя информация о нем отобразится в разделе **Параметры** → **Пользователи**. Поля **Логин** и **Пароль**, полученные из домена, недоступны для редактирования. Роль пользователя также будет недоступна для редактирования: для изменения роли потребуется изменить группы ролей пользователей. Изменения роли применяются после повторной аутентификации пользователя. До истечения текущей сессии пользователь продолжает работу с действующей ролью.

Если в свойствах доменной учетной записи изменяется имя или адрес электронной почты пользователя, требуется вручную внести эти изменения в учетную запись KUMA.

Настройка подключения на стороне Active Directory Federation Services

В этом разделе приведены инструкции по созданию новой группы подключения и настройке правил для созданной группы подключения на стороне Active Directory Federation Services (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/windowsaccountnam
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.

Действия при ошибке Da

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`.

Данная ошибка свидетельствует о том, что изменился сертификат ADFS. Чтобы исправить ошибку и возобновить доменную аутентификацию, следует обновить отпечаток сертификата, сохраненный в KUMA.

Чтобы обновить отпечаток сертификата на хосте с Linux или Oracle:

1. Для получения бинарного файла adfs_fingerprint_changer_tool обратитесь в техническую поддержку.

2. Поместите полученный бинарный файл adfs_fingerprint_changer_tool в любую папку на хосте с ядром KUMA. Например, /root/kuma-ansible-installer.

3. На хосте с ядром KUMA запустите интерпретатор командной строки и с помощью команды cd перейдите в папку, где находится файл adfs_fingerprint_changer_tool.

   Например, вы можете ввести команду `cd /root/kuma-ansible-installer` и нажать на клавишу **Enter**.

4. Чтобы выдать права на запуск бинарного файла и запустить бинарный файл, последовательно выполните следующие команды:

   ```
   chmod +x adfs_fingerprint_changer_tool
   ./adfs_fingerprint_changer_tool
   ```

Чтобы обновить отпечаток сертификата на хосте с Kubernetes:

1. Для получения бинарного файла adfs_fingerprint_changer_tool обратитесь в техническую поддержку.

2. Поместите полученный бинарный файл adfs_fingerprint_changer_tool в любую папку на компьютере администратора с доступом к кластеру Kubernetes и выполните последовательно следующие команды:

```
k0s kubectl cp <путь к adfs_fingerprint_changer_tool> $(k0s kubectl get pod -l app=core -n kuma -o name | cut -d/ -f2):/tmp/ -c mongodb -n kuma
```

```
k0s kubectl exec $(k0s kubectl get pod -l app=core -n kuma -o name) -c mongodb -n kuma -- bash -c "chmod a+x /tmp/adfs_fingerprint_changer_tool && /tmp/adfs_fingerprint_changer_tool"
```

После того, как вы запустите бинарный файл, отпечаток сертификата будет обновлен и доменная аутентификация через ADFS будет снова доступна.

Интеграция с НКЦКИ

Вы можете создать в веб-интерфейсе KUMA подключение к Национальному координационному центру по компьютерным инцидентам (далее "НКЦКИ"). Это позволит вам экспортировать в него инциденты, зарегистрированные в KUMA. Интеграция настраивается в разделе **Параметры** → **НКЦКИ** веб-интерфейса KUMA.

Данные между KUMA и НКЦКИ синхронизируются каждые 5-10 минут.

Чтобы создать подключение к НКЦКИ:

1. Откройте раздел веб-интерфейса KUMA **Параметры** → **НКЦКИ**.

2. В поле **URL** введите URL, по которому доступен НКЦКИ.

3. В блоке параметров **Токен** создайте или выберите существующий ресурс секрета с API-токеном, который был выдан вашей организации для подключения к НКЦКИ:

   - Если у вас уже есть секрет, его можно выбрать в раскрывающемся списке.

   - Если вы хотите создать новый секрет:

     a. Нажмите на кнопку + и укажите следующие параметры:

     - **Название** (обязательно) – уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов Юникода.

     - **Токен** (обязательно) – токен, который был выдан вашей организации для подключения к НКЦКИ.

- **Описание** – описание сервиса: до 256 символов Юникода.

b. Нажмите **Сохранить**.

Секрет с токеном для подключения к НКЦКИ создан. Он хранится в разделе **Ресурсы** → **Секреты** и принадлежит главному тенанту.

Выбранный секрет можно изменить, нажав на кнопку .

4. В раскрывающемся списке **Сфера деятельности компании** выберите сферу, в которой работает ваша организация.

Доступные сферы деятельности компании

- Атомная энергетика
- Банковская сфера и иные сферы финансового рынка
- Горнодобывающая промышленность
- Государственная/муниципальная власть
- Здравоохранение
- Металлургическая промышленность
- Наука
- Оборонная промышленность
- Образование
- Ракетно-космическая промышленность
- Связь
- СМИ
- Топливно-энергетический комплекс
- Транспорт
- Химическая промышленность
- Иная

5. В поле **Название компании** укажите название вашей компании. Эти данные будут передаваться в НКЦКИ при экспорте инцидентов.

6. С помощью раскрывающегося списка **Местоположение** укажите, где располагается ваша компания. Эти данные будут передаваться в НКЦКИ при экспорте инцидентов.

7. При необходимости в блоке параметров **Прокси-сервер** создайте или выберите существующий ресурс прокси-сервера, который должен использоваться при подключении к НКЦКИ.

8. Нажмите **Сохранить**.

KUMA интегрирована с НКЦКИ. Теперь вы можете экспортировать в него инциденты. Вы можете нажать на кнопку **Проверить подключение**, чтобы убедиться, что с НКЦКИ устанавливается соединение.

Интеграцию можно включить или выключить с помощью флажка **Выключено**.

Возможные ошибки

Если при настройке интеграции с НКЦКИ возвращается ошибка "https://lk.cert.gov.ru/api/v2/incidents? x509: certificate signed by unknown authority", необходимо установить следующие сертификаты промежуточных удостоверяющих центров на сервер Ядра KUMA:

- Сертификат ISRG Root X1 можно скачать по ссылке: https://letsencrypt.org/certs/isrgrootx1.der
- Сертификат R3 можно скачать по ссылке: https://letsencrypt.org/certs/lets-encrypt-r3.der

Чтобы установить скачанные сертификаты в Oracle:

1. Поместите скачанный сертификат в директорию /etc/pki/ca-trust/source/anchors на сервере Ядра KUMA.

2. Чтобы установить скачанный сертификат, выполните команду `update-ca-trust.`

3. Чтобы применить изменения, перезапустите сервер Ядра KUMA с помощью команды `systemctl restart kuma-core.`

Чтобы установить скачанные сертификаты в Astra:

1. Поместите скачанный сертификат в директорию /usr/share/ca-certificates на сервере Ядра KUMA.

2. Чтобы установить скачанный сертификат, выполните команду `sudo dpkg-reconfigure ca-certificates`.

3. Чтобы применить изменения, перезапустите сервер Ядра KUMA с помощью команды `systemctl restart kuma-core.service`.

После того, как вы перезапустите сервер Ядра, сертификат будет установлен и вы сможете продолжить настройку интеграции с НКЦКИ.

Интеграция с Security Vision Incident Response Platform

Security Vision Incident Response Platform (далее Security Vision IRP) – это программная платформа для автоматизации мониторинга, обработки и реагирования на инциденты информационной безопасности. Она объединяет данные о киберугрозах из различных источников в единую базу данных для дальнейшего анализа и расследования, что позволяет облегчить реагирование на инциденты.

Security Vision IRP можно интегрировать с KUMA. После настройки интеграции в Security Vision IRP можно выполнять следующие задачи:

- Запрашивать из KUMA сведения об алертах. При этом в Security Vision IRP по полученным данным создаются *инциденты*.
- Отправлять в KUMA запросы на закрытие алертов.

Интеграция реализована с помощью KUMA REST API. На стороне Security Vision IRP интеграция осуществляется с помощью преднастроенного коннектора **Kaspersky KUMA**. О способах и условиях получения коннектора **Kaspersky KUMA** вы можете узнать у вашего поставщика Security Vision IRP.

Работа с инцидентами Security Vision IRP

Инциденты Security Vision IRP, созданные на основе данных об алертах KUMA, можно просмотреть в Security Vision IRP в разделе **Инциденты** → **Инциденты (2 линии)** → **Все инциденты (2 линии)**. В каждый инцидент Security Vision IRP записываются события, относящиеся к алертам KUMA. Импортированные события можно просмотреть на закладке **Реагирование**.

Алерт KUMA, импортированный в Security Vision IRP в качестве инцидента

Полная карточка

Общая информация | Реагирование | Чат | История | Расположение

Id: 1781339 Тип: Инцидент (2 линии)

Дата и время создания: 16:06:07 14.04.2022

Доступные базовые действия:

Взять в работу

Доступные действия по реагированию:

Общая информация

Наименование: Обнаружен инцидент Test Correlation rule у Main

Описание: Обнаружен алерт [redacted] вида "Test Correlation rule" на инфраструктуре Main в 13:05:56 14.04.2022. Адрес источника - [redacted], Адрес назначения - [redacted]

Информация об источнике

IP-адрес источника: [redacted]

Порт источника: [redacted]

Имя узла источника:

Имя пользователя:

Активы источника

Информация о назначении

IP-адрес назначения: [redacted]

Порт назначения:

Имя узла назначения: [redacted]

Имя пользователя назначения:

Активы назначения

Обработка инцидента

Приоритет: Низкий

Группа исполнения: Мониторинг инцидентов КБ

Исполнитель:

Этап обработки: Ожидание взятия в работу

Статус: Новый

Ложное срабатывание:

Вердикт:

Рекомендации:

Обработка инцидента(SLA)

Дата и время создания: 16:06:07 14.04.2022

Дата и время взятия в работу:

Дата и время закрытия:

Сохранить | Сохранить и выйти | Отмена

Инцидент в Security Vision IRP, созданный на основе алерта KUMA

Полная карточка

Общая информация | Реагирование | Чат | История | Расположение

Jira

Идентификатор Jira:

Статус Jira:

Переписка с пользователем

Почтовая переписка:

Вложения почтовой переписки:

Обогащение из AD

Информация о пользователе из AD:

Координата X:

Координата Y:

События QRadar

Событие	Время события	Имя пользователя	IP-адрес источника	Порт источника	IP-адрес назначения
service started	2022-04-14T16:05:51.000+03:00		[redacted]	[redacted]	[redacted]
service started	2022-04-14T16:05:56.000+03:00		[redacted]	[redacted]	[redacted]

События из алерта KUMA, импортированные в Security Vision IRP

Настройка интеграции в KUMA

Для того чтобы настроить интеграцию KUMA и Security Vision IRP необходимо настроить авторизацию API-запросов в KUMA. Для этого требуется создать токен для пользователя KUMA, от имени которого будут обрабатываться API-запросы на стороне KUMA.

Токен можно сгенерировать в профиле своей учетной записи. Пользователи с ролью главный администратор могут генерировать токены в учетных записях других пользователей. Вы всегда можете сгенерировать новый токен.

Чтобы сгенерировать токен в профиле своей учетной записи:

1. В веб-интерфейсе KUMA в левом нижнем углу окна нажмите на имя учетной записи пользователя и в открывшемся меню нажмите на кнопку **Профиль**.

   Откроется окно **Пользователь** с параметрами вашей учетной записи.

2. Нажмите на кнопку **Сгенерировать токен**.

3. В открывшемся окне скопируйте созданный токен. Он потребуется для настройки Security Vision IRP.

   При закрытии окна токен больше не отображается, и, если вы его не скопировали, потребуется сгенерировать новый токен.

Сгенерированный токен требуется указать в параметрах коннектора Security Vision IRP.

Настройка интеграции в Security Vision IRP

Настройка интеграции в Security Vision IRP заключается в импорте и настройки коннектора. При необходимости можно также изменить другие параметры Security Vision IRP, связанные с обработкой данных KUMA: например, расписание обработки данных и рабочий процесс.

Более подробные сведения о настройке Security Vision IRP см. в документации продукта.

Импорт и настройка коннектора

Добавление коннектора в Security Vision IRP

Интеграция Security Vision IRP и KUMA осуществляется с помощью коннектора **Kaspersky KUMA**. О способах и условиях получения коннектора **Kaspersky KUMA** вы можете узнать у вашего поставщика Security Vision IRP..

*Чтобы импортировать коннектор **Kaspersky KUMA** в Security Vision IRP:*

1. В Security Vision IRP откройте раздел **Настройки** → **Коннекторы** → **Коннекторы**.

   Отобразится список коннекторов, добавленных в Security Vision IRP.

2. В верхней части экрана нажмите на кнопку импорта и выберите zip-архив с коннектором **Kaspersky KUMA**.

Коннектор импортирован в Security Vision IRP и готов к настройке.

Настройка в коннекторе подключения к KUMA

Для использования коннектора нужно настроить его подключение к KUMA.

*Чтобы настроить в Security Vision IRP подключение к KUMA с помощью коннектора **Kaspersky KUMA**:*

1. В Security Vision IRP откройте раздел **Настройки** → **Коннекторы** → **Коннекторы**.

   Отобразится список коннекторов, добавленных в вашу Security Vision IRP.

2. Выберите коннектор **Kaspersky KUMA**.

   Отобразятся общие параметры коннектора.

3. В разделе **Параметры коннектора** нажмите на кнопку **Редактировать**.

   Отобразится конфигурация коннектора.

4. В поле **URL** укажите адрес и порт KUMA. Например, `kuma.example.com:7223`.

5. В поле **Token** укажите API-токен пользователя KUMA.

Подключение к KUMA настроено в коннекторе Security Vision IRP.

Настройки коннектора Security Vision IRP

Настройка в коннекторе Security Vision IRP команд для взаимодействия с KUMA

С помощью Security Vision IRP можно получать сведения об алертах KUMA (или *инцидентах* в терминологии Security Vision IRP), а также отправлять запросы на их закрытие. Для выполнения этих действий в коннекторе Security Vision IRP нужно настроить соответствующие команды.

В инструкциях ниже описано, как добавить команды на получение и закрытие алертов, однако при необходимости реализовать более сложную логику взаимодействия Security Vision IRP и KUMA вы можете аналогичным образом создать команды с другими API-запросами.

Чтобы настроить команду на получение из KUMA сведений об алертах:

1. В Security Vision IRP откройте раздел **Настройки** → **Коннекторы** → **Коннекторы**.

   Отобразится список коннекторов, добавленных в Security Vision IRP.

2. Выберите коннектор **Kaspersky KUMA**.

   Отобразятся общие настройки коннектора.

3. Нажмите на кнопку **+Команда**.

   Откроется окно создания команды.

4. Укажите параметры команды для получения алертов:

   - В поле **Наименование** введите название команды: `Получение инцидентов`.
   - В раскрывающемся списке **Тип запроса** выберите **GET**.
   - В поле **Вызываемый метод** введите API-запрос на поиск алертов: `api/v1/alerts/?withEvents&status=new`
   - В разделе **Заголовки запроса** в поле **Название** укажите `authorization`, а в поле **Значение** укажите **Bearer <token>**.
   - В раскрывающемся списке **Тип контента** выберите **application/json**.

5. Сохраните команду и закройте окно.

   Команда коннектора настроена. При этой команды коннектор Security Vision IRP будет запрашивать в KUMA сведения обо всех алертах со статусом **Новый** и всех относящихся к ним событиях. Полученные данные будут передаваться в обработчик Security Vision IRP, который на их основе будет создавать инциденты Security Vision IRP. Если алерт уже был импортирован в Security Vision IRP, но в нем появились новые данные, сведения о нем будут обновлены в Security Vision IRP.

Чтобы настроить команду на закрытие алертов KUMA:

1. В Security Vision IRP откройте раздел **Настройки** → **Коннекторы** → **Коннекторы**.

   Отобразится список коннекторов, добавленных в Security Vision IRP.

2. Выберите коннектор **Kaspersky KUMA**.

   Отобразятся общие настройки коннектора.

3. Нажмите на кнопку **+Команда**.

   Отобразится окно создания команды.

4. Укажите параметры команды для получения алертов:

   - В поле **Наименование** введите название команды: `Закрытие инцидента`.
   - В раскрывающемся списке **Тип запроса** выберите **POST**.
   - В поле **Вызываемый метод** введите API-запрос на закрытие алерта: `api/v1/alerts/close`
   - В поле **Запрос** введите содержимое отправляемого API-запроса: `{"id":"<Идентификатор алерта>","reason":"responded"}`

Можно создать несколько команд для разных причин закрытия алертов: responded, incorrect data, incorrect correlation rule.

- В разделе **Заголовки запроса** в поле **Название** укажите `authorization`, а в поле **Значение** укажите **Bearer <token>**.
- В раскрывающемся списке **Тип контента** выберите **application/json**.

5. Сохраните команду и закройте окно.

Команда коннектора настроена. При выполнении этой команды в Security Vision IRP будет закрыт инцидент, а в KUMA будет закрыт соответствующий ему алерт.

Создание команд в Security Vision IRP

После настройки коннектора Security Vision IRP алерты KUMA будут поступать в платформу в виде инцидентов Security Vision IRP. Далее необходимо настроить обработку инцидентов в Security Vision IRP в соответствии с существующей в вашей организации политикой безопасности.

Настройка обработчика, расписания и рабочего процесса

Обработчик Security Vision IRP

Обработчик Security Vision IRP принимает от коннектора Security Vision IRP данные об алертах KUMA и создает на их основе инциденты Security Vision IRP. Для обработки используется предустановленный обработчик **KUMA (Инциденты)**. Настройки обработчика **KUMA (Инциденты)** доступны в Security Vision IRP в разделе **Настройки** → **Обработка событий** → **Обработчики событий**:

- Правила обработки алертов KUMA можно просмотреть в настройках обработчика на закладке **Нормализация**.

- Действия при создании новых объектов можно просмотреть в настройках обработчика на закладке **Действия** для создания объектов типа **Инцидент (2 линии)**.

Расписание запуска обработчика

Запуск коннектора и обработчика выполняется по предустановленному расписанию **KUMA**. Настройка этого расписания доступна в Security Vision IRP в разделе **Настройки** → **Обработка событий** → **Расписание**:

- В блоке параметров **Настройки коннектора** можно настроить параметры запуска коннектора.
- В блоке параметров **Настройки обработки** можно настроить параметры запуска обработчика.

Рабочий процесс Security Vision IRP

Жизненный цикл инцидентов Security Vision IRP, созданных на основе алертов KUMA, проходит по преднастроенному процессу **Обработка инц. (2 линии)**. Настройка рабочего процесса доступна в Security Vision IRP в разделе **Настройки** → **Рабочие процессы** → **Шаблоны рабочих процессов**: выберите процесс **Обработка инц. (2 линии)** и нажмите на транзакцию или состояние, которое необходимо изменить.

Интеграция с Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity for Networks (далее "KICS for Networks") – программа для защиты инфраструктуры промышленных предприятий от угроз информационной безопасности и для обеспечения непрерывности технологических процессов. Программа анализирует трафик промышленной сети для выявления отклонений в значениях технологических параметров, обнаружения признаков сетевых атак, контроля работы и текущего состояния устройств в сети.

KICS for Networks версии 4.0 и выше можно интегрировать с KUMA. После настройки интеграции в KUMA можно выполнять следующие задачи:

- Импортировать из KICS for Networks в KUMA сведения об активах.
- Отправлять из KUMA в KICS for Networks команды на изменение статусов активов.

> В отличие от KUMA, в KICS for Networks активы называются устройствами.

Интеграцию KICS for Networks и KUMA необходимо настроить на стороне обеих программ:

1. В KICS for Networks необходимо создать коннектор KUMA и сохранить файл свертки этого коннектора.

2. В KUMA с помощью файла свертки коннектора создается подключение к KICS for Networks.

Описываемая в этом разделе интеграция касается импорта сведений об активах. KICS for Networks можно также настроить на отправку событий в KUMA. Для этого необходимо в KICS for Networks создать коннектор типа SIEM/Syslog, а на стороне KUMA – настроить коллектор.

Настройка интеграции в KICS for Networks

Интеграция поддерживается с KICS for Networks версий 4.0 и выше.

Настройку интеграции KICS for Networks и KUMA рекомендуется проводить после завершения режима обучения правилам контроля процесса. Подробнее см. в документации KICS for Networks.

На стороне KICS for Networks настройка интеграции заключается в создании *коннектора типа KUMA*. В KICS for Networks коннекторы – это специальные программные модули, которые обеспечивают обмен данными KICS for Networks со сторонними системами, в том числе с KUMA. Подробнее о создании коннекторов см. в документации KICS for Networks.

При добавлении в KICS for Networks коннектора автоматически создается *файл свертки* для этого коннектора. Это зашифрованный файл конфигурации для подключения к KICS for Networks, который используется при настройке интеграции на стороне KUMA.

Настройка интеграции в KUMA

Настройку интеграции KICS for Networks и KUMA рекомендуется проводить после завершения режима обучения правилам контроля процесса. Подробнее см. в документации KICS for Networks.

Чтобы настроить в KUMA интеграцию с KICS for Networks:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Kaspersky Industrial CyberSecurity for Networks**.

   Откроется окно **Интеграция с Kaspersky Industrial CyberSecurity for Networks по тенантам**.

2. Выберите или создайте тенант, для которого хотите создать интеграцию с KICS for Networks.

   Откроется окно **Интеграция с Kaspersky Industrial CyberSecurity for Networks**.

3. Нажмите на поле **Файл свертки** и выберите файл свертки коннектора, созданный в KICS for Networks.

4. В поле **Пароль файла свертки** введите пароль файла свертки.

5. Установите флажок **Включить реагирование**, если вы хотите изменять статусы активов KICS for Networks с помощью правил реагирования KUMA.

6. Нажмите **Сохранить**.

В KUMA настроена интеграция с KICS for Networks, в окне отображается IP-адрес узла, на котором будет работать коннектор KICS for Networks, а также его идентификатор.

Включение и выключение интеграции с KICS for Networks

Чтобы включить или выключить для тенанта интеграцию с KICS for Networks:

1. Откройте раздел **Параметры** → **Kaspersky Industrial CyberSecurity for Networks** веб-интерфейса KUMA и выберите тенант, у которого вы хотите включить или выключить интеграцию с KICS for Networks.

   Откроется окно **Интеграция с Kaspersky Industrial CyberSecurity for Networks**.

2. Установите или снимите флажок **Выключено**.

3. Нажмите **Сохранить**.

Изменение частоты обновления данных

KUMA обращается к KICS for Networks для обновления сведений об активах. Это происходит в следующих случаях:

- Сразу после создания новой интеграции.

- Сразу после изменения параметров существующей интеграции.

- Регулярно по расписанию каждые несколько часов. По умолчанию каждые 3 часа.
- При создании пользователем задачи на обновление данных об активах.

При обращении к KICS for Networks создается задача в разделе **Диспетчер задач** веб-интерфейса KUMA.

Чтобы изменить расписание импорта сведений об активах KICS for Networks:

1. Откройте в веб-интерфейсе KUMA раздел **Параметры** → **Kaspersky Industrial CyberSecurity for Networks**.
2. Выберите нужный тенант.

   Откроется окно **Интеграция с Kaspersky Industrial CyberSecurity for Networks**.
3. В поле **Период обновления данных** укажите требуемую частоту в часах. Значение по умолчанию – 3.

Расписание импорта изменено.

Особенности импорта информации об активах из KICS for Networks

Импорт активов

Активы импортируются в соответствии с правилами импорта активов. Импортируются только активы со статусами **Разрешенное** и **Неразрешенное**.

Активы KICS for Networks идентифицируются по комбинации следующих параметров:

- IP-адрес экземпляра KICS for Networks, с которым настроена интеграция.
- Идентификатор коннектора KICS for Networks, с помощью которого настроена интеграция.
- Идентификатор, присвоенный активу (или "устройству") в экземпляре KICS for Networks.

Импорт сведений об уязвимостях

При импорте активов в KUMA также поступают сведения об активных уязвимостях KICS for Networks. Если в KICS for Networks уязвимость была помечена как устраненная или незначительная, сведения о ней удаляются из KUMA при следующем импорте.

Сведения об уязвимостях активов отображаются в окне **Информация об активе** в блоке параметров **Уязвимости** на языке локализации KICS for Networks.

В KICS for Networks уязвимости называются рисками и разделяются на несколько типов. В KUMA импортируются все типы рисков.

Срок хранения импортированных данных

Если сведения о ранее импортированном активе перестают поступать из KICS for Networks, актив удаляется по прошествии 30 дней.

Изменение статуса актива KICS for Networks

После настройки интеграции вы можете менять статусы активов KICS for Networks из KUMA. Статусы можно менять автоматически и вручную.

Статусы активов можно менять, только если вы включили реагирование в настройках подключения к KICS for Networks.

Изменение статуса актива KICS for Networks вручную

Пользователи с ролями Главный Администратор, Администратор и Аналитик в доступных им тенантах могут вручную менять статусы активов, импортированных из KICS for Networks.

Чтобы вручную изменить статус актива KICS for Networks:

1. В разделе **Активы** веб-интерфейса KUMA нажмите на актив, который вы хотите изменить.

   В правой части окна откроется область **Информация об активе**.

2. В раскрывающемся списке **Статус KICS for Networks** выберите статус, который необходимо присвоить активу KICS for Networks. Доступны статусы *Разрешенное* или *Неразрешенное*.

Статус актива изменен. Новый статус отображается в KICS for Networks и в KUMA.

Изменение статуса актива KICS for Networks автоматически

Автоматическое изменение статусов активов KICS for Networks реализовано с помощью правил реагирования. Правила необходимо добавить в коррелятор, который будет определять условия их срабатывания.

Интеграция с Kaspersky Automated Security Awareness Platform

Kaspersky Automated Security Awareness Platform (далее также "ASAP") – это платформа для онлайн-обучения, с помощью которой пользователи смогут усвоить правила соблюдения информационной безопасности, узнать о связанных с ней угрозах, подстерегающих их в ежедневной деятельности, и потренироваться на практических примерах.

Платформу ASAP можно интегрировать с KUMA. После настройки интеграции в KUMA можно выполнять следующие задачи:

- Менять группы обучения пользователей.
- Просматривать информацию пользователей о пройденных курсах и полученных сертификатах.

Интеграция ASAP и KUMA заключается в настройте API-подключения к платформе ASAP. Процесс происходит в обоих продуктах:

1. В ASAP необходимо создать токен для авторизации API-запросов и получить адрес для API-запросов.
2. В KUMA необходимо указать адрес для API-запросов в ASAP, добавить токен для авторизации API-запросов, а также указать адрес электронной почты администратора ASAP для получения уведомлений.

Создание токена в ASAP и получение ссылки для API-запросов

Для авторизации API-запросов из KUMA в ASAP их необходимо подписывать токеном, созданном в платформе ASAP. Только администраторы компании могут создать токены.

Создание токена

Чтобы создать токен:

1. Войдите в веб-интерфейс платформы ASAP.
2. В разделе **Контрольная панель** нажмите на кнопку **Импорт и синхронизация**, а затем откройте закладку **Open API**.
3. Нажмите на кнопку **Новый токен** и в открывшемся окне выберите методы API, используемые при интеграции:

- GET /openapi/v1/groups
- POST /openapi/v1/report
- PATCH /openapi/v1/user/:userid

4. Нажмите на кнопку **Сгенерировать токен**.
5. Скопируйте токен и сохраните его любым удобным для вас способом: этот токен потребуется указать при настройке интеграции в KUMA.

> Токен не хранится в системе ASAP в открытом виде. После закрытия окна **Получить токен** он становится недоступным для просмотра. Если вы закрыли это окно, не скопировав токен, вам требуется нажать на кнопку **Новый токен** повторно, чтобы система сгенерировала новый токен.

Выпущенный токен действителен в течение 12 месяцев. По истечении этого срока токен будет отозван. Выпущенный токен будет также отозван, если он не используется в течении 6 месяцев.

Получение ссылки для API-запросов

Чтобы получить ссылку, используемую в ASAP для API-запросов:

1. Войдите в веб-интерфейс платформы ASAP.
2. В разделе **Контрольная панель** нажмите на кнопку **Импорт и синхронизация**, а затем откройте закладку **Open API**.
3. Ссылка для обращения к ASAP через Open API расположена в нижней части окна. Скопируйте ее и сохраните любым удобным для вас способом: эту ссылку потребуется указать при настройке интеграции в KUMA.

Настройка интеграции в KUMA

Чтобы настроить в KUMA интеграцию с ASAP:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Kaspersky Automated Security Awareness Platform**.

   Откроется окно **Интеграция с Kaspersky Automated Security Awareness Platform**.

2. В поле **Секрет** с помощью кнопки + создайте секрет типа **token**, указав в нем токен, полученный в платформе ASAP:

   a. В поле **Название** введите название для секрета. Должно содержать от 1 до 128 символов Юникода.

   b. В поле **Токен** введите токен для авторизации API-запросов в ASAP.

   c. При необходимости добавьте описание секрета в поле **Описание**.

   d. Нажмите **Сохранить**.

3. В поле **URL для OpenAPI ASAP** укажите адрес, используемый платформой ASAP для API-запросов.

4. В поле **Адрес электронной почты администратора ASAP** укажите адрес электронной почты администратора ASAP, который должен получать уведомления при добавлении пользователей в группы обучения через KUMA.

5. При необходимости в раскрывающемся списке **Прокси-сервер** выберите ресурс прокси-сервера, который следует использовать для подключения к платформе ASAP.

6. При необходимости выключить или включить интеграцию с ASAP установите или снимите флажок **Выключено**.

7. Нажмите **Сохранить**.

В KUMA настроена интеграция с ASAP. Теперь при просмотре информации об алертах и инцидентах можно выбрать относящихся к ним пользователей, чтобы просмотреть, какие курсы обучения прошли пользователи, а также изменить их группу обучения.

Просмотр данных о пользователях ASAP и изменение учебных групп

После настройки интеграции ASAP и KUMA в алертах и инцидентах при просмотре данных о связанных с ними пользователях становятся доступны данные из ASAP:

- Сведения об учебной группе, к которой принадлежит пользователь.
- Сведения о пройденных курсах.
- Сведения о запланированном обучении и текущем прогрессе.
- Сведения о полученных сертификатах.

Чтобы просмотреть данные о пользователе из ASAP:

1. В веб-интерфейсе KUMA в разделе **Алерты** или **Инциденты** выберите нужный алерт или инцидент.

2. В разделе **Связанные пользователи** нажмите на нужную учетную запись.

   В правой части экрана откроется окно **Информация об учетной записи**.

3. Выберите закладку **Данные о курсах ASAP**.

В окне отображаются данные пользователя из ASAP.

Вы можете изменить учебную группу пользователя ASAP.

Чтобы изменить учебную группу ASAP:

1. В веб-интерфейсе KUMA в разделе **Алерты** или **Инциденты** выберите нужный алерт или инцидент.

2. В разделе **Связанные пользователи** нажмите на нужную учетную запись.

   В правой части экрана откроется окно **Информация об учетной записи**.

3. В раскрывающемся списке **Присвоить пользователю группу ASAP** выберите учебную группу ASAP, в которую вы хотите поместить пользователя.

4. Нажмите **Применить**.

   Пользователь будет перемещен в выбранную группу ASAP, администратор компании платформы ASAP получит уведомление об изменении состава учебных групп, а для выбранной учебной группы начнет пересчитываться учебный план.

Подробнее об учебных группах и начале обучения см. в документации ASAP.

Ресурсы KUMA

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

Ресурсы содержатся в разделе веб-интерфейса KUMA **Ресурсы** в блоке **Ресурсы**. Доступные типы ресурсов:

- **Правила корреляции** – в ресурсах этого типа содержатся правила определения в событиях закономерностей, указывающих на угрозы. Если условия, заданные в этих ресурсах, выполняются, создается корреляционное событие.

- **Нормализаторы** – в ресурсах этого типа содержатся правила для приведения поступающих событий к формату, принятому в KUMA. После обработки в нормализаторе "сырое" событие становится нормализованным и может обрабатываться другими ресурсами и сервисами KUMA.

- **Коннекторы** – в ресурсах этого типа содержатся параметры для установления сетевых подключений.

- **Правила агрегации** – в ресурсах этого типа содержатся правила для объединения нескольких однотипных базовых событий в одно агрегационное событие.

- **Правила обогащения** – в ресурсах этого типа содержатся правила для дополнения событий информацией из сторонних источников.

- **Точки назначения** – в ресурсах этого типа содержатся параметры для пересылки событий в пункт дальнейшей обработки или хранения.

- **Фильтры** – в ресурсах этого типа содержатся условия для отсева или выделения отдельных событий из потока событий.

- **Правила реагирования** – ресурсы этого типа используются в корреляторах для запуска, например, скриптов или задач Kaspersky Security Center при выполнении определенных условий.

- **Шаблоны уведомлений** – ресурсы этого типа используются при рассылке уведомлений о новых алертах.

- **Активные листы** – ресурсы этого типа используются корреляторами для динамической работы с данными при анализе событий по правилам корреляции.

- **Словари** – ресурсы этого типа используются для хранения ключей и их значений, которые могут потребоваться другим ресурсам и сервисам KUMA.

- **Прокси-серверы** – в ресурсах этого типа содержатся параметры использования прокси-серверов.

- **Секреты** – ресурсы этого типа используются для безопасного хранения конфиденциальной информации (например, учетных данных), которые должны использоваться KUMA для взаимодействия с внешними службами.

При нажатии на тип ресурса открывается окно, в котором отображается таблица с имеющимися ресурсами этого типа. Таблица содержит следующие столбцы:

- **Название** – имя ресурса. Может использоваться для поиска и сортировки ресурсов.
- **Последнее обновление** – дата и время последнего обновления ресурса. Может использоваться для сортировки ресурсов.
- **Создал** – имя пользователя, создавшего ресурс.
- **Описание** – описание ресурса.

Ресурсы можно расположить по папкам. В левой части каждого окна отображается структура папок, причем количество и названия корневых папок соответствуют созданным в KUMA тенантам. 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.

Операции с ресурсами

Вы можете управлять ресурсами KUMA: создавать, перемещать, копировать, редактировать и удалять ресурсы, а также импортировать и экспортировать их. Перечисленные операции доступны для всех ресурсов, вне зависимости от типа ресурса.

Ресурсы KUMA располагаются в папках. Вы можете добавлять, переименовывать, перемещать и удалять папки ресурсов.

Создание, переименование, перемещение и удаление папок ресурсов

Папки можно создавать, переименовывать, перемещать и удалять.

Чтобы создать папку:

1. Выберите в дереве папку, в которой требуется новая папка.
2. Нажмите на кнопку **Добавить папку**.

Папка будет создана.

Чтобы переименовать папку:

1. Найдите нужную папку в структуре папок.
2. Наведите курсор на название папки.

Рядом с названием папки появится значок ...

3. В раскрывающемся списке ... выберите **Переименовать**.

   Название папки станет доступным для редактирования.

4. Введите новое название папки и нажмите **ENTER**.

   > Название папки не может быть пустым.

Папка будет переименована.

Чтобы переместить папку,

Нажмите название папки и перетащите ее в требуемое место в структуре папок.

> Папки невозможно переместить из одного тенанта в другой

Чтобы удалить папку:

1. Найдите нужную папку в структуре папок.
2. Наведите курсор на название папки.

   Рядом с названием папки появится значок ...

3. В раскрывающемся списке ... выберите **Удалить**.

   Появится окно подтверждения.

4. Нажмите **OK**.

Папка будет удалена.

> Программа не удаляет папки, которые содержат файлы или подпапки.

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 ⣿.

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**.

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. Нажмите **Сохранить**.

Ресурс будет обновлен. Если этот ресурс используется в сервисе, перезапустите сервис, чтобы он задействовал новые параметры.

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**.

   Откроется окно подтверждения.

3. Нажмите **OK**.

Ресурс будет удален.

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, корреляторам или агентам и обновите параметры.

Чтобы настроить автоматическое обновление:

1. В разделе **Параметры – Обновление репозитория** настройте **Интервал обновления в часах**. Значение по умолчанию - 24 часа.
2. Укажите **Источник обновления**. Доступны следующие варианты:
   - Серверы обновления "Лаборатории Касперского".
   - 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 её содержимому.

3. 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.

4. 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 хостеустанови с ядром KUMA.

       В случае использования локальной папки у пользователя kuma должен быть доступ к этой папке и её содержимому.

3. 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.

4. Нажмите **Запустить обновление**. Таким образом, вы одновременно сохраните настройки и вручную запустите выполнение задачи **Обновление репозитория**.

Настройка пользовательского источника с использованием Kaspersky Update Utility

Вы можете обновлять ресурсы без доступа к интернету через пользовательский источник обновления с помощью утилиты Kaspersky Update Utility.

Настройка состоит из следующих шагов:

1. Настройка пользовательского источника с помощью Kaspersky Update Utility:

   a. Установка и настройка Kaspersky Update Utility на одном из компьютеров локальной сети организации.

   b. Настройка копирования обновлений в папку общего доступа в параметрах Kaspersky Update Utility.

2. Настройка обновления репозитория KUMA из пользовательского источника.

Настройка пользовательского источника с помощью Kaspersky Update Utility:

Вы можете загрузить дистрибутив Kaspersky Update Utility с веб-сайта Службы технической поддержки "Лаборатории Касперского".

1. В Kaspersky Update Utility включите скачивание обновлений для KUMA версии 2.1:

   - В разделе **Программы** - **Контроль периметра** установите флажок рядом с KUMA 2.1, 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_2_1=true
     ```

2. В разделе **Загрузки** укажите источник обновлений. По умолчанию в качестве источника используются сервера обновления "Лаборатории Касперского".

3. В разделе **Загрузки** в группе параметров **Папки для обновлений** укажите папку общего доступа, в которую Kaspersky Update Utility будет загружать обновления. Доступны следующие 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

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 тенанта, 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.

5. Нажмите на кнопку **Экспортировать**.

Ресурсы в защищенном паролем файле сохранятся на вашем компьютере в зависимости от настроек вашего браузера. Ресурсы секретов экспортируются пустыми.

Импорт ресурсов

Чтобы импортировать ресурсы:

1. В 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**.

     Импортированные ресурсы можно только удалить. Если вы хотите переименовать, отредактировать 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.

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**.

        Нажмите **Пропустить все**, чтобы сохранить все существующие ресурсы.

   b. Нажмите на кнопку **Устранить**.

   Ресурсы импортируются в KUMA. Ресурсы секретов импортируются пустыми.

О разрешении конфликтов

Когда ресурсы импортируются в KUMA из файла, программа сравнивает их с существующими ресурсами, проверяя их *название*, *тип* и параметр *guid* (идентификатор).

Если *имя* и *тип* импортируемого ресурса совпадают с параметрами существующего ресурса, имя импортированного ресурса автоматически изменяется.

Если идентификаторы двух ресурсов совпадают, возникает конфликт, который должен разрешить пользователь. Такая ситуация может возникнуть, когда вы импортируете ресурсы на тот же сервер KUMA, с которого они были экспортированы.

При разрешении конфликта вы можете либо *заменить существующий ресурс* импортированным, либо *оставить существующий ресурс*.

Некоторые ресурсы связаны между собой: например, в некоторых типах коннекторов обязательно нужно указывать секрет коннектора. Секреты также импортируются, если они привязаны к коннектору. Такие связанные ресурсы экспортируются и импортируются вместе. Если во время импорта возникает конфликт, и вы выбираете замену существующего ресурса новым, все связанные с ним ресурсы также будут автоматически заменены импортированными ресурсами, даже если вы выбрали для них **Пропустить**.

При импорте все ресурсы импортируются в один тенант, даже если при экспорте они принадлежали разным тенантам: например, если связанный ресурс находился в общем тенанте.

Правила корреляции

Ресурсы правила корреляции используются в сервисах корреляторов для распознавания определенных последовательностей обрабатываемых событий и выполнения определенных действий после распознавания: например, создание корреляционных событий или алертов, взаимодействие с активным листом.

Доступные параметры правила корреляции зависят от выбранного типа. Типы правил корреляции:

- standard – используется для поиска корреляций между несколькими событиями. Ресурсы этого типа могут создавать корреляционные события.

  Этот тип ресурсов используется для определения сложных закономерностей в последовательности событий. Для более простых комбинаций следует использовать другие типы правил корреляции, которые требуют меньше ресурсов.

- simple – используется для создания корреляционных событий при обнаружении определенного события.

- operational – используется для операций с активными листами. Этот тип ресурсов не может создавать корреляционные события.

Для этих ресурсов в полях ввода, кроме поля **Описание**, можно включить отображение непечатаемых символов.

Если правило корреляции используется в корреляторе и по нему был создан алерт, то при изменении ресурса правила корреляции существующий алерт не будет изменен, даже если перезапустить сервис коррелятора. Например, если у правила корреляции было изменено название, название алерта останется прежним. Если существующий алерт закрыть, то новый алерт будет создан уже с учетом изменений ресурса правила корреляции.

Правила корреляции типа standard

Правила корреляции типа **standard** используются для определения сложных закономерностей в обрабатываемых событиях.

Поиск закономерностей происходит с помощью контейнеров

Контейнеры правила корреляции – это временные хранилища данных, которые используются ресурсами правила корреляции при определении необходимости создания корреляционных событий. Эти контейнеры выполняет следующие функции:

- Группируют события, которые были отобраны фильтрами в группе настроек **Селекторы** ресурса правила корреляции. События группируются по полям, которые указываются пользователем в поле **Группирующие поля**.
- Определяют момент, когда должно сработать правило корреляции, меняя соответствующим образом события, сгруппированные в контейнере.
- Выполняют действия, указанные в группе настроек **Действия**.
- Создают корреляционные события.

Доступные состояния контейнера:

- `Пусто` – в контейнере нет событий. Это может произойти только в момент своего создания при срабатывании правила корреляции.
- `Частичное совпадение` – в контейнере есть некоторые из ожидаемых событий (события восстановления не учитываются).
- `Полное совпадение` – в корзине есть все ожидаемые события (события восстановления не учитываются). При достижении этого состояния:
  - Срабатывает правило корреляции
  - События удаляются из контейнера

    - Счетчик срабатываний контейнера обновляется
    - Контейнера переводится в состояние `Пусто`
  - `Ложное совпадение` – такое состояние контейнера возможно в следующих случаях:
    - когда было достигнуто состояние `Полное совпадение`, но объединяющий фильтр возвратил значение false.
    - когда при установленном флажке **Обнуление** были получены события восстановления.

  Когда это условие достигается, правило корреляции не срабатывает. События удаляются из контейнера, счетчик срабатываний обновляется, контейнер переводится в состояния `Пусто`.

Окно ресурса правила корреляции содержит следующие закладки параметров:

- **Общие** – используется для указания основных параметров ресурса правила корреляции. На этой закладке можно выбрать тип правила корреляции.
- **Селекторы** – используется для определения условий, которым должны удовлетворять обрабатываемые события для срабатывания правила корреляции. Доступные параметры зависят от выбранного типа ресурса.
- **Действия** – используется для установки триггеров, срабатывающих при выполнении условий, заданных в группе настроек **Селекторы**. У ресурса правила корреляции должен быть хотя бы один триггер. Доступные параметры зависят от выбранного типа ресурса.

Закладка **Общие**

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – тенант, которому принадлежит правило корреляции.
- **Тип** (обязательно) – раскрывающийся список для выбора типа правила корреляции. Выберите **standard**, если хотите создать правило корреляции типа standard.
- **Группирующие поля** (обязательно) – поля событий, которые должны быть сгруппированы в контейнере. Хеш-код значений выбранных полей используется в качестве ключа контейнера. Если срабатывает селектор (см. ниже), отобранные поля копируются в корреляционное событие.

- **Уникальные поля** – поля событий, которые должны быть отправлены в контейнер. Если задан этот параметр, в контейнер будут отправляться только уникальные поля. Хеш-код значений отобранных полей используется в качестве ключа контейнера. Если срабатывает правило корреляции, отобранные поля копируются в корреляционное событие.

- **Частота срабатываний** – максимальное количество срабатываний правила корреляции в секунду. Значение по умолчанию: 100.

  > Если правила корреляции, в которых реализована сложная логика обнаружения закономерностей, не срабатывают, причиной могут быть особенности подсчета срабатываний правила в KUMA. Попробуйте увеличить значение **Частота срабатываний**, например, до `1000000`.

- **Время жизни контейнера, сек.** (обязательно) – время жизни контейнера в секундах. Этот таймер запускается при создании контейнера (когда он получает первое событие). Время жизни не обновляется, и когда оно истекает, срабатывает триггер **По истечении времени жизни контейнера** из группы настроек **Действия**, а контейнер удаляется. Триггеры **На каждом срабатывании правила** и **На последующих срабатываниях правила** могут срабатывать более одного раза в течение времени жизни контейнера.

- **Политика хранения базовых событий** – этот раскрывающийся список используется, чтобы определить, какие базовые события должны быть сохранены в корреляционном событии:

  - **first** (значение по умолчанию) – поместить в корреляционное событие первое базовое событие из коллекции событий, инициировавшей создание корреляционного события.

  - **last** – поместить в корреляционное событие последнее базовое событие из коллекции событий, инициировавшей создание корреляционного события.

  - **all** – поместить в корреляционное событие все базовые события из коллекции событий, инициировавшей создание корреляционного события.

- **Уровень важности** – базовый коэффициент, используемый для определения уровня важности правила корреляции. Значение по умолчанию: **Низкий**.

- **Сортировать по** – в этом раскрывающемся списке можно выбрать поле события, по которому селекторы правила корреляции будут отслеживать изменение ситуации. Это может пригодиться, если, например, вы захотите настроить правило корреляции на срабатывание при последовательном возникновении нескольких типов событий.

- **Описание** – описание ресурса. До 256 символов Юникода.

Закладка **Селекторы**

В ресурсе типа **standard** может быть несколько селекторов. Селекторы можно добавлять с помощью кнопки **Добавить селектор** и удалять с помощью кнопки **Удалить селектор**. Селекторы можно перемещать с помощью кнопки ⣿.

Для каждого селектора доступны две закладки **Параметры** и **Локальные переменные**.

Закладка **Параметры** содержит следующие параметры:

- **Название** (обязательно) – уникальное имя группы событий, удовлетворяющих условиям селектора. Название используется для идентификации событий в объединяющем фильтре. Должно содержать от 1 до 128 символов Юникода.

- **Порог срабатывания селектора (количество событий)** (обязательно) – количество событий, которое необходимо получить для срабатывания селектора.

- **Фильтр** (обязательно) – используется для установки критериев определения событий, из-за которых будет срабатывать селектор. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах

  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. Название должно содержать от 1 до 128 символов Юникода.

  4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

c. В раскрывающемся списке **оператор** выберите нужный вам 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).
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Фильтрация по данным из поля события Extra

Условия для фильтров по данным из поля события **Extra**:

- Условие – **Если**.

- Левый операнд – **поле события**.

- В поле события вы можете указать одно из следующих значений:
  - Поле **Extra**.
  - Значение из поля Extra в следующем формате:

    `Extra.<название поля>`

    Например, `Extra.app`.

    > Значение этого типа указывается вручную.

  - Значение из массива, записанного в поле **Extra**, в следующем формате:

    `Extra.<название поля>.<элемент массива>`

    Например, `Extra.array.0`.

    Нумерация значений в массиве начинается с 0.

    > Значение этого типа указывается вручную.

- Оператор – =.
- Правый операнд – **константа**.
- Значение – значение, по которому требуется фильтровать события.

- **Обнуление** – этот флажок должен быть установлен, если правило корреляции НЕ должно срабатывать при получении селектором определенного количества событий. По умолчанию этот флажок снят.

На закладке **Локальные переменные** с помощью кнопки **Добавить переменную** можно объявлять переменные, которые будут действовать в пределах этого правила корреляции.

Закладка **Действия**

В ресурсе типа **standard** может быть несколько триггеров.

- **На первом срабатывании правила** – этот триггер срабатывает, когда контейнер регистрирует первое в течение срока своей жизни срабатывание селектора.
- **На последующих срабатываниях правила** – этот триггер срабатывает, когда контейнер регистрирует в течение срока своей жизни второе и последующие срабатывания

селектора.

- **На каждом срабатывании правила** – этот триггер срабатывает каждый раз, когда контейнер регистрирует срабатывание селектора.

- **По истечении времени жизни контейнера** – этот триггер срабатывает по истечении времени жизни контейнера и используется в связке с селектором с установленным флажком **Обнуление**. То есть триггер срабатывает, если в течение заданного времени ситуация, обнаруженная правилом корреляции, не разрешается.

Каждый триггер представлен в виде группы настроек со следующими доступными параметрами:

- **Отправить событие на дальнейшую обработку** – если этот флажок установлен, корреляционное событие будет отправлено на пост-обработку: на обогащение, для реагирования и в точки назначения.

- **Отправить событие снова в коррелятор** – если этот флажок установлен, созданное корреляционное событие будет обрабатываться текущим ресурсом правила корреляции. Это позволяет достичь иерархической корреляции.

  > Если установлены оба флажка, правило корреляции будет отправлено сначала на пост-обработку, а затем в селекторы текущего правила корреляции.

- **Не создавать алерт** – если этот флажок установлен, алерт не будет создаваться при срабатывании этого правила корреляции.

- Группа параметров **Обновление активных листов** – используется для назначения триггера на одну или несколько операций с активными листами. С помощью кнопок **Добавить действие с активным листом** и **Удалить действие с активным листом** можно добавлять и удалять операции с активными листами.

  Доступные параметры:

  - **Название** (обязательно) – этот раскрывающийся список используется для выбора ресурсов активного листа.

  - **Операция** (обязательно) – этот раскрывающийся список используется для выбора операции, которую необходимо выполнить:

    - **Получить** – получить запись активного листа и записать значения указанных полей в корреляционное событие.

    - **Установить** – записать значения указанных полей корреляционного события в активный лист, создав новую или обновив существующую запись активного

листа. При обновлении записи активного листа данные объединяются, и только указанные поля перезаписываются.

- **Удалить** – удалить запись из активного листа.

- **Ключевые поля** (обязательно) – это список полей события, используемых для создания записи активного листа. Этот список также используется в качестве ключа записи активного листа.

  > Ключ записи активного листа зависит только от состава полей и не зависит от порядка их отображения в веб-интерфейсе KUMA.

- **Сопоставление** (требуется для операций **Получить** и **Установить**) – используется для сопоставления полей активного листа с полями событий. Можно установить более одного правила сопоставления.

  - Левое поле используется для указания поля активного листа.

    > Поле не должно содержать специальные символы или только цифры.

  - Средний раскрывающийся список используется для выбора полей событий.

  - Правое поле можно использовать для назначения константы полю активного листа, если была выбрана операция **Установить**.

- Группа параметров **Обогащение** – вы можете менять значения полей корреляционных событий, используя правила обогащения, аналогичные ресурсам правил обогащения. Эти правила обогащения хранятся в ресурсе правила корреляции, в котором они были созданы. Можно создать более одного правила обогащения. Правила обогащения можно добавлять или удалять с помощью кнопок **Добавить обогащение** и **Удалить обогащение**.

  - **Тип источника** – в этом раскрывающемся списке можно выбрать тип обогащения. В зависимости от выбранного типа отобразятся дополнительные параметры, которые также потребуется заполнить.

    Доступные типы обогащения:

    - константа

      > Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

- В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов Юникода. Если оставить это поле пустым, существующее значение поля события будет удалено.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

- словарь

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

  При выборе этого типа в раскрывающемся списке **Название словаря** необходимо выбрать словарь, из которого будут браться значения, а в блоке параметров **Ключевые поля** с помощью кнопки **Добавить поле** требуется выбрать поля события, значения которых будут использоваться для выбора записи словаря.

- таблица

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**.

  При выборе этого типа обогащения в раскрывающемся списке **Название словаря** необходимо выбрать словарь, из которого будут браться значения, а в блоке параметров **Ключевые поля** с помощью кнопки **Добавить поле** требуется выбрать поля события, значения которых будут использоваться для выбора записи словаря.

  Также в таблице **Сопоставление** необходимо настроить, из каких полей словаря и в какие поля события будут передаваться данные:

  - В столбце **Поле словаря** необходимо выбрать поле словаря. Доступные поля зависят от выбранного ресурса словаря.

  - В столбце **Поле KUMA** необходимо выбрать поле события, в которое следует записать значение. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** можно задать название для помещаемых в них данных.

  Новые строки в таблицу можно добавлять с помощью кнопки **Добавить элемент**. Столбцы можно удалить с помощью кнопки ✕.

- **событие**

  Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

  - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.
  - В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.
  - Если нажать на кнопку , откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

    Доступные преобразования

    Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

    Доступные преобразования:

    - **lower** – используется для перевода всех символов значения в нижний регистр
    - **upper** – используется для перевода всех символов значения в верхний регистр
    - **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
    - **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.
    - **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:
      - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует

заменить.

    - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.

- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.

    - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.

    - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **decodeHexString** – используется для конвертации HEX-строки в текст.

- **decodeBase64String** – используется для конвертации Base64-строки в текст.

- **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

- шаблон

Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

- В поле **Шаблон** поместите шаблон Go.

  Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт.

  Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

- **Отладка** – с помощью этого раскрывающегося списка можно включить логирование операций сервиса.

- **Описание** – описание ресурса. До 256 символов Юникода.

- Блок параметров **Фильтр** – позволяет выбрать, какие события будут отправляться на обогащение. Настройка происходит, как описано выше.

- Группа параметров **Изменение категорий** – используется для изменения категорий активов, указанных в событии. Правил категоризации может быть несколько: их можно добавить или удалить с помощью кнопок **Добавить категоризацию** или **Удалить категоризацию**. Активам можно добавлять или удалять только реактивные категории.

  - **Действие** – этот раскрывающийся список используется для выбора операции над категорией:

    - **Добавить** – присвоить категорию активу.

    - **Удалить** – отвязать актив от категории.

  - **Поле события** – поле события, в котором указан актив, над которым будет совершена операция.

  - **Идентификатор категории** – с помощью кнопки можно выбрать категорию, над которой будет совершена операция. При нажатии на нее открывается окно **Выбор категорий**, где отображается дерево категорий.

Правила корреляции типа simple

Правила корреляции типа **simple** используются для определения простых последовательностей событий.

Окно ресурса правила корреляции содержит следующие закладки параметров:

- **Общие** – используется для указания основных параметров ресурса правила корреляции. На этой закладке можно выбрать тип правила корреляции.
- **Селекторы** – используется для определения условий, которым должны удовлетворять обрабатываемые события для срабатывания правила корреляции. Доступные параметры зависят от выбранного типа ресурса.
- **Действия** – используется для установки триггеров, срабатывающих при выполнении условий, заданных в группе настроек **Селекторы**. У ресурса правила корреляции должен быть хотя бы один триггер. Доступные параметры зависят от выбранного типа ресурса.

Закладка **Общие**

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – тенант, которому принадлежит правило корреляции.
- **Тип** (обязательно) – раскрывающийся список для выбора типа правила корреляции. Выберите **simple**, если хотите создать правило корреляции типа simple.
- **Наследуемые поля** (обязательно) – поля событий, по которым отбираются события. При срабатывания селектора (см. ниже) эти поля будут записаны в корреляционное событие.
- **Частота срабатываний** – максимальное количество срабатываний правила корреляции в секунду. Значение по умолчанию: 100.

  Если правила корреляции, в которых реализована сложная логика обнаружения закономерностей, не срабатывают, причиной могут быть особенности подсчета срабатываний правила в KUMA. Попробуйте увеличить значение **Частота срабатываний**, например, до `1000000`.

- **Уровень важности** – базовый коэффициент, используемый для определения уровня важности правила корреляции. Значение по умолчанию: `Низкий`.
- **Описание** – описание ресурса. До 256 символов Юникода.

Закладка **Селекторы**

В ресурсе типа **simple** может быть только один селектор, для которого доступны закладки **Параметры** и **Локальные переменные**.

Закладка **Параметры** содержит параметры с блоком параметров **Фильтр**:

- **Фильтр** (обязательно) – используется для установки критериев определения событий, из-за которых будет срабатывать селектор. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах

  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. Название должно содержать от 1 до 128 символов Юникода.
  4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

     c. В раскрывающемся списке **оператор** выберите нужный вам 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).
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно

использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Фильтрация по данным из поля события Extra

Условия для фильтров по данным из поля события **Extra**:

- Условие – **Если**.
- Левый операнд – **поле события**.
- В поле события вы можете указать одно из следующих значений:
  - Поле **Extra**.
  - Значение из поля Extra в следующем формате:

    `Extra.<название поля>`

    Например, `Extra.app`.

    Значение этого типа указывается вручную.

- Значение из массива, записанного в поле **Extra**, в следующем формате:

  `Extra.<название поля>.<элемент массива>`

  Например, `Extra.array.0`.

  Нумерация значений в массиве начинается с 0.

  > Значение этого типа указывается вручную.

- Оператор – =.
- Правый операнд – **константа**.
- Значение – значение, по которому требуется фильтровать события.

На закладке **Локальные переменные** с помощью кнопки **Добавить переменную** можно объявлять переменные, которые будут действовать в пределах этого правила корреляции.

Закладка **Действия**

В ресурсе типа **simple** может быть только один триггер: **На каждом событии**. Он активируется каждый раз, когда срабатывает селектор.

Доступные параметры триггера:

- **Отправить событие на дальнейшую обработку** – если этот флажок установлен, корреляционное событие будет отправлено на пост-обработку: на обогащение, для реагирования и в точки назначения.
- **Отправить событие снова в коррелятор** – если этот флажок установлен, созданное корреляционное событие будет обрабатываться текущим ресурсом правила корреляции. Это позволяет достичь иерархической корреляции.

  > Если установлены оба флажка, правило корреляции будет отправлено сначала на пост-обработку, а затем в селекторы текущего правила корреляции.

- **Не создавать алерт** – если этот флажок установлен, алерт не будет создаваться при срабатывании этого правила корреляции.
- Группа параметров **Обновление активных листов** – используется для назначения триггера на одну или несколько операций с активными листами. С помощью кнопок

Добавить действие с активным листом и **Удалить действие с активным листом** можно добавлять и удалять операции с активными листами.

Доступные параметры:

- **Название** (обязательно) – этот раскрывающийся список используется для выбора ресурсов активного листа.
- **Операция** (обязательно) – этот раскрывающийся список используется для выбора операции, которую необходимо выполнить:
  - **Получить** – получить запись активного листа и записать значения указанных полей в корреляционное событие.
  - **Установить** – записать значения указанных полей корреляционного события в активный лист, создав новую или обновив существующую запись активного листа. При обновлении записи активного листа данные объединяются, и только указанные поля перезаписываются.
  - **Удалить** – удалить запись из активного листа.
- **Ключевые поля** (обязательно) – это список полей события, используемые для создания записи активного листа. Этот список также используется в качестве ключа записи активного листа.

  > Ключ записи активного листа зависит только от состава полей и не зависит от порядка их отображения в веб-интерфейсе KUMA.

- **Сопоставление** (требуется для операций **Получить** и **Установить**) – используется для сопоставления полей активного листа с полями событий. Можно установить более одного правила сопоставления.
  - Левое поле используется для указания поля активного листа.

    > Поле не должно содержать специальные символы или только цифры.

  - Средний раскрывающийся список используется для выбора полей событий.
  - Правое поле можно использовать для назначения константы полю активного листа, если была выбрана операция **Установить**.

- Группа параметров **Обогащение** – вы можете менять значения полей корреляционных событий, используя правила обогащения, аналогичные ресурсам правил обогащения. Эти

правила обогащения хранятся в ресурсе правила корреляции, в котором они были созданы. Можно создать более одного правила обогащения. Правила обогащения можно добавлять или удалять с помощью кнопок **Добавить обогащение** и **Удалить обогащение**.

- **Тип источника** – в этом раскрывающемся списке можно выбрать тип обогащения. В зависимости от выбранного типа отобразятся дополнительные параметры, которые также потребуется заполнить.

  Доступные типы обогащения:

  - константа

    Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

    - В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов Юникода. Если оставить это поле пустым, существующее значение поля события будет удалено.
    - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

  - словарь

    Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

    При выборе этого типа в раскрывающемся списке **Название словаря** необходимо выбрать словарь, из которого будут браться значения, а в блоке параметров **Ключевые поля** с помощью кнопки **Добавить поле** требуется выбрать поля события, значения которых будут использоваться для выбора записи словаря.

  - таблица

    Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**.

    При выборе этого типа обогащения в раскрывающемся списке **Название словаря** необходимо выбрать словарь, из которого будут браться значения, а в блоке параметров **Ключевые поля** с помощью кнопки **Добавить поле** требуется выбрать поля события, значения которых будут использоваться для выбора записи словаря.

Также в таблице **Сопоставление** необходимо настроить, из каких полей словаря и в какие поля события будут передаваться данные:

- В столбце **Поле словаря** необходимо выбрать поле словаря. Доступные поля зависят от выбранного ресурса словаря.
- В столбце **Поле KUMA** необходимо выбрать поле события, в которое следует записать значение. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** можно задать название для помещаемых в них данных.

Новые строки в таблицу можно добавлять с помощью кнопки **Добавить элемент**. Столбцы можно удалить с помощью кнопки ✕.

- событие

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.
- В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.
- Если нажать на кнопку 🔧, откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

  Доступные преобразования

  Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

  Доступные преобразования:

  - **lower** – используется для перевода всех символов значения в нижний регистр
  - **upper** – используется для перевода всех символов значения в верхний регистр

- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.

- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:

  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.

- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.

  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.

- **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **decodeHexString** – используется для конвертации HEX-строки в текст.

- **decodeBase64String** – используется для конвертации Base64-строки в текст.

- **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

- шаблон

Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

- В поле **Шаблон** поместите шаблон Go.

  Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт.

  Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

- **Отладка** – с помощью этого раскрывающегося списка можно включить логирование операций сервиса.

- **Описание** – описание ресурса. До 256 символов Юникода.

- Блок параметров **Фильтр** – позволяет выбрать, какие события будут отправляться на обогащение. Настройка происходит, как описано выше.

- Группа параметров **Изменение категорий** – используется для изменения категорий активов, указанных в событии. Правил категоризации может быть несколько: их можно добавить или удалить с помощью кнопок **Добавить категоризацию** или **Удалить категоризацию**. Активам можно добавлять или удалять только реактивные категории.

- **Действие** – этот раскрывающийся список используется для выбора операции над категорией:
  - **Добавить** – присвоить категорию активу.
  - **Удалить** – отвязать актив от категории.
- **Поле события** – поле события, в котором указан актив, над которым будет совершена операция.
- **Идентификатор категории** – с помощью кнопки можно выбрать категорию, над которой будет совершена операция. При нажатии на нее открывается окно **Выбор категорий**, где отображается дерево категорий.

Правила корреляции типа operational

Правила корреляции типа **operational** используются для работы с активными листами.

Окно ресурса правила корреляции содержит следующие закладки:

- **Общие** – используется для указания основных параметров ресурса правила корреляции. На этой закладке можно выбрать тип правила корреляции.
- **Селекторы** – используется для определения условий, которым должны удовлетворять обрабатываемые события для срабатывания правила корреляции. Доступные параметры зависят от выбранного типа ресурса.
- **Действия** – используется для установки триггеров, срабатывающих при выполнении условий, заданных в группе настроек **Селекторы**. У ресурса правила корреляции должен быть хотя бы один триггер. Доступные параметры зависят от выбранного типа ресурса.

Закладка **Общие**

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – тенант, которому принадлежит правило корреляции.
- **Тип** (обязательно) – раскрывающийся список для выбора типа правила корреляции. Выберите **operational**, если хотите создать правило корреляции типа operational.
- **Частота срабатываний** – максимальное количество срабатываний правила корреляции в секунду. Значение по умолчанию: 100.

Если правила корреляции, в которых реализована сложная логика обнаружения закономерностей, не срабатывают, причиной могут быть особенности подсчета срабатываний правила в KUMA. Попробуйте увеличить значение **Частота срабатываний**, например, до `1000000`.

- **Описание** – описание ресурса. До 256 символов Юникода.

Закладка **Селекторы**

В ресурсе типа **operational** может быть только один селектор, для которого доступны закладки **Параметры** и **Локальные переменные**.

Закладка **Параметры** содержит параметры с блоком параметров **Фильтр**:

- **Фильтр** (обязательно) – используется для установки критериев определения событий, из-за которых будет срабатывать селектор. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах

  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. Название должно содержать от 1 до 128 символов Юникода.
  4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

c. В раскрывающемся списке **оператор** выберите нужный вам 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).
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Фильтрация по данным из поля события Extra

Условия для фильтров по данным из поля события **Extra**:

- Условие – **Если**.

- Левый операнд – **поле события**.

- В поле события вы можете указать одно из следующих значений:
  - Поле **Extra**.
  - Значение из поля Extra в следующем формате:

    `Extra.<название поля>`

    Например, `Extra.app`.

    > Значение этого типа указывается вручную.

  - Значение из массива, записанного в поле **Extra**, в следующем формате:

    `Extra.<название поля>.<элемент массива>`

    Например, `Extra.array.0`.

    Нумерация значений в массиве начинается с 0.

    > Значение этого типа указывается вручную.

- Оператор – =.
- Правый операнд – **константа**.
- Значение – значение, по которому требуется фильтровать события.

На закладке **Локальные переменные** с помощью кнопки **Добавить переменную** можно объявлять переменные, которые будут действовать в пределах этого правила корреляции.

Закладка **Действия**

В ресурсе типа **operational** может быть только один триггер: **На каждом событии**. Он активируется каждый раз, когда срабатывает селектор.

Доступные параметры триггера:

- Группа параметров **Обновление активных листов** – используется для назначения триггера на одну или несколько операций с активными листами. С помощью кнопок **Добавить действие с активным листом** и **Удалить действие с активным листом** можно добавлять и удалять операции с активными листами.

  Доступные параметры:

- **Название** (обязательно) – этот раскрывающийся список используется для выбора ресурсов активного листа.

- **Операция** (обязательно) – этот раскрывающийся список используется для выбора операции, которую необходимо выполнить:

  - **Получить** – получить запись активного листа и записать значения указанных полей в корреляционное событие.

  - **Установить** – записать значения указанных полей корреляционного события в активный лист, создав новую или обновив существующую запись активного листа. При обновлении записи активного листа данные объединяются, и только указанные поля перезаписываются.

  - **Удалить** – удалить запись из активного листа.

- **Ключевые поля** (обязательно) – это список полей события, используемые для создания записи активного листа. Этот список также используется в качестве ключа записи активного листа.

  > Ключ записи активного листа зависит только от состава полей и не зависит от порядка их отображения в веб-интерфейсе KUMA.

- **Сопоставление** (требуется для операций **Получить** и **Установить**) – используется для сопоставления полей активного листа с полями событий. Можно установить более одного правила сопоставления.

  - Левое поле используется для указания поля активного листа.

    > Поле не должно содержать специальные символы или только цифры.

  - Средний раскрывающийся список используется для выбора полей событий.

  - Правое поле можно использовать для назначения константы полю активного листа, если была выбрана операция **Установить**.

Переменные в корреляторах

Если для покрытия каких-то сценариев обеспечения безопасности недостаточно отслеживания значений в полях событий, активных листах или словарях, вы можете воспользоваться глобальными и локальными *переменными*. С их помощью можно выполнять различные действия над поступающими в корреляторы значениями, реализуя сложную логику выявления угроз. Переменные можно объявить в корреляторе (*глобальные переменные*) или в правиле корреляции (*локальные переменные*), присвоив им какую-либо функцию, а затем обращаться к ним из правил корреляции, как к обычным полям событий, получая в ответ результат срабатывания функции.

Область применения переменных:

- При поиске группирующих или уникальных значений полей в правилах корреляции.
- В селекторах правил корреляции в фильтрах условий, при которых должно срабатывать правило корреляции.
- При обогащении корреляционных событий. В качестве типа источника следует выбирать **Событие**.
- При наполнении активных листов значениями.

К переменным можно обращаться так же, как к полям события, предваряя их название символом $.

Свойства переменных

Локальные и глобальные переменные

Свойства глобальных и локальных переменных различаются.

Глобальные переменные:

- Глобальные переменные объявляются на уровне коррелятора и действуют только в пределах этого коррелятора.
- К глобальным переменным коррелятора можно обращаться из всех правил корреляции, которые в нем указаны.
- В правилах корреляции типа standard одна и та же глобальная переменная в каждом селекторе может принимать разные значения.
- Невозможно переносить глобальные переменные между разными корреляторами.

Локальные переменные:

- Локальные переменные объявляются на уровне правила корреляции и действуют только в пределах этого правила.
- В правилах корреляции типа standard областью действия локальной переменной является только тот селектор, в котором переменная была объявлена.
- Локальные переменные можно объявлять в любых типах правил корреляции.
- Невозможно переносить локальные переменные между правилами или селекторами.
- Локальная переменная не может быть использована в качестве глобальной переменной.

Переменные в разных типах правил корреляции

- В правилах корреляции типа **operational** в закладке **Действия** можно указывать все доступные или объявленные в этом правиле переменные.
- В правилах корреляции типа **standard** в закладке **Действия** можно указывать только переменные, указанные в этих правилах на закладке **Общие** в поле **Группирующие поля**.
- В правилах корреляции типа **simple** в закладке **Действия** можно указывать только переменные, указанные в этих правилах на закладке **Общие** в поле **Наследуемые поля**.

Требования к переменным

Добавляя функцию переменной необходимо сначала указать название функции, а затем в круглых скобках перечислить ее параметры. Исключением являются простейшие математические операции (сложение, вычитание, умножение, деление), при их использовании скобками обозначается приоритет выполнения операций.

Требования к названиям функций:

- Должно быть уникально в рамках коррелятора.
- Должно содержать от 1 до 128 символов Юникода.
- Не может начинаться с символа $.
- Должно быть написано в camelCase или CamelCase.

Особенности указания функций переменных:

- Последовательность указания параметров имеет значение.
- Параметры передаются через запятую: `,`.

- Строковые параметры передаются в одинарных кавычках: `'`.
- Наименования полей событий и переменные указываются без кавычек.
- При обращении к переменной как параметру перед ее названием необходимо добавлять символ `$`.
- Ставить пробел между параметрами необязательно.
- Во всех функциях, где в качестве параметров допускается использование переменной, допускается создавать вложенные функции.

Функции переменных

Операции с активными листами и словарями

Функции "active_list" и "active_list_dyn"

Функции позволяют получать информацию из активного листа и динамически формировать имя поля активного листа и ключа.

Необходимо указать параметры в следующей последовательности:

1. название активного листа;
2. выражение, возвращающее название поля активного листа;
3. одно или несколько выражений, из результатов которых будет составлен ключ.

Пример использования	Результат выполнения
active_list('Test', to_lower('DeviceHostName'), to_lower(DeviceCustomString2), to_lower(DeviceCustomString1))	Получение значения поля активного листа.

С помощью этих функций из переменной можно обратиться к активному листу общего тенанта. Для этого после названия активного листа необходимо добавить суффикс @Shared (регистр имеет значение). Например, active_list('exampleActiveList@Shared', 'score', SourceAddress,SourceUserName).

Функция "table_dict"

Получение информации о значении в указанном столбце словаря типа таблица.

Необходимо указать параметры в следующей последовательности:

1. название словаря;
2. название столбца словаря;
3. одно или несколько выражений, из результатов которых будет составлен ключ строки словаря.

Пример использования	Результат выполнения
`table_dict('exampleTableDict', 'office', SourceUserName)`	Получение данных из словаря `exampleTableDict` из строки с ключом `SourceUserName` из столбца `office`.
`table_dict('exampleTableDict', 'office', SourceAddress, to_lower(SourceUserName))`	Получение данных из словаря `exampleTableDict` из строки с составным ключом из значения поля `SourceAddress` и значения поля `SourceUserName` в нижнем регистре из столбца `office`.

С помощью этой функции из переменной можно обратиться к словарю общего тенанта. Для этого после названия активного листа необходимо добавить суффикс `@Shared` (регистр имеет значение). Например, `table_dict('exampleTableDict@Shared', 'office', SourceUserName)`.

Функция "dict"

Получение информации о значении в указанном столбце словаря типа словарь.

Необходимо указать параметры в следующей последовательности:

1. название словаря;
2. одно или несколько выражений, из результатов которых будет составлен ключ строки словаря.

Пример использования	Результат выполнения
`dict('exampleDictionary', SourceAddress)`	Получение данных из словаря `exampleDictionary` из строки с ключом `SourceAddress`.
`dict('exampleDictionary', SourceAddress, to_lower(SourceUserName))`	Получение данных из словаря `exampleDictionary` из строки с составным ключом из значения поля `SourceAddress` и значения поля `SourceUserName` в нижнем регистре.

С помощью этой функции из переменной можно обратиться к словарю общего тенанта. Для этого после названия активного листа необходимо добавить суффикс `@Shared` (регистр имеет значение). Например, `dict('exampleDictionary@Shared', SourceAddress)`.

Операции со строками

Функция "len"

Возвращает число символов в строке.

Строку можно передать строкой, названием поля или переменной.

Примеры использования

```
len('SomeText')
```

```
len(Message)
```

```
len($otherVariable)
```

Функция "to_lower"

Перевод символов в строке в нижний регистр.

Строку можно передать строкой, названием поля или переменной.

Примеры использования

```
to_lower(SourceUserName)
```

```
to_lower('SomeText')
```

```
to_lower($otherVariable)
```

Функция "to_upper"

Перевод символов в строке в верхний регистр. Строку можно передать строкой, названием поля или переменной.

Примеры использования

```
to_upper(SourceUserName)
```

```
to_upper('SomeText')
```

```
to_upper($otherVariable)
```

Функция "append"

Добавление символов в конец строки.

Необходимо указать параметры в следующей последовательности:

1. исходная строка;
2. добавляемая строка.

Строки можно передать строкой, названием поля или переменной.

Примеры использования	Результат использования
`append(Message, '123')`	Строка из поля `Message`, в конце которой добавлена строка `123`.
`append($otherVariable, 'text')`	Строка из переменной `otherVariable`, в конце которой добавлена строка `text`.
`append(Message, $otherVariable)`	Строка из поля `Message`, в конце которой добавлена строка из переменной `otherVariable`.

Функция "prepend"

Добавление символов в начало строки.

Необходимо указать параметры в следующей последовательности:

1. исходная строка;
2. добавляемая строка.

Строки можно передать строкой, названием поля или переменной.

Примеры использования	Результат использования
`prepend(Message, '123')`	Строка из поля `Message`, в начало которой добавлена строка `123`.
`prepend($otherVariable, 'text')`	Строка из переменной `otherVariable`, в начало которой добавлена строка `text`.
`prepend(Message, $otherVariable)`	Строка из поля `Message`, в начало которой добавлена строка из переменной `otherVariable`.

Функция "substring"

Возвращает подстроку из строки.

Необходимо указать параметры в следующей последовательности:

1. исходная строка;
2. позиция начала подстроки (натуральное число или 0);
3. (необязательно) позиция конца подстроки.

Строки можно передать строкой, названием поля или переменной. Если номер позиции больше, чем длина строки исходных данных, возвращается пустая строка.

Примеры использования	Результат использования
`substring(Message, 2)`	Возвращает часть строки из поля `Message`: от 3 символа до конца.

`substring($otherVariable, 2, 5)`	Возвращает часть строки из переменной `otherVariable`: от 3 до 6 символа.
`substring(Message, 0, len(Message) - 1)`	Возвращает всю строку из поля `Message`, кроме последнего символа.

Функция "tr"

Убирает из начала и конца строки указанные символы.

Необходимо указать параметры в следующей последовательности:

1. исходная строка;
2. (необязательно) строка, которую следует удалить из начала и конца исходной строки.

Строки можно передать строкой, названием поля или переменной. Если строку на удаление не указать, в начале и в конце исходной строки будут удалены пробелы.

Примеры использования	Результат использования
`tr(Message)`	В начале и в конце строки из поля `Message` удалены пробелы.
`tr($otherVariable, '_')`	Если переменной `otherVariable` соответствует значение `_test_`, будет возвращена строка `test`.
`tr(Message, '@example.com')`	Если в поле события `Message` находится строка `user@example.com`, будет возвращена строка `user`.

Функция "replace"

Замена в строке всех вхождений последовательности символов A на последовательность символов B.

Необходимо указать параметры в следующей последовательности:

1. исходная строка;

2. строка поиска: последовательность символов, подлежащая замене;

3. строка замены: последовательность символов, на которую необходимо заменить строку поиска.

Строки можно передать выражением.

Примеры использования	Результат использования
`replace(Name, 'UserA', 'UserB')`	Возвращается строка из поля события `Name`, в которой все вхождения `UserA` заменены на `UserB`.
`replace($otherVariable, ' text ', '_text_')`	Возвращается строка из переменной `otherVariable`, в которой все вхождения `' text '` заменены на `'_text_'`.

Функция "regexp_replace"

Замена в строке последовательности символов, удовлетворяющих регулярному выражению, на последовательность символов и группы захвата регулярного выражения.

Необходимо указать параметры в следующей последовательности:

1. исходная строка;

2. строка поиска: регулярное выражение;

3. строка замены: последовательность символов, на которую необходимо заменить строку поиска, и идентификаторы групп захвата регулярного выражения. Строку можно передать выражением.

Строки можно передать строкой, названием поля или переменной. Допускается использовать неименованные группы захвата.

В регулярных выражениях, используемых в функциях переменных, каждый символ обратной косой черты необходимо дополнительно экранировать. Например, вместо регулярного выражения `^example\\` необходимо указывать выражение `^example\\\\`.

Примеры использования	Результат использования

`regexp_replace(SourceAddress, '([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3})', 'newIP: $1.$2.$3.10')`	Возвращается строка из поля события `SourceAddress`, в которой перед IP-адресами вставлен текст `newIP`. Также последние цифры адреса заменены на `10`.

Функция "regexp_capture"

Получение из исходной строки результата, удовлетворяющего условию регулярного выражения.

Необходимо указать параметры в следующей последовательности:

1. исходная строка;
2. строка поиска: регулярное выражение.

Строки можно передать строкой, названием поля или переменной. Допускается использовать неименованные группы захвата.

В регулярных выражениях, используемых в функциях переменных, каждый символ обратной косой черты необходимо дополнительно экранировать. Например, вместо регулярного выражения `^example\\` необходимо указывать выражение `^example\\\\`.

Примеры использования

```
regexp_capture(Message, '(\\\\d{1,3}\\\\.\\\\d{1,3}\\\\.\\\\d{1,3}\\\\.\\\\
```

Операции с метками времени

Функция now

Получение временной метки в формате epoch. Запускается без аргументов.

Примеры использования

```
now()
```

Функция "extract_from_timestamp"

Получение атомарных представлений времени (в виде год, месяц, день, час, минута, секунда, день недели) из полей и переменных с временем в формате epoch.

Параметры необходимо указать в следующей последовательности:

1. Поле события, имеющего тип timestamp, или переменная.
2. Обозначение атомарного представления времени. Параметр регистрозависимый.

   Возможные варианты обозначения атомарного времени:

   - y – год в виде числа.
   - M – месяц, числовое обозначение.
   - d – число месяца.
   - wd – день недели: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday.
   - h – часы в 24-часовом формате.

- m – минуты.
- s – секунды.

3. (необязательно) Обозначение часового пояса. Если параметр не указан, время высчитывается в формате UTC.

Примеры использования

```
extract_from_timestamp(Timestamp, 'wd')
```

```
extract_from_timestamp(Timestamp, 'h')
```

```
extract_from_timestamp($otherVariable, 'h')
```

```
extract_from_timestamp(Timestamp, 'h', 'Europe/Moscow')
```

Функция "parse_timestamp"

Представление времени из формата RFC3339 (например, "2022-05-24 00:00:00", "2022-05-24 00:00:00+0300) в формат epoch.

Примеры использования

```
parse_timestamp(Message)
```

```
parse_timestamp($otherVariable)
```

Функция "format_timestamp"

Представление времени из формата epoch в формат RFC3339.

Параметры необходимо указать в следующей последовательности:

1. Поле события, имеющего тип timestamp, или переменная.
2. Обозначение формата времени: RFC3339.
3. (необязательно) Обозначение часового пояса. Если параметр не указан, время высчитывается в формате UTC.

Примеры использования

```
format_timestamp(Timestamp, 'RFC3339')
```

```
format_timestamp($otherVariable, 'RFC3339')
```

```
format_timestamp(Timestamp, 'RFC3339', 'Europe/Moscow')
```

Функция "truncate_timestamp"

Округление времени в формате epoch. После округления время возвращается в формате epoch. Время округляется в меньшую сторону.

Параметры необходимо указать в следующей последовательности:

1. Поле события, имеющего тип timestamp, или переменная.
2. Параметр округления:
   - 1s – округление до секунд;
   - 1m – округление до минут;
   - 1h – округление до часов;
   - 24h – округление до суток.
3. (необязательно) Обозначение часового пояса. Если параметр не указан, время высчитывается в формате UTC.

Примеры использования	Примеры округляемых значений
`truncate_timestamp(Timestamp, '1m')`	1654631774175 (7 June 2022 г., 19:56:14.175)
`truncate_timestamp($otherVariable, '1h')`	1654631774175 (7 June 2022 г., 19:56:14.175)
`truncate_timestamp(Timestamp, '24h', 'Europe/Moscow')`	1654631774175 (7 June 2022 г., 19:56:14.175)

Функция "time_diff"

Получение интервала времени между двумя метками времени в формате epoch.

Параметры необходимо указать в следующей последовательности:

1. Время конца отрезка. Поле события, имеющего тип timestamp, или переменная.
2. Время начала отрезка. Поле события, имеющего тип timestamp, или переменная.
3. Представление временного интервала:
    - ms – в миллисекундах;
    - s – в секундах;
    - m – в минутах;
    - h – в часах;
    - d – в днях.

Примеры использования

```
time_diff(EndTime, StartTime, 's')
time_diff($otherVariable, Timestamp, 'h')
time_diff(Timestamp, DeviceReceiptTime, 'd')
```

Математические операции

Представлены как простейшими математическими операциями, так и функциями.

Простейшие математические операции

Операции:

- сложение;
- вычитание;
- умножение;
- деление;
- деление по модулю.

Использование круглых скобок определяет последовательность действий

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- вещественные числа.

  При делении по модулю в качестве аргументов можно использовать только натуральные числа.

Ограничения использования:

- деление на ноль возвращает ноль;
- математические операции между числами и строками возвращают ноль;
- целые числа, полученные в результате операций, возвращаются без точки.

Примеры использования `(Type=3; otherVariable=2; Message=text)`	Результат использования
`Type + 1`	4
`$otherVariable - Type`	-1
`2 * 2.5`	5
`2 / 0`	0
`Type * Message`	0
`(Type + 2) * 2`	10
`Type % $otherVariable`	1

Функция "round"

Округление чисел.

Доступные аргументы:

- числовые поля события;
- числовые переменные;

- числовые константы.

Примеры использования (DeviceCustomFloatingPoint1=7.75; DeviceCustomFloatingPoint2=7.5 otherVariable=7.2)	Результат использования
`round(DeviceCustomFloatingPoint1)`	8
`round(DeviceCustomFloatingPoint2)`	8
`round($otherVariable)`	7

Функция "ceil"

Округление чисел в большую сторону.

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- числовые константы.

Примеры использования (DeviceCustomFloatingPoint1=7.15; otherVariable=8.2)	Результат использования
`ceil(DeviceCustomFloatingPoint1)`	8
`ceil($otherVariable)`	9

Функция "floor"

Округление чисел в меньшую сторону.

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- числовые константы.

Примеры использования (DeviceCustomFloatingPoint1=7.15; otherVariable=8.2)	Результат использования
`floor(DeviceCustomFloatingPoint1)`	7
`floor($otherVariable)`	8

Функция "abs"

Получение числа по модулю.

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- числовые константы.

Примеры использования (DeviceCustomNumber1=-7; otherVariable=-2)	Результат использования
`abs(DeviceCustomFloatingPoint1)`	7
`abs($otherVariable)`	2

Функция "pow"

Возведение числа в степень.

Параметры необходимо указать в следующей последовательности:

1. База. Вещественные числа.
2. Степень. Натуральные числа.

Доступные аргументы:

- числовые поля события;
- числовые переменные;

- числовые константы.

Примеры использования

```
pow(DeviceCustomNumber1, DeviceCustomNumber2)
```

```
pow($otherVariable, DeviceCustomNumber1)
```

Функция "str_join"

Позволяет объединить несколько строк в одну с использованием разделителя.

Параметры необходимо указать в следующей последовательности:

1. Разделитель. Строка.
2. Строка1, строка2, строкаN. Минимум 2 выражения.

Примеры использования	Результат использования
`str_join('|', to_lower(Name), to_upper(Name), Name)`	Строка.

Функция "conditional"

Позволяет получить одно значения в случае выполнения условия и другое значение, если условие не выполнится.

Параметры необходимо указать в следующей последовательности:

1. Условие. Строка. Синтаксис аналогичен условиям в SQL Where. В условии можно использовать функции переменных KUMA и ссылаться на другие переменные.
2. Значение при выполнении условия. Выражение.
3. Значение при невыполнении условия. Выражение.

Поддерживаемые операторы:

- AND
- OR

- NOT
- =
- !=
- <
- <=
- >
- >=
- LIKE (передается регулярное выражение RE2, а не SQL-выражение)
- ILIKE (передается регулярное выражение RE2, а не SQL-выражение)
- BETWEEN
- IN
- IS NULL (проверка на пустое значение, например 0 или пустую строку)

Примеры использования (значение зависит от аргументов 2 и 3)

```
conditional('SourceUserName = \\'root\\' AND DestinationUserName =
SourceUserName', 'match', 'no match')
```

```
conditional(`DestinationUserName ILIKE 'svc_.*'`, 'match', 'no
match')
```

```
conditional(`DestinationUserName NOT LIKE 'svc_.*'`, 'match', 'no
match')
```

Объявление переменных

Для объявления переменных их необходимо добавить в коррелятор или правило корреляции.

Чтобы добавить глобальную переменную в существующий коррелятор:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Корреляторы** выберите набор ресурсов нужного коррелятора.

   Откроется мастер установки коррелятора.

2. Выберите шаг мастера установки **Глобальные переменные**.

3. Нажмите на кнопку **Добавить переменную** и укажите следующие параметры:

   - В окне **Переменная** введите название переменной.

     Требования к наименованию переменных

     - Должно быть уникально в рамках коррелятора.
     - Должно содержать от 1 до 128 символов Юникода.
     - Не может начинаться с символа $.
     - Должно быть написано в camelCase или CamelCase.

   - В окне **Значение** введите функцию переменной.

     Описание функций переменных.

   Переменных можно добавить несколько. Добавленные переменные можно изменить или удалить с помощью значка ✕.

4. Выберите шаг мастера установки **Проверка параметров** и нажмите **Сохранить**.

Глобальная переменная добавлена в коррелятор. К ней можно обращаться, как к полю события, указывая перед названием переменной символ $. Переменная будет использоваться при корреляции после перезапуска сервиса коррелятора.

Чтобы добавить локальную переменную в существующее правило корреляции:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Правила корреляции** выберите ресурс нужного правила корреляции.

   Откроется окно параметров правила корреляции. Параметры правила корреляции можно также открыть из коррелятора, в которое оно было добавлено, перейдя на шаг мастера установки **Корреляция**.

2. Откройте закладку **Селекторы**.

3. В селекторе откройте закладку **Локальные переменные**, нажмите на кнопку **Добавить переменную** и укажите следующие параметры:

   - В окне **Переменная** введите название переменной.

     Требования к наименованию переменных

     - Должно быть уникально в рамках коррелятора.

- Должно содержать от 1 до 128 символов Юникода.
- Не может начинаться с символа $.
- Должно быть написано в camelCase или CamelCase.

- В окне **Значение** введите функцию переменной.

  Описание функций переменных.

Переменных можно добавить несколько. Добавленные переменные можно изменить или удалить с помощью значка ✕.

Для правил корреляции типа standard повторите этот шаг для каждого селектора, в которым вы хотите объявить переменные.

4. Нажмите **Сохранить**.

Локальная переменная добавлена в правило корреляции. К ней можно обращаться, как к полю события, указывая перед названием переменной символ $. Переменная будет использоваться при корреляции после перезапуска сервиса коррелятора.

Добавленные переменные можно изменить или удалить. Если правило корреляции обращается к необъявленной переменной (например, если ее название было изменено), в качестве результата возвращается пустая строка.

Если вы измените название переменной, вам потребуется вручную изменить название этой переменной во всех правилах корреляции, где вы ее использовали.

Нормализаторы

Ресурсы нормализатора используются для приведения исходных, "сырых", событий из различных форматов к модели данных событий KUMA. Это превращает получаемые события в нормализованные, которые могут обрабатываться другими ресурсами и сервисами KUMA.

Ресурс нормализатора состоит из *основного* и необязательных *дополнительных правил парсинга событий*. Данные передаются по древовидной структуре правил парсинга в зависимости от заданных *условий*. В ресурсе нормализатора из одного основного и множества дополнительных правил парсинга можно создать сложную логику обработки событий. Последовательность создания правил парсинга имеет значение: событие обрабатывается последовательно и его путь отображается в виде стрелочек.

Ресурс нормализатора создается в несколько этапов:

1. **Подготовка к созданию ресурса нормализатора**

   Ресурс нормализатора можно создать в веб-интерфейсе KUMA:

- В разделе **Ресурсы** → **Нормализаторы**.
- При создании коллектора на шаге **Парсинг событий**.

Затем в нормализаторе необходимо создать правила парсинга.

2 **Создание основного правила парсинга событий**

Основное правило парсинга создается с помощью кнопки **Добавить парсинг событий**. При этом открывается окно **Парсинг событий**, в котором вы можете задать параметры основного правила парсинга:

- Задать параметры парсинга событий.
- Задать параметры обогащения событий.

Основное правило парсинга событий отображается в ресурсе нормализатора в виде темного кружка. Параметры основного правила парсинга можно просмотреть или изменить, нажав на его кружок. При наведении на кружок отображается значок плюса: при нажатии на него можно добавить дополнительные правила парсинга.

Название основного правила парсинга используется в KUMA в качестве названия нормализатора.

3 **Создание дополнительных правил парсинга событий**

При нажатии на значок плюса, который отображается при наведении указателя мыши на кружок или блок, обозначающей парсер событий, откроется окно **Дополнительный парсинг события**, 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 ресурсе нормализатора 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 парсер. Параметры дополнительного правила парсинга можно просмотреть или изменить, нажав его блок.

Если навести указатель 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.

4 **Завершение создания ресурса нормализатора**

Создание ресурса нормализатора завершается нажатием кнопки **Сохранить**.

В ресурсе нормализатора в верхнем правом углу окна располагается окно поиска, с помощью которого можно искать по названию среди дополнительных правил парсинга данного ресурса.

Для этих ресурсов 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 ресурс нормализатора может быть поврежден. При необходимости изменить преобразования в нормализаторе, который уже является частью сервиса, вносите правки непосредственно в ресурс нормализатора в разделе веб-интерфейса **Ресурсы** → **Нормализаторы**.

Параметры парсинга событий

При создании правил парсинга событий в окне параметров парсера в закладке **Схема нормализации** вы можете настроить правила приведения поступающих событий к формату KUMA.

Доступные параметры:

- **Название** (обязательно) – название правил парсинга. Должно содержать от 1 до 128 символов Юникода. Название основного правила парсинга будет использоваться в качестве названия ресурса нормализатора.

- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

  Этот параметр недоступен для дополнительных правил парсинга.

- **Метод парсинга** (обязательно) – выпадающий список для выбора типа входящих событий. В зависимости от выбора можно будет воспользоваться преднастроенными правилами сопоставления полей событий или же задать свои собственные правила. При выборе некоторых методов парсинга могут стать доступны дополнительные параметры, требуемые для заполнения.

  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 можно обращаться к полям вложенных объектов, поочередно через точку указывая названия параметров. Например, к параметру `username` из строки `"user": {"username":"system:node:example-01"}` можно обратиться с помощью запроса `user.username`.

Файлы обрабатываются построчно. Многострочные объекты с вложенными структурами могут быть нормализованны некорректно.

- **cef**

  Этот метод парсинга используется для обработки данных в формате CEF.

  При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

- **regexp**

  Этот метод парсинга используется для создания собственных правил обработки данных в формате JSON.

  В поле блока параметров **Нормализация** необходимо добавить регулярное выражение (синтаксис RE2) с именованными группами захвата: имя группы и ее значение будут считаться полем и значением "сырого" события, которое можно будет преобразовать в поле события формата KUMA.

  Чтобы добавить правила обработки событий:

  1. Скопируйте в поле **Примеры событий** пример данных, которые вы хотите обработать. Это необязательный, но рекомендуемый шаг.

  2. В поле блока параметров **Нормализация** добавьте регулярное выражение с именованными группами захвата в синтаксисе RE2, например "(?P<name>regexp)".

     Можно добавить несколько регулярных выражений с помощью кнопки **Добавить регулярное выражение**. При необходимости удалить регулярное выражение, воспользуйтесь кнопкой ✕.

  3. Нажмите на кнопку **Перенести названия полей в таблицу**.

Имена групп захвата отображаются в столбце **Поле KUMA** таблицы **Сопоставление**. Теперь в столбце напротив каждой группы захвата можно выбрать соответствующее ей поле KUMA или, если вы именовали группы захвата в соответствии с форматом CEF, можно воспользоваться автоматическим сопоставлением CEF, поставив флажок **Использовать синтаксис CEF при нормализации**.

Правила обработки событий добавлены.

- syslog

  Этот метод парсинга используется для обработки данных в формате syslog.

  При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

- csv

  Этот метод парсинга используется для создания собственных правил обработки данных в формате CSV.

  При выборе этого метода необходимо в поле **Разделитель** указать разделитель значений в строке. В качестве разделителя допускается использовать любой однобайтовый символ ASCII.

- kv

  Этот метод парсинга используется для обработки данных в формате ключ-значение.

  При выборе этого метода необходимо указать значения в следующих обязательных полях:

  - **Разделитель пар** – укажите символ, которые будет служит разделителем пар ключ-значение. Допускается указать любое односимвольное (1 байт) значение при условии, что символ не будет совпадать с разделителем значений.

  - **Разделитель значений** – укажите символ, который будет служить разделителем между ключом и значением. Допускается указать любое односимвольное (1 байт) значение при условии, что символ не будет совпадать с разделителем пар ключ-значение.

- xml

  Этот метод парсинга используется для обработки данных в формате XML, в которых каждый объект, включая его вложенные объекты, занимает одну строку файла. Файлы обрабатываются построчно.

  При выборе этого метода в блоке параметров **Атрибуты XML** можно указать ключевые атрибуты, которые следует извлекать из тегов. Если в структуре XML в одном теге есть атрибуты с разными значениями, можно определить нужное значение, указав ключ к нему в столбце **Исходные данные** таблицы **Сопоставление**.

  Чтобы добавить ключевые атрибуты XML,

  Нажмите на кнопку **Добавить поле** и в появившемся окне укажите путь к нужному атрибуту.

  Можно добавить несколько атрибутов. Атрибуты можно удалить по одному с помощью значка с крестиком или все сразу с помощью кнопки **Сбросить**.

  Если ключевые атрибуты XML не указаны, при сопоставлении полей уникальный путь к значению XML будет представлен последовательностью тегов.

- netflow5

  Этот метод парсинга используется для обработки данных в формате NetFlow v5.

  При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

  В правилах сопоставления по умолчанию для типа **netflow5** тип протокола не указывается в полях событий KUMA. При парсинге данных в формате NetFlow в закладке нормализатора **Обогащение** следует создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

- netflow9

  Этот метод парсинга используется для обработки данных в формате NetFlow v9.

При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

В правилах сопоставления по умолчанию для типа **netflow9** тип протокола не указывается в полях событий KUMA. При парсинге данных в формате NetFlow в закладке нормализатора **Обогащение** следует создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

- sflow5

  Этот метод парсинга используется для обработки данных в формате sFlow5.

  При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

- ipfix

  Этот метод парсинга используется для обработки данных в формате IPFIX.

  При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

  В правилах сопоставления по умолчанию для типа **ipfix** тип протокола не указывается в полях событий KUMA. При парсинге данных в формате NetFlow в закладке нормализатора **Обогащение** следует создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

- sql

  Этот метод парсинга используется для обработки данных в формате SQL.

- **Сохранить исходное событие** (обязательно) – с помощью этого раскрывающегося списка можно указать, надо ли сохранять исходное событие 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: 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.

Этот параметр недоступен для дополнительных правил парсинга.

- **Сохранить дополнительные поля** (обязательно) – в этом раскрывающемся списке можно выбрать, хотите ли вы сохранять поля и их значения, для которых не настроены правила сопоставления (см. ниже). Эти 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`.

      > Значение этого типа указывается вручную.

- Значение из массива, записанного в поле **Extra**, в следующем формате:

  `Extra.<название поля>.<элемент массива>`

  Например, `Extra.array.0`.

  Нумерация значений в массиве начинается с 0.

  > Значение этого типа указывается вручную.

- Оператор – =.
- Правый операнд – **константа**.
- Значение – значение, по которому требуется фильтровать события.

По умолчанию дополнительные поля не сохраняются.

- **Описание** – описание ресурса: до 256 символов Юникода.

  Этот параметр недоступен для дополнительных правил парсинга.

- **Примеры событий** – в это поле можно поместить пример данных, которые вы хотите обработать.

  Этот параметр недоступен для методов парсинга **netflow5**, **netflow9**, **sflow5**, **ipfix**, **sql**.

- Блок параметров **Сопоставление** – здесь можно настроить сопоставление полей исходного события с полями события в формате KUMA:

  - **Исходные данные** – столбец для названий полей исходного события, которые вы хотите преобразовать в поля события KUMA.

    Если рядом с названиями полей в столбце **Исходные данные** нажать на кнопку 🔧, откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA. В окне **Преобразования** добавленные правила можно менять местами, перетягивая их за значок ⠿, а также удалять с помощью значка ✕.

    Доступные преобразования

    > Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.
    >
    > Доступные преобразования:

- **lower** – используется для перевода всех символов значения в нижний регистр

- **upper** – используется для перевода всех символов значения в верхний регистр

- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.

- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:

  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.

- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.

  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.

- **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **decodeHexString** – используется для конвертации HEX-строки в текст.

- **decodeBase64String** – используется для конвертации Base64-строки в текст.

- **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

- **Поле KUMA** – раскрывающийся список для выбора требуемых полей событий KUMA. Поля можно искать, вводя в поле их названия.

- **Подпись** – в этом столбце можно добавить уникальную пользовательскую метку полям событий, которые начинаются с `DeviceCustom*` и `Flex*`.

Новые строки таблицы можно добавлять с помощью кнопки **Добавить строку**. Строки можно удалять по отдельности с помощью кнопки ✕ или все сразу с помощью кнопки **Очистить все**.

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

Обогащение в нормализаторе

При создании правил парсинга событий в окне параметров парсера в закладке **Обогащение** вы можете настроить правила дополнения полей нормализованного события другими данными с помощью правил обогащения, аналогичным правилам в ресурсах правил обогащения. Эти правила хранятся в ресурсе нормализатора, в котором они были созданы.

Обогащения создаются с помощью кнопки **Добавить обогащение**. Правил обогащения может быть несколько. Правила обогащения можно удалять с помощью кнопки ✕.

Параметры, доступные в блоке параметров правила обогащения:

- **Тип источника** (обязательно) – раскрывающийся список для выбора типа обогащения. В зависимости от выбранного типа отобразятся дополнительные параметры, которые также потребуется заполнить.

  Доступные типы источников обогащения:

  - **константа**

Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

- В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов Юникода. Если оставить это поле пустым, существующее значение поля события будет удалено.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

- словарь

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

При выборе этого типа в раскрывающемся списке **Название словаря** необходимо выбрать словарь, из которого будут браться значения, а в блоке параметров **Ключевые поля** с помощью кнопки **Добавить поле** требуется выбрать поля события, значения которых будут использоваться для выбора записи словаря.

- таблица

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**.

При выборе этого типа обогащения в раскрывающемся списке **Название словаря** необходимо выбрать словарь, из которого будут браться значения, а в блоке параметров **Ключевые поля** с помощью кнопки **Добавить поле** требуется выбрать поля события, значения которых будут использоваться для выбора записи словаря.

Также в таблице **Сопоставление** необходимо настроить, из каких полей словаря и в какие поля события будут передаваться данные:

- В столбце **Поле словаря** необходимо выбрать поле словаря. Доступные поля зависят от выбранного ресурса словаря.

- В столбце **Поле KUMA** необходимо выбрать поле события, в которое следует записать значение. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** можно задать название для помещаемых в них данных.

Новые строки в таблицу можно добавлять с помощью кнопки **Добавить элемент**. Столбцы можно удалить с помощью кнопки ✕.

- **событие**

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.
- В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.
- Если нажать на кнопку 🔧, откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

  Доступные преобразования

  Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

  Доступные преобразования:

  - **lower** – используется для перевода всех символов значения в нижний регистр
  - **upper** – используется для перевода всех символов значения в верхний регистр
  - **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
  - **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.
  - **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:

    - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.

    - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.

- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.

    - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.

    - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **decodeHexString** – используется для конвертации HEX-строки в текст.

- **decodeBase64String** – используется для конвертации Base64-строки в текст.

- **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

- шаблон

Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

- В поле **Шаблон** поместите шаблон Go.

  Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт.

  Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

- **Целевое поле** (обязательно) – раскрывающийся список для выбора поля события KUMA, в которое следует поместить данные.

  Этот параметр недоступен для типа источника обогащения **таблица**.

Условия передачи данных в дополнительный парсер

При создании дополнительных правил парсинга событий вы можете задать условия, при выполнении которых события будут поступать на обработку в это правило парсинга. Условия можно задать в окне **Дополнительное правило парсинга** в закладке **Условия дополнительной нормализации**. В основных правилах парсинга эта закладка отсутствует.

Доступные параметры:

- **Поле, которое следует передать в нормализатор** – используется для указания поля события в том случае, если вы хотите отправлять на дополнительный парсинг только события с определенными полями.

  Если оставить это поле пустым, в дополнительный парсер будет передано событие целиком.

- Блок фильтров – используется для формулирования сложных условий, которым должны удовлетворять поступающие в парсер события.

  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 указываются названия полей событий, поступающих в парсер. Данные обрабатываются только как текстовые строки.

- Операторы:

  - **=** – полное совпадение левого и правого операндов.
  - **startsWith** – левый операнд начинается с символов, указанных в правом операнде.
  - **endsWith** – левый операнд заканчивается символами, указанными в правом операнде.
  - **match** – левые операнд соответствует регулярному выражению (RE2), указанному в правом операнде.
  - **in** – левый операнд соответствует одному из значений, указанных в правом операнде.

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 можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

Доступные преобразования:

- **lower** – используется для перевода всех символов значения в нижний регистр
- **upper** – используется для перевода всех символов значения в верхний регистр
- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:

  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.

- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.

  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **decodeHexString** – используется для конвертации HEX-строки в текст.

- **decodeBase64String** – используется для конвертации Base64-строки в текст.

- **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

Предустановленные нормализаторы

В поставку KUMA включены перечисленные в таблице ниже нормализаторы.

Наименование нормализатора	Источник событий	Тип	Комментарий
[OOTB] 1C EventJournal Normalizer	Журнал регистрации 1С.	xml	
[OOTB] 1C TechJournal Normalizer	Технологический журнал 1С.	regexp	
[OOTB] Apache Access file (Common or Combined Log Format)	Apache access.log в формате Common or Combined Log Format).	regexp	Чтение файла.
[OOTB] Apache Access Syslog (Common or Combined Log Format)	Apache access.log в формате Common or Combined Log Format), с Syslog-заголовком.	syslog	
[OOTB] Bastion SKDPU-GW	ИТ Бастион Система СКДПУ.	syslog	
[OOTB] BIND file	Журналы DNS сервера BIND.	regexp	Чтение файла.
[OOTB] BIND Syslog	Журналы DNS сервера BIND, с заголовком Syslog.	syslog	
[OOTB] C-Terra	События С-Терра Шлюз.	syslog	Получение по Syslog.
[OOTB] CEF	События в формате CEF от произвольных источников.	cef	Поддерживает чтение файлов от источников: ИнфоТеКС IDS, АйТи Бастион – СКДПУ НТ Мониторинг и аналитика, UserGate.

[OOTB] Checkpoint Syslog CEF by CheckPoint	Checkpoint, нормализация на основании вендорской схемы представления событий в формат CEF.	syslog	
[OOTB] Checkpoint Syslog basic	Пользовательское сопоставление полей Checkpoint, нормализация в зависимости от типа устройства.	syslog	
[OOTB] Cisco ASA Extended v 0.1	Cisco ASA базовый расширенный набор событий.	syslog	
[OOTB] Cisco Basic	Cisco ASA базовый набор событий.	syslog	
[OOTB] Cisco WSA AccessFile	Прокси-сервер Cisco WSA, файл access.log.	regexp	Чтение файла.
[OOTB] Continent SQL	Континент АПКШ, запросы к БД, таблицы AlertLog, PacketLog, ServerAccessLog, SystemLog.	sql	
[OOTB] CyberTrace	События Kaspersky CyberTrace.	regexp	
[OOTB] DNS Windows	Журналы DNS сервера Windows.	regexp	Чтение файла.
[OOTB] Dovecot Syslog	Журналы POP3/IMAP сервера dovecpt.	syslog	
[OOTB] Exchange CSV	Журналы MTA сервера Exchange.	csv	Чтение файла.
[OOTB] FortiGate KV	Журналы FortiGate в формате Key-Value.	regexp	
[OOTB] Fortimail	Журналы почтовой системы Fortimail.	regexp	

[OOTB] FreeIPA	Журналы службы каталогов Free IPA.	json	
[OOTB] Huawei USG Basic	Журналы основных модулей USG.	syslog	
[OOTB] IIS Log File Format	Журналы Microsoft IIS.	regexp	Чтение файла.
[OOTB] InfoWatch Traffic Monitor	DLP система Traffic Monitor компании InfoWatch.	sql	
[OOTB] IPFIX	События Netflow формата IPFIX.	ipfix	
[OOTB] Juniper - JUNOS	Журналы сетевого оборудования Juniper.	regexp	
[OOTB] KATA	Kaspersky Anti Targeted Attack.	cef	
[OOTB] KICS4Net v2.x	Kaspersky Industrial Cyber Security v 2.x.	cef	
[OOTB] KICS4Net v3.x	Kaspersky Industrial Cyber Security v 3.x.	syslog	
[OOTB] KSC	Kaspersky Security Center.	cef	Пассивное получение событий от KSC: KUMA прослушивает порт, KSC отправляет события.
[OOTB] KSC from SQL	Kaspersky Security Center, запросы к БД MS SQL.	sql	Активное получение событий из KSC: KUMA получает события из БД KSC.
[OOTB] KSMG	Kaspersky Security Mail Gateway.	syslog	
[OOTB] KWTS (KV)	Журналы KWTS в случае их отправки в формате Key-Value.	syslog	
[OOTB] Linux audit and iptables Syslog	События Linux.	syslog	

[OOTB] Linux audit.log file	События Linux.	regexp	Чтение файла.
[OOTB] MS DHCP file	Журналы DHCP сервера Windows.	csv	Чтение файла.
[OOTB] NetFlow v5	События Netflow v5.	netflow5	
[OOTB] NetFlow v9	События Netflow v9.	netflow9	
[OOTB] Nginx regexp	Журнал Nginx.	regexp	
[OOTB] PA-NGFW (Syslog-CSV)	Журналы Palo Alto в формате CSV.	csv	Предпочтительный вариант отправки журналов – формат CEF. Отправка журналов в csv, только если отправка в CEF невозможна.
[OOTB] pfSense Syslog	События pfSence.	syslog	
[OOTB] pfSense w/o hostname	Пользовательский нормализатор события pfSence (некорректный формат Syslog заголовка).	regexp	
[OOTB] PTsecurity NAD	Network Anomaly Detection компании Positive Technologies.	syslog	
[OOTB] PTsecurity WAF	Web Application Firewall компании Positive Technologies.	syslog	
[OOTB] SecretNet SQL	Secret Net 7.	sql	
[OOTB] Squid access Syslog	Журналы access.log прокси-сервера Squid.	syslog	Получение по Syslog.
[OOTB] Squid access.log file	Журналы access.log прокси-сервера Squid.	regexp	Чтение из файла.

[OOTB] Syslog header	События в формате Syslog от произвольных источников. Осуществляется парсинг syslog-заголовка.	syslog	Выполняется парсинг заголовка. В процессе парсинга поле message не затрагивается. В случае необходимости вы можете выполнить парсинг поля message другими нормализаторами.
[OOTB] Syslog-CEF	События в формате CEF от произвольных источников, с заголовком Syslog.	syslog	Поддерживает чтение файлов от источников: ИнфоТеКС IDS, АйТи Бастион – СКДПУ НТ Мониторинг и аналитика, UserGate.
[OOTB] Unbound Syslog	Журналы DNS сервера unbount.	syslog	
[OOTB] VipNet Coordinator Syslog	Журналы VipNet Coordinator.	syslog	
[OOTB] VMWare Horizon - Syslog	Журналы VMWare Horizon. Получение по Syslog.	syslog	
[OOTB] Windows Basic	Базовый набор событий Windows Security.	xml	
[OOTB] Windows Extended v.0.3	Расширенный набор событий Windows.	xml	Поддерживает события с терминальных серверов.
[OOTB][regexp] Continent IPS/IDS & TLS	Континент СОВ, TSL.	regexp	Чтение файла.
[OOTB][Syslog] Continent IPS/IDS & TLS	Континент СОВ, TSL.	syslog	Получение по Syslog.
[OOTB] Oracle Audit Trail	Таблица базы данных Oracle	sql	

[OOTB] SNMP. Windows {XP/2003}	Журналы Windows XP	snmp-trap	Отправка через SNMP
[OOTB] KEDR telemetry	Размеченная KATA телеметрия EDR	kafka	EnrichedEventTopic
[OOTB] Ahnlab UTM	Системные, операционные журналы, подключения, IPS	syslog	
[OOTB] Broadcom Symantec Endpoint Protection	События Symantec Endpoint Protection	syslog	
[OOTB] Citrix NetScaler	События Citrix NetScaler	syslog	
[OOTB] Eltex MES Switches	События коммутаторов Eltex MES	syslog	
[OOTB] Huawei Eudemon	События МЭ Huawei Eudemon	syslog	
[OOTB] Kerio Control	События Kerio Control	syslog	
[OOTB] Minerva EDR	События Minerva EDR	syslog	
[OOTB] PTC Winchill Fracas	События Winchill Fracas	syslog	
[OOTB] PTsecurity ISIM	События ISIM компании Positive Technologies	syslog	
[OOTB] PTsecurity Sandbox	События Sandbox компании Positive Technologies	syslog	
[OOTB] Radware DefensePro AntiDDoS	События Radware DefensePro AntiDDoS	syslog	

[OOTB] Sophos XG	События МЭ Sophos XG	syslog
[OOTB] Конфидент Dallas Lock	События Dallas Lock компании Конфидент	syslog
[OOTB] Bifit Mitigator	События AntiDDoS решения Bifit Mitigator	syslog
[OOTB] Sonicwall TZ Firewall	События межсетевых экранов серии TZ	syslog
[OOTB] WatchGuard Firebox	События межсетевых экранов Firebox	syslog

Коннекторы

Ресурсы коннекторов используются для установления соединений между сервисами KUMA, сетевыми активами и / или другими службами.

В программе доступны следующие типы коннекторов:

- internal – используется для установления связи между сервисами KUMA.
- tcp – используется для связи по протоколу TCP. Доступен для Windows- и Linux-агентов.
- udp – используется для связи по протоколу UDP. Доступен для Windows- и Linux-агентов.
- netflow – используется для установления соединений NetFlow.
- sflow – используется для установления соединений SFlow.
- nats – используется для коммуникации через NATS. Доступен для Windows- и Linux-агентов.
- kafka – используется для коммуникации с помощью kafka. Доступен для Windows- и Linux-агентов.
- http – используется для связи по протоколу HTTP. Доступен для Windows- и Linux-агентов.
- sql – используется для связи с базой данных и СУБД.

Программа поддерживает работу со следующими типами баз данных SQL:

  - SQLite.
  - MsSQL.
  - MySQL.
  - PostgreSQL.
  - Cockroach.
  - Oracle.
  - Firebird.

- file – используется для получения данных из любого текстового файла. Доступен для Linux-агентов.
- 1c-log и 1c-xml – используются для получения данных из журналов 1С.
- diode – используется для однонаправленной передачи данных в промышленных ICS-сетях с использованием диодов данных.
- ftp – используется для получения данных по протоколу File Transfer Protocol. Доступен для Windows- и Linux-агентов.
- nfs – используется для получения данных по протоколу Network File System. Доступен для Windows- и Linux-агентов.
- wmi – используется для получения данных с помощью Windows Management Instrumentation. Доступен для Windows-агентов.
- wec – используется для получения данных с помощью Windows Event Collector. Доступен для Windows-агентов.
- snmp – используется для получения данных с помощью Simple Network Management Protocol. Доступен для Windows- и Linux-агентов.
- snmp-trap – используется для получения данных с помощью "ловушек" Simple Network Management Protocol (SNMP Trap). Доступен для Windows- и Linux-агентов.

Просмотр параметров коннектора

Чтобы просмотреть параметры коннектора:

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **Коннекторы**.

2. В структуре папок выберите папку, в которой располагается нужный вам коннектор.

3. Выберите коннектор, параметры которого вы хотите просмотреть.

   Параметры коннекторов отображаются на двух вкладках: **Основные параметры** и **Дополнительные параметры**. Подробное описание параметров каждого коннектора см. в разделе *Параметры коннекторов*.

Добавление коннектора

> Вы можете включить отображение непечатаемых символов для всех полей ввода, кроме поля **Описание**.

Чтобы добавить коннектор:

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **Коннекторы**.

2. В структуре папок выберите папку, в которой должен располагаться ресурс.

   > Корневые папки соответствуют тенантам. Для того, чтобы ресурс был доступен определенному тенанту, его следует создать в папке этого тенанта.

   Если в дереве папок отсутствует требуемая папка, вам нужно создать ее.

   По умолчанию добавляемые коннекторы создаются в папке **Общий**.

3. Нажмите на кнопку **Добавить коннектор**.

4. Укажите параметры для выбранного типа коннектора.

   Параметры, которые требуется указать для каждого типа коннектора, приведены в разделе *Параметры коннекторов*.

5. Нажмите на кнопку **Сохранить**.

Параметры коннекторов

Этот раздел содержит описание параметров всех поддерживаемых KUMA типов коннекторов.

Тип internal

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора, **internal**.
  - **URL** (обязательно) – URL, с которым необходимо установить связь.

    Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.
  - **Описание** – описание ресурса: до 256 символов Юникода.
- Закладка **Дополнительные параметры**:
  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса.

    По умолчанию указывается значение **Выключено**.

Тип tcp

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора, **tcp**.
  - **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.
  - **Разделитель** – используется для указания символа, определяющего границу между событиями. Доступные значения: `\n`, `\t`, `\0`. Если разделитель не задан (выбрано пустое значение), то по умолчанию используется значение: `\n`.
  - **Описание** – описание ресурса: до 256 символов Юникода.

- Закладка **Дополнительные параметры**:

  - **Размер буфера** – используется для установки размера буфера коннектора. Значение по умолчанию: 1 МБ; максимальное: 64 МБ.

  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.

  - **Режим TLS** – использование шифрования TLS:

    - **Выключено** (по умолчанию) – не использовать шифрование TLS.

    - **Включено** – использовать шифрование, но без верификации.

    - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

    При использовании TLS невозможно указать IP-адрес в качестве URL.

  - **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.

  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

Тип udp

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:

  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.

  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

  - **Тип** (обязательно) – тип коннектора, **udp**.

  - **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.

  - **Разделитель** – используется для указания символа, определяющего границу между событиями. Доступные значения: `\n`, `\t`, `\0`. Если разделитель не задан (выбрано пустое значение), то события не разделяются.

    - **Описание** – описание ресурса: до 256 символов Юникода.

- Закладка **Дополнительные параметры**:

    - **Размер буфера** – используется для установки размера буфера коннектора. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.

    - **Рабочие процессы** – используется для установки числа рабочих процессов для коннектора. Значение по умолчанию: 1.

    - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.

    - **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.

    - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

Тип netflow

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:

    - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.

    - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

    - **Тип** (обязательно) – тип коннектора, **netflow**.

    - **URL** (обязательно) – URL, с которым необходимо установить связь.

    - **Описание** – описание ресурса: до 256 символов Юникода.

- Закладка **Дополнительные параметры**:

    - **Размер буфера** – используется для установки размера буфера коннектора. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.

    - **Рабочие процессы** – используется для установки числа рабочих процессов для коннектора. Значение по умолчанию: 1.

    - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.

- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

Тип sflow

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора, **sflow**.
  - **URL** (обязательно) – URL, с которым требуется установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.
  - **Описание** – описание ресурса: до 256 символов Юникода.
- Закладка **Дополнительные параметры**:
  - **Размер буфера** – используется для установки размера буфера коннектора. Значение по умолчанию: 1 МБ; максимальное: 64 МБ.
  - **Рабочие процессы** – используется для установки количества рабочих процессов для коннектора. Значение по умолчанию: 1.
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
  - **Отладка** – раскрывающийся список, позволяющий включить логирование ресурса. По умолчанию указывается значение **Выключено**.

Тип nats

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.

- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Тип** (обязательно) – тип коннектора, **nats**.
- **URL** (обязательно) – URL, с которым необходимо установить связь.
- **Топик** (обязательно) – тема сообщений NATS. Должно содержать символы Юникода.
- **Разделитель** – используется для указания символа, определяющего границу между событиями. Доступные значения: `\n`, `\t`, `\0`. Если разделитель не задан (выбрано пустое значение), то события не разделяются.
- **Описание** – описание ресурса: до 256 символов Юникода.

- Закладка **Дополнительные параметры**:
  - **Размер буфера** – используется для установки размера буфера коннектора. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.
  - **Идентификатор группы** – параметр GroupID для сообщений NATS. Должно содержать от 1 до 255 символов Юникода. Значение по умолчанию: `default`.
  - **Рабочие процессы** – используется для установки числа рабочих процессов для коннектора. Значение по умолчанию: 1.
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
  - **Идентификатор кластера** – идентификатор кластера NATS.
  - **Режим TLS** – использование шифрования TLS:
    - **Выключено** (по умолчанию) – не использовать шифрование TLS.
    - **Включено** – использовать шифрование, но без верификации сертификата.
    - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.
    - **Нестандартный CA** – использовать шифрование с верификацией сертификата, подписанного центром сертификации. Секрет с сертификатом выбирается в раскрывающемся списке **Нестандартный CA**, который отображается при выборе этого пункта.

      Создание сертификата, подписанного центром сертификации

Для использования этого режима TLS необходимо выполнить следующие действия на сервере Ядра KUMA (в примерах команд ниже используется OpenSSL):

1. Создать ключ, который будет использоваться центром сертификации.

   Пример команды: `openssl genrsa -out ca.key 2048`

2. Создать сертификат для только что созданного ключа.

   Пример команды: `openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<общее имя хоста центра сертификации>" -out ca.crt`

3. Создать приватный ключ и запрос на его подписание в центре сертификации.

   Пример команды: `openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<общее имя хоста сервера KUMA>" -out server.csr`

4. Создать сертификат, подписанный центром сертификации. Необходимо включить в subjectAltName доменные имена или IP-адреса сервера, для которого создается сертификат.

   Пример команды: `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. Полученный сертификат `server.crt` следует загрузить в веб-интерфейсе KUMA в секрет типа **certificate**, который затем следует выбрать в раскрывающемся списке **Нестандартный CA**.

При использовании TLS невозможно указать IP-адрес в качестве URL.

Для использования сертификатов KUMA на сторонних машинах необходимо изменить расширение файла сертификата с CERT на CRT. В противном случае может возвращаться ошибка x509: certificate signed by unknown authority.

- **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

Тип kafka

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора, **kafka**.
  - **URL** – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port.
  - **Топик** – тема сообщений Kafka. Должен содержать от 1 до 255 следующих символов: a–z, A–Z, 0–9, ".", "_", "-".
  - **Авторизация** – необходимость агентам проходить авторизацию при подключении к коннектору:
    - **выключена** (по умолчанию).
    - **PFX**.

      При выборе этого варианта требуется сформировать сертификат с закрытым ключом в формате PKCS#12-контейнера во внешнем центре сертификации, экспортировать сертификат из хранилища и загрузить его в веб-интерфейс KUMA в виде PFX-секрета.

      Добавить PFX-секрет

      1. Если вы загрузили PFX-сертификат ранее, выберите его в раскрывающемся списке **Секрет**.

         Если ранее не было добавлено ни одного сертификата, в раскрывающемся списке отобразится **Нет данных**.
      2. Если вы хотите добавить новый сертификат, справа от списка **Секрет** нажмите на кнопку +.

         Откроется окно **Секрет**.
      3. В поле **Название** введите название, под которым секрет будет отображаться в списке доступных.

4. По кнопке **Загрузить PFX** выберите файл, в который вы экспортировали сертификат с закрытым ключом, в формате PKCS#12-контейнера.

5. В поле **Пароль** введите пароль для защиты сертификата, заданный в мастере экспорта сертификата.

6. Нажмите на кнопку **Сохранить**.

Сертификат будет добавлен и отобразится в списке **Секрет**.

- **обычная**.

  При выборе этого варианта требуется указать секрет, содержащий данные учетной записи пользователя для авторизации при подключении к коннектору.

  Добавить секрет

1. Если вы создали секрет ранее, выберите его в раскрывающемся списке **Секрет**.

   Если ранее не было добавлено ни одного секрета, в раскрывающемся списке отобразится **Нет данных**.

2. Если вы хотите добавить новый секрет, справа от списка **Секрет** нажмите на кнопку +.

   Откроется окно **Секрет**.

3. В поле **Название** введите название, под которым секрет будет отображаться в списке доступных.

4. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору.

5. Если требуется, в поле **Описание** добавьте любую дополнительную информацию о секрете.

6. Нажмите на кнопку **Сохранить**.

Секрет будет добавлен и отобразится в списке **Секрет**.

- **Идентификатор группы** – параметр GroupID для сообщений Kafka. Должен содержать от 1 до 255 следующих символов: a–z, A–Z, 0–9, ".", "_", "-".

- **Описание** – описание ресурса: до 256 символов Юникода.

- Закладка **Дополнительные параметры**:
  - **Размер одного сообщения в запросе** – размер сообщения в запросе следует указывать в байтах. Значение по умолчанию 16 Мб.
  - **Максимальное время ожидания одного сообщения** – время ожидания сообщения заданного размера. Значение по умолчанию 5 секунд.
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
  - **Режим TLS** – использование шифрования TLS:
    - **Выключено** (по умолчанию) – не использовать шифрование TLS.
    - **Включено** – использовать шифрование, но без верификации сертификата.
    - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.
    - **Нестандартный CA** – использовать шифрование с верификацией сертификата, подписанного центром сертификации. Секрет с сертификатом выбирается в раскрывающемся списке **Нестандартный CA**, который отображается при выборе этого пункта.

      Создание сертификата, подписанного центром сертификации

      Для использования этого режима TLS необходимо выполнить следующие действия на сервере Ядра KUMA (в примерах команд ниже используется OpenSSL):

      1. Создать ключ, который будет использоваться центром сертификации.

         Пример команды: `openssl genrsa -out ca.key 2048`

      2. Создать сертификат для только что созданного ключа.

         Пример команды: `openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<общее имя хоста центра сертификации>" -out ca.crt`

      3. Создать приватный ключ и запрос на его подписание в центре сертификации.

Пример команды: `openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<общее имя хоста сервера KUMA>" -out server.csr`

4. Создать сертификат, подписанный центром сертификации. Необходимо включить в subjectAltName доменные имена или IP-адреса сервера, для которого создается сертификат.

   Пример команды: `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. Полученный сертификат `server.crt` следует загрузить в веб-интерфейсе KUMA в секрет типа **certificate**, который затем следует выбрать в раскрывающемся списке **Нестандартный CA**.

При использовании TLS невозможно указать IP-адрес в качестве URL.

Для использования сертификатов KUMA на сторонних машинах необходимо изменить расширение файла сертификата с CERT на CRT. В противном случае может возвращаться ошибка x509: certificate signed by unknown authority.

- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

Тип http

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:

  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.

  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

  - **Тип** (обязательно) – тип коннектора, **http**.

  - **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.

- **Разделитель** – используется для указания символа, определяющего границу между событиями. Доступные значения: `\n`, `\t`, `\0`. Если разделитель не задан (выбрано пустое значение), то события не разделяются.

- **Описание** – описание ресурса: до 256 символов Юникода.

- Закладка **Дополнительные параметры**:

  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.

  - **Режим TLS** – использование шифрования TLS:

    - **Выключено** (по умолчанию) – не использовать шифрование TLS.

    - **Включено** – использовать шифрование, но без верификации.

    - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

    При использовании TLS невозможно указать IP-адрес в качестве URL.

  - **Прокси-сервер** – раскрывающийся список, в котором можно выбрать ресурс прокси-сервера.

  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

Тип sql

KUMA поддерживает работу с несколькими **типами баз данных**.

Программа поддерживает работу со следующими типами баз данных SQL:

- SQLite.
- MsSQL.
- MySQL.
- PostgreSQL.
- Cockroach.

- Oracle.
- Firebird.

При создании коннектора вам требуется задать значения для общих параметров коннектора и индивидуальных параметров подключения к базе данных.

Для коннектора на закладке **Основные параметры** вам требуется задать значения следующих параметров:

- **Название** (обязательно) – уникальное имя ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тип** (обязательно) – тип коннектора, **sql**.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Запрос по умолчанию** (обязательно) – SQL-запрос, который выполняется при подключении к базе данных.
- **Интервал запросов, сек.** – интервал выполнения SQL-запросов. Указывается в секундах.

  Значение по умолчанию: 10 секунд.
- **Описание** – описание ресурса: до 256 символов Юникода.

Для подключения к базе данных на закладке **Основные параметры** вам требуется задать значения следующих параметров:

- **URL** (обязательно) – секрет, в котором хранится список URL-адресов для подключения к базе данных.

  При необходимости вы можете **изменить** или **создать секрет**.

  1. Нажмите на кнопку +.

     Откроется окно секрета.
  2. Укажите значения для следующих параметров:

     a. **Название** – имя добавляемого секрета.

     b. **Тип** – **urls**.

     Значение установлено по умолчанию, его редактирование недоступно.

     c. **URL** – URL-адрес базы данных.

Вам требуется учитывать, что для подключения к каждому типу базы данных используется свой формат URL-адреса.

Доступные форматы URL-адресов:

- Для SQLite:
  - `sqlite3://file:<file_path>`

  > В качестве плейсхолдера используется знак вопроса: ?.

- Для MsSQL:
  - `sqlserver://<user>:<password>@<server:port>/<instance_name>?database=<database>` (рекомендуется)
  - `sqlserver://<user>:<password>@<server>?database=<database>&encrypt=disable`

  > В качестве плейсхолдера используются символы @p1.

- Для MySQL:
  - `mysql://<user>:<password>@tcp(<server>:<port>)/<database>`

  > В качестве плейсхолдера используются символы %s.

- Для PostgreSQL:
  - `postgres://<user>:<password>@<server>/<database>?sslmode=disable`

  > В качестве плейсхолдера используются символы $1.

- Для Cockroach:

- `postgres://<user>:<password>@<server>:<port>/<database>?sslmode=disable`

В качестве плейсхолдера используются символы $1.

- Для Firebird:

  - `firebirdsql://<user>:<password>@<server>:<port>/<database>`

В качестве плейсхолдера используется знак вопроса: ?.

d. **Описание** – любая дополнительная информация.

3. При необходимости нажмите на кнопку **Добавить** и укажите дополнительный URL-адрес.

   В этом случае при недоступности одного URL-адреса программа подключается к следующему URL-адресу, указанному в списке адресов.

4. Нажмите на кнопку **Сохранить**.

1. Нажмите на кнопку .

   Откроется окно секрета.

2. Укажите значения для параметров, которые требуется изменить.

   Вы можете изменить значения для следующих параметров:

   a. **Название** – имя добавляемого секрета.

   b. **URL** – URL-адрес базы данных.

   Вам требуется учитывать, что для подключения к каждому типу базы данных используется свой формат URL-адреса.

   Доступные форматы URL-адресов:

   - Для SQLite:

     - `sqlite3://file:<file_path>`

В качестве плейсхолдера используется знак вопроса: ?.

- Для MsSQL:
  - `sqlserver://<user>:<password>@<server:port>/<instance_name>?database=<database>` (рекомендуется)
  - `sqlserver://<user>:<password>@<server>?database=<database>&encrypt=disable`

В качестве плейсхолдера используются символы @p1.

- Для MySQL:
  - `mysql://<user>:<password>@tcp(<server>:<port>)/<database>`

В качестве плейсхолдера используется символ `?`.

- Для PostgreSQL:
  - `postgres://<user>:<password>@<server>/<database>?sslmode=disable`

В качестве плейсхолдера используются символы $1.

- Для Cockroach:
  - `postgres://<user>:<password>@<server>:<port>/<database>?sslmode=disable`

В качестве плейсхолдера используются символы $1.

- Для Firebird:

- firebirdsql://<user>:<password>@<server>:<port>/<database>

В качестве плейсхолдера используется знак вопроса: ?.

c. **Описание** – любая дополнительная информация.

3. При необходимости нажмите на кнопку **Добавить** и укажите дополнительный URL-адрес.

   В этом случае при недоступности одного URL-адреса программа подключается к следующему URL-адресу, указанному в списке адресов.

4. Нажмите на кнопку **Сохранить**.

При создании подключений могут некорректно обрабатываться строки с учетными данными, содержащими специальные символы. Если при создании подключения возникает ошибка, но вы уверены в том, что значения параметров корректны, укажите специальные символы в процентной кодировке.

Коды специальных символов

!	#	$	%	&	'	(	)	*
%21	%23	%24	%25	%26	%27	%28	%29	%2
,	/	:	;	=	?	@	[	]
%2C	%2F	%3A	%3B	%3D	%3F	%40	%5B	%5

Следующие специальные символы не поддерживаются в паролях доступа к базам SQL: пробел, [,], :, /, #, %, \.

- **Столбец идентификатора** (обязательно) – название столбца, содержащего идентификатор для каждой строки таблицы.

- **Начальное значение идентификатора** (обязательно) – значение в столбце идентификатора, по которому будет определена строка, с которой требуется начать

считывание данных из SQL-таблицы.

- **Запрос** – поле для дополнительного SQL-запроса. Запрос, указанный в этом поле, выполняется вместо запроса по умолчанию.

- **Интервал запросов, сек.** – интервал выполнения SQL-запросов. Интервал, указанный в этом поле, используется вместо интервала, указанного по умолчанию для коннектора.

  Указывается в секундах. Значение по умолчанию: 10 секунд.

Для коннектора на закладке **Дополнительные параметры** вам требуется задать значения следующих параметров:

- **Кодировка символов** – кодировка символов. Значение по умолчанию: `UTF-8`.

  > KUMA конвертирует ответы SQL в кодировку UTF-8. Вы можете настроить SQL-сервер на отправку ответов в кодировке UTF-8 или выбрать их кодировку на стороне KUMA.

- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

В рамках одного коннектора вы можете **создать подключение** для нескольких поддерживаемых баз данных.

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

> Оператор UNION не поддерживается коннекторами типа SQL.

Поддерживаются следующие типы SQL:

- MSSQL

Примеры URL:

- `sqlserver://{user}:{password}@{server:port}/{instance_name}?database={database}` – (рекомендуемый вариант)
- `sqlserver://{user}:{password}@{server}?database={database}`

В качестве плейсхолдера в SQL-запросе используются символы `@p1`.

> Если вам требуется 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

  Пример URL: `mysql://{user}:{password}@tcp({server}:{port})/{database}`

  В качестве плейсхолдера в SQL-запросе используются символ `?`.

- PostgreSQL

  Пример URL: `postgres://{user}:{password}@{server}/{database}?sslmode=disable`

  В качестве плейсхолдера в SQL-запросе используются символы `$1`.

- CockroachDB

  Пример URL: `postgres://{user}:{password}@{server}:{port}/{database}?sslmode=disable`

  В качестве плейсхолдера в SQL-запросе используются символы `$1`.

- SQLite3

  Пример URL: `sqlite3://file:{file_path}`

  В качестве плейсхолдера в SQL-запросе используется знак вопроса: `?`.

- Oracle DB

  Пример URL: `oracle://{user}/{password}@{server}:{port}/{service_name}`

  Используется синтаксис Easy Connect. В качестве плейсхолдера в SQL-запросе используется символы `:val`.

При обращении к Oracle DB, если начальное значение идентификатора используется в формате datetime, в SQL-запрос нужно добавить преобразование даты с помощью функции Oracle `to_timestamp_tz`. Например, `select * from connections where login_time > to_timestamp_tz(:val, 'YYYY-MM-DD"T"HH24:MI:SSTZH:TZM')`. В этом примере `Connections` – это таблица Oracle DB, а значение переменной `:val` берется из поля **Начальное значение идентификатора**, поэтому его требуется указывать в формате с timezone (например, `2021-01-01T00:10:00+03:00`).

> Для обращения к Oracle DB необходимо установить пакет libaio1.

- Firebird SQL

  Пример URL: `firebirdsql://{user}:{password}@{server}:{port}/{database}`

  В качестве плейсхолдера в SQL-запросе используется знак вопроса: `?`.

В SQL-запросах поддерживается последовательный запрос сведений из базы данных. Например, если в поле **Запрос** указать запрос `select * from <название таблицы с данными> where id > <плейсхолдер>`, то 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.

Примеры SQL-запросов

```
SQLite, Firebird – select * from table_name where id > ?

MsSQL – select * from table_name where id > @p1

MySQL – select * from table_name where id > ?

PostgreSQL, Cockroach – select * from table_name where id > $1

Oracle – select * from table_name where id > :val
```

Тип file

Тип **file** используется для получения данных из любого текстового файла. Одна строка файла считается одним событием. Разделители между строк: \n. Коннектор этого типа доступен для Linux-агентов.

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора, **file**.
  - **URL** (обязательно) – полный путь до файла, с которым требуется выполнять взаимодействие. Например, `/var/log/*som?[1-9].log`.

    Шаблоны масок для файлов и директорий

    Маски:

    - '*' – соответствует любой последовательности символов;
    - '[' ['^'] { диапазон символов } ']' – класс символов (не должен быть пустым);
    - '?' – соответствует любому одиночному символу.

    Диапазоны символов:

    - [0-9] – числа;
    - [a-zA-Z] – буквы латинского алфавита.

    Примеры:

    - /var/log/*som?[1-9].log
    - /mnt/dns_logs/*/dns.log
    - /mnt/proxy/access*.log

    Ограничения при использовании префиксов к путям файлов

    Префиксы, которые невозможно использовать при указании путей к файлам:

    - /*
    - /bin

- /boot
- /dev
- /etc
- /home
- /lib
- /lib64
- /proc
- /root
- /run
- /sys
- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

Файлы по указанным ниже путям доступны:

- /opt/kaspersky/kuma/clickhouse/logs/
- /opt/kaspersky/kuma/mongodb/log/
- /opt/kaspersky/kuma/victoria-metrics/log/

- **Описание** – описание ресурса: до 256 символов Юникода.

- Закладка **Дополнительные параметры**:
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

Тип 1c-xml

Тип **1c-xml** используется для получения данных из журналов регистрации программы 1С. При обработке коннектором многострочные события преобразовываются в однострочные. Коннектор этого типа доступен для Linux-агентов.

При создании этого типа коннектора требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора, **1c-xml**.
  - **URL** (обязательно) – полный путь до директории с файлами, с которыми требуется выполнять взаимодействие. Например, `/var/log/1c/logs/`. Путь до директории должен заканчиваться косой чертой.

    Ограничения при использовании префиксов к путям файлов

    Префиксы, которые невозможно использовать при указании путей к файлам:

    - /*
    - /bin

- /boot
- /dev
- /etc
- /home
- /lib
- /lib64
- /proc
- /root
- /run
- /sys
- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

Файлы по указанным ниже путям доступны:

- /opt/kaspersky/kuma/clickhouse/logs/
- /opt/kaspersky/kuma/mongodb/log/
- /opt/kaspersky/kuma/victoria-metrics/log/

- **Описание** – описание ресурса: до 256 символов Юникода.

- Закладка **Дополнительные параметры**:
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

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.
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.
- Не читаются файлы с некорректным форматом событий.
- 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.

Тип 1c-log

Тип **1c-log** используется для получения данных из технологических журналов программы 1С. Разделители между строк: \n. Из многострочной записи о событии коннектор принимает только первую строку. Коннектор этого типа доступен для Linux-агентов.

При создании этого типа коннектора требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора, **1c-log**.
  - **URL** (обязательно) – полный путь до директории с файлами, с которыми требуется выполнять взаимодействие. Например, `/var/log/1c/logs/`. Путь до директории должен заканчиваться косой чертой.

    Ограничения при использовании префиксов к путям файлов

    Префиксы, которые невозможно использовать при указании путей к файлам:

    - /*
    - /bin
    - /boot
    - /dev
    - /etc
    - /home
    - /lib
    - /lib64
    - /proc
    - /root
    - /run

- /sys
- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

Файлы по указанным ниже путям доступны:

- /opt/kaspersky/kuma/clickhouse/logs/
- /opt/kaspersky/kuma/mongodb/log/
- /opt/kaspersky/kuma/victoria-metrics/log/

- **Описание** – описание ресурса: до 256 символов Юникода.

- Закладка **Дополнительные параметры**:

  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.

  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

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.

     Пример поддерживаемый структуры технологических журналов 1с

```
/var/log/1c
└── logs
    ├── ragent_1426
    │   ├── 22121505.log
    │   ├── 22121506.log
    │   ├── 22121507.log
    │   ├── 22121508.log
    │   ├── 22121509.log
    │   ├── 22121510.log
    │   ├── 22121511.log
    │   ├── 22121512.log
    │   ├── 22121513.log
    │   ├── 22121514.log
    │   ├── 22121515.log
    │   ├── 22121516.log
    │   ├── 22121517.log
    │   └── 22121518.log
    ├── ragent_1427
    │   ├── 22121518.log
    │   ├── 22121519.log
    │   ├── 22121520.log
    │   ├── 22121521.log
    │   ├── 22121522.log
    │   ├── 22121523.log
    │   ├── 22121600.log
    │   ├── 22121601.log
    │   ├── 22121602.log
    │   ├── 22121603.log
    │   ├── 22121604.log
    │   └── 22121605.log
    ├── rmngr_1542
    │   ├── 22121505.log
    │   ├── 22121506.log
    │   ├── 22121507.log
    │   ├── 22121508.log
    │   ├── 22121509.log
    │   ├── 22121510.log
    │   ├── 22121511.log
    │   ├── 22121512.log
    │   ├── 22121513.log
    │   ├── 22121514.log
    │   ├── 22121515.log
    │   ├── 22121516.log
    │   ├── 22121517.log
    │   └── 22121518.log
    ├── rmngr_1544
    │   ├── 22121518.log
    │   ├── 22121519.log
```

- 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.

- 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

Тип diode

Используется для передачи событий с помощью диода данных.

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора, **diode**.
  - **Директория с событиями от диода данных** (обязательно) – полный путь до директории на сервере коллектора KUMA, в которую диод данных перемещает файлы с событиями из изолированного сегмента сети. После считывания коннектором файлы удаляются из директории. Путь может содержать до 255 символов Юникода.

    Ограничения при использовании префиксов к путям

Префиксы, которые невозможно использовать при указании путей к файлам:

- /*
- /bin
- /boot
- /dev
- /etc
- /home
- /lib
- /lib64
- /proc
- /root
- /run
- /sys
- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*

- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

Файлы по указанным ниже путям доступны:

- /opt/kaspersky/kuma/clickhouse/logs/
- /opt/kaspersky/kuma/mongodb/log/
- /opt/kaspersky/kuma/victoria-metrics/log/

- **Разделитель** – используется для указания символа, определяющего границу между событиями. Доступные значения: `\n`, `\t`, `\0`. Если разделитель не задан (выбрано пустое значение), то по умолчанию используется значение: `\n`.

  Этот параметр должен совпадать ресурсах коннектор и точка назначения, используемых для передачи событий из изолированного сегмента сети с помощью диода данных.

- **Описание** – описание ресурса: до 256 символов Юникода.

- Закладка **Дополнительные параметры**:

  - **Рабочие процессы** – количество служб, обрабатывающих очередь запросов. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

  - **Интервал запросов, сек.** – регулярность считывания файлов из директории с событиями от диода данных. Значение по умолчанию: 2. Значение указывается в секундах.

  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.

  - **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.

    Этот параметр должен совпадать ресурсах коннектор и точка назначения, используемых для передачи событий из изолированного сегмента сети с помощью диода данных.

  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

Тип ftp

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:

  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.

  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

  - **Тип** (обязательно) – тип коннектора, **ftp**.

  - **URL** (обязательно) – Действительный URL файла или маски файлов, который начинается со схемы 'ftp://'. Для маски файлов допустимо использование * ? [...].

    Шаблоны масок для файлов

    Маски:

    - '*' – соответствует любой последовательности символов;

    - '[' ['^'] { диапазон символов } ']' – класс символов (не должен быть пустым);

    - '?' – соответствует любому одиночному символу.

    Диапазоны символов:

    - [0-9] – числа;

    - [a-zA-Z] – буквы латинского алфавита.

    Примеры:

    - /var/log/*som?[1-9].log

    - /mnt/dns_logs/*/dns.log

    - /mnt/proxy/access*.log

    Если в URL не содержится порт ftp сервера, подставляется 21 порт.

  - **Учетные данные для URL** – для указания логина и пароля к FTP серверу. При отсутствии логина и пароля строка остается пустой.

- **Описание** – описание ресурса: до 256 символов Юникода.

- Закладка **Дополнительные параметры**:

  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.

  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

Тип nfs

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:

  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.

  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

  - **Тип** (обязательно) – тип коннектора, **nfs**.

  - **URL** (обязательно) – путь до удаленной директории в формате nfs://host/path.

  - **Маска имени файла** (обязательно) – маска, по которой фильтруются файлы с событиями. Допустимо использование масок "`*`", "`?`", "`[...]`".

  - **Интервал запросов, сек.** – интервал опроса. Промежуток времени, через который перечитываются файлы с удаленной системы. Значение указывается в секундах. По умолчанию указано значение: 0.

  - **Описание** – описание ресурса: до 256 символов Юникода.

- Закладка **Дополнительные параметры**:

  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.

  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

Тип wmi

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора, **wmi**.
  - **URL** (обязательно) – URL создаваемого коллектора, например `kuma-collector.example.com:7221`.

    При создании коллектора для получения данных с помощью Windows Management Instrumentation автоматически создается агент, который будет получать необходимые данные на удаленной машине и перенаправлять их в сервис коллектора. В поле **URL** требуется указать адрес этого коллектора. URL известен заранее, если вы знаете, на каком сервере планируете установить сервис, но это поле можно заполнить и после завершения мастера установки, скопировав данные из раздела **Ресурсы** → **Активные сервисы**.
  - **Описание** – описание ресурса: до 256 символов Юникода.
  - **Учетные данные по умолчанию** – раскрывающийся список, в котором выбирать значение не требуется. Учетные данные для подключения к хостам необходимо указывать в таблице **Удаленные хосты** (см. ниже).
  - В таблице **Удаленные хосты** перечисляются удаленные устройства Windows, к которым требуется установить подключение. Доступные столбцы:
    - **Хост** (обязательно) – IP-адрес или доменное имя устройства, с которого необходимо принимать данные. Например, "machine-1.example.com".
    - **Домен** (обязательно) – название домена, в котором расположено удаленное устройство. Например, "example.com".
    - **Тип журналов** – раскрывающийся список для выбора названия журналов Windows, которые требуется получить. По умолчанию в списке отображаются только предварительно настроенные журналы, но вы можете расширить список пользовательскими журналами, введя их название в поле **Журналы Windows**, а затем нажав **ENTER**. Конфигурация сервисов и ресурсов KUMA может потребовать дополнительных изменений для правильной обработки настраиваемых журналов.

      Журналы, доступные по умолчанию:

- Application
- ForwardedEvents
- Security
- System
- HardwareEvents

Если в одном из подключений WMI используется хотя бы один журнал с неверным названием, в этом случае 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 корректно.

- **Секрет** – учетные данные для доступа к удаленному устройству Windows с правами на чтение журналов. Если оставить это поле пустым, то будут использоваться учетные данные из секрета, выбранного в раскрывающемся списке Учетные данные, используемые по умолчанию. Логин в ресурсе секрета необходимо указывать без домена, значение домена для доступа к хосту берется из столбца **Домен** таблицы **Удаленные хосты**.

  Можно выбрать ресурс секрета в раскрывающемся списке или создать его с помощью кнопки +. Выбранный секрет можно изменить, нажав на кнопку ✎.

- Закладка **Дополнительные параметры**:
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

Получение событий с удаленной машины

Условия для получения событий с удаленной машины Windows с агентом KUMA:

- Для запуска агента KUMA на удаленной машине необходимо использовать учетную запись с правами Log on as a service.
- Для получения событий от агента KUMA необходимо 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 машинах Windows необходимо открыть следующие TCP-порты 135, 445, 49152-65535.
- На удаленных машинах требуется запустить следующие службы:
  - Remote Procedure Call (RPC)
  - RPC Endpoint Mapper

Тип wec

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора, **wec**.
  - **URL** (обязательно) – URL создаваемого коллектора, например `kuma-collector.example.com:7221`.

    При создании коллектора для получения данных с помощью Windows Event Collector автоматически создается агент, который будет получать необходимые данные на удаленной машине и перенаправлять их в сервис коллектора. В поле **URL** требуется указать адрес этого коллектора. URL известен заранее, если вы знаете, на каком сервере планируете установить сервис, но это поле можно заполнить и после завершения мастера установки, скопировав данные из раздела **Ресурсы** → **Активные сервисы**.
  - **Описание** – описание ресурса: до 256 символов Юникода.
  - **Журналы Windows** (обязательно) – в этом раскрывающемся списке необходимо выбрать названия журналов Windows, которые требуется получить. По умолчанию в списке отображаются только предварительно настроенные журналы, но вы можете расширить список пользовательскими журналами, введя их название в поле **Журналы Windows**, а затем нажав **ENTER**. Конфигурация сервисов и ресурсов KUMA может потребовать дополнительных изменений для правильной обработки настраиваемых журналов.

Преднастроенные журналы:

- Application
- ForwardedEvents
- Security
- System
- HardwareEvents

Если неверно указать название хотя бы одного журнала, в этом случае агент, использующий коннектор, не будет получать события из всех журналов, даже если их названия указаны верно.

- Закладка **Дополнительные параметры**:
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

Для запуска агента KUMA на удаленной машине необходимо использовать учетную запись с правами Log on as a service.

Для получения событий необходимо 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.

Тип snmp

Для обработки событий, полученных по SNMP, необходимо использовать нормализатор типа json.

Доступен для Windows- и Linux-агентов. Поддерживаемые версии протокола:

- snmpV1
- snmpV2
- snmpV3

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора, **snmp**.
  - **Версия SNMP** (обязательно) – в этом раскрывающемся списке можно выбрать версию используемого протокола.
  - **Хост** (обязательно) – имя хоста или его IP-адрес. Доступные форматы: hostname, IPv4, IPv6.
  - **Порт** (обязательно) – порт для подключения к хосту. Обычно используются значения 161 или 162.

  С помощью параметров **Версия SNMP**, **Хост** и **Порт** определяется одно подключение к SNMP-ресурсу. Таких подключений в одном коннекторе можно создать несколько, добавляя новые с помощью кнопки **SNMP-ресурс**. Удалить подключения можно с помощью кнопки .

  - **Секрет** (обязательно) – раскрывающийся список для выбора ресурса секрета, в котором хранятся учетные данные для подключения через Simple Network Management Protocol. Тип секрета должен соответствовать версии SNMP. При необходимости секрет можно создать в окне создания коннектора с помощью кнопки . Выбранный секрет можно изменить, нажав на кнопку .
  - В таблице **Данные источника** можно задать правила именования получаемых данных, по которым идентификаторы объектов OID будут преобразовываться в ключи, с которыми сможет взаимодействовать нормализатор. Доступные столбцы таблицы:
    - **Название параметра** (обязательно) – произвольное название для типа данных. Например, "Имя узла" или "Время работы узла".

    - **OID** (обязательно) – уникальный идентификатор, который определяет, где искать требуемые данные на источнике событий. Например, "1.3.6.1.2.1.1.5".

    - **Ключ** (обязательно) – уникальный идентификатор, возвращается в ответ на запрос к устройству со значением запрошенного параметра. Например, "sysName". К этому ключу можно обращаться при нормализации данных.

  - **Описание** – описание ресурса: до 256 символов Юникода.

- Закладка **Дополнительные параметры**:

  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.

  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

Тип snmp-trap

Коннектор типа **snmp-trap** используется в агентах и коллекторах для пассивного приема SNMP-Trap сообщений. В коннекторе сообщения принимаются и подготавливаются к нормализации путем сопоставления идентификаторов SNMP-объектов с временными ключами. Затем сообщение необходимо передать в JSON-нормализатор, где временные ключи будут сопоставлены с полями KUMA и будет создано событие.

> Для обработки событий, полученных по SNMP, необходимо использовать нормализатор типа json.

Доступен для Windows- и Linux-агентов. Поддерживаемые версии протокола:

- snmpV1

- snmpV2

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:

  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.

  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

- **Тип** (обязательно) – тип коннектора, **snmp-trap**.

- **Версия SNMP** (обязательно) – в этом раскрывающемся списке необходимо выбрать версию используемого протокола: **snmpV1** или **snmpV2**.

  Например, Windows по умолчанию использует версию **snmpV2**.

- **URL** (обязательно) – URL, на котором будут ожидаться сообщения SNMP Trap. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.

С помощью параметров **Версия SNMP** и **URL** определяется одно соединение для приема событий SNMP Trap. Таких соединений в одном коннекторе можно создать несколько, добавляя новые с помощью кнопки **SNMP-ресурс**. Удалить соединения можно с помощью кнопки .

- В таблице **Данные источника** необходимо задать правила именования получаемых данных, по которым идентификаторы объектов OID будут преобразовываться в ключи, с которыми сможет взаимодействовать нормализатор.

  При создании коннектора таблица предзаполняется примерами значений идентификаторов объектов и их ключей. Если в поступающих событиях необходимо определить и нормализовать больше данных, дополните таблицу строками с перечнем OID-объектов и их ключей.

  Доступные столбцы таблицы:

  - **Название параметра** – произвольное название для типа данных. Например, "`Имя узла`" или "`Время работы узла`".

  - **OID** (обязательно) – уникальный идентификатор, который определяет, где искать требуемые данные на источнике событий. Например, "`1.3.6.1.2.1.1.1`".

  - **Ключ** (обязательно) – уникальный идентификатор, возвращается в ответ на запрос к устройству со значением запрошенного параметра. Например, "`sysDescr`". К этому ключу можно обращаться при нормализации данных.

  Данные обрабатываются по принципу списка разрешенных: объекты, которые не указаны в таблице, не будут переданы в нормализатор для дальнейшей обработки.

- **Описание** – описание ресурса: до 256 символов Юникода.

- Закладка **Дополнительные параметры**:

  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.

- **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

Настройка источника SNMP-trap сообщений для Windows

Настройка машины Windows для отправки SNMP-trap сообщений в коллектор KUMA происходит в несколько этапов:

1. **Настройка и запуск служб SNMP и SNMP Trap**
2. **Настройка службы Event to Trap Translator**

События от источника SNMP-trap сообщений должен принимать коллектор KUMA, в котором используется коннектор типа snmp-trap и нормализатор типа json.

Настройка и запуск служб SNMP и SNMP Trap

Чтобы настроить и запустить службы SNMP и SNMP Trap в Windows 10:

1. Откройте раздел **Settings** → **Apps** → **Apps and features** → **Optional features** → **Add feature** → **Simple Network Management Protocol (SNMP)** и нажмите **Install**.
2. Дождитесь завершения установки и перезагрузите компьютер.
3. Убедитесь, что служба SNMP запущена. Если какие-то из перечисленных ниже служб не запущены, включите их:
   - **Services** → **SNMP Service**.
   - **Services** → **SNMP Trap**.
4. Нажмите правой кнопкой мыши на службе **Services** → **SNMP Service**, в контекстном меню выберите **Properties** и задайте следующие параметры:
   - На закладке **Log On** установите флажок **Local System account**.
   - На закладке **Agent** заполните поля **Contact** (например, укажите `User-win10`) и Location (например, укажите `ekaterinburg`).
   - На закладке **Traps**:
     - В поле **Community Name** введите **community public** и нажмите **Add to list**.
     - В поле **Trap destination** нажмите **Add**, укажите IP-адрес или хост сервера KUMA, на котором развернут коллектор, ожидающий SNMP-события, и нажмите **Add**.

- На закладке **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 закладке **Log On** установите флажок **Local System account**.
   - На закладке **Agent** заполните поля **Contact** (например, укажите `User-win10`) и Location (например, укажите `ekaterinburg`).
   - На закладке **Traps**:
     - В поле **Community Name** введите **community public** и нажмите **Add to list**.
     - В поле **Trap destination** нажмите **Add**, укажите IP-адрес или хост сервера KUMA, на котором развернут коллектор, ожидающий SNMP-события, и нажмите **Add**.

- На закладке **Security**:
  - Установите флажок **Send authentication trap**.
  - В таблице **Accepted community names** нажмите **Add**, а затем введите **Community Name public**, указав в качестве **Community rights** значение **READ WRITE**.
  - Установите флажок **Accept SNMP packets from any hosts**.

6. Нажмите **Apply** и подтвердите выбор.
7. Нажмите правой кнопкой мыши на службу **Services** → **SNMP Service** и выберите **Restart**.

Изменение порта службы snmptrap

При необходимости вы можете изменить порт службы snmptrap.

Чтобы изменить порт службы snmptrap:

1. Откройте папку C:\Windows\System32\drivers\etc.
2. Откройте файл **services** с помощью программы Notepad от имени администратора.
3. В разделе файла **service name** для службы **snmptrap** укажите порт коннектора snmp-trap, добавленный в коллектор KUMA.
4. Сохраните файл.
5. Откройте панель управления и выберите **Administrative Tools** → **Services**.
6. Нажмите на службу **SNMP Service** правой кнопкой мыши и выберите **Restart**.

Настройка службы Event to Trap Translator

Чтобы настроить службу Event to Trap Translator, с помощью которой события Windows переводятся в SNMP-trap сообщения:

1. Наберите в командной строке `evntwin` и нажмите **Enter**.
2. В переключателе **Configuration type** выберите **Custom**, а затем нажмите на кнопку **Edit**.
3. В блоке параметров **Event sources** найдите и добавьте с помощью кнопки **Add** события, которые вы хотите отправить в коллектор KUMA с установленным коннектором SNMP Trap.

4. Нажмите на кнопку **Settings**, в открывшемся окне установите флажок **Don't apply throttle** и нажмите **OK**.

5. Нажмите **Apply** и подтвердите выбор.

Правила агрегации

Ресурсы правил агрегации используются для объединения повторяющихся событий.

Доступные параметры:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Предел событий** – количество событий, которое должно быть получено для того, чтобы сработало правило агрегации и события были объединены. Значение по умолчанию: `100`.
- **Время ожидания событий** (обязательно) – время (в секундах), в течение которого получаются события для объединения. По истечении этого срока правило агрегирования срабатывает и создается новое событие. Значение по умолчанию: `60`.
- **Описание** – описание ресурса: до 256 символов Юникода.
- **Группирующие поля** (обязательно) – в этом раскрывающемся списке можно выбрать поля, по которым будут определяться однотипные события.
- **Уникальные поля** – в этом раскрывающемся списке можно выбрать поля, наличие которых выведет событие из процесса агрегации даже при наличие полей, указанных в разделе **Группирующие поля**.
- **Поля суммы** – в этом раскрывающемся списке можно выбрать поля, значения которых при агрегации будут суммироваться.
- **Фильтр** – блок параметров, в котором можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

> Не используйте в ресурсах правил 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

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. Название должно содержать от 1 до 128 символов Юникода.

4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам 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).

- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Правила обогащения

Ресурсы правил обогащения используются для обновления полей событий.

Доступные параметры ресурсов правил обогащения:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Тип источника данных** (обязательно) – выпадающий список для выбора типа входящих событий. В зависимости от выбранного типа отображаются дополнительные параметры:
  - константа

    Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

    - В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов Юникода. Если оставить это поле пустым, существующее значение поля события будет удалено.
    - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

  - словарь

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

При выборе этого типа в раскрывающемся списке **Название словаря** необходимо выбрать словарь, из которого будут браться значения, а в блоке параметров **Ключевые поля** с помощью кнопки **Добавить поле** требуется выбрать поля события, значения которых будут использоваться для выбора записи словаря.

- **таблица**

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**.

При выборе этого типа обогащения в раскрывающемся списке **Название словаря** необходимо выбрать словарь, из которого будут браться значения, а в блоке параметров **Ключевые поля** с помощью кнопки **Добавить поле** требуется выбрать поля события, значения которых будут использоваться для выбора записи словаря.

Также в таблице **Сопоставление** необходимо настроить, из каких полей словаря и в какие поля события будут передаваться данные:

- В столбце **Поле словаря** необходимо выбрать поле словаря. Доступные поля зависят от выбранного ресурса словаря.
- В столбце **Поле KUMA** необходимо выбрать поле события, в которое следует записать значение. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** можно задать название для помещаемых в них данных.

Новые строки в таблицу можно добавлять с помощью кнопки **Добавить элемент**. Столбцы можно удалить с помощью кнопки ✕.

- **событие**

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.
- В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.

- В блоке параметров **Преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA. Тип преобразования можно выбрать в раскрывающемся списке. С помощью кнопок **Добавить преобразование** и **Удалить** можно добавить или удалить преобразование. Порядок преобразований имеет значение.

  Доступные преобразования

  Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

  Доступные преобразования:

  - **lower** – используется для перевода всех символов значения в нижний регистр
  - **upper** – используется для перевода всех символов значения в верхний регистр
  - **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
  - **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.
  - **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:
    - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.
    - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
  - **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-`

`Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.

- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.

  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **decodeHexString** – используется для конвертации HEX-строки в текст.

- **decodeBase64String** – используется для конвертации Base64-строки в текст.

- **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

- шаблон

Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

- В поле **Шаблон** поместите шаблон Go.

  Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт.

  Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

- dns

  Этот тип обогащения используется для отправки запросов на DNS-сервер частной сети для преобразования IP-адресов в доменные имена или наоборот.

  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`.
  - **Рабочие процессы** – максимальное количество запросов в один момент времени. Значение по умолчанию: `1`.
  - **Количество задач** – максимальное количество одновременно выполняемых запросов. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
  - **Срок жизни кеша** – время жизни значений, хранящихся в кеше. Значение по умолчанию: `60`.
  - **Кеш отключен** – с помощью этого раскрывающегося списка можно включить или отключить кеширование. По умолчанию кеширование включено.

- cybertrace

  Этот тип обогащения используется для добавления в поля события сведений из потоков данных CyberTrace.

  Доступные параметры:

  - **URL** (обязательно) – в этом поле можно указать URL сервера CyberTrace, которому вы хотите отправлять запросы.
  - **Количество подключений** – максимальное количество подключений к серверу CyberTrace, которые может одновременно установить KUMA.

Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

- **Запросов в секунду** – максимальное количество запросов к серверу в секунду. Значение по умолчанию: `1000`.
- **Время ожидания** – время ожидания отклика от сервера CyberTrace в секундах. Значение по умолчанию: `30`.
- **Сопоставление** (обязательно) – этот блок параметров содержит таблицу сопоставления полей событий KUMA с типами индикаторов CyberTrace. В столбце **Поле KUMA** указаны названия полей событий KUMA, а в столбце **Индикатор CyberTrace** указаны типы индикаторов CyberTrace.

  Доступные типы индикаторов CyberTrace:

  - ip
  - url
  - hash

  В таблице сопоставления требуется указать как минимум одну строку. С помощью кнопки **Добавить строку** можно добавить строку, а с помощью кнопки ✕ – удалить.

- **часовой пояс**

  Этот тип обогащения используется в коллекторах и корреляторах для присваивания событию определенного часового пояса. Сведения о часовом поясе могут пригодиться при поиске событий, случившихся в нетипичное время, например ночью.

  При выборе этого типа обогащения в раскрывающемся списке **Часовой пояс** необходимо выбрать требуемую временную зону.

  > Убедитесь, что требуемый часовой пояс установлен на сервере сервиса, использующего обогащение. Например, это можно сделать с помощью команды `timedatectl list-timezones`, которая показывает все установленные на сервере часовые пояса. Подробнее об установке часовых поясов смотрите в документации используемой вами операционной системы.

При обогащении события в поле события DeviceTimeZone записывается смещение времени выбранного часового пояса относительно всемирного координированного времени (UTC) в формате `+-чч:мм`. Например, если выбрать временную зону **Asia/Yekaterinburg** в поле DeviceTimeZone будет записано значение `+05:00`. Если в обогащаемом событии есть значение поля DeviceTimeZone, оно будет перезаписано.

По умолчанию, если в обрабатываемом событии не указан часовой пояс и не настроены правила обогащения по часовому поясу, событию присваивается часовой пояс сервера, на котором установлен сервис (коллектор или коррелятор), обрабатывающий событие. При изменении времени сервера сервис необходимо перезапустить.

Допустимые форматы времени при обогащении поля DeviceTimeZone

При обработке в коллекторе поступающих "сырых" событий следующие форматы времени могут быть автоматически приведены к формату +-чч:мм:

Формат времени в обрабатываемом событии	Пример
+-чч:мм	-07:00
+-ччмм	-0700
+-чч	-07

Если формат даты в поле `DeviceTimeZone` отличается от указанных выше, при обогащении события сведениями о часовом поясе в поле записывается часовой пояс серверного времени коллектора. Вы можете создать особые правила нормализации для нестандартных форматов времени.

- **геоданные**

Этот тип обогащения используется для добавления в поля событий сведений о географическом расположении IP-адресов. Подробнее о привязке IP-адресов к географическим данным.

При выборе этого типа в блоке параметров **Сопоставление геоданных с полями события** необходимо указать, из какого поля события будет считан IP-адрес, а также выбрать требуемые атрибуты геоданных и определить поля событий, в которые геоданные будут записаны:

1. В раскрывающемся списке **Поле события с IP-адресом** выберите поле события, из которого считывается IP-адрес. По этому IP-адресу будет произведен поиск соответствий по загруженным в KUMA геоданным.

   С помощью кнопки **Добавить поле события с IP-адресом** можно указать несколько полей события с IP-адресами, по которым требуется обогащение геоданными. Удалить добавленные таким образом поля событий можно с помощью кнопки **Удалить поле события с IP-адресом**.

   > При выборе полей события `SourceAddress`, `DestinationAddress` и `DeviceAddress` становится доступна кнопка **Применить сопоставление по умолчанию**. С ее помощью можно добавить преднастроенные пары соответствий атрибутов геоданных и полей события.

2. Для каждого поля события, откуда требуется считать IP-адрес, выберите тип геоданных и поле события, в которое следует записать геоданные.

   С помощью кнопки **Добавить атрибут геоданных** вы можете добавить пары полей **Атрибут геоданных** – **Поле события для записи**. Так вы можете настроить запись разных типов геоданных одного IP-адреса в разные поля события. Пары полей можно удалить с помощью значка ✕.

   - В поле **Атрибут геоданных** выберите, какие географические сведения, соответствующие считанному IP-адресу, необходимо записать в событие. Доступные атрибуты геоданных: **Страна**, **Регион**, **Город**, **Долгота**, **Широта**.

   - В поле **Поле события для записи** выберите поле события, в которое необходимо записать выбранный атрибут геоданных.

   Вы можете записать одинаковые атрибуты геоданных в разные поля событий. Если вы настроите запись нескольких атрибутов геоданных в одно поле события, событие будет обогащено последним по очереди сопоставлением.

- **Отладка** – с помощью этого раскрывающегося списка можно включить логирование операций сервиса. По умолчанию логирование выключено.

- **Описание** – описание ресурса: до 256 символов Юникода.

- **Фильтр** – блок параметров, в котором можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно

выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

Создание фильтра в ресурсах

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. Название должно содержать от 1 до 128 символов Юникода.
4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам 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).

- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Точки назначения

Ресурсы точек назначения используются для получения событий и их последующей отправки в другие сервисы. Параметры точек назначения указываются на двух закладках: **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа точки назначения:

- **nats** – 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.
- **storage** – используется для передачи данных в хранилище.
- **correlator** – используется для передачи данных в коррелятор.

Тип nats

Тип **nats** используется для коммуникации через NATS.

Доступные параметры:

Закладка **Основные параметры**:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- Переключатель **Выключено** – используется в том случае, если события не нужно отправляться в точку назначения. По умолчанию отправка событий включена.
- **Тип** (обязательно) – тип точки назначения, **nats**.
- **URL** (обязательно) – URL, с которым необходимо установить связь.
- **Топик** (обязательно) – тема сообщений NATS. Должно содержать символы Юникода.
- **Разделитель** – используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.
- **Авторизация** – тип авторизации при подключении к указанному URL:
  - **выключена** (по умолчанию).
  - **обычная**.

    При выборе этого варианта требуется указать секрет, содержащий данные учетной записи пользователя для авторизации при подключении к коннектору.

    Добавить секрет

    1. Если вы создали секрет ранее, выберите его в раскрывающемся списке **Секрет**.

       Если ранее не было добавлено ни одного секрета, в раскрывающемся списке отобразится **Нет данных**.

    2. Если вы хотите добавить новый секрет, справа от списка **Секрет** нажмите на кнопку +.

       Откроется окно **Секрет**.

3. В поле **Название** введите название, под которым секрет будет отображаться в списке доступных.

4. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору.

5. Если требуется, в поле **Описание** добавьте любую дополнительную информацию о секрете.

6. Нажмите на кнопку **Сохранить**.

Секрет будет добавлен и отобразится в списке **Секрет**.

- **Описание** – описание ресурса: до 256 символов Юникода.

Закладка **Дополнительные параметры**:

- **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
- **Размер буфера** – используется для установки размера буфера. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.
- **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. Значение по умолчанию: `30`.
- **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.
- **Идентификатор кластера** – идентификатор кластера NATS.
- **Режим TLS** – использование шифрования TLS:
  - **Выключено** (по умолчанию) – не использовать шифрование TLS.
  - **Включено** – использовать шифрование, но без верификации сертификата.
  - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.
  - **Нестандартный CA** – использовать шифрование с верификацией сертификата, подписанного центром сертификации. Секрет с сертификатом выбирается в

раскрывающемся списке **Нестандартный CA**, который отображается при выборе этого пункта.

Создание сертификата, подписанного центром сертификации

Для использования этого режима TLS необходимо выполнить следующие действия на сервере Ядра KUMA (в примерах команд ниже используется OpenSSL):

1. Создать ключ, который будет использоваться центром сертификации.

   Пример команды: `openssl genrsa -out ca.key 2048`

2. Создать сертификат для только что созданного ключа.

   Пример команды: `openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<общее имя хоста центра сертификации>" -out ca.crt`

3. Создать приватный ключ и запрос на его подписание в центре сертификации.

   Пример команды: `openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<общее имя хоста сервера KUMA>" -out server.csr`

4. Создать сертификат, подписанный центром сертификации. Необходимо включить в subjectAltName доменные имена или IP-адреса сервера, для которого создается сертификат.

   Пример команды: `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. Полученный сертификат `server.crt` следует загрузить в веб-интерфейсе KUMA в секрет типа **certificate**, который затем следует выбрать в раскрывающемся списке **Нестандартный CA**.

При использовании TLS невозможно указать IP-адрес в качестве URL.

- **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.

- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.

- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на

котором установлено Ядро KUMA.

- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.

- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах

  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. Название должно содержать от 1 до 128 символов Юникода.

  4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

     c. В раскрывающемся списке **оператор** выберите нужный вам 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).
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку ↗.

Тип tcp

Тип **tcp** используется для связи по протоколу TCP.

Доступные параметры:

Закладка **Основные параметры**:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.

- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

- Переключатель **Выключено** – используется в том случае, если события не нужно отправляться в точку назначения. По умолчанию отправка событий включена.

- **Тип** (обязательно) – тип точки назначения, **tcp**.

- **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: `хост:порт`, `IPv4:порт`, `:порт`. Также поддерживаются адреса IPv6, однако при их использовании необходимо также указывать интерфейс: `[адрес%интерфейс]:порт` (пример: `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`).

- **Описание** – описание ресурса: до 256 символов Юникода.

Закладка **Дополнительные параметры**:

- **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.

- **Размер буфера** – используется для установки размера буфера. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.

- **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. Значение по умолчанию: `30`.

- **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.

- **Режим TLS** – использование шифрования TLS:

  - **Выключено** (по умолчанию) – не использовать шифрование TLS.

  - **Включено** – использовать шифрование, но без верификации сертификата.

  - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

  При использовании TLS невозможно указать IP-адрес в качестве URL.

- **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.

- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.

- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.

- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах

  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. Название должно содержать от 1 до 128 символов Юникода.

  4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

     c. В раскрывающемся списке **оператор** выберите нужный вам 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).
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку ↗.

Тип http

Тип **http** используется для связи по протоколу HTTP.

Доступные параметры:

Закладка **Основные параметры**:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- Переключатель **Выключено** – используется в том случае, если события не нужно отправляться в точку назначения. По умолчанию отправка событий включена.
- **Тип** (обязательно) – тип точки назначения, **http**.
- **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: `хост:порт`, `IPv4:порт`, `:порт`. Также поддерживаются адреса IPv6, однако при их использовании необходимо также указывать интерфейс: `[адрес%интерфейс]:порт` (пример: `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`).
- **Авторизация** – тип авторизации при подключении к указанному URL:

- **выключена** (по умолчанию).

- **обычная**.

  При выборе этого варианта требуется указать секрет, содержащий данные учетной записи пользователя для авторизации при подключении к коннектору.

  Добавить секрет

  1. Если вы создали секрет ранее, выберите его в раскрывающемся списке **Секрет**.

     Если ранее не было добавлено ни одного секрета, в раскрывающемся списке отобразится **Нет данных**.

  2. Если вы хотите добавить новый секрет, справа от списка **Секрет** нажмите на кнопку +.

     Откроется окно **Секрет**.

  3. В поле **Название** введите название, под которым секрет будет отображаться в списке доступных.

  4. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору.

  5. Если требуется, в поле **Описание** добавьте любую дополнительную информацию о секрете.

  6. Нажмите на кнопку **Сохранить**.

  Секрет будет добавлен и отобразится в списке **Секрет**.

- **Описание** – описание ресурса: до 256 символов Юникода.

Закладка **Дополнительные параметры**:

- **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.

- **Прокси-сервер** – раскрывающийся список для выбора ресурса прокси-сервера.

- **Размер буфера** – используется для установки размера буфера. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.

- **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. Значение по умолчанию: `30`.

- **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.

- **Режим TLS** – использование шифрования TLS:

  - **Выключено** (по умолчанию) – не использовать шифрование TLS.

  - **Включено** – использовать шифрование, но без верификации сертификата.

  - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

  - **Нестандартный CA** – использовать шифрование с верификацией сертификата, подписанного центром сертификации. Секрет с сертификатом выбирается в раскрывающемся списке **Нестандартный CA**, который отображается при выборе этого пункта.

    Создание сертификата, подписанного центром сертификации

    Для использования этого режима TLS необходимо выполнить следующие действия на сервере Ядра KUMA (в примерах команд ниже используется OpenSSL):

    1. Создать ключ, который будет использоваться центром сертификации.

       Пример команды: `openssl genrsa -out ca.key 2048`

    2. Создать сертификат для только что созданного ключа.

       Пример команды: `openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<общее имя хоста центра сертификации>" -out ca.crt`

    3. Создать приватный ключ и запрос на его подписание в центре сертификации.

       Пример команды: `openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<общее имя хоста сервера KUMA>" -out server.csr`

    4. Создать сертификат, подписанный центром сертификации. Необходимо включить в subjectAltName доменные имена или IP-адреса сервера, для которого создается сертификат.

Пример команды: `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. Полученный сертификат `server.crt` следует загрузить в веб-интерфейсе KUMA в секрет типа **certificate**, который затем следует выбрать в раскрывающемся списке **Нестандартный CA**.

При использовании TLS невозможно указать IP-адрес в качестве URL.

- **Политика выбора URL** – раскрывающийся список, в котором можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько:

  - **Любой** – события отправляются в один из доступных URL до тех пор, пока этот URL принимает события. При разрыве связи (например, при отключении принимающего узла) для отправки событий будет выбран другой URL.

  - **Сначала первый** – события отправляются в первый URL из списка добавленных адресов. Если он становится недоступен, события отправляются в следующий по очереди доступный узел. Когда первый URL снова становится доступен, события снова начинаются отправляться в него.

  - **По очереди** – пакеты с событиями по очереди отправляться в доступные URL из списка. Поскольку пакеты отправляются или при переполнении буфера точки назначения, или при срабатывании таймера очистки буфера, эта политика выбора URL не гарантирует равное распределение событий по точкам назначения.

- **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.

- **Путь** – путь, который необходимо добавить для URL-запроса. Например, если указать путь `/input`, а в качестве URL ввести `10.10.10.10`, то от точки назначения будут исходить запросы `10.10.10.10/input`.

- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.

- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

- Вы можете установить проверки работоспособности, используя поля **Путь проверки работоспособности** и **Ожидание проверки работоспособности**. Вы также можете

отключить проверку работоспособности, установив флажок **Проверка работоспособности отключена**.

- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.

- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах

  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. Название должно содержать от 1 до 128 символов Юникода.

  4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

     c. В раскрывающемся списке **оператор** выберите нужный вам 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).
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку ↗.

Тип diode

Тип **diode** используется для передачи событий с помощью диода данных.

Доступные параметры:

Закладка **Основные параметры**:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- Переключатель **Выключено** – используется в том случае, если события не нужно отправляться в точку назначения. По умолчанию отправка событий включена.
- **Тип** (обязательно) – тип точки назначения, **diode**.

- **Директория, из которой диод данных получает события** (обязательно) – директория, откуда диод данных перемещает события. Путь может содержать до 255 символов Юникода.

  Ограничения при использовании префиксов к путям на серверах Windows

  На серверах Windows необходимо указывать абсолютные пути к директориям. Невозможно использовать директории, названия которых соответствуют указанным ниже регулярным выражениям:

  - `^[a-zA-Z]:\\Program Files`
  - `^[a-zA-Z]:\\Program Files \(x86\)`
  - `^[a-zA-Z]:\\Windows`
  - `^[a-zA-Z]:\\Program Files\\Kaspersky Lab\\KUMA`

  Ограничения при использовании префиксов к путям на серверах Linux

  Префиксы, которые невозможно использовать при указании путей к файлам:

  - /*
  - /bin
  - /boot
  - /dev
  - /etc
  - /home
  - /lib
  - /lib64
  - /proc
  - /root
  - /run
  - /sys

- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

Файлы по указанным ниже путям доступны:

- /opt/kaspersky/kuma/clickhouse/logs/
- /opt/kaspersky/kuma/mongodb/log/
- /opt/kaspersky/kuma/victoria-metrics/log/

- **Временная директория** – директория, в которой события готовятся для передачи диоду данных.

  События собираются в файл по истечении времени ожидания (по умолчанию 10 секунд) или при переполнении буфера. Подготовленный файл перемещается в директорию, указанную в поле **Директория, из которой диод данных получает события**. В качестве названия файла с событиями используется хеш-сумма (SHA-256) содержимого файла.

  Временная директория не должна совпадать с директорией, из которой диод данных получает события.

- **Описание** – описание ресурса: до 256 символов Юникода.

Закладка **Дополнительные параметры**:

- **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.

  Этот параметр должен совпадать ресурсах коннектор и точка назначения, используемых для передачи событий из изолированного сегмента сети с помощью диода данных.

- **Размер буфера** – используется для установки размера буфера. По умолчанию размер равен 64 МБ. Не может быть больше 64 МБ.

- **Время ожидания** – поле, в котором можно указать интервал (в секундах) между перемещением данных из временной директории в директорию для диода данных. Значение по умолчанию: `10`.

- **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.

  Этот параметр должен совпадать ресурсах коннектор и точка назначения, используемых для передачи событий из изолированного сегмента сети с помощью диода данных.

- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.

- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.

- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах

  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. Название должно содержать от 1 до 128 символов Юникода.

4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам 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).

- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку ↗.

Тип kafka

Тип **kafka** используется для коммуникаций с помощью kafka.

Доступные параметры:

Закладка **Основные параметры**:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- Переключатель **Выключено** – используется в том случае, если события не нужно отправляться в точку назначения. По умолчанию отправка событий включена.
- **Тип** (обязательно) – тип точки назначения, **kafka**.
- **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: `хост:порт`, `IPv4:порт`, `:порт`. Также поддерживаются адреса IPv6, однако при их использовании необходимо также указывать интерфейс: `[адрес%интерфейс]:порт` (пример: `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`).

  С помощью кнопки **URL** можно добавить несколько адресов.
- **Топик** (обязательно) – тема сообщений Kafka. Должен содержать от 1 до 255 следующих символов: a–z, A–Z, 0–9, ".", "_", "-".
- **Разделитель** – используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.
- **Авторизация** – тип авторизации при подключении к указанному URL:
  - **выключена** (по умолчанию).
  - **PFX**.

    При выборе этого варианта требуется сформировать сертификат с закрытым ключом в формате PKCS#12-контейнера во внешнем центре сертификации, экспортировать сертификат из хранилища и загрузить его в веб-интерфейс KUMA в виде PFX-секрета.

Добавить PFX-секрет

1. Если вы загрузили PFX-сертификат ранее, выберите его в раскрывающемся списке **Секрет**.

   Если ранее не было добавлено ни одного сертификата, в раскрывающемся списке отобразится **Нет данных**.

2. Если вы хотите добавить новый сертификат, справа от списка **Секрет** нажмите на кнопку +.

   Откроется окно **Секрет**.

3. В поле **Название** введите название, под которым секрет будет отображаться в списке доступных.

4. По кнопке **Загрузить PFX** выберите файл, в который вы экспортировали сертификат с закрытым ключом, в формате PKCS#12-контейнера.

5. В поле **Пароль** введите пароль для защиты сертификата, заданный в мастере экспорта сертификата.

6. Нажмите на кнопку **Сохранить**.

Сертификат будет добавлен и отобразится в списке **Секрет**.

- **обычная**.

При выборе этого варианта требуется указать секрет, содержащий данные учетной записи пользователя для авторизации при подключении к коннектору.

Добавить секрет

1. Если вы создали секрет ранее, выберите его в раскрывающемся списке **Секрет**.

   Если ранее не было добавлено ни одного секрета, в раскрывающемся списке отобразится **Нет данных**.

2. Если вы хотите добавить новый секрет, справа от списка **Секрет** нажмите на кнопку +.

   Откроется окно **Секрет**.

3. В поле **Название** введите название, под которым секрет будет отображаться в списке доступных.

4. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору.

5. Если требуется, в поле **Описание** добавьте любую дополнительную информацию о секрете.

6. Нажмите на кнопку **Сохранить**.

Секрет будет добавлен и отобразится в списке **Секрет**.

- **Описание** – описание ресурса: до 256 символов Юникода.

Закладка **Дополнительные параметры**:

- **Размер буфера** – используется для установки размера буфера. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.

- **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. Значение по умолчанию: `30`.

- **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.

- **Режим TLS** – использование шифрования TLS:

  - **Выключено** (по умолчанию) – не использовать шифрование TLS.

  - **Включено** – использовать шифрование, но без верификации сертификата.

  - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

  - **Нестандартный CA** – использовать шифрование с верификацией сертификата, подписанного центром сертификации. Секрет с сертификатом выбирается в раскрывающемся списке **Нестандартный CA**, который отображается при выборе этого пункта.

    Создание сертификата, подписанного центром сертификации

    Для использования этого режима TLS необходимо выполнить следующие действия на сервере Ядра KUMA (в примерах команд ниже используется OpenSSL):

1. Создать ключ, который будет использоваться центром сертификации.

   Пример команды: `openssl genrsa -out ca.key 2048`

2. Создать сертификат для только что созданного ключа.

   Пример команды: `openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<общее имя хоста центра сертификации>" -out ca.crt`

3. Создать приватный ключ и запрос на его подписание в центре сертификации.

   Пример команды: `openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<общее имя хоста сервера KUMA>" -out server.csr`

4. Создать сертификат, подписанный центром сертификации. Необходимо включить в subjectAltName доменные имена или IP-адреса сервера, для которого создается сертификат.

   Пример команды: `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. Полученный сертификат `server.crt` следует загрузить в веб-интерфейсе KUMA в секрет типа **certificate**, который затем следует выбрать в раскрывающемся списке **Нестандартный CA**.

При использовании TLS невозможно указать IP-адрес в качестве URL.

- **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.

- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.

- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.

- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах

  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. Название должно содержать от 1 до 128 символов Юникода.
  4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

     c. В раскрывающемся списке **оператор** выберите нужный вам 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).

- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Тип file

Тип **file** используется для записи в файл.

Доступные параметры:

Закладка **Основные параметры**:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- Переключатель **Выключено** – используется в том случае, если события не нужно отправляться в точку назначения. По умолчанию отправка событий включена.
- **Тип** (обязательно) – тип точки назначения, **file**.
- **URL** (обязательно) – путь к файлу, в который необходимо записать события.

  Ограничения при использовании префиксов к путям файлов

  Префиксы, которые невозможно использовать при указании путей к файлам:

- /*
- /bin
- /boot
- /dev
- /etc
- /home
- /lib
- /lib64
- /proc
- /root
- /run
- /sys
- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/

- /var/run/
- /opt/kaspersky/kuma/

Файлы по указанным ниже путям доступны:

- /opt/kaspersky/kuma/clickhouse/logs/
- /opt/kaspersky/kuma/mongodb/log/
- /opt/kaspersky/kuma/victoria-metrics/log/

- **Описание** – описание ресурса: до 256 символов Юникода.

Закладка **Дополнительные параметры**:

- **Размер буфера** – используется для установки размера буфера. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.
- **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. Значение по умолчанию: `30`.
- **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.
- **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.
- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.
- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.
- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.
- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

Создание фильтра в ресурсах

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. Название должно содержать от 1 до 128 символов Юникода.

4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам 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).

- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Тип storage

Тип **storage** используется для передачи данных в хранилище.

Доступные параметры:

Закладка **Основные параметры**:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- Переключатель **Выключено** – используется в том случае, если события не нужно отправляться в точку назначения. По умолчанию отправка событий включена.
- **Тип** (обязательно) – тип точки назначения, **storage**.
- **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: `хост:порт`, `IPv4:порт`, `:порт`. Также поддерживаются адреса IPv6, однако при их использовании необходимо также указывать интерфейс: `[адрес%интерфейс]:порт` (пример: `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`).

  С помощью кнопки **URL** можно добавить несколько адресов.

  В поле **URL** поддерживается поиск сервисов по FQDN, IP-адресу и названию. Особенности поиска по указанным в поле значениям:

  - `<Поисковое значение>` – поиск ведется по FQDN, IP-адресам и названиям сервисов.

- `<Первое поисковое значение, оканчивающееся на одну или несколько цифр>:<второе поисковое значение>` – поиск по первому значению ведется по FQDN, IP-адресам сервисов, а второе значение используется для поиска по порту.

- `:<значение>` – поиск ведется по порту.

- **Описание** – описание ресурса: до 256 символов Юникода.

Закладка **Дополнительные параметры**:

- **Прокси-сервер** – раскрывающийся список для выбора ресурса прокси-сервера.

- **Размер буфера** – используется для установки размера буфера. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.

- **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. Значение по умолчанию: `30`.

- **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.

- **Политика выбора URL** – раскрывающийся список, в котором можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько:

  - **Любой** – события отправляются в один из доступных URL до тех пор, пока этот URL принимает события. При разрыве связи (например, при отключении принимающего узла) для отправки событий будет выбран другой URL.

  - **Сначала первый** – события отправляются в первый URL из списка добавленных адресов. Если он становится недоступен, события отправляются в следующий по очереди доступный узел. Когда первый URL снова становится доступен, события снова начинаются отправляться в него.

  - **По очереди** – пакеты с событиями по очереди отправляться в доступные URL из списка. Поскольку пакеты отправляются или при переполнении буфера точки назначения, или при срабатывании таймера очистки буфера, эта политика выбора URL не гарантирует равное распределение событий по точкам назначения.

- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.

- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

- **Ожидание проверки работоспособности** – частота проверки работоспособности в секундах.

- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.

- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах

  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. Название должно содержать от 1 до 128 символов Юникода.

  4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

     c. В раскрывающемся списке **оператор** выберите нужный вам 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).
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку ↗.

Тип correlator

Тип **correlator** используется для передачи данных в коррелятор.

Доступные параметры:

Закладка **Основные параметры**:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.

- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

- Переключатель **Выключено** – используется в том случае, если события не нужно отправляться в точку назначения. По умолчанию отправка событий включена.

- **Тип** (обязательно) – тип точки назначения, **correlator**.

- **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: `хост:порт`, `IPv4:порт`, `:порт`. Также поддерживаются адреса IPv6, однако при их использовании необходимо также указывать интерфейс: `[адрес%интерфейс]:порт` (пример: `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`).

  С помощью кнопки **URL** можно добавить несколько адресов.

  В поле **URL** поддерживается поиск сервисов по FQDN, IP-адресу и названию. Особенности поиска по указанным в поле значениям:

  - `<Поисковое значение>` – поиск ведется по FQDN, IP-адресам и названиям сервисов.

  - `<Первое поисковое значение, оканчивающееся на одну или несколько цифр>:<второе поисковое значение>` – поиск по первому значению ведется по FQDN, IP-адресам сервисов, а второе значение используется для поиска по порту.

  - `:<значение>` – поиск ведется по порту.

- **Описание** – описание ресурса: до 256 символов Юникода.

Закладка **Дополнительные параметры**:

- **Прокси-сервер** – раскрывающийся список для выбора ресурса прокси-сервера.

- **Размер буфера** – используется для установки размера буфера. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.

- **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. Значение по умолчанию: `30`.

- **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.

- **Политика выбора URL** – раскрывающийся список, в котором можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько:

  - **Любой** – события отправляются в один из доступных URL до тех пор, пока этот URL принимает события. При разрыве связи (например, при отключении принимающего узла) для отправки событий будет выбран другой URL.

  - **Сначала первый** – события отправляются в первый URL из списка добавленных адресов. Если он становится недоступен, события отправляются в следующий по очереди доступный узел. Когда первый URL снова становится доступен, события снова начинаются отправляться в него.

- **По очереди** – пакеты с событиями по очереди отправляться в доступные URL из списка. Поскольку пакеты отправляются или при переполнении буфера точки назначения, или при срабатывании таймера очистки буфера, эта политика выбора URL не гарантирует равное распределение событий по точкам назначения.

- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.

- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

- **Ожидание проверки работоспособности** – частота проверки работоспособности в секундах.

- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.

- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах

  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. Название должно содержать от 1 до 128 символов Юникода.

  4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

c. В раскрывающемся списке **оператор** выберите нужный вам 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).
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Фильтры

Ресурсы фильтров используются для выбора событий на основе определенных пользователем условий.

Это неверно только тогда, когда фильтры используются в сервисе коллектор, где они выбирают все события, которые НЕ удовлетворяют условиям фильтра.

Фильтры можно использовать в сервисах коллектора, ресурсах правил обогащения, ресурсах правил агрегации, ресурсах правил реагирования, ресурсах правил корреляции и ресурсах точек назначения: либо как отдельные ресурсы фильтра, либо как встроенные фильтры, которые хранятся в сервисе или ресурсе, где они были созданы.

Для этих ресурсов в полях ввода, кроме поля **Описание**, можно включить отображение непечатаемых символов.

Доступные параметры ресурсов фильтра:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода. Встроенные фильтры создаются в других ресурсах или сервисах и не имеют имен.

- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

- Блок параметров **Условия** – здесь вы можете сформулировать критерии фильтрации, создав условия фильтрации и группы фильтров, а также добавив существующие ресурсы фильтров.

  С помощью кнопки **Добавить группу** можно добавить группу фильтров. Можно переключать групповые операторы между **И**, **ИЛИ**, **НЕ**. В группы фильтров можно добавить группы, условия и существующие ресурсы фильтров.

  С помощью кнопки **Добавить фильтр** можно добавить существующий ресурс фильтра, который следует выбрать в раскрывающемся списке **Выберите фильтр**.

  С помощью кнопки **Добавить условие** можно добавить строку с полями для определения условия (см. ниже).

  Условия, группы и фильтры можно удалить с помощью кнопки ✕.

Параметры условий:

- **Если** (обязательно) – в этом раскрывающемся списке можно указать, требуется ли использовать инвертированную функцию оператора

- **Левый операнд** и **Правый операнд** (обязательно) – используются для указания значений, которые будет обрабатывать оператор. Доступные типы зависят от выбранного оператора.

  Операнды фильтров

- **Поле события** – используется для присвоения операнду значения поля события. Дополнительные параметры:
  - **поле события** (обязательно) – этот раскрывающийся список используется для выбора поля, из которого следует извлечь значение операнда.
- **Активный лист** – используется для присвоения операнду значения записи активного листа. Дополнительные параметры:
  - **название активного листа** (обязательно) – этот раскрывающийся список используется для выбора активного листа.
  - **ключевые поля** (обязательно) – это список полей событий, используемых для создания записи активного листа и служащих ключом записи активного листа.
  - **поле** (требуется, если не выбран оператор **inActiveList**) – используется для ввода имени поля активного листа, из которого следует извлечь значение операнда.
- **Словарь** – используется для присвоения значения операнду значения из ресурса словарь. Дополнительные параметры:
  - **словарь** (обязательно) – этот раскрывающийся список используется для выбора словаря.
  - **ключевые поля** (обязательно) – это список полей событий, используемых для формирования ключа значения словаря.
- **Константа** – используется для присвоения операнду пользовательского значения. Дополнительные параметры:
  - **значение** (обязательно) – здесь вы вводите константу, которую хотите присвоить операнду.
- **Таблица** – используется для присвоения операнду нескольких пользовательских значений. Дополнительные параметры:
  - **словарь** (обязательно) – этот раскрывающийся список используется для выбора словаря типа **Таблица**.
  - **ключевые поля** (обязательно) – это список полей событий, используемых для формирования ключа значения словаря.

- **Список** – используется для присвоения операнду нескольких пользовательских значений. Дополнительные параметры:
  - **значение** (обязательно) – здесь вы вводите список констант, которые хотите назначить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.
- **TI** – используется для чтения данных CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
  - **канал** (обязательно) – в этом поле указывается категория угрозы CyberTrace.
  - **ключевые поля** (обязательно) – этот раскрывающийся список используется для выбора поля события с индикаторами угроз CyberTrace.
  - **поле** (обязательно) – в этом поле указывается поле фида CyberTrace с индикаторами угроз.

- **Оператор** (обязательно) – используется для выбора оператора условия.

  В этом же раскрывающемся списке можно установить флажок **без учета регистра**, если требуется, чтобы оператор игнорировал регистр значений. Флажок игнорируется, если выбраны операторы **inSubnet**, **inActiveList**, **inCategory**, **InActiveDirectoryGroup, hasBit**, **inDictionary**. По умолчанию флажок снят.

  Операторы фильтров

  - **=** – левый операнд равен правому операнду.
  - **<** – левый операнд меньше правого операнда.
  - **<=** – левый операнд меньше или равен правому операнду.
  - **>** – левый операнд больше правого операнда.
  - **>=** – левый операнд больше или равен правому операнду.
  - **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
  - **contains** – левый операнд содержит значения правого операнда.
  - **startsWith** – левый операнд начинается с одного из значений правого операнда.

- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

Доступные типы операндов зависят от того, является ли операнд левым (L) или правым (R).

Доступные типы операндов для левого (L) и правого (R) операндов

Оператор	Тип "поле события"	Тип "активный лист"	Тип "словарь"	Тип "таблица"	Тип "TI"	Т "конс
=	L,R	L,R	L,R	L,R	L,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	L,R	L,R	L,R	L	R
inSubnet	L,R	L,R	L,R	L,R	L,R	R

contains	L,R	L,R	L,R	L,R	L,R	R
startsWith	L,R	L,R	L,R	L,R	L,R	R
endsWith	L,R	L,R	L,R	L,R	L,R	R
match	L	L	L	L	L	R
hasVulnerability	L	L	L	L		
hasBit	L	L	L	L		R
inActiveList						
inDictionary						
inCategory	L	L	L	L		R
inActiveDirectoryGroup	L	L	L	L		R
TIDetect						

Правила реагирования

Вы можете настроить автоматическое выполнение задач Kaspersky Security Center, действий по реагированию Kaspersky Endpoint Detection and Response и запуска пользовательского скрипта при получении событий, для которых настроены правила реагирования.

> Автоматическое выполнение задач Kaspersky Security Center, Kaspersky Endpoint Detection and Response и KICS for Networks по правилам реагирования доступно при интеграции с перечисленными программами.

Правила реагирования для Kaspersky Security Center

Вы можете настроить правила реагирования для автоматического запуска задач антивирусной проверки и обновления на активах Kaspersky Security Center.

При создании и изменении правил реагирования для Kaspersky Security Center вам требуется задать значения для следующих параметров:

- **Название** (обязательно) – уникальное имя ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

- **Тип** (обязательно) – **ksctasks**.

  Доступно при интеграции KUMA с Kaspersky Security Center.

- **Задача Kaspersky Security Center** (обязательно) – название задачи Kaspersky Security Center, которую требуется запустить. Задачи должны быть созданы заранее, и их названия должны начинаться со слова "`KUMA `". Например, `KUMA antivirus check` (без учета регистра и без кавычек).

  Типы задач Kaspersky Security Center, которые можно запустить с помощью KUMA:

  - обновление;
  - поиск вирусов.

- **Поле события** (обязательно) – определяет поле события для актива, для которого нужно запустить задачу Kaspersky Security Center. Возможные значения:

  - SourceAssetID.
  - DestinationAssetID.
  - DeviceAssetID.

- **Рабочие процессы** – количество процессов, которые сервис может запускать одновременно.

  По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.

- **Описание** – вы можете добавить до 4000 символов Юникода, описывающих ресурс.

- **Фильтр** – используется для определения условий, при соответствии которым события будут обрабатываться ресурсом правила реагирования. В раскрывающемся списке можно выбрать существующий ресурс фильтра или создать новый фильтр.

Для отправки запросов в Kaspersky Security Center необходимо убедиться, что Kaspersky Security Center доступен по протоколу UDP.

Если ресурс правила реагирования принадлежит общему тенанту, то в качестве доступных для выбора задач Kaspersky Security Center отображаются задачи от сервера Kaspersky Security Center, к которому подключен главный тенант.

Если в ресурсе правила реагирования выбрана задача, которая отсутствует на сервере Kaspersky Security Center, к которому подключен тенант, для активов этого тенанта задача не будет выполнена. Такая ситуация может возникнуть, например, когда два тенанта используют общий коррелятор.

Правила реагирования для пользовательского скрипта

Вы можете создать скрипт с командами, которые требуется выполнить на сервере KUMA при обнаружении выбранных событий, и настроить правила реагирования для автоматического запуска этого скрипта. В этом случае программа запустит скрипт при получении событий, соответствующих правилам реагирования.

Файл скрипта хранится на сервере, где установлен сервис коррелятора, использующий ресурс реагирования: /opt/kaspersky/kuma/correlator/<Идентификатор коррелятора>/scripts. Пользователю `kuma` этого сервера требуются права на запуск скрипта.

При создании и изменении правил реагирования для произвольного скрипта вам требуется задать значения для следующих параметров:

- **Название** (обязательно) – уникальное имя ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Тип** (обязательно) – **script**.
- **Время ожидания** – количество секунд, в течение которого должно завершиться выполнение скрипта. Если это время превышено, выполнение скрипта прерывается.
- **Название скрипта** (обязательно) – имя файла скрипта.

  Если ресурс реагирования прикреплен к сервису коррелятора, но в папке /opt/kaspersky/kuma/correlator/<Идентификатор коррелятора>/scripts файл скрипта отсутствует, коррелятор не будет работать.

- **Аргументы скрипта** – параметры или значения полей событий, которые необходимо передать скрипту.

  Если в скрипте производятся какие-либо действия с файлами, к ним следует указывать абсолютный путь.

Параметры можно обрамлять кавычками (").

Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это имя поля события, значение которого должно быть передано в скрипт.

Пример: `-n "\"usr\": {{.SourceUserName}}"`

- **Рабочие процессы** – количество процессов, которые сервис может запускать одновременно.

  По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.

- **Описание** – вы можете добавить до 4000 символов Юникода, описывающих ресурс.

- **Фильтр** – используется для определения условий, при соответствии которым события будут обрабатываться ресурсом правила реагирования. В раскрывающемся списке можно выбрать существующий ресурс фильтра или создать новый фильтр.

  Создание фильтра в ресурсах

  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. Название должно содержать от 1 до 128 символов Юникода.

  4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

     c. В раскрывающемся списке **оператор** выберите нужный вам 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).
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Правила реагирования для KICS for Networks

Вы можете настроить правила реагирования для автоматического запуска действий по реагированию на активах KICS for Networks. Например, изменить статус актива в KICS for Networks.

При создании и изменении правил реагирования для KICS for Networks вам требуется задать значения для следующих параметров:

- **Название** (обязательно) – уникальное имя ресурса. Должно содержать от 1 до 128 символов Юникода.

- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

- **Тип** (обязательно) – **kics**.
- **Поле события** (обязательно) – поле события с активом, для которого нужно выполнить действия по реагированию. Возможные значения:
  - SourceAssetID.
  - DestinationAssetID.
  - DeviceAssetID.
- **Задача KICS for Networks** – действие по реагированию, которое требуется выполнить при получении данных, соответствующих фильтру. Доступны следующие типы действий по реагированию:
  - **Изменить статус актива на Разрешенное**.
  - **Изменить статус актива на Неразрешенное**.

  При срабатывании правила реагирования из KUMA в KICS for Networks будет отправлен API-запрос на изменение статуса указанного устройства на **Разрешенное** или **Неразрешенное**.
- **Рабочие процессы** – количество процессов, которые сервис может запускать одновременно.

  По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.
- **Описание** – вы можете добавить до 4000 символов Юникода, описывающих ресурс.
- **Фильтр** – используется для определения условий, при соответствии которым события будут обрабатываться ресурсом правила реагирования. В раскрывающемся списке можно выбрать существующий ресурс фильтра или создать новый фильтр.

  Создание фильтра в ресурсах

  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. Название должно содержать от 1

до 128 символов Юникода.

4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам 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).

- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Правила реагирования для Kaspersky Endpoint Detection and Response

Вы можете настроить правила реагирования для автоматического запуска действий по реагированию на активах Kaspersky Endpoint Detection and Response. Например, вы можете настроить автоматическую изоляцию актива от сети.

При создании и изменении правил реагирования для Kaspersky Endpoint Detection and Response вам требуется задать значения для следующих параметров:

- **Поле события** (обязательно) – поле события с активом, для которого нужно выполнить действия по реагированию. Возможные значения:
  - SourceAssetID.
  - DestinationAssetID.
  - DeviceAssetID.
- **Тип задачи** – действие по реагированию, которое требуется выполнить при получении данных, соответствующих фильтру. Доступны следующие типы действий по реагированию:
  - Включить сетевую изоляцию.

    При выборе этого типа реагирования вам нужно задать значения для следующих параметров:

    - **Срок действия изоляции** – количество часов, в течение которых будет действовать сетевая изоляция актива. Вы можете указать от 1 до 9999 часов.

      При необходимости вы можете **добавить исключение для сетевой изоляции**.

      Чтобы добавить исключение для сетевой изоляции:

      a. Нажмите на кнопку **Добавить исключение**.

      b. Выберите направление сетевого трафика, которое не должно быть заблокировано:

      - Входящее.
      - Исходящее.

- Входящее/Исходящее.

c. В поле **IP актива** введите IP-адрес актива, сетевой трафик которого не должен быть заблокирован.

d. Если вы выбрали **Входящее** или **Исходящее**, укажите порты подключения в полях **Удаленные порты** и **Локальные порты**.

e. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить исключение** и повторите действия по заполнению полей **Направление трафика**, **IP актива**, **Удаленные порты** и **Локальные порты**.

f. Если вы хотите удалить исключение, нажмите на кнопку **Удалить** под нужным вам исключением.

При добавлении исключений в правило сетей изоляции Kaspersky Endpoint Detection and Response может некорректно отображать значения портов в информации о правиле. Это не влияет на работоспособность программы. Подробнее о просмотре правила сетевой изоляции см. в *справке Kaspersky Anti Targeted Attack Platform*.

- Выключить сетевую изоляцию.

- Добавить правило запрета.

  При выборе этого типа реагирования вам нужно задать значения для следующих параметров:

  - **Поля события для получения хеш-суммы** – поля событий, из которых KUMA извлекает SHA256- или MD5-хеши файлов, запуск которых требуется запретить.

    Выбранные поля событий, а также значения, выбранные в **Поле события**, требуется добавить в наследуемые поля правила корреляции.

  - **Хеш файла №1** – SHA256- или MD5-хеш файла, который требуется запретить.

  Хотя бы одно из указанных выше полей должно быть заполнено.

- Удалить правило запрета.

- Запустить программу.

  При выборе этого типа реагирования вам нужно задать значения для следующих параметров:

  - **Путь к файлу** – путь к файлу процесса, который вы хотите запустить.
  - **Аргументы командной строки** – параметры, с которыми вы хотите запустить файл.
  - **Текущая директория** – директория, в которой на момент запуска располагается файл.

  При срабатывании правила реагирования для пользователей с ролью главный администратор в разделе **Диспетчер задач** веб-интерфейса программы отобразится задача **Запустить программу**. В столбце **Создал** таблицы задач для этой задачи отображается **Задача по расписанию**. Вы можете просмотреть результат выполнения задачи.

  > Все перечисленные операции выполняются на активах с Kaspersky Endpoint Agent для Windows. На активах с Kaspersky Endpoint Agent для Linux выполняется только запуск программы.

  > На программном уровне возможность создания правил запрета и сетевой изоляции для активов с Kaspersky Endpoint Agent для Linux не ограничена. KUMA и Kaspersky Endpoint Detection and Response не уведомляют о неуспешном применении этих правил.

- **Рабочие процессы** – количество процессов, которые сервис может запускать одновременно.

  По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.

- **Описание** – вы можете добавить до 4000 символов Юникода, описывающих ресурс.

- **Фильтр** – используется для определения условий, при соответствии которым события будут обрабатываться ресурсом правила реагирования. В раскрывающемся списке можно выбрать существующий ресурс фильтра или **создать новый 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. Название должно содержать от 1 до 128 символов Юникода.

4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам 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).

- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Правила реагирования через Active Directory

Правила реагирования через Active Directory определяют действия, которые будут применяться к учетной записи в случае срабатывания правила.
При создании и изменении правил реагирования через Active Directory вам требуется задать значения для следующих параметров:

- **Название** (обязательно) – уникальное имя ресурса. Должно содержать от 1 до 128 символов Юникода.

- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

- **Тип** (обязательно) – **Реагирование через Active Directory**.

- **Источник идентификатора аккаунта** – Поле события, откуда будет взято значение идентификатора учетной записи Active Directory. Возможные значения:

  - SourceAccountID

  - DestinationAccountID

- **Команда Active Directory** – команда, которая будет применяться к учетной записи при срабатывании правила реагирования.
  Доступные значения:

  - Добавить учетную запись в группу

    Группа Active Directory, из которой или в которую необходимо переместить учетную запись.
    В обязательном для заполнения поле **Distinguished name** необходимо указать полный путь к группе.
    Например, CN=HQ Team,OU=Groups,OU=ExchangeObjects,DC=avp,DC=ru.
    В рамках одной операции можно указать только одну группу.

- Удалить учетную запись из группы

  Группа Active Directory, из которой или в которую необходимо переместить учетную запись.
  В обязательном для заполнения поле **Distinguished name** необходимо указать полный путь к группе.
  Например, CN=HQ Team,OU=Groups,OU=ExchangeObjects,DC=avp,DC=ru.
  В рамках одной операции можно указать только одну группу.

- Сбросить пароль учетной записи

- Блокировать учетную запись

- **Фильтр** – используется для определения условий, при соответствии которым события будут обрабатываться ресурсом правила реагирования. В раскрывающемся списке можно выбрать существующий ресурс фильтра или создать новый фильтр.

  Создание фильтра в ресурсах

  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. Название должно содержать от 1 до 128 символов Юникода.

  4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

     c. В раскрывающемся списке **оператор** выберите нужный вам 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).
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

Шаблоны уведомлений

Параметры ресурса

Ресурсы шаблонов уведомлений используются в уведомлениях о создании алертов.

Параметры ресурса шаблона уведомления:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.

- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

- **Тема** (обязательно) – тема электронного письма с уведомлением о создании алерта. В теме письма можно обращаться к полям алерта.

  Пример: `Новый алерт в KUMA: {{.CorrelationRuleName}}`. Вместо `{{.CorrelationRuleName}}` в теме письма с уведомлением будет подставлено название правила корреляции, содержащееся в поле алерта `CorrelationRuleName`.

- **Шаблон** (обязательно) – тело электронного письма с уведомлением о создании алерта. Шаблон поддерживает синтаксис, с помощью которого уведомление можно наполнить данными из алерта.

  Для удобства можно открыть текст письма в отдельном окне, нажав на значок . При этом открывается окно **Шаблон**, в котором можно править текст письма с уведомлением. Сохранить изменения и закрыть окно можно с помощью кнопки **Сохранить**.

Функции в шаблонах

- `date` – принимает первым параметром время в миллисекундах (unix time), вторым параметром можно передать формат времени по стандартам RFC. Часовой пояс изменить нельзя.

  Пример вызова: `{{ date .FirstSeen "02 Jan 06 15:04" }}`

  Результат вызова: 18 Nov 2022 13:46

  Примеры форматов дат, поддерживаемые функцией:

  - `"02 Jan 06 15:04 MST"`
  - `"02 Jan 06 15:04 -0700"`
  - `"Monday, 02-Jan-06 15:04:05 MST"`
  - `"Mon, 02 Jan 2006 15:04:05 MST"`
  - `"Mon, 02 Jan 2006 15:04:05 -0700"`
  - `"2006-01-02T15:04:05Z07:00"`

- `limit` – функция вызывается внутри функции range для ограничения списка данных. Обрабатывает списки которые не имеют ключей, принимает любой список данных первым параметром и обрезает список по второму значению. Например, в функцию можно передавать поляй алерта `.Events`, `.Assets`, `.Accounts`, `.Actions`.

  Пример вызова:

  ```
  {{ range (limit .Assets 5) }}
  <strong>Устройство</strong>: {{ .DisplayName }},
  ```

```
<strong>Дата создания</strong>: {{ .CreatedAt }}
{{ end }}
```

- `link_alert` – формирует ссылку на алерт с URL, указанным в настройках подключения к SMTP-серверу в качестве псевдонима сервера Ядра KUMA или с реальным URL сервиса Ядра KUMA, если псевдоним не задан.

  Пример вызова:

  ```
  {{ link_alert }}
  ```

- `link` – принимает вид ссылки, доступной для перехода.

  Пример вызова:

  ```
  {{ link "https://support.kaspersky.com/KUMA/2.1/ru-RU/233508.htm" }}
  ```

Синтаксис шаблона уведомления

В шаблоне можно обращаться к полям алерта, содержащим строку или число:

```
{{ .CorrelationRuleName }}
```

В письме будет отображаться название алерта, то есть содержимое поля `CorrelationRuleName`.

Некоторые поля алерта содержат массивы данных. Например, это поля алерта с относящимися к нему событиями, активами, учетными записями. К таким вложенным объектам можно обращаться с помощью функции **range**, которая последовательно обращается к полям 50 первых вложенных объектов. При обращении с помощью функции **range** к полю, в котором нет массива данных, возвращается ошибка. Пример:

```
{{ range .Assets }}
Устройство: {{ .DisplayName }}, дата создания: {{ .CreatedAt }}
{{ end }}
```

В письме будут отображаться значения полей `DeviceHostName` и `CreatedAt` из 50 связанных с алертом активов:

```
Устройство: <значение поля DisplayName из актива 1>, дата создания:
<значение поля CreatedAt из актива 1>
Устройство: <значение поля DisplayName из актива 2>, дата создания:
<значение поля CreatedAt из актива 2>
...
// Всего 50 строк
```

С помощью параметра **limit** можно ограничить количество объектов, возвращаемых функцией **range**:

```
{{ range (limit .Assets 5) }}
<strong>Устройство</strong>: {{ .DisplayName }},
<strong>Дата создания</strong>: {{ .CreatedAt }}
{{ end }}
```

В письме будут отображаться значения полей `DisplayName` и `CreatedAt` из 5 связанных с алертом активов, слова "Устройства" и "Дата создания" выделены HTML-тегами :

```
<strong>Устройство</strong>: <значение поля DeviceHostName из актива 1>,
<strong>Дата создания</strong>: <значение поля CreatedAt из актива 1>
<strong>Устройство</strong>: <значение поля DeviceHostName из актива N>,
<strong>Дата создания</strong>: <значение поля CreatedAt из актива N>
...
// Всего 10 строк
```

Вложенные объекты могут иметь свои вложенные объекты. К ним можно обратиться с помощью вложенных функций **range**:

```
{{ range (limit .Events 5) }}
    {{ range (limit .Event.BaseEvents 10) }}
    Идентификатор сервиса: {{ .ServiceID }}
    {{ end }}
{{ end }}
```

В письме будет отображаться по десять идентификаторов сервисов (поле `ServiceID`) из базовых событий, относящихся к пяти корреляционным событиям алерта. Всего 50 строк. Обратите внимание, что обращение к событиям происходит через вложенную структуру EventWrapper, которая находится в алерте в поле Events. События доступны в поле Event этой структуры, что отражено в примере выше. Таким образом, если поле A содержит вложенную структуру [B] и в структуре [B] есть поле C, которое является строкой или числом, то чтобы обратиться к полю C необходимо указать путь {{ A.C }}.

Некоторые поля объектов содержат вложенные словари в формате "ключ - значение" (например, поле событий `Extra`). К ним можно обратиться с помощью функции **range** с переданными ей переменными: `range $placeholder1, $placeholder2 := .FieldName`. Значения переменных затем можно вызывать, указывая из названия. Пример:

```
{{ range (limit .Events 3) }}
    {{ range (limit .Event.BaseEvents 5) }}
    Список полей в поле события Extra: {{ range $name, $value := .Extra
}} {{ $name }} - {{ $value }} <br> {{ end }}
    {{ end }}
{{ end }}
```

В письме через HTML-тег
 будут отображаться пары "ключ - значение" из полей `Extra` базовых событий, принадлежащих корреляционным событиям. Вызываются данные из пяти базовых событий из каждого из трех корреляционных событий.

В шаблонах уведомлений можно использовать HTML-теги, выстраивая их в сложные структуры. Ниже приводится пример таблицы для полей корреляционного события:

```
<style type="text/css">
  TD, TH {
    padding: 3px;
    border: 1px solid black;
  }
</style>
<table>
  <thead>
    <tr>
        <th>Название сервиса</th>
```

```
        <th>Название корреляционного правила</th>
        <th>Версия устройства</th>
    </tr>
  </thead>
  <tbody>
    {{ range .Events }}
    <tr>
        <td>{{ .Event.ServiceName }}</td>
        <td>{{ .Event.CorrelationRuleName }}</td>
        <td>{{ .Event.DeviceVersion }}</td>
    </tr>
    {{ end }}
  </tbody>
</table>
```

С помощью функции **link_alert** в письмо с уведомлением можно вставить HTML-ссылку на алерт:

```
{{link_alert}}
```

В письме будет отображаться ссылка на окно алерта.

Ниже приведен пример, как можно из связанных с алертом данных извлечь сведения о наивысшей категории активов и поместить ее в уведомления:

```
{{ $criticalCategoryName := "" }}{{ $maxCategoryWeight := 0 }}{{ range
.Assets }}{{ range .CategoryModels }}{{ if gt .Weight $maxCategoryWeight
}}{{ $maxCategoryWeight = .Weight }}{{ $criticalCategoryName = .Name }}
{{ end }}{{ end }}{{ end }}{{ if gt $maxCategoryWeight 1 }}
Наивысшая категория активов: {{ $criticalCategoryName }}{{ end }}
```

Активные листы

Активный лист – это контейнер для данных, которые используются корреляторами KUMA при анализе событий по правилам корреляции.

Например, если у вас есть список IP-адресов с плохой репутацией, вы можете:

1. Создать корреляционное правило типа operational и добавить в активный лист эти IP-адреса.

2. Создать корреляционное правило типа standart и указать активный лист в качестве условия фильтрации.

3. Создать коррелятор с этим правилом.

   В этом случае KUMA выберет все события, которые содержат IP-адреса, внесенные в активный лист, и создаст корреляционное событие.

Вы можете наполнять активные листы автоматически с помощью корреляционных правил типа simple или импортировать файл с данными для активного листа.

Вы можете добавлять, копировать и удалять активные листы.

Один и тот же активный лист может использоваться в разных корреляторах. При этом для каждого коррелятора создается своя сущность активного листа. Таким образом, содержимое активных листов, используемых разными корреляторами, различается, даже если идентификатор и название активных листов одинаковые.

В активный лист добавляются данные только по правилам корреляции, добавленным в коррелятор.

Вы можете добавлять, изменять, дублировать, удалять и экспортировать записи в активном листе коррелятора.

В процессе корреляции при удалении записей из активных листов в корреляторах создаются служебные события. Эти события существуют только в корреляторах, они не перенаправляются в другие точки назначения. Правила корреляции можно настроить на отслеживание этих событий, чтобы с их помощью распознавать угрозы. Поля служебных событий удаления записи из активного листа описаны ниже.

Поле события	Значение или комментарий
`ID`	Идентификатор события
`Timestamp`	Время удаления записи, срок жизни которой истек
`Name`	`"active list record expired"`
`DeviceVendor`	`"Kaspersky"`
`DeviceProduct`	`"KUMA"`
`ServiceID`	Идентификатор коррелятора

`ServiceName`	Название коррелятора
`DeviceExternalID`	Идентификатор активного листа
`DevicePayloadID`	Ключ записи, чей срок жизни истек.
`BaseEventCount`	Увеличенное на единицу количество обновлений удаленной записи

Просмотр таблицы активных листов

Чтобы просмотреть таблицу активных листов коррелятора:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.

Таблица содержит следующие данные:

- **Название** – имя активного листа.
- **Записи** – количество записей в активном листе.
- **Размер на диске** – размер активного листа.
- **Каталог** – путь к активному листу на сервере коррелятора KUMA.

Добавление активного листа

Чтобы добавить активный лист:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. В разделе **Ресурсы** нажмите на кнопку **Активные листы**.
3. Нажмите на кнопку **Добавить активный лист**.

4. Выполните следующие действия:

   a. В поле **Название** введите имя активного листа.

   b. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.

   c. В поле **Срок жизни** укажите время, в течение которого в активном листе будет храниться добавленная в него запись.

      По истечении указанного времени запись удаляется. Время указывается в секундах.

      Максимальный срок жизни: `31536000` (один год).

      Значение по умолчанию: `0`. Если в поле указано значение 0, запись хранится бессрочно.

   d. В поле **Описание** введите любую дополнительную информацию.

      Вы можете использовать до 256 символов Юникода.

      Поле необязательно для заполнения.

5. Нажмите на кнопку **Сохранить**.

Активный лист будет добавлен.

Просмотр параметров активного листа

Чтобы просмотреть параметры активного листа:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.

2. В разделе **Ресурсы** нажмите на кнопку **Активные листы**.

3. В столбце **Название** выберите активный лист, параметры которого вы хотите просмотреть.

Откроется окно с параметрами активного листа. В нем отображается следующая информация:

- **Идентификатор** – идентификатор активного листа.

- **Название** – уникальное имя ресурса.

- **Тенант** – название тенанта, которому принадлежит ресурс.

- **Срок жизни** – время, в течение которого в активном листе будет храниться добавленная в него запись. Указывается в секундах.

- **Описание** – любая дополнительную информация о ресурсе.

Изменение параметров активного листа

Чтобы изменить параметры активного листа:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. В разделе **Ресурсы** нажмите на кнопку **Активные листы**.
3. В столбце **Название** выберите активный лист, параметры которого вы хотите изменить.
4. Укажите значения для следующих параметров:
   - **Название** – уникальное имя ресурса.
   - **Срок жизни** – время, в течение которого в активном листе будет храниться добавленная в него запись. Указывается в секундах.

     Если в поле указано значение 0, запись хранится бессрочно.
   - **Описание** – любая дополнительную информация о ресурсе.

   Поля **Идентификатор** и **Тенант** недоступны для редактирования.

Дублирование параметров активного листа

Чтобы скопировать активный лист:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. В разделе **Ресурсы** нажмите на кнопку **Активные листы**.
3. Установите флажок рядом с активным листом, который вы хотите скопировать.
4. Нажмите на кнопку **Дублировать**.
5. Укажите нужные вам параметры.
6. Нажмите на кнопку **Сохранить**.

Активный лист будет скопирован.

Удаление активного листа

Чтобы удалить активный лист:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. В разделе **Ресурсы** нажмите на кнопку **Активные листы**.
3. Установите флажки рядом с активными листами, которые вы хотите удалить.

   Если вы хотите удалить все листы, установите флажок рядом со столбцом **Название**.

   > Должен быть установлен хотя бы один флажок.

4. Нажмите на кнопку **Удалить**.
5. Нажмите на кнопку **Ок**.

Активные листы будут удалены.

Просмотр записей в активном листе

Чтобы просмотреть список записей в активном листе:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.

5. В столбце **Название** выберите нужный вам активный лист.

Откроется таблица записей для выбранного листа.

Таблица содержит следующие данные:

- **Ключ** – значение ключа записи.

- **Повторы записи** – общее количество упоминаний записи в событиях и загрузок идентичных записей при импорте активных листов в KUMA.
- **Срок действия** – дата и время, когда запись должна быть удалена.
- **Создано** – время создания активного листа.
- **Последнее обновление** – время последнего обновления активного листа.

Поиск записей в активном листе

Чтобы найти запись в активном листе:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.
5. В столбце **Название** выберите нужный вам активный лист.

   Откроется окно со списком записей для выбранного листа.
6. В поле **Поиск** введите значение ключа записи или несколько знаков из ее ключа.

В таблице записей активного листа отобразятся только те записи, в ключе которых есть введенные символы.

Добавление записи в активный лист

Чтобы добавить запись в активный лист:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив нужного коррелятора.
4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.

5. В столбце **Название** выберите нужный вам активный лист.

   Откроется окно со списком записей для выбранного листа.

6. Нажмите на кнопку **Добавить**.

   Откроется окно **Создать новую запись**.

7. Укажите значения для следующих параметров:

   a. В поле **Ключ** введите имя записи.

      Вы можете указать несколько значений, используя символ "|".

      > Поле **Ключ** не может быть пустым. Если поле остается пустым, при попытке сохранить изменения KUMA возвращает ошибку.

   b. В поле **Значение** укажите значение для полей **message** и **code**.

      Вы можете удалить эти поля при необходимости.

   c. Если вы хотите добавить дополнительное значение, нажмите на кнопку **Добавить элемент**.

   d. В столбце **Поле** укажите название поля.

      Оно должно соответствовать следующим требованиям:

      - название уникально;
      - не содержит буквы русского алфавита;
      - не содержит пробелы и табуляцию;
      - не содержит специальные символы, кроме символа нижнего подчеркивания;
      - максимальное количество символов – 128.

        > Название не может начинаться с символа нижнего подчеркивания и содержать только цифры.

   e. В столбце **Значение** укажите значение для этого поля.

      Оно должно соответствовать следующим требованиям:

      - не содержит буквы русского алфавита;

- не содержит пробелы и табуляцию;
- не содержит специальные символы, кроме символа нижнего подчеркивания;
- максимальное количество символов – 128.

Поле необязательно для заполнения.

8. Нажмите на кнопку **Сохранить**.

Запись будет добавлена. После сохранения записи в активном листе будут отсортированы в алфавитном порядке.

Дублирование записей в активном листе

Чтобы дублировать запись в активном листе:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.
5. В столбце **Название** выберите нужный вам активный лист.

   Откроется окно со списком записей для выбранного листа.
6. Установите флажок для записи, которую вы хотите скопировать.
7. Нажмите на кнопку **Дублировать**.
8. Укажите нужные вам параметры.

   Поле **Ключ** не может быть пустым. Если поле остается пустым, при попытке сохранить изменения KUMA возвращает ошибку.

Редактирование названий полей в столбце **Поле** для записей, добавленных в активный лист ранее, недоступно. Вы можете менять названия только для записей, добавленных в момент редактирования. Название не может начинаться с символа нижнего подчеркивания и содержать только цифры.

9. Нажмите на кнопку **Сохранить**.

Запись будет скопирована. После сохранения записи в активном листе будут отсортированы в алфавитном порядке.

Изменение записи в активном листе

Чтобы изменить запись в активном листе:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.
5. В столбце **Название** выберите нужный вам активный лист.

   Откроется окно со списком записей для выбранного листа.
6. Нажмите на название записи в столбце **Ключ**.
7. Укажите требуемые значения.
8. Нажмите на кнопку **Сохранить**.

Запись будет изменена. После сохранения записи в активном листе будут выстроены в алфавитном порядке.

Ограничения, действующие при редактировании записи:

- Название записи недоступно для редактирования. Вы можете изменить его, выполнив импорт аналогичных данных с другим названием.
- Поля **code** и **message** недоступны для редактирования.

- Редактирование названий полей в столбце **Поле** для записей, добавленных в активный лист ранее, недоступно. Вы можете менять названия только для записей, добавленных в момент редактирования. Название не может начинаться с символа нижнего подчеркивания и содержать только цифры.

- Значения в столбце **Значение** должны соответствовать следующим требованиям:

  - не содержит буквы русского алфавита;

  - не содержит пробелы и табуляцию;

  - не содержит специальные символы, кроме символа нижнего подчеркивания;

  - максимальное количество символов – 128.

Удаление записей в активном листе

Чтобы удалить записи из активного листа:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.

2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.

3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.

4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.

5. В столбце **Название** выберите нужный вам активный лист.

   Откроется окно со списком записей для выбранного листа.

6. Установите флажки для записей, которые вы хотите удалить.

   Если вы хотите удалить все записи, установите флажок рядом с названием столбца **Ключ**.

   > Должен быть установлен хотя бы один флажок.

7. Нажмите на кнопку **Удалить**.

8. Нажмите на кнопку **Ок**.

Записи будут удалены.

Импорт данных в активный лист

Чтобы импортировать данные в активный лист:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.
3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.
5. Наведите курсор мыши на строку с требуемым активным листом.
6. Нажмите на ... слева от названия активного листа.
7. Выберите **Импортировать**.

   Откроется окно импорта активного листа.
8. В поле **Файл** выберите файл, который требуется импортировать.
9. В раскрывающемся списке **Формат** выберите формат файла:
   - **csv**.
   - **tsv**.
   - **internal**.
10. В поле **Ключевое поле** введите название столбца с ключами записей активного листа.
11. Нажмите на кнопку **Импортировать**.

Данные из файла будут импортированы в активный лист. Записи, внесенные в лист ранее, сохраняются.

Экспорт данных из активного листа

Чтобы экспортировать активный лист:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. В разделе **Сервисы** нажмите на кнопку **Активные сервисы**.

3. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.

4. Нажмите на кнопку **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.

5. Наведите курсор мыши на строку с требуемым активным листом.

6. Нажмите на ••• слева от нужного активного листа.

7. Нажмите на кнопку **Экспортировать**.

Активный лист будет загружен в формате JSON, используя настройки вашего браузера. Название загруженного файла соответствует названию активного листа.

Словари

Описание параметров

Словари – это ресурсы, в которых хранятся данные, которые могут использоваться другими ресурсами и сервисами KUMA.

Доступные параметры:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.

- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

- **Описание** – вы можете добавить до 256 символов Юникода, описывающих ресурс.

- **Тип** (обязательно) – тип словаря. От выбранного типа зависит формат данных, которые может содержать словарь:

  - В тип **Словарь** можно добавлять пары ключ–значение.

    Не рекомендуется добавлять в словари этого типа более 50 000 записей.

    > При добавлении в словарь строк с одинаковыми ключами каждая новая строка будет записана поверх уже существующий строки с тем же самым ключом. В итоге в словарь будет добавлена только одна строка.

- В тип **Таблица** можно добавлять данные в виде сложных таблиц. С этим типом словарей можно взаимодействовать с помощью REST API.

- Блок параметров **Значения** – содержит таблицу с данными словаря:

  - Для типа **Словарь** в блоке отображается перечень пар **Ключ** – **Значение**. Таблицу можно дополнять строками с помощью кнопки +. Удалить строки можно с помощью кнопки ×, которая отображается при наведении курсора мыши на нужную строку.

  - Для типа **Таблица** в блоке отображается таблица с данными. Таблицу можно дополнять строками и столбцами с помощью кнопки +. Удалить строки и столбцы можно с помощью кнопок ×, которые отображаются при наведении курсора мыши на нужную строку или заголовок нужного столбца. Заголовки столбцов доступны для редактирования.

  Если словарь содержит больше 5000 записей, они не отображаются в веб-интерфейсе KUMA. Для просмотра содержимого таких словарей содержимое необходимо экспортировать в формат CSV. Если CSV-файл отредактировать и снова импортировать в KUMA, ресурс словаря 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 Юникода.

  Значения должны содержать от нуля до 256 символов Юникода.

При импорте содержимое словаря перезаписывается загружаемым файлом. При импорте в словарь также изменяется название ресурса, чтобы отразить имя импортированного файла.

При экспорте, если ключ или значение содержат символы запятой или кавычек (, и "), они заключаются в кавычки ("). 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.

Прокси-серверы

Ресурсы прокси-сервера используются для хранения параметров конфигурации прокси-серверов.

Доступные параметры:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Брать URL из секрета** (обязательно) – раскрывающийся список для выбора ресурса секрета, в котором хранятся URL прокси-серверов. При необходимости секрет можно создать в окне создания прокси-сервера с помощью кнопки +. Выбранный секрет можно изменить, нажав на кнопку .
- **Не использовать на доменах** – один или несколько доменов, к которым требуется прямой доступ.
- **Описание** – вы можете добавить до 256 символов Юникода, описывающих ресурс.

Секреты

Ресурсы секретов используются для безопасного хранения конфиденциальной информации, такой как логины и пароли, которые должны использоваться KUMA для взаимодействия с внешними службами.

Доступные параметры:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.

- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

- **Тип** (обязательно) – тип секрета.

  При выборе в раскрывающемся списке типа секрета отображаются параметры для настройки выбранного типа секрета. Эти параметры описаны ниже.

- **Описание** – вы можете добавить до 256 символов Юникода, описывающих ресурс.

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**.

- **token** – тип секрета используется для хранения токенов для API-запросов. Токены используются, например, при подключении к IRP-системам. При выборе этого типа секрета требуется заполнить поле **Токен**.

- **ktl** – тип секрета используется для хранения данных учетной записи Kaspersky Threat Intelligence Portal. При выборе этого типа секрета требуется заполнить следующие поля:

  - **Пользователь** и **Пароль** (обязательные поля) – имя пользователя и пароль вашей учетной записи Kaspersky Threat Intelligence Portal.

  - **Файл обмена личной информацией - PKCS (.PFX)** (обязательно) – позволяет загрузить ключ сертификата Kaspersky Threat Intelligence Portal.

  - **Пароль PFX-файла** (обязательно) – пароль для доступа к ключу сертификата Kaspersky Threat Intelligence Portal.

- **urls** – тип секрета используется для хранения URL для подключения к базам SQL и прокси-серверам. В поле **Описание** требуется описать, для какого именно подключения вы используете секрет **urls**.

  Вы можете указать URL в следующих форматах: hostname:port, IPv4:port, IPv6:port, :port.

- **pfx** – тип секрета используется для импорта PFX-файла с сертификатами. При выборе этого типа секрета требуется заполнить следующие поля:

  - **Файл обмена личной информацией - PKCS (.PFX)** (обязательно) – используется для загрузки PFX-файла. Файл должен содержать сертификат и ключ. В PFX-файлы можно включать сертификаты, подписанными центрами сертификации, для проверки сертификатов сервера.

- **Пароль PFX-файла** (обязательно) – используется для ввода пароля для доступа к ключу сертификата.

- **kata/edr** – тип секрета используется для хранения файла сертификата и закрытого ключа, требуемых при подключении к серверу Kaspersky Endpoint Detection and Response. При выборе этого типа секрета вам требуется загрузить следующие файлы:

  - Файл сертификата – сертификат сервера KUMA.

    Файл должен иметь формат PEM. Вы можете загрузить только один файл сертификата.

  - Закрытый ключ шифрования соединения – RSA-ключ сервера KUMA.

    Ключ должен быть без пароля и с заголовком PRIVATE KEY. Вы можете загрузить только один файл ключа.

    > Вы можете сгенерировать файлы сертификата и ключа по кнопке .

- **snmpV1** – тип секрета используется для хранения значения **Уровень доступа** (например, `public` или `private`), которое требуется при взаимодействии по протоколу Simple Network Management Protocol.

- **snmpV3** – тип секрета используется для хранения данных, требуемых при взаимодействии по протоколу Simple Network Management Protocol. При выборе этого типа секрета требуется заполнить 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**.

- **cetrificate** – 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.

Правила сегментации

В KUMA можно настроить *правила сегментации алертов*, то есть правила разделения однотипных корреляционных событий по разным алертам.

По умолчанию, если в корреляторе какое-то правило корреляции сработает несколько раз, все созданные в результате этого корреляционные события будут присоединены к одному алерту. Правила сегментации алертов дают возможность определить условия, при которых на основе таких однотипных корреляционных событий будут создаваться разные алерты. Это может пригодиться, если вы хотите разделить поток корреляционных событий, например, по количеству событий или объединить некоторых из событий, отличающиеся чем-то важным от других, в отдельный алерт.

Сегментация алертов настраивается в два этапа:

1. **Создаются ресурсы *правил сегментации*, в которых определяются условия, по которым будет разделяться поток корреляционных событий.**

2. **К правилам сегментации привязываются правила корреляции, в которых должны срабатывать правила сегментации.**

Параметры правил сегментации

Ресурсы правил сегментации создаются в разделе **Ресурсы** → **Правила сегментации** веб-интерфейса KUMA.

Доступные параметры:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.

- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

- **Тип** (обязательно) – тип правила сегментации. Доступные значения:

  - **По фильтру** – алерты создаются, если корреляционные события соответствуют условиям фильтра, заданным в блоке параметров **Фильтр**.

    С помощью кнопки **Добавить условие** можно добавить строку с полями для определения условия. С помощью кнопки **Добавить группу** можно добавить группу фильтров. Можно переключать групповые операторы между **И**, **ИЛИ**, **НЕ**. В группы фильтров можно добавить другие группы условий и отдельные условия. Условия и группы можно менять местами, перетягивая их за значок ⣿, а также удалять с помощью значка ✕.

    - Левый операнд и Правый операнд – используются для указания значений, которые будет обрабатывать оператор.

      В левом операнде указываются названия полей событий, которые обрабатывает фильтр.

      В правом операнде можно выбрать тип значения – **константа** или **список**, – а также указать само значение.

    - Доступные операторы

      - **=** – левый операнд равен правому операнду.
      - **<** – левый операнд меньше правого операнда.
      - **<=** – левый операнд меньше или равен правому операнду.
      - **>** – левый операнд больше правого операнда.
      - **>=** – левый операнд больше или равен правому операнду.
      - **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
      - **contains** – левый операнд содержит значения правого операнда.
      - **startsWith** – левый операнд начинается с одного из значений правого операнда.

- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

- **По группирующим полям** – алерт создается, если корреляционное событие содержит поля событий, указанные в блоке параметров **Группирующие поля правила корреляции**.

  Поля добавляются с помощью кнопки **Добавить поле**. Добавленные поля можно удалить, нажав на значок креста или на кнопку **Сбросить**.

  Пример использования группирующих полей

  Правило, детектирующее сканирование сети, создаст только один алерт, даже если в сети есть несколько машин, сканирующих сеть. Если создать правило сегментации алертов по группирующему полю событий `SourceAddress`, а затем привязать это правило сегментации к правилу корреляции, при срабатывании правила будут созданы алерты для каждого адреса, с которого происходит сканирование.

  В этом примере, если правило корреляции называется "`Network. Possible port scan`", а в ресурсе правила сегментации в качестве шаблона именования алертов указано "`from {{.SourceAddress}}`", будут созданы алерты такого вида:

  - `Network. Possible port scan (from 10.20.20.20 <Дата создания алерта>)`
  - `Network. Possible port scan (from 10.10.10.10 <Дата создания алерта>)`

- **По количеству событий** – алерт создается, если количество корреляционных событий в предыдущем алерте превысило значение, указанное в поле **Количество корреляционных событий**.

- **Шаблон именование алертов** (обязательно) – шаблон, по которому будут получать название алерты, создаваемые по этому правилу сегментации. Значение по умолчанию:

`{{.Timestamp}}`.

В поле шаблона можно указывать текст, а также поля события в формате `{{.<название поля события>}}`. При формировании названия алерта вместо названия поля события будет подставляться содержащееся в нем значение.

Название алерта, созданного с помощью правил сегментации, имеет следующий формат: "<Название правила корреляции, создавшего алерт> (<текст из поля шаблона именования алертов> <дата создания алерта>)".

- **Описание** – описание ресурса: до 256 символов Юникода.

Привязка правил сегментации к правилам корреляции

Связи правила сегментации и правил корреляции создаются отдельно для каждого тенанта. Они отображаются в разделе **Параметры** → **Алерты** → **Сегментация** веб-интерфейса KUMA в таблице со следующими столбцами:

- **Тенант** – название тенанта, которому принадлежат правила сегментации.
- **Обновлено** – дата и время последнего обновления правил сегментации.
- **Выключено** – в этом столбце отображается метка, если правила сегментации выключены.

Чтобы привязать правило сегментации алерта к правилам корреляции:

1. Откройте раздел **Параметры** → **Алерты** → **Сегментация** веб-интерфейса KUMA.
2. Выберите тенант, для которого вы хотите создать правило сегментации:
   - Если у тенанта уже есть правила сегментации, выберите его в таблице.
   - Если у тенанта нет правил сегментации, нажмите **Добавить параметры для нового тенанта** и в раскрывающемся списке **Тенант** выберите нужный тенант.

   Отображается таблица с созданными связями правил сегментации и корреляции.
3. В блоке параметров **Связи правил сегментации** нажмите **Добавить** и укажите параметры правила сегментации:
   - **Название** (обязательно) – в этом поле укажите название правила сегментации. Должно содержать от 1 до 128 символов Юникода.
   - **Тенанты и правила корреляции** (обязательно) – в этом раскрывающемся списке выберите тенант и принадлежащее ему правило корреляции, события которого вы хотите выделить в отдельный алерт. Можно выбрать более одного правила корреляции.

- **Правило сегментации** (обязательно) – в этом блоке параметров требуется выбрать ранее созданный ресурс правила сегментации, в котором определены условия сегментации

- **Выключено** – установите этот флажок при необходимости выключить связь правила сегментации.

4. Нажмите **Сохранить**.

   Правило сегментации и правила корреляции связаны. Корреляционные события, создаваемые указанными правилами корреляции, будут объединены в отдельный алерт с названием, определенном в ресурсе правила сегментации.

Чтобы выключить связи правил сегментации и правил корреляции для тенанта:

1. Откройте раздел **Параметры** → **Алерты** веб-интерфейса KUMA и выберите тенант, правила сегментации которого вы хотите выключить.

2. Установите флажок **Выключено**.

3. Нажмите **Сохранить**.

   Связи правил сегментации и правил корреляции для выбранного тенанта выключены.

Сервисы KUMA

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

- Одна часть сервиса создается внутри веб-интерфейса KUMA на основе набора ресурсов для сервисов.

- Вторая часть сервиса устанавливается в сетевой инфраструктуре, где развернута система KUMA, в качестве одного из ее компонентов. Серверная часть сервиса может состоять из нескольких экземпляров: например, сервисы одного и того же агента или хранилища могут быть установлены сразу на нескольких машинах.

  > В серверной части сервисы KUMA располагаются в директории `/opt/kaspersky/kuma`.

  При установке KUMA в отказоустойчивом варианте коллекторы, корреляторы и хранилища размещаются внутри кластера Kubernetes.

Между собой части сервисов соединены с помощью идентификатора сервисов.

Типы сервисов:

- Коллекторы – используются для получения события и конвертации их в формат KUMA.
- Корреляторы – используются для анализа событий и поиска заданных закономерностей.
- Хранилища – используются для хранения событий.
- Агенты – используются для получения событий на удаленных устройствах и пересылки их в коллекторы KUMA.

В веб-интерфейсе KUMA сервисы отображаются в разделе **Ресурсы** → **Активные сервисы** в виде таблицы. Таблицу сервисов можно обновить с помощью кнопки **Обновить** и сортировать по столбцам, нажимая на активные заголовки.

Столбцы таблицы:

- **Статус** – статус сервиса:
  - Зеленый – сервис работает.
  - Красный – сервис не работает.
  - Желтый – этот статус применяется только к сервисам хранилища и означает, что нет соединения с узлами ClickHouse. Причина указывается в журнале сервиса, если было включено логирование.

    Таблицу можно фильтровать по этому параметру.
- **Тип** – вид сервиса: **агент**, **коллектор**, **коррелятор**, **хранилище**.
- **Название** – название сервиса. При нажатии на название сервиса открываются его настройки.
- **Версия** – версия сервиса.
- **Тенант** – название тенанта, которому принадлежит сервис.
- **Полное доменное имя** – доменное имя сервера, на котором установлен сервис.
- **IP-адрес** – IP-адрес сервера, на котором установлен сервис.
- **Порт API** – номер порта для внутренних коммуникаций.
- **Время работы** – как долго сервис работает.

- **Создан** – дата и время создания сервиса.

С помощью кнопки **Добавить сервис** можно создавать новые сервисы на основе существующих наборов ресурсов для сервисов. Также с помощью кнопок в верхней части этого окна можно выполнить следующие действия:

- перезапустить сервис;
- удалить сертификат сервиса;
- скопировать идентификатор сервиса;
- удалить сервис;
- просмотреть разделы хранилищ;
- просмотреть активные листы корреляторов;
- скачать журнал сервиса.

Сервисы можно изменить, нажав на них в разделе **Ресурсы** → **Активные сервисы**. При этом открывается окно с набором ресурсов, на основе которых они были созданы. Сервис меняется путем изменения параметров набора ресурсов. Изменения сохраняются с помощью кнопки **Сохранить** и вступают в силу после перезапуска сервиса.

Если вы, меняя параметры набора ресурсов коллектора, измените или удалите преобразования в подключенном к нему нормализаторе, правки не сохранятся, а сам ресурс нормализатора может быть поврежден. При необходимости изменить преобразования в нормализаторе, который уже является частью сервиса, вносите правки непосредственно в ресурс нормализатора в разделе веб-интерфейса **Ресурсы** → **Нормализаторы**.

Инструменты сервисов

В этом разделе описываются инструменты по работе с сервисами, доступные в разделе веб-интерфейса KUMA **Ресурсы** → **Активные сервисы**.

Получение идентификатора сервиса

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

Чтобы получить идентификатор сервиса:

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

2. 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.

Перезапуск сервиса

Чтобы перезапустить сервис:

1. Войдите в веб-интерфейс KUMA 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 KUMA:

     - Агент KUMA для Windows может быть перезагружен, как описано выше, только если он запущен на удаленном компьютере. Если сервис на удаленном компьютере неактивен, при попытке перезагрузки из KUMA вы получите сообщение об ошибке. В этом случае следует перезапустить сервис Агент KUMA для Windows на удаленном компьютере с Windows. Чтобы узнать, как перезапустить сервисы Windows, обратитесь к документации, относящейся к версии операционной системы вашего удаленного компьютера с Windows.

     - Агент KUMA для Linux при использовании этой опции останавливается. Для запуска агента необходимо выполнить команду, с помощью которой он был запущен.

   - **Сбросить сертификат** – удалить сертификаты, используемые сервисом для внутренней связи. Например, эту опцию можно использовать для обновления сертификата Ядра.

     Особенности удаления сертификатов для агентов Windows:

     - Если агент находится в зеленом статусе и вы выбрали **Сбросить сертификат**, KUMA удаляет действующий сертификат и создает новый, агент продолжает

работу с новым сертификатом.

- Если агент находится в красном статусе и вы выбрали **Сбросить сертификат**, KUMA выдаст ошибку о том, что агент не запущен. В папке установки агента %APPDATA%\kaspersky\kuma\<ID агента>\certficates 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. Он потребуется, чтобы удалить сервис с сервера.

Чтобы удалить сервис:

1. Войдите в веб-интерфейс KUMA 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 KUMA.

Чтобы удалить сервис с сервера:

Удалите файл /usr/lib/systemd/system/kuma-<Тип сервиса: collector, correlator или storage >-<идентификатор сервиса>.service с сервера, на котором был установлен сервис.

Окно Разделы

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

*Чтобы открыть таблицу **Разделы**:*

1. Войдите в веб-интерфейс KUMA и откройте раздел **Ресурсы** → **Активные сервисы**.
2. Установите флажок рядом с нужным хранилищем 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 коррелятором или коллектором.

Чтобы найти события, относящиеся к коррелятору или коллектору:

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

2. Установите флажок рядом с нужным коррелятором или коллектором и нажмите **Перейти к событиям**.

   Откроется новая закладка браузера с открытым разделом KUMA **События**.

3. Чтобы найти события, нажмите на значок .

   Отобразится таблица с событиями, отобранными по поисковому выражению `ServiceID = <идентификатор выбранного сервиса>`.

Результаты поиска событий

Наборы ресурсов для сервисов

Наборы ресурсов для сервисов – это тип ресурсов, компонент KUMA, представляющий собой комплект настроек, на основе которых создаются и функционируют сервисы KUMA. Наборы ресурсов для сервисов собираются из ресурсов.

Ресурсы, объединяемые в набор ресурсов, должны принадлежать к тому же тенанту, что и создаваемый набор ресурсов. Исключением является общий тенант: принадлежащие ему ресурсы можно использовать в наборах ресурсов других тенантов.

Наборы ресурсов для сервисов отображаются в разделе веб-интерфейса KUMA **Ресурсы** → **<Тип набора ресурсов для сервиса>**. Доступные типы:

- Коллекторы

- Корреляторы
- Хранилища
- Агенты

При выборе нужного типа открывается таблица с имеющимися наборами ресурсов для сервисов этого типа. Таблица содержит следующие столбцы:

- **Название** – имя набора ресурсов. Может использоваться для поиска и сортировки.
- **Последнее обновление** – дата и время последнего обновления набора ресурсов. Может использоваться для сортировки.
- **Создал** – имя пользователя, создавшего набор ресурсов.
- **Описание** – описание набора ресурсов.

Создание хранилища

Хранилище состоит из двух частей: одна часть создается внутри веб-интерфейса KUMA, а вторая устанавливается на серверах сетевой инфраструктуры, предназначенных для хранения событий. Серверная часть хранилища KUMA представляет собой собранные в кластер узлы ClickHouse. Кластеры ClickHouse можно дополнять дисками холодного хранения данных.

Для каждого кластера ClickHouse требуется установить отдельное хранилище.

> Перед созданием хранилища продумайте структуру кластера и разверните требуемую сетевую инфраструктуру. При выборе конфигурации кластера ClickHouse учитывайте требования вашей организации к хранению событий.

> В качестве файловой системы рекомендуется использовать ext4.

Создание хранилища производится в несколько этапов:

1. **Создание набора ресурсов хранилища в веб-интерфейсе KUMA**
2. **Создание сервиса хранилища в веб-интерфейсе KUMA**
3. **Установка узлов хранилища в сетевой инфраструктуре**

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

При изменении параметров хранилища его сервис необходимо перезапустить.

Структура кластера ClickHouse

Кластер ClickHouse – логическая группа машин, обладающих всеми накопленными нормализованными событиями KUMA. Подразумевает наличие одного или нескольких логических *шардов*.

Шард – логическая группа машин, 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 машинами.

Реплика – машина, являющаяся членом логического шарда и обладающая 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 – машина, участвующая в **координации** репликации данных на уровне **всего** кластера. На весь кластер требуется хотя бы одна машина с этой ролью. Рекомендуемое количество машин с такой ролью – 3. Число машин, участвующих в координации репликации, должно быть **нечетным**. Роль *кипера* и *реплики* можно совмещать.

Параметры узлов кластера ClickHouse

Перед созданием хранилища продумайте структуру кластера и разверните требуемую сетевую инфраструктуру. При выборе конфигурации кластера ClickHouse учитывайте требования вашей организации к хранению событий.

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

Для каждого узла кластера ClickHouse требуется указать следующие параметры:

- Полное доменное имя (FQDN) – уникальный адрес, по которому должен быть доступен узел. Необходимо указывать FQDN целиком, например `kuma-storage.example.com`.
- Идентификаторы шарда, реплики и кипера – комбинация этих параметров определяет положение узла в структуре кластера ClickHouse и его роль.

Роли узлов

Роли узлов зависят от указанных параметров:

- шард, реплика, кипер – узел участвует в накоплении и поиске нормализованных событий KUMA, а также в координации репликации данных на уровне всего кластера.
- шард, реплика – узел участвует в накоплении и поиске нормализованных событий KUMA.
- кипер – узел **не** накапливает нормализованные события, но участвует в координации репликации данных на уровне всего кластера.

Требования к идентификаторам:

- Если в одном кластере создано несколько шардов, идентификаторы шардов должны быть уникальными в рамках этого кластера.
- Если в одном шарде создано несколько реплик, идентификаторы реплик должны быть уникальными в рамках этого шарда.
- Идентификаторы киперов должны быть уникальными в рамках кластера.

Пример идентификаторов узлов кластера ClickHouse:

- шард 1, реплика 1, кипер 1;

- шард 1, реплика 2;
- шард 2, реплика 1;
- шард 2, реплика 2, кипер 3;
- шард 2, реплика 3;
- кипер 2.

Холодное хранение событий

В KUMA можно настроить перенос устаревших данных с кластера ClickHouse 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.

Диски холодного хранения можно добавлять и удалять.

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

При задействованном холодном хранении KUMA раз в час проверяет сроки хранения пространств:

- Если срок хранения пространства на кластере ClickHouse истек, данные переносятся на диски холодного хранения. Если диск холодного хранения настроен неверно, данные удаляются.
- Если срок хранения пространства на диске холодного хранения истек, данные удаляются.

- Если диски кластера ClickHouse заполнены на 90%, самые старые данные кластера автоматически переносятся на диски холодного хранения. Это действие может происходить больше одного раза в час.

- При начале и окончании переноса данных создаются события аудита.

Во время переноса данных сервис хранилища продолжает работать, при этом в разделе веб-интерфейса KUMA **Ресурсы** → **Активные сервисы** для него отображается желтый статус. При наведении указателя мыши на значок статуса отображается сообщение о переносе данных.

Особенности хранения событий и доступа к ним

- При использовании для холодного хранения HDFS-дисков необходимо обеспечить защиту данных одним из следующих способов:

  - Настроить отдельный физический интерфейс в сети VLAN, в котором будут расположены только HDFS-диски и кластер ClickHouse.

  - Настроить правила сегментации сети и фильтрации трафика, исключающие прямой доступ к HDFS-диску или перехват трафика к диску со стороны ClickHouse.

- События, находящиеся в кластере ClickHouse и на дисках холодного хранения, одинаково доступны в веб-интерфейсе KUMA. Например, при поиске событий или при просмотре событий, относящихся к алертам.

- Допускается не хранить события или события аудита на дисках холодного хранения: для этого в параметрах хранилища в поле **Срок холодного хранения** или **Срок холодного хранения события аудита** необходимо указать `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, где 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.

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 KUMA перейдите в раздел **Ресурсы** → **Хранилища** выберите нужный ресурс хранилища.

  Откроется ресурс хранилища.

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

  Данные с удаляемого диска автоматически начинают переноситься на другие диски холодного хранения или, если их нет, в кластер ClickHouse. В процессе переноса данных значок статуса хранилища светится желтым цветом. При начале и окончании переноса данных создаются события аудита.

- 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.

Создание набора ресурсов для хранилища

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

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

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

   Откроется окно создания хранилища.

2. В поле **Название хранилища** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов Юникода.

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

4. В поле **Описание** можно добавить описание сервиса: до 256 символов Юникода.

5. В поле **Срок хранения** укажите, в течение какого количества дней вы хотите хранить события в кластере ClickHouse.

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

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

   - **Срок холодного хранения** – количество дней хранения событий. Минимальное значение – `1`.

   - **Срок холодного хранения событий аудита** – количество дней хранения событий аудита. Минимальное значение – 0.

8. При необходимости в поле **Переопределение параметров конфигурации** можно ввести содержимое XML-файла конфигурации ClickHouse (без корневых элементов). Эта конфигурация будет использоваться вместо параметров по умолчанию.

Пример: `<merge_tree><parts_to_delay_insert>500</parts_to_delay_insert><parts_to_delay_insert>1000</parts_to_delay_insert></merge_tree>`

9. 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 с помощью кнопки **Удалить пространство**.

   Доступные параметры:

   - В поле **Название** укажите название пространства: от 1 до 128 символов Юникода.
   - В поле **Срок хранения** укажите количество дней, в течение которых события будут храниться в кластере ClickHouse.
   - При необходимости в поле **Срок холодного хранения** укажите количество дней, в течение которого события должны находиться на холодном хранении. Минимальное значение – `1`.
   - В разделе **Фильтр** можно задать условия определения событий, которые будут помещаться в это пространство. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

     Создание фильтра в ресурсах

     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. Название должно содержать от 1 до 128 символов Юникода.
     4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

c. В раскрывающемся списке **оператор** выберите нужный вам 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).
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

После создания сервиса пространства можно просматривать и удалять в параметрах набора ресурсов хранилища.

Нет необходимости создавать отдельное пространство для событий аудита. События этого типа ("`type`"="`4`") автоматически помещаются в отдельное пространство Audit со сроком хранения не менее 365 дней, которое недоступно для редактирования или удаления из веб-интерфейса KUMA.

10. При необходимости в разделе **Диски холодного хранения** добавьте в хранилище диски, на которые вы хотите переносить события на длительное хранение из кластера ClickHouse.

    Дисков может быть несколько. Диски можно добавить с помощью кнопки **Добавить диск** и удалить с помощью кнопки **Удалить диск**.

    Доступные параметры:

    - В раскрывающемся списке **Тип** выберите тип 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 Юникода.
    - Если в качестве типа диска вы выбрали **Локальный**, в поле **Путь** введите абсолютный путь директории смонтированного локального диска. Путь должен начинаться и оканчиваться символом "/".
    - Если в качестве типа диска вы выбрали **HDFS**, в поле **Хост** введите путь к HDFS. Например: `hdfs://hdfs1:9000/clickhouse/`.

11. 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 с помощью кнопки **Удалить узел**.

    Доступные параметры:

    - В поле **Полное доменное имя** укажите FQDN добавляемого узла. Например, `kuma-storage-1.example.com`.
    - В полях идентификаторов шарда, реплики и кипера укажите комбинацию параметров, определяющую роль узла в кластере ClickHouse.

Набор ресурсов для хранилища создан и отображается в разделе **Ресурсы** → **Хранилища**. Теперь можно создать сервис хранилища.

Создание сервиса хранилища в веб-интерфейсе KUMA

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

Чтобы создать сервис хранилища в веб-интерфейсе KUMA:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** нажмите **Добавить сервис**.

2. В открывшемся окне **Выберите сервис** выберите только что созданный набор ресурсов для хранилища и нажмите **Создать сервис**.

Сервис хранилища создан в веб-интерфейсе KUMA и отображается в разделе **Ресурсы** → **Активные сервисы**. Теперь сервисы хранилища необходимо установить на каждом узле кластера ClickHouse, используя идентификатор сервиса.

Установка хранилища в сетевой инфраструктуре KUMA

Чтобы создать хранилище:

1. Войдите на сервер, на котором вы хотите установить сервис.

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/.

   Убедитесь, что файл kuma имеет достаточные права для запуска.

4. Выполните следующую команду:

   ```
   sudo /opt/kaspersky/kuma/kuma storage --core https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса KUMA> --install
   ```

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

При развертывании нескольких сервисов KUMA на одном хосте в процессе установки необходимо указать уникальные порты для каждого компонента с помощью параметра `--api.port <порт>`. По умолчанию используется значение `--api.port 7221`.

5. Повторите шаги 1–2 для каждого узла хранилища.

Хранилище установлено.

Создание коррелятора

Коррелятор состоит из двух частей: одна часть создается внутри веб-интерфейса KUMA, а другая устанавливается на сервере сетевой инфраструктуры, предназначенном для обработки событий.

Действия в веб-интерфейсе KUMA

Создание коррелятора в веб-интерфейсе KUMA производится с помощью мастера установки, в процессе выполнения которого необходимые ресурсы объединяются в набор ресурсов для коррелятора, а по завершении мастера на основе этого набора ресурсов автоматически создается и сам сервис.

Чтобы создать коррелятор в веб-интерфейсе KUMA,

запустите мастер установки коррелятора:

- В веб-интерфейсе KUMA в разделе **Ресурсы** нажмите **Создать коррелятор**.
- В веб-интерфейсе KUMA в разделе **Ресурсы** → **Корреляторы** нажмите **Добавить коррелятор**.

В результате выполнения шагов мастера в веб-интерфейсе KUMA создается сервис коррелятора.

В набор ресурсов для коррелятора объединяются следующие ресурсы:

- правила корреляции;
- правила обогащения (при необходимости);
- правила реагирования (при необходимости);
- точки назначения (как правило, одна: задается отправка событий в хранилище).

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

Действия на сервере коррелятора KUMA

При установке коррелятора на сервер, предназначенный для обработки событий, на сервере требуется запустить команду, которая отображается на последнем шаге мастера установки. При установке необходимо указать идентификатор, автоматически присвоенный сервису в веб-интерфейсе KUMA, а также используемый для связи порт.

Проверка установки

После создания коррелятора рекомендуется убедиться в правильности его работы.

Запуск мастера установки коррелятора

Чтобы запустить мастер установки коррелятора:

- В веб-интерфейсе KUMA в разделе **Ресурсы** нажмите **Добавить коррелятор**.
- В веб-интерфейсе KUMA в разделе **Ресурсы** → **Корреляторы** нажмите **Добавить коррелятор**.

Следуйте указаниям мастера.

Шаги мастера, кроме первого и последнего, можно выполнять в произвольном порядке. Переключаться между шагами можно с помощью кнопок **Вперед** и **Назад**, а также нажимая на названия шагов в левой части окна.

По завершении мастера в веб-интерфейсе KUMA в разделе **Ресурсы** → **Корреляторы** создается набор ресурсов для коррелятора, а в разделе **Ресурсы** → **Активные сервисы** добавляется сервис коррелятора.

Шаг 1. Общие параметры коррелятора

Это обязательный шаг мастера установки. На этом шаге указываются основные параметры коррелятора: название и тенант, которому он будет принадлежать.

Чтобы задать основные параметры коррелятора:

- В поле **Название** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов Юникода.

- В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать коррелятор. От выбора тенанта зависит, какие ресурсы будут доступны при его создании.

  > Если вы с какого-либо последующего шага мастера установки вернетесь в это окно и выберите другого тенанта, вам потребуется вручную изменить все ресурсы, которые вы успели добавить в сервис. В сервис можно добавлять только ресурсы из выбранного и общего тенантов.

- В поле **Рабочие процессы** при необходимости укажите количество процессов, которые может одновременно запускать сервис. По умолчанию количество рабочих процессов соответствует количеству vCPU сервера, на котором установлен сервис.

- При необходимости с помощью раскрывающегося списка **Отладка** включите логирование операций сервиса.

- В поле **Описание** можно добавить описание сервиса: до 256 символов Юникода.

Основные параметры коррелятора заданы. Перейдите к следующему шагу мастера установки.

Шаг 2. Глобальные переменные

Если для покрытия каких-то сценариев обеспечения безопасности недостаточно отслеживания значений в полях событий, активных листах или словарях, вы можете воспользоваться глобальными и локальными переменными. С их помощью можно выполнять различные действия над поступающими в корреляторы значениями, реализуя сложную логику выявления угроз. Переменным можно присвоить какую-либо функцию, а затем обращаться к ним из правил корреляции, как к обычным полям событий, получая в ответ результат срабатывания функции.

Чтобы добавить глобальную переменную в корреляторе,

Нажмите на кнопку **Добавить переменную** и укажите следующие параметры:

- В окне **Переменная** введите название переменной.

  Требования к наименованию переменных

  > - Должно быть уникально в рамках коррелятора.
  > - Должно содержать от 1 до 128 символов Юникода.
  > - Не может начинаться с символа $.

- Должно быть написано в camelCase или CamelCase.

- В окне **Значение** введите функцию переменной.

  Описание функций переменных.

Глобальная переменная добавлена. К ней можно обращаться из правил корреляции, добавляя перед названием переменной символ $. Переменных может быть несколько. Добавленные переменные можно изменить или удалить с помощью значка ✕.

Перейдите к следующему шагу мастера установки.

Шаг 3. Корреляция

Это необязательный, но рекомендуемый шаг мастера установки. В закладке мастера установки **Корреляция** следует выбрать или создать ресурсы правил корреляции. В этих ресурсах задаются последовательности событий, указывающих на происшествия, связанные с безопасностью: при обнаружении таких последовательностей коррелятор создает корреляционное событие и алерт.

Если вы добавили в коррелятор глобальные переменные, все добавленные правила корреляции могут к ним обращаться.

Добавленные в набор ресурсов для коррелятора правила корреляции отображаются в таблице со следующими столбцами:

- **Правила корреляции** – название ресурса правила корреляции.

- **Тип** – тип правила корреляции: **standard**, **simple**, **operational**. Таблицу можно отфильтровать по значениям этого столбца, нажав на его заголовок и выбрав нужные значения.

- **Действия** – перечень действий, которые совершит коррелятор при срабатывании правила корреляции. Действия указываются в параметрах правила корреляции. Таблицу можно отфильтровать по значениям этого столбца, нажав на его заголовок и выбрав нужные значения.

  Доступные значения:

  - **В дальнейшую обработку** – корреляционные события, создаваемые этим правилом корреляции, передается в другие ресурсы коррелятора: в обогащение, в правиле реагирования, а затем в другие сервисы KUMA.

  - **Изменение активного листа** – правило корреляции вносит изменения в активные листы.

- **В коррелятор** – корреляционное событие отправляется на повторную обработку в то же правило корреляции.
- **Изменение категории актива** – корреляционное правило изменяет категории активов.
- **Обогащение событий** – в корреляционном правиле настроено обогащение корреляционных событий.
- **Не создавать алерт** – когда в результате срабатывания правила корреляции создается корреляционное событие, одновременно с ним НЕ создается алерт.
- **Используются общие ресурсы** – правило корреляции или ресурсы, которые задействованы в правиле корреляции, расположены в общем тенанте.

С помощью поля **Поиск** можно искать правила корреляции. Добавленные правила корреляции можно убрать из набора ресурсов, выбрав нужные правила и нажав **Удалить**.

При выборе правила корреляции открывается окно с его параметрами: параметры ресурса можно изменить и сохранить с помощью кнопки **Сохранить**. При нажатии в этом окне на кнопку **Удалить**, правило корреляции отвязывается от набора ресурсов.

С помощью кнопок **Поднять** и **Опустить** можно изменять положение выбранных правил корреляции в таблице правил корреляции, что отражается на последовательности их выполнения при обработке событий. С помощью кнопки **Поднять operational-правила** можно переместить правила корреляции типа **operational** в начало списка правил корреляции.

Чтобы привязать к набору ресурсов для коррелятора существующие правила корреляции:

1. Нажмите **Привязать**.

   Откроется окно выбора ресурсов.

2. Выберите нужные правила корреляции и нажмите **OK**.

   Правила корреляции привязаны к набору ресурсов для коррелятора и отображаются в таблице правил.

Чтобы создать в наборе ресурсов для коррелятора новое правило корреляции:

1. Нажмите **Добавить**.

   Откроется окно создания правила корреляции.

2. Укажите параметры правила корреляции и нажмите **Сохранить**.

Правило корреляции создано и привязано к набору ресурсов для коррелятора. Оно отображается в таблице правил корреляции, а также в списке ресурсов в разделе **Ресурсы** → **Правила корреляции**.

Перейдите к следующему шагу мастера установки.

Шаг 4. Обогащение

Это необязательный шаг мастера установки. В закладке мастера установки **Обогащение** можно выбрать или создать ресурс правил обогащения с указанием, какими данными и из каких источников следует дополнить создаваемые коррелятором корреляционные события. Правил обогащения может быть несколько. Их можно добавить с помощью кнопки **Добавить** или удалить с помощью кнопки ✕.

Чтобы добавить в набор ресурсов существующее правило обогащения:

1. Нажмите **Добавить**.

   Откроется блок параметров правила обогащения.

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

Правило обогащения добавлено в набор ресурсов для коррелятора.

Чтобы создать в наборе ресурсов новое правило обогащения:

1. Нажмите **Добавить**.

   Откроется блок параметров правила обогащения.

2. В раскрывающемся списке **Правило обогащения** выберите **Создать**.

3. В раскрывающемся списке **Тип источника данных** выберите, откуда будут поступать данные для обогащения, и заполните относящиеся к нему параметры:

   - константа

     Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

     - В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов Юникода. Если оставить это поле пустым, существующее значение поля события будет удалено.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

- словарь

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

  При выборе этого типа в раскрывающемся списке **Название словаря** необходимо выбрать словарь, из которого будут браться значения, а в блоке параметров **Ключевые поля** с помощью кнопки **Добавить поле** требуется выбрать поля события, значения которых будут использоваться для выбора записи словаря.

- событие

  Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

  - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.
  - В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.
  - В блоке параметров **Преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA. Тип преобразования можно выбрать в раскрывающемся списке. С помощью кнопок **Добавить преобразование** и **Удалить** можно добавить или удалить преобразование. Порядок преобразований имеет значение.

    Доступные преобразования

    Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

    Доступные преобразования:

    - **lower** – используется для перевода всех символов значения в нижний регистр
    - **upper** – используется для перевода всех символов значения в верхний регистр

- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.

- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:

  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.

- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.

  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна

использоваться вместо заменяемой последовательности символов.

- **decodeHexString** – используется для конвертации HEX-строки в текст.
- **decodeBase64String** – используется для конвертации Base64-строки в текст.
- **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

- шаблон

Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

- В поле **Шаблон** поместите шаблон Go.

  Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт.

  Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

- dns

Этот тип обогащения используется для отправки запросов на DNS-сервер частной сети для преобразования IP-адресов в доменные имена или наоборот.

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`.

- **Рабочие процессы** – максимальное количество запросов в один момент времени. Значение по умолчанию: `1`.

- **Количество задач** – максимальное количество одновременно выполняемых запросов. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

- **Срок жизни кеша** – время жизни значений, хранящихся в кеше. Значение по умолчанию: `60`.

- **Кеш отключен** – с помощью этого раскрывающегося списка можно включить или отключить кеширование. По умолчанию кеширование включено.

- cybertrace

  Этот тип обогащения используется для добавления в поля события сведений из потоков данных CyberTrace.

  Доступные параметры:

  - **URL** (обязательно) – в этом поле можно указать URL сервера CyberTrace, которому вы хотите отправлять запросы.

  - **Количество подключений** – максимальное количество подключений к серверу CyberTrace, которые может одновременно установить KUMA. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

  - **Запросов в секунду** – максимальное количество запросов к серверу в секунду. Значение по умолчанию: `1000`.

  - **Время ожидания** – время ожидания отклика от сервера CyberTrace в секундах. Значение по умолчанию: `30`.

  - **Сопоставление** (обязательно) – этот блок параметров содержит таблицу сопоставления полей событий KUMA с типами индикаторов CyberTrace. В столбце **Поле KUMA** указаны названия полей событий KUMA, а в столбце **Индикатор CyberTrace** указаны типы индикаторов CyberTrace.

    Доступные типы индикаторов CyberTrace:

    - ip

    - url

- hash

В таблице сопоставления требуется указать как минимум одну строку. С помощью кнопки **Добавить строку** можно добавить строку, а с помощью кнопки ✕ – удалить.

- часовой пояс

Этот тип обогащения используется в коллекторах и корреляторах для присваивания событию определенного часового пояса. Сведения о часовом поясе могут пригодиться при поиске событий, случившихся в нетипичное время, например ночью.

При выборе этого типа обогащения в раскрывающемся списке **Часовой пояс** необходимо выбрать требуемую временную зону.

> Убедитесь, что требуемый часовой пояс установлен на сервере сервиса, использующего обогащение. Например, это можно сделать с помощью команды `timedatectl list-timezones`, которая показывает все установленные на сервере часовые пояса. Подробнее об установке часовых поясов смотрите в документации используемой вами операционной системы.

При обогащении события в поле события DeviceTimeZone записывается смещение времени выбранного часового пояса относительно всемирного координированного времени (UTC) в формате `+-чч:мм`. Например, если выбрать временную зону **Asia/Yekaterinburg** в поле DeviceTimeZone будет записано значение `+05:00`. Если в обогащаемом событии есть значение поля DeviceTimeZone, оно будет перезаписано.

По умолчанию, если в обрабатываемом событии не указан часовой пояс и не настроены правила обогащения по часовому поясу, событию присваивается часовой пояс сервера, на котором установлен сервис (коллектор или коррелятор), обрабатывающий событие. При изменении времени сервера сервис необходимо перезапустить.

Допустимые форматы времени при обогащении поля DeviceTimeZone

> При обработке в коллекторе поступающих "сырых" событий следующие форматы времени могут быть автоматически приведены к формату +-чч:мм:

Формат времени в обрабатываемом событии	Пример
+-чч:мм	-07:00
+-ччмм	-0700
+-чч	-07

Если формат даты в поле `DeviceTimeZone` отличается от указанных выше, при обогащении события сведениями о часовом поясе в поле записывается часовой пояс серверного времени коллектора. Вы можете создать особые правила нормализации для нестандартных форматов времени.

4. С помощью раскрывающегося списка **Отладка** укажите, следует ли включить логирование операций сервиса. По умолчанию логирование выключено.

5. В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом правила обогащения. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

   Создание фильтра в ресурсах

   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. Название должно содержать от 1 до 128 символов Юникода.

   4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

c. В раскрывающемся списке **оператор** выберите нужный вам 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).
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

В набор ресурсов для коррелятора добавлено новое правило обогащения.

Перейдите к следующему шагу мастера установки.

Шаг 5. Правила реагирования

Это необязательный шаг мастера установки. В закладке мастера установки **Правила реагирования** можно выбрать или создать ресурс правил реагирования с указанием, какие действия требуется выполнить при срабатывании правил корреляции. Правил реагирования может быть несколько. Их можно добавить с помощью кнопки **Добавить** или удалить с помощью кнопки ✕.

Чтобы добавить в набор ресурсов существующее правило реагирования:

1. Нажмите **Добавить**.

   Откроется окно с параметрами правила реагирования.

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

Правило реагирования добавлено в набор ресурсов для коррелятора.

Чтобы создать в наборе ресурсов новое правило реагирования:

1. Нажмите **Добавить**.

   Откроется окно с параметрами правила реагирования.

2. В раскрывающемся списке **Правило реагирования** выберите **Создать**.

3. В раскрывающемся списке **Тип** выберите тип правила реагирования и заполните относящиеся к нему параметры:

   - **Реагирование через KSC** – правила реагирования для автоматического запуска задач на активах Kaspersky Security Center. Например, вы можете настроить автоматический запуск антивирусной проверки или обновление базы данных.

     Автоматический запуск задач выполняется при интеграции KUMA с Kaspersky Security Center. Задачи запускаются только на активах, импортированных из Kaspersky Security Center.

     Параметры реагирования ?

     - **Задача Kaspersky Security Center** (обязательно) – название задачи Kaspersky Security Center, которую требуется запустить. Задачи должны быть созданы заранее, и их названия должны начинаться со слова "`KUMA `". Например, "`KUMA antivirus check`".

       Типы задач Kaspersky Security Center, которые можно запустить с помощью KUMA:

       - обновление;
       - поиск вирусов.

- **Поле события** (обязательно) – определяет поле события для актива, для которого нужно запустить задачу Kaspersky Security Center. Возможные значения:
  - SourceAssetID
  - DestinationAssetID
  - DeviceAssetID

  Для отправки запросов в Kaspersky Security Center необходимо убедиться, что Kaspersky Security Center доступен по протоколу UDP.

- **Запуск скрипта** – правила реагирования для автоматического запуска скрипта. Например, вы можете создать скрипт с командами, которые требуется выполнить на сервере KUMA при обнаружении выбранных событий.

  Файл скрипта хранится на сервере, где установлен сервис коррелятора, использующий ресурс реагирования: /opt/kaspersky/kuma/correlator/<Идентификатор коррелятора>/scripts.

  Пользователю `kuma` этого сервера требуются права на запуск скрипта.

  Параметры реагирования

  - **Время ожидания** – количество секунд, которое выждет система, прежде чем запустить скрипт.
  - **Название скрипта** (обязательно) – имя файла скрипта.

    Если ресурс реагирования прикреплен к сервису коррелятора, однако в папке /opt/kaspersky/kuma/correlator/<Идентификатор коррелятора>/scripts файл скрипта отсутствует, коррелятор не будет работать.
  - **Аргументы скрипта** – параметры или значения полей событий, которые необходимо передать скрипту.

    Если в скрипте производятся какие-либо действия с файлами, к ним следует указывать абсолютный путь.

    Параметры можно обрамлять кавычками (").

Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это имя поля события, значение которого должно быть передано в скрипт.

Пример: `-n "\"usr\": {{.SourceUserName}}"`

- **Реагирование через KEDR** – правила реагирования для автоматического создания правил запрета, запуска сетевой изоляции или запуска программы на активах Kaspersky Endpoint Detection and Response и Kaspersky Security Center.

  Автоматические действия по реагированию выполняются при интеграции KUMA с Kaspersky Endpoint Detection and Response.

  Параметры реагирования

  - **Поле события** (обязательно) – поле события с активом, для которого нужно выполнить действия по реагированию. Возможные значения:
    - SourceAssetID.
    - DestinationAssetID.
    - DeviceAssetID.
  - **Тип задачи** – действие по реагированию, которое требуется выполнить при получении данных, соответствующих фильтру. Доступны следующие типы действий по реагированию:
    - Включить сетевую изоляцию.

      При выборе этого типа реагирования вам нужно задать значения для следующих параметров:

      - **Срок действия изоляции** – количество часов, в течение которых будет действовать сетевая изоляция актива. Вы можете указать от 1 до 9999 часов.

        При необходимости вы можете **добавить исключение для сетевой изоляции**.

        Чтобы добавить исключение для сетевой изоляции:

        a. Нажмите на кнопку **Добавить исключение**.

        b. Выберите направление сетевого трафика, которое не должно быть заблокировано:

- Входящее.
- Исходящее.
- Входящее/Исходящее.

c. В поле **IP актива** введите IP-адрес актива, сетевой трафик которого не должен быть заблокирован.

d. Если вы выбрали **Входящее** или **Исходящее**, укажите порты подключения в полях **Удаленные порты** и **Локальные порты**.

e. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить исключение** и повторите действия по заполнению полей **Направление трафика**, **IP актива**, **Удаленные порты** и **Локальные порты**.

f. Если вы хотите удалить исключение, нажмите на кнопку **Удалить** под нужным вам исключением.

При добавлении исключений в правило сетей изоляции Kaspersky Endpoint Detection and Response может некорректно отображать значения портов в информации о правиле. Это не влияет на работоспособность программы. Подробнее о просмотре правила сетевой изоляции см. в *справке Kaspersky Anti Targeted Attack Platform*.

- Выключить сетевую изоляцию.
- Добавить правило запрета.

  При выборе этого типа реагирования вам нужно задать значения для следующих параметров:

  - **Поля события для получения хеш-суммы** – поля событий, из которых KUMA извлекает SHA256- или MD5-хеши файлов, запуск которых требуется запретить.

    Выбранные поля событий, а также значения, выбранные в **Поле события**, требуется добавить в наследуемые поля правила корреляции.

- **Хеш файла №1** – SHA256- или MD5-хеш файла, который требуется запретить.

Хотя бы одно из указанных выше полей должно быть заполнено.

- Удалить правило запрета.
- Запустить программу.

  При выборе этого типа реагирования вам нужно задать значения для следующих параметров:

  - **Путь к файлу** – путь к файлу процесса, который вы хотите запустить.
  - **Аргументы командной строки** – параметры, с которыми вы хотите запустить файл.
  - **Текущая директория** – директория, в которой на момент запуска располагается файл.

  При срабатывании правила реагирования для пользователей с ролью главный администратор в разделе **Диспетчер задач** веб-интерфейса программы отобразится задача **Запустить программу**. В столбце **Создал** таблицы задач для этой задачи отображается **Задача по расписанию**. Вы можете просмотреть результат выполнения задачи.

  Все перечисленные операции выполняются на активах с Kaspersky Endpoint Agent для Windows. На активах с Kaspersky Endpoint Agent для Linux выполняется только запуск программы.

  На программном уровне возможность создания правил запрета и сетевой изоляции для активов с Kaspersky Endpoint Agent для Linux не ограничена. KUMA и Kaspersky Endpoint Detection and Response не уведомляют о неуспешном применении этих правил.

- **Реагирование через KICS for Networks** – правила реагирования для автоматического запуска задач в на активах KICS for Networks. Например, изменить статус актива в KICS for Networks.

Автоматический запуск задач выполняется при интеграции KUMA с KICS for Networks.

Параметры реагирования

- **Поле события** (обязательно) – поле события с активом, для которого нужно выполнить действия по реагированию. Возможные значения:
  - SourceAssetID.
  - DestinationAssetID.
  - DeviceAssetID.
- **Задача KICS for Networks** – действие по реагированию, которое требуется выполнить при получении данных, соответствующих фильтру. Доступны следующие типы действий по реагированию:
  - **Изменить статус актива на Разрешенное**.
  - **Изменить статус актива на Неразрешенное**.

  При срабатывании правила реагирования из KUMA в KICS for Networks будет отправлен API-запрос на изменение статуса указанного устройства на **Разрешенное** или **Неразрешенное**.

- **Реагирование через Active Directory** – правила реагирования для изменения прав пользователей Active Directory. Например, блокировать пользователя.

  Запуск задач выполняется при интеграции с Active Directory.

  Параметры реагирования

  - **Источник идентификатора аккаунта** – поле события, откуда будет взято значение идентификатора учетной записи Active Directory. Возможные значения:
    - SourceAccountID
    - DestinationAccountID
  - **Команда Active Directory** – команда, которая будет применяться к учетной записи при срабатывании правила реагирования. Доступные значения:
    - Добавить учетную запись в группу

- Удалить учетную запись из группы
- Сбросить пароль учетной записи
- Блокировать учетную запись

- В поле **Рабочие процессы** укажите количество процессов, которые сервис может запускать одновременно.

  По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.

  Поле не обязательно для заполнения.

1. В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом правила реагирования. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

   Создание фильтра в ресурсах

   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. Название должно содержать от 1 до 128 символов Юникода.
   4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

c. В раскрывающемся списке **оператор** выберите нужный вам 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).
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

В набор ресурсов для коррелятора добавлено новое правило реагирования.

Перейдите к следующему шагу мастера установки.

Шаг 6. Маршрутизация

Это необязательный шаг мастера установки. В закладке мастера установки **Маршрутизация** можно выбрать или создать ресурсы точек назначения, в параметрах которых будут определено, куда следует перенаправлять созданные коррелятором события. Обычно события от коррелятора перенаправляются в хранилище для хранения и для возможности просматривать их позднее. При необходимости события можно отправлять в другие места. Точек назначения может быть несколько.

Чтобы добавить в набор ресурсов коррелятора существующую точку назначения:

1. В раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, которую вы хотите добавить:

   - Выберите **Хранилище**, если хотите настроить отправку обработанных событий в хранилище.

   - Выберите **Коррелятор**, если хотите настроить отправку обработанных событий в коррелятор.

   - Выберите **Другое**, если хотите отправлять события в другие места.

     > К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях программы.

   Открывается окно **Добавить точку назначения**, где можно указать параметры пересылки событий.

2. В раскрывающемся списке **Точка назначения** выберите нужную точку назначения.

   Название окна меняется на **Изменить точку назначения**, параметры выбранного ресурса отображаются в окне. Ресурс можно открыть для редактирования в новой вкладке браузера с помощью кнопки ↗.

3. Нажмите **Сохранить**.

Выбранная точка назначения отображается в закладке мастера установки. Точку назначения можно удалить из набора ресурсов, выбрав ее и в открывшемся окне нажав **Удалить**.

Чтобы добавить в набор ресурсов коррелятора новую точку назначения:

1. В раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, которую вы хотите добавить:

   - Выберите **Хранилище**, если хотите настроить отправку обработанных событий в хранилище.

- Выберите **Коррелятор**, если хотите настроить отправку обработанных событий в коррелятор.

- Выберите **Другое**, если хотите отправлять события в другие места.

  > К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях программы.

Открывается окно **Добавить точку назначения**, где можно указать параметры пересылки событий.

2. Укажите параметры в закладке **Основные параметры**:

   - В раскрывающемся списке **Точка назначения** выберите **Создать**.

   - Введите в поле **Название** уникальное имя для точки назначения. Название должно содержать от 1 до 128 символов Юникода.

   - С помощью переключателя **Выключено**, выберите, будут ли события отправляться в эту точку назначения. По умолчанию отправка событий включена.

   - Выберите **Тип** точки назначения:

     - Выберите **storage**, если хотите настроить отправку обработанных событий в хранилище.

     - Выберите **correlator**, если хотите настроить отправку обработанных событий в коррелятор.

     - Выберите **nats**, **tcp**, **http**, **kafka** или **file**, если хотите настроить отправку событий в другие места.

   - Укажите **URL**, куда следует отправлять события, в формате hostname:<порт API>.

     Для всех типов, кроме **nats** и **file** с помощью кнопки **URL** можно указать несколько адресов отправки.

   - Для типов **nats** и **kafka** в поле **Топик** укажите, в какой топик должны записываться данные. Топик должен содержать символы Юникода. Топик для Kafka имеет ограничение длины в 255 символов.

3. При необходимости укажите параметры в закладке **Дополнительные параметры**. Доступные параметры зависят от выбранного типа точки назначения:

- **Сжатие** – раскрывающийся список, в котором можно включить сжатие Snappy. По умолчанию сжатие **Выключено**.

- **Прокси-сервер** – раскрывающийся список для выбора ресурса прокси-сервера.

- **Размер буфера** – поле, в котором можно указать размер буфера (в байтах) для ресурса точки назначения. Значение по умолчанию: 1 МБ; максимальное: 64 МБ.

- **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. Значение по умолчанию: `30`.

- **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.

- **Идентификатор кластера** – идентификатор кластера NATS.

- **Режим TLS** – раскрывающийся список, в котором можно указать условия использование шифрования TLS:

  - **Выключено** (по умолчанию) – не использовать шифрование TLS.

  - **Включено** – использовать шифрование, но без верификации.

  - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

  При использовании TLS невозможно указать IP-адрес в качестве URL.

- **Политика выбора URL** – раскрывающийся список, в котором можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько:

  - **Любой** – события отправляются в один из доступных URL до тех пор, пока этот URL принимает события. При разрыве связи (например, при отключении принимающего узла) для отправки событий будет выбран другой URL.

  - **Сначала первый** – события отправляются в первый URL из списка добавленных адресов. Если он становится недоступен, события отправляются в следующий по очереди доступный узел. Когда первый URL снова становится доступен, события снова начинаются отправляться в него.

  - **По очереди** – пакеты с событиями по очереди отправляться в доступные URL из списка. Поскольку пакеты отправляются или при переполнении буфера точки

назначения, или при срабатывании таймера очистки буфера, эта политика выбора URL не гарантирует равное распределение событий по точкам назначения.

- **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.

- **Путь** – путь к файлу, если выбран тип точки назначения **file**.

- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.

- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

- Вы можете установить проверки работоспособности, используя поля **Путь проверки работоспособности** и **Ожидание проверки работоспособности**. Вы также можете отключить проверку работоспособности, установив флажок **Проверка работоспособности отключена**.

- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.

- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах

  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. Название должно содержать от 1 до 128 символов Юникода.

4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам 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).

- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

4. Нажмите **Сохранить**.

   Созданная точка назначения отображается в закладке мастера установки. Точку назначения можно удалить из набора ресурсов, выбрав ее и в открывшемся окне нажав **Удалить**.

Перейдите к следующему шагу мастера установки.

Шаг 7. Проверка параметров

Это обязательный и заключительный шаг мастера установки. На этом шаге в KUMA создается набор ресурсов для сервиса и на основе этого набора автоматически создаются сервисы:

- Набор ресурсов для коррелятора отображается в разделе **Ресурсы** → **Корреляторы**. Его можно использовать для создания новых сервисов коррелятора. При изменении этого набора ресурсов все сервисы, которые работают на его основе, будут использовать новые параметры, если сервисы перезапустить: для этого можно использовать кнопки **Сохранить и перезапустить сервисы** и **Сохранить и обновить параметры сервисов**.

  Набор ресурсов можно изменять, копировать, переносить из папки в папку, удалять, импортировать и экспортировать, как другие ресурсы.

- Сервисы отображаются в разделе **Ресурсы** → **Активные сервисы**. Созданные с помощью мастера установки сервисы выполняют функции внутри программы KUMA – для связи с внешними частями сетевой инфраструктуры необходимо установить аналогичные внешние сервисы на предназначенных для них серверах и устройствах. Например, внешний сервис коррелятора следует установить на сервере, предназначенном для обработки событий; внешние сервисы хранилища – на серверах с развернутой службой ClickHouse; внешние сервисы агентов – на тех устройствах Windows, где требуется получать и откуда необходимо пересылать события Windows.

Чтобы завершить мастер установки:

1. Нажмите **Сохранить и создать сервис**.

   В закладке мастера установки **Проверка параметров** отображается таблица сервисов, созданных на основе набора ресурсов, выбранных в мастере установки. В нижней части окна отображаются примеры команд, с помощью которых необходимо установить внешние аналоги этих сервисов на предназначенные для них серверы и устройства.

   Например:

/opt/kaspersky/kuma/kuma correlator --core https://kuma-example:<порт, используемый для связи с Ядром KUMA> --id <идентификатор сервиса> --api.port <порт, используемый для связи с сервисом> --install

> Файл kuma можно найти внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

Порт для связи с Ядром KUMA, идентификатор сервиса и порт для связи с сервисом добавляются в команду автоматически. Также следует убедиться в сетевой связности системы KUMA и при необходимости открыть используемые ее компонентами порты.

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

Сервис коррелятора создан в KUMA. Теперь аналогичный сервис необходимо установить на сервере, предназначенном для обработки событий.

Установка коррелятора в сетевой инфраструктуре KUMA

Коррелятор состоит из двух частей: одна часть создается внутри веб-интерфейса KUMA, а другая устанавливается на сервере сетевой инфраструктуры, предназначенном для обработки событий. В сетевой инфраструктуре устанавливается вторая часть коррелятора.

Чтобы установить коррелятор:

1. Войдите на сервер, на котором вы хотите установить сервис.

2. 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/.

> Убедитесь, что файл kuma имеет достаточные права для запуска.

4. Выполните следующую команду:

```
sudo /opt/kaspersky/kuma/kuma correlator --core https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса KUMA> --api.port <порт, используемый для связи с устанавливаемым компонентом> --install
```

Пример: `sudo /opt/kaspersky/kuma/kuma correlator --core https://kuma.example.com:7210 --id XXXX --api.port YYYY --install`

Команду, с помощью которой можно установить коррелятор на сервере, можно скопировать на последнем шаге мастера установщика. В ней автоматически указывается адрес и порт сервера Ядра KUMA, идентификатор устанавливаемого коррелятора, а также порт, который этот коррелятор использует для связи. Перед установкой необходимо убедиться в сетевой связности компонентов KUMA.

При развертывании нескольких сервисов KUMA на одном хосте в процессе установки необходимо указать уникальные порты для каждого компонента с помощью параметра `--api.port <порт>`. По умолчанию используется значение `--api.port 7221`.

Коррелятор установлен. С его помощью можно анализировать события на предмет угроз.

Проверка правильности установки коррелятора

Проверить готовность коррелятора к получению событий можно следующим образом:

1. В веб-интерфейсе KUMA откройте раздел **Ресурсы** → **Активные сервисы**.
2. Убедитесь, что у установленного вами коррелятора зеленый статус.

Если в коррелятор поступают события, удовлетворяющие условиям фильтра правил корреляции, на закладке событий будут отображаться события с параметрами `DeviceVendor=Kaspersky` и `DeviceProduct=KUMA`. Название сработавшего правила корреляции будет отображаться как название этих корреляционных событий.

Если корреляционные события не найдены

Можно создать более простую версию правила корреляции, чтобы найти возможные ошибки. Используйте правило корреляции типа **simple** и одно действие **Отправить событие на дальнейшую обработку**. Рекомендуется создать фильтр для поиска событий, которые KUMA получает регулярно.

При обновлении, добавлении или удалении правила корреляции требуется обновить параметры коррелятора.

Когда вы закончите тестирование правил корреляции, необходимо удалить все тестовые и временные правила корреляции из KUMA и обновить параметры коррелятора.

Создание коллектора

Коллектор состоит из двух частей: одна часть создается внутри веб-интерфейса KUMA, а другая устанавливается на сервере сетевой инфраструктуры, предназначенном для получения событий.

Действия в веб-интерфейсе KUMA

Создание коллектора в веб-интерфейсе KUMA производится с помощью мастера установки, в процессе выполнения которого необходимые ресурсы объединяются в набор ресурсов для коллектора, а по завершении мастера на основе этого набора ресурсов автоматически создается и сам сервис.

Чтобы создать коллектор в веб-интерфейсе KUMA,

Запустите мастер установки коллектора:

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

В результате выполнения шагов мастера в веб-интерфейсе KUMA создается сервис коллектора.

В набор ресурсов для коллектора объединяются следующие ресурсы:

- коннектор;
- нормализатор (как минимум один);
- фильтры (при необходимости);
- правила агрегации (при необходимости);
- правила обогащения (при необходимости);
- точки назначения (как правило, две: задается отправка событий в коррелятор и хранилище).

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

Действия на сервере коллектора KUMA

При установке коллектора на сервер, предназначенный для получения событий, требуется в запустить команду, которая отображается на последнем шаге мастера установки. При установке необходимо указать идентификатор, автоматически присвоенный сервису в веб-интерфейсе KUMA, а также используемый для связи порт.

Проверка установки

После создания коллектора рекомендуется убедиться в правильности его работы.

Запуск мастера установки коллектора

Коллектор состоит из двух частей: одна часть создается внутри веб-интерфейса KUMA, а другая устанавливается на сервере сетевой инфраструктуры, предназначенной для получения событий. В мастере установки создается первая часть коллектора.

Чтобы запустить мастер установки коллектора:

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

Следуйте указаниям мастера.

Мастер Подключения источников событий

Шаги мастера, кроме первого и последнего, можно выполнять в произвольном порядке. Переключаться между шагами можно с помощью кнопок **Вперед** и **Назад**, а также нажимая на названия шагов в левой части окна.

По завершении мастера в веб-интерфейсе KUMA в разделе **Ресурсы** → **Коллекторы** создается набор ресурсов для коллектора, а в разделе **Ресурсы** → **Активные сервисы** добавляется сервис коллектора.

Шаг 1. Подключение источников событий

Это обязательный шаг мастера установки. На этом шаге указываются основные параметры коллектора: название и тенант, которому он будет принадлежать.

Чтобы задать основные параметры коллектора:

1. В поле **Название коллектора** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов Юникода.

   > При создании некоторых типов коллекторов вместе с ними автоматически создаются агенты, имеющие название "agent: <Название коллектора>, auto created". Если такой агент уже создавался ранее и не был удален, то коллектор с названием <Название коллектора> невозможно будет создать. В такой ситуации необходимо или указать другое название коллектора, или удалить ранее созданный агент.

2. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать коллектор. От выбора тенанта зависит, какие ресурсы будут доступны при его создании.

   > Если вы с какого-либо последующего шага мастера установки вернетесь в это окно и выберите другой тенант, вам потребуется вручную изменить все ресурсы, которые вы успели добавить в сервис. В сервис можно добавлять только ресурсы из выбранного и общего тенантов.

3. В поле **Рабочие процессы** при необходимости укажите количество процессов, которые может одновременно запускать сервис. По умолчанию количество рабочих процессов соответствует количеству vCPU сервера, на котором установлен сервис.

4. При необходимости с помощью раскрывающегося списка **Отладка** включите логирование операций сервиса.

5. В поле **Описание** можно добавить описание сервиса: до 256 символов Юникода.

Основные параметры коллектора будут заданы. Перейдите к следующему шагу мастера установки.

Шаг 2. Транспорт

Это обязательный шаг мастера установки. В закладке мастера установки **Транспорт** следует выбрать или создать ресурс коннектора, 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.

В закладке мастера установки **Транспорт** отобразятся параметры выбранного коннектора. Выбранный ресурс 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 в закладках **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа коннектора:
   - internal
   - tcp
   - udp
   - netflow
   - sflow
   - nats
   - kafka
   - http
   - sql
   - file
   - ftp

- nfs
- wmi
- wec
- snmp

При использовании типа коннектора **tcp** или **upd** 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** или **wec** будут автоматически созданы агенты для приема событий Windows.

Рекомендуется использовать кодировку по умолчанию (то есть UTF-8) и применять другие параметры только при получении в полях событий битых символов.

> Для настройки коллекторов KUMA на прослушивание портов с номерами меньше 1000 сервис нужного коллектора необходимо запускать с правами root. Для этого после установки коллектора в его конфигурационный файл systemd в раздел [Service] требуется дописать строку `AmbientCapabilities=CAP_NET_BIND_SERVICE`.
> Systemd-файл располагается в директории /lib/systemd/system/kuma-collector-<идентификатор коллектора>.service.

Ресурс коннектора добавлен в набор ресурсов коллектора. Созданный ресурс 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. В закладке мастера установки **Парсинг событий** следует выбрать или создать ресурс нормализатора, в параметрах которого будут определены правила преобразования "сырых" событий в нормализованные. В нормализатор можно добавить несколько правил парсинга событий, реализуя таким образом сложную логику обработки событий.

При создании нового нормализатора в мастере установки по умолчанию он будет сохранен в наборе ресурсов для коллектора и не сможет быть использован в других коллекторах. С помощью флажка **Сохранить нормализатор** вы можете создать нормализатор в виде отдельного ресурса.

Если вы, меняя параметры набора ресурсов коллектора, измените или удалите преобразования в подключенном к нему нормализаторе, правки не сохранятся, а сам ресурс нормализатора может быть поврежден. При необходимости изменить преобразования в нормализаторе, который уже является частью сервиса, вносите правки непосредственно в ресурс нормализатора в разделе веб-интерфейса **Ресурсы** → **Нормализаторы**.

Добавление нормализатора

Чтобы добавить в набор ресурсов существующий нормализатор:

1. Нажмите на кнопку **Добавить парсинг событий**.

   Откроется окно **Парсинг событий** с параметрами нормализатора и активной закладкой **Схема нормализации**.

2. В раскрывающемся списке **Нормализатор** выберите нужный нормализатор.

   В окне **Парсинг событий** отобразятся параметры выбранного нормализатора. Выбранный ресурс можно открыть для редактирования в новой вкладке браузера с помощью кнопки .

3. Нажмите **OK**.

В закладке мастера установки **Парсинг событий** отображается нормализатор в виде темного кружка. Можно нажать на кружок, чтобы открыть параметры нормализатора для редактирования. При наведении на кружок отображается значок плюса: при нажатии на него можно добавить дополнительные нормализаторы (см. ниже).

Чтобы создать новый нормализатор:

1. Выберите в раскрывающемся списке **Нормализатор** пункт **Создать**.

   Откроется окно **Парсинг событий** с параметрами нормализатора и активной закладкой **Схема нормализации**.

2. Если хотите сохранить нормализатор в качестве отдельного ресурса, установите флажок **Сохранить нормализатор**. По умолчанию флажок снят.

3. Введите в поле **Название** уникальное имя для нормализатора. Название должно содержать от 1 до 128 символов Юникода.

4. В раскрывающемся списке **Метод парсинга** выберите тип получаемых событий. В зависимости от выбора можно будет воспользоваться преднастроенными правилами сопоставления полей событий или же задать свои собственные правила. При выборе

некоторых методов парсинга могут стать доступны дополнительные параметры, требуемые для заполнения.

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 можно обращаться к полям вложенных объектов, поочередно через точку указывая названия параметров. Например, к параметру `username` из строки `"user": {"username":"system:node:example-01"}` можно обратиться с помощью запроса `user.username`.

  Файлы обрабатываются построчно. Многострочные объекты с вложенными структурами могут быть нормализованны некорректно.

- **cef**

  Этот метод парсинга используется для обработки данных в формате CEF.

  При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

- **regexp**

  Этот метод парсинга используется для создания собственных правил обработки данных в формате JSON.

  В поле блока параметров **Нормализация** необходимо добавить регулярное выражение (синтаксис RE2) с именованными группами захвата: имя группы и ее значение будут считаться полем и значением "сырого" события, которое можно будет преобразовать в поле события формата KUMA.

  Чтобы добавить правила обработки событий:

  1. Скопируйте в поле **Примеры событий** пример данных, которые вы хотите обработать. Это необязательный, но рекомендуемый шаг.

  2. В поле блока параметров **Нормализация** добавьте регулярное выражение с именованными группами захвата в синтаксисе RE2, например "(?

P<name>regexp)".

Можно добавить несколько регулярных выражений с помощью кнопки **Добавить регулярное выражение**. При необходимости удалить регулярное выражение, воспользуйтесь кнопкой ✕.

3. Нажмите на кнопку **Перенести названия полей в таблицу**.

   Имена групп захвата отображаются в столбце **Поле KUMA** таблицы **Сопоставление**. Теперь в столбце напротив каждой группы захвата можно выбрать соответствующее ей поле KUMA или, если вы именовали группы захвата в соответствии с форматом CEF, можно воспользоваться автоматическим сопоставлением CEF, поставив флажок **Использовать синтаксис CEF при нормализации**.

Правила обработки событий добавлены.

- syslog

  Этот метод парсинга используется для обработки данных в формате syslog.

  При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

- csv

  Этот метод парсинга используется для создания собственных правил обработки данных в формате CSV.

  При выборе этого метода необходимо в поле **Разделитель** указать разделитель значений в строке. В качестве разделителя допускается использовать любой однобайтовый символ ASCII.

- kv

  Этот метод парсинга используется для обработки данных в формате ключ-значение.

  При выборе этого метода необходимо указать значения в следующих обязательных полях:

  - **Разделитель пар** – укажите символ, которые будет служит разделителем пар ключ-значение. Допускается указать любое односимвольное (1 байт)

значение при условии, что символ не будет совпадать с разделителем значений.

- **Разделитель значений** – укажите символ, который будет служить разделителем между ключом и значением. Допускается указать любое односимвольное (1 байт) значение при условии, что символ не будет совпадать с разделителем пар ключ-значение.

- xml

Этот метод парсинга используется для обработки данных в формате XML, в которых каждый объект, включая его вложенные объекты, занимает одну строку файла. Файлы обрабатываются построчно.

При выборе этого метода в блоке параметров **Атрибуты XML** можно указать ключевые атрибуты, которые следует извлекать из тегов. Если в структуре XML в одном теге есть атрибуты с разными значениями, можно определить нужное значение, указав ключ к нему в столбце **Исходные данные** таблицы **Сопоставление**.

Чтобы добавить ключевые атрибуты XML,

Нажмите на кнопку **Добавить поле** и в появившемся окне укажите путь к нужному атрибуту.

Можно добавить несколько атрибутов. Атрибуты можно удалить по одному с помощью значка с крестиком или все сразу с помощью кнопки **Сбросить**.

Если ключевые атрибуты XML не указаны, при сопоставлении полей уникальный путь к значению XML будет представлен последовательностью тегов.

- netflow5

Этот метод парсинга используется для обработки данных в формате NetFlow v5.

При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

В правилах сопоставления по умолчанию для типа **netflow5** тип протокола не указывается в полях событий KUMA. При парсинге данных в формате NetFlow в закладке нормализатора **Обогащение** следует создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

- **netflow9**

  Этот метод парсинга используется для обработки данных в формате NetFlow v9.

  При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

  В правилах сопоставления по умолчанию для типа **netflow9** тип протокола не указывается в полях событий KUMA. При парсинге данных в формате NetFlow в закладке нормализатора **Обогащение** следует создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

- **ipfix**

  Этот метод парсинга используется для обработки данных в формате IPFIX.

  При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

  В правилах сопоставления по умолчанию для типа **ipfix** тип протокола не указывается в полях событий KUMA. При парсинге данных в формате NetFlow в закладке нормализатора **Обогащение** следует создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

- **sql** – этот метод становится доступным, только при использовании коннектора типа sql

Этот метод парсинга используется для обработки данных в формате SQL.

5. В раскрывающемся списке **Сохранить исходное событие** укажите, надо ли сохранять исходное "сырое" событие 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: 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 были настроены правила сопоставления (см. ниже). Данные сохраняются в поле события Extra. По умолчанию поля не сохраняются.

7. Скопируйте в поле **Примеры событий** пример данных, которые вы хотите обработать. Это необязательный, но рекомендуемый шаг.

8. В таблице **Сопоставление** настройте сопоставление полей исходного события с полями события в формате KUMA:

   a. В столбце **Исходные данные** укажите название поля исходного события, которое вы хотите преобразовать в поле события KUMA.

   Если рядом с названиями полей в столбце **Исходные данные** нажать на кнопку 🔧, откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

   Доступные преобразования ?

   Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

   Доступные преобразования:

   - **lower** – используется для перевода всех символов значения в нижний регистр

- **upper** – используется для перевода всех символов значения в верхний регистр

- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.

- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:

  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.

- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.

  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **decodeHexString** – используется для конвертации HEX-строки в текст.
- **decodeBase64String** – используется для конвертации Base64-строки в текст.
- **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

В окне **Преобразования** добавленные правила можно менять местами, перетягивая их за значок ⠿, а также удалять с помощью значка ✕.

b. В столбце **Поле KUMA** в раскрывающемся списке выберите требуемое поле события KUMA. Поля можно искать, вводя в поле их названия.

c. Если название поля события KUMA, выбранного на предыдущем шаге, начинается с `DeviceCustom*` и `Flex*`, в поле **Подпись** можно добавить уникальную пользовательскую метку.

Новые строки таблицы можно добавлять с помощью кнопки **Добавить строку**. Строки можно удалять по отдельности с помощью кнопки ✕ или все сразу с помощью кнопки **Очистить все**.

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

9. Нажмите **OK**.

В закладке мастера установки **Парсинг событий** отображается нормализатор в виде темного кружка. Можно нажать на кружок, чтобы открыть его параметры для редактирования. При наведении на кружок отображается значок плюса: при нажатии на него можно добавить дополнительные правила парсинга событий (см. ниже).

Обогащение нормализованного события дополнительными данными

В только что созданные нормализованные события можно добавлять дополнительные данные, создавая в нормализаторе правила обогащения, аналогичные правилам в ресурсах правил обогащения. Эти правила хранятся в ресурсе нормализатора, в котором они были созданы. Правил обогащения может быть несколько.

Чтобы добавить правила обогащения в нормализатор:

1. Выберите основное или дополнительное правило нормализации, а затем в открывшемся окне перейдите на закладку **Обогащение**.

2. Нажмите на кнопку **Добавить обогащение**.

   Появится блок параметров правила обогащения. Блок параметров можно удалить с помощью кнопки ✕.

3. В раскрывающемся списке **Тип источника** выберите тип обогащения. В зависимости от выбранного типа отобразятся дополнительные параметры, которые также потребуется заполнить.

   Доступные типы источников обогащения:

   - константа

     Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

     - В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов Юникода. Если оставить это поле пустым, существующее значение поля события будет удалено.
     - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

   - словарь

     Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

     При выборе этого типа в раскрывающемся списке **Название словаря** необходимо выбрать словарь, из которого будут браться значения, а в блоке параметров **Ключевые поля** с помощью кнопки **Добавить поле** требуется выбрать поля события, значения которых будут использоваться для выбора записи словаря.

   - таблица

     Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**.

При выборе этого типа обогащения в раскрывающемся списке **Название словаря** необходимо выбрать словарь, из которого будут браться значения, а в блоке параметров **Ключевые поля** с помощью кнопки **Добавить поле** требуется выбрать поля события, значения которых будут использоваться для выбора записи словаря.

Также в таблице **Сопоставление** необходимо настроить, из каких полей словаря и в какие поля события будут передаваться данные:

- В столбце **Поле словаря** необходимо выбрать поле словаря. Доступные поля зависят от выбранного ресурса словаря.
- В столбце **Поле KUMA** необходимо выбрать поле события, в которое следует записать значение. Для некоторых выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** можно задать название для помещаемых в них данных.

Новые строки в таблицу можно добавлять с помощью кнопки **Добавить элемент**. Столбцы можно удалить с помощью кнопки ✕.

- событие

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.
- В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.
- Если нажать на кнопку 🔧, откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

  Доступные преобразования

  Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

  Доступные преобразования:

  - **lower** – используется для перевода всех символов значения в нижний регистр

- **upper** – используется для перевода всех символов значения в верхний регистр

- **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.

- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:

  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.

- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.

  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.

- **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **decodeHexString** – используется для конвертации HEX-строки в текст.

- **decodeBase64String** – используется для конвертации Base64-строки в текст.

- **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

- шаблон

Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

- В поле **Шаблон** поместите шаблон Go.

  Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт.

  Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

4. В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

   Этот параметр недоступен для типа источника обогащения **таблица**.

5. Нажмите **OK**.

В нормализатор, в выбранное правило парсинга, добавлены правила обогащения событий дополнительными данными.

Создание структуры правил нормализации событий

Для реализации сложной логики обработки событий в нормализатор можно добавить более одного правила парсинга событий. События передаются между правилами парсинга в зависимости от заданных условий. Последовательность создания правил парсинга имеет значение: событие обрабатывается последовательно и его путь отображается в виде стрелочек.

Чтобы создать дополнительное правило парсинга:

1. Создайте нормализатор (см. выше).

   Созданный номрализатор отобразится в окне в виде темного кружка.

2. Наведите указатель мыши на кружок и нажмите на появившуюся кнопку со значком плюса.

3. В открывшемся окне **Дополнительный парсинг события** задайте параметры дополнительного правила парсинга события:

   - Закладка **Условия дополнительной нормализации**:

     Если вы хотите отправлять в дополнительный нормализатор только события с определенным полем, укажите его в поле **Поле, которое следует передать в нормализатор**.

     На этой закладке вы также можете определить другие условия, при выполнении которых событие будет поступать на дополнительный парсинг.

   - Закладка **Схема нормализации**:

     На этой закладке можно настроить правила обработки событий, по аналогии с параметрами основного нормализатора (см. выше). Параметр **Сохранить исходное событие** недоступен. В поле **Примеры событий** отображаются значения, указанные при создании начального нормализатора.

   - Закладка **Обогащение**:

     На этой закладке можно настроить правила обогащения событий (см. выше).

4. Нажмите **OK**.

Дополнительное правило парсинга добавлено в нормализатор и отображается в виде темного блока, на котором указаны условия, при котором это правило будет задействовано. Параметры дополнительного правила парсинга можно изменить, нажав на него. Если навести указатель мыши на дополнительное правило парсинга, отобразится кнопка со значком плюса, с помощью которой можно создать новое дополнительное правило парсинга. С помощью кнопки со значком корзины нормализатор можно удалить.

В ресурсе нормализатора в верхнем правом углу окна располагается окно поиска, с помощью которого можно искать по названию среди правил парсинга.

Перейдите к следующему шагу мастера установки.

Шаг 4. Фильтрация событий

Это необязательный шаг мастера установки. В закладке мастера установки **Фильтрация событий** можно выбрать или создать ресурс фильтра, в параметрах которого будут определены условия для отсева ненужных событий. В коллектор можно добавить более одного фильтра. Фильтры можно менять местами, перетягивая их мышью за значок ⣿, и удалять. Фильтры объединены оператором И.

Чтобы добавить в набор ресурсов коллектора существующий фильтр,

Нажмите на кнопку **Добавить фильтр** и в раскрывающемся меню **Фильтр** выберите требуемый фильтр.

Чтобы добавить в набор ресурсов коллектора новый фильтр:

1. Нажмите на кнопку **Добавить фильтр** и в раскрывающемся меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов Юникода.

4. В разделе **Условия** задайте условия, которым должны соответствовать отсеиваемые события:

   - С помощью кнопки **Добавить условие** 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).
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

- 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 ресурсы фильтров, которые выбираются в раскрывающемся списке **Выберите фильтр**. В ресурс 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. В закладке мастера установки **Агрегация событий** можно выбрать или создать ресурс правила агрегации, в параметрах которого будут определены условия для объединения однотипных событий. В коллектор можно добавить более одного правила агрегации.

Чтобы добавить в набор ресурсов коллектора существующее правило агрегации,

Нажмите на кнопку **Добавить правило агрегации** и в раскрывающемся меню **Правило агрегации** выберите требуемый ресурс.

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 ресурса правила агрегации. Название должно содержать от 1 до 128 символов Юникода.

3. В поле **Предел событий** укажите количество событий, которое должно быть получено для того, чтобы сработало правило агрегации и события были объединены. Значение по умолчанию: `100`.

4. В поле **Время ожидания событий** укажите количество секунд, в течение которых получаются события для объединения. По истечении этого срока правило агрегирования срабатывает и создается новое событие. Значение по умолчанию: `60`.

5. В разделе **Группирующие поля** с помощью кнопки **Добавить поле** выберите поля, по которым будут определяться однотипные события. Выбранные события можно удалять с помощью кнопок со значком крестика.

6. В разделе **Уникальные поля** с помощью кнопки **Добавить поле** можно выбрать поля, наличие которых выведет 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 ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

   Создание фильтра в ресурсах

   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. Название должно содержать от 1 до 128 символов Юникода.

4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

   c. В раскрывающемся списке **оператор** выберите нужный вам 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).

- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, 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. В закладке мастера установки **Обогащение событий** можно указать, какими данными и из каких источников следует дополнить обрабатываемые коллектором события. События можно обогащать данными, полученными с помощью LDAP, или посредством правил обогащения.

Обогащение с помощью LDAP

Чтобы включить обогащение с помощью LDAP:

1. Нажмите **Добавить сопоставление с учетными записями LDAP**.

   Откроется блок параметров обогащения с помощью LDAP.

2. В блоке параметров **Сопоставление с учетными записями LDAP** с помощью кнопки **Добавить домен** укажите домен учетных записей. Доменов можно указать несколько.

3. В таблице **Обогащение полей KUMA** задайте правила сопоставления полей KUMA с атрибутами LDAP:

   - В столбце **Поле KUMA** укажите поле события KUMA, данные из которого следует сравнить с атрибутом LDAP.

   - В столбце **LDAP-атрибут**, укажите атрибут, с которым необходимо сравнить поле события KUMA. Раскрывающийся список содержит стандартные атрибуты и может быть дополнен **пользовательскими атрибутами** ?.

     Перед настройкой обогащения событий с помощью пользовательских атрибутов убедитесь, что пользовательские атрибуты настроены в AD.

     Чтобы обогащать события учетными записями с помощью пользовательских атрибутов:

1. Добавьте **Пользовательские атрибуты учетных записей AD** в Параметрах подключения к LDAP.

   Невозможно добавить стандартные **Импортируемые атрибуты из AD** в качестве пользовательских. Например, если вы захотите добавить стандартны

   й атрибут

   `accountExpires` в качестве пользовательского атрибута, при сохранении параметров подключения KUMA вернет ошибку.

   Из Active Directory можно запросить следующие атрибуты учетных записей:

   - `accountExpires`
   - `badPasswordTime`
   - `cn`
   - `co`
   - `company`
   - `department`
   - `description`
   - `displayName` (по этому атрибуту события можно искать при корреляции)
   - `distinguishedName` (по этому атрибуту события можно искать при корреляции)
   - `division`
   - `employeeID`
   - `givenName`
   - `l`
   - `lastLogon`
   - `lastLogonTimestamp`

- `mail` (по этому атрибуту события можно искать при корреляции)
- `mailNickname`
- `managedObjects`
- `manager`
- `memberOf` (по этому атрибуту события можно искать при корреляции)
- `mobile`
- `name`
- `objectCategory`
- `objectGUID` (этот атрибут запрашивается из Active Directory всегда)
- `objectSid`
- `physicalDeliveryOfficeName`
- `pwdLastSet`
- `sAMAccountName` (по этому атрибуту события можно искать при корреляции)
- `sAMAccountType`
- `sn` (по этому атрибуту события можно искать при корреляции)
- `streetAddress`
- `telephoneNumber`
- `title`
- `userAccountControl` (по этому атрибуту события можно искать при корреляции)
- `userPrincipalName` (по этому атрибуту события можно искать при корреляции)

- `whenChanged`
- `whenCreated`

После того, как вы добавите пользовательские атрибуты в Параметрах подключения к LDAP, раскрывающийся список **LDAP-атрибуты** в коллекторе будет автоматически дополнен. Пользовательские атрибуты можно отличить по знаку вопроса рядом с именем атрибута. Если для нескольких доменов вы добавили один и тот же атрибут, в раскрывающемся списке атрибут будет указан один раз, а домены можно просмотреть, если навести курсор на знак вопроса. Названия доменов отображаются в виде ссылок: если вы нажмете на ссылку, домен автоматически добавится в **Сопоставление с учетными записями LDAP**, если прежде он не был добавлен.

Если вы удалили пользовательский атрибут в Параметрах подключения к LDAP, удалите вручную строку с атрибутом из таблицы сопоставления в коллекторе. Информация об атрибутах учетных записей в KUMA обновляется каждый раз после того, как вы выполните импорт учетных записей.

2. Импортируйте учетные записи.
3. В коллекторе в таблице **Обогащение полей KUMA** задайте правила сопоставления полей KUMA с атрибутами LDAP.
4. Перезапустите коллектор.

   После перезапуска коллектора KUMA начнет обогащать события учётными записями.

- В столбце **Поле для записи данных** укажите, в какое поле события KUMA следует поместить идентификатор пользовательской учетной записи, импортированной из LDAP, если сопоставление было успешно.

С помощью кнопки **Добавить строку** в таблицу можно добавить строку, а с помощью кнопки ✕ – удалить. С помощью кнопки **Применить сопоставление по умолчанию** можно заполнить таблицу сопоставления стандартными значениями.

В блок ресурсов для коллектора добавлены правила обогащения события данными, полученными из LDAP.

При добавлении в существующий коллектор обогащения с помощью LDAP или изменении параметров обогащения требуется остановить и запустить сервис снова.

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 ресурсы правил обогащения или же создать правила непосредственно в мастере установки.

Чтобы добавить в набор ресурсов существующее правило обогащения:

1. Нажмите **Добавить обогащение**.

   Откроется блок параметров правил обогащения.

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

Правило обогащения добавлено в набор ресурсов для коллектора.

Чтобы создать в наборе ресурсов новое правило обогащения:

1. Нажмите **Добавить обогащение**.

   Откроется блок параметров правил обогащения.

2. В раскрывающемся списке **Правило обогащения** выберите **Создать**.

3. В раскрывающемся списке **Тип источника данных** выберите, откуда будут поступать данные для обогащения, и заполните относящиеся к нему параметры:

   - константа

     Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

     - В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов Юникода. Если оставить это поле пустым, существующее значение поля события будет удалено.

     - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

- словарь

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**.

  При выборе этого типа в раскрывающемся списке **Название словаря** необходимо выбрать словарь, из которого будут браться значения, а в блоке параметров **Ключевые поля** с помощью кнопки **Добавить поле** требуется выбрать поля события, значения которых будут использоваться для выбора записи словаря.

- событие

  Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

  - В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.
  - В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.
  - В блоке параметров **Преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA. Тип преобразования можно выбрать в раскрывающемся списке. С помощью кнопок **Добавить преобразование** и **Удалить** можно добавить или удалить преобразование. Порядок преобразований имеет значение.

    Доступные преобразования

    Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

    Доступные преобразования:

    - **lower** – используется для перевода всех символов значения в нижний регистр
    - **upper** – используется для перевода всех символов значения в верхний регистр
    - **regexp** – используется для преобразования значения с помощью регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.

- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:

  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sysmon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.

- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.

  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.

  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

- **decodeHexString** – используется для конвертации HEX-строки в текст.

- **decodeBase64String** – используется для конвертации Base64-строки в текст.
- **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

- шаблон

Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

- В поле **Шаблон** поместите шаблон Go.

  Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт.

  Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

- dns

Этот тип обогащения используется для отправки запросов на DNS-сервер частной сети для преобразования IP-адресов в доменные имена или наоборот.

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`.
- **Рабочие процессы** – максимальное количество запросов в один момент времени. Значение по умолчанию: `1`.
- **Количество задач** – максимальное количество одновременно выполняемых запросов. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

- **Срок жизни кеша** – время жизни значений, хранящихся в кеше. Значение по умолчанию: `60`.

- **Кеш отключен** – с помощью этого раскрывающегося списка можно включить или отключить кеширование. По умолчанию кеширование включено.

- cybertrace

Этот тип обогащения используется для добавления в поля события сведений из потоков данных CyberTrace.

Доступные параметры:

- **URL** (обязательно) – в этом поле можно указать URL сервера CyberTrace, которому вы хотите отправлять запросы.

- **Количество подключений** – максимальное количество подключений к серверу CyberTrace, которые может одновременно установить KUMA. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

- **Запросов в секунду** – максимальное количество запросов к серверу в секунду. Значение по умолчанию: `1000`.

- **Время ожидания** – время ожидания отклика от сервера CyberTrace в секундах. Значение по умолчанию: `30`.

- **Сопоставление** (обязательно) – этот блок параметров содержит таблицу сопоставления полей событий KUMA с типами индикаторов CyberTrace. В столбце **Поле KUMA** указаны названия полей событий KUMA, а в столбце **Индикатор CyberTrace** указаны типы индикаторов CyberTrace.

  Доступные типы индикаторов CyberTrace:

  - ip
  - url
  - hash

  В таблице сопоставления требуется указать как минимум одну строку. С помощью кнопки **Добавить строку** можно добавить строку, а с помощью кнопки ✕ – удалить.

- **часовой пояс**

Этот тип обогащения используется в коллекторах и корреляторах для присваивания событию определенного часового пояса. Сведения о часовом поясе могут пригодиться при поиске событий, случившихся в нетипичное время, например ночью.

При выборе этого типа обогащения в раскрывающемся списке **Часовой пояс** необходимо выбрать требуемую временную зону.

> Убедитесь, что требуемый часовой пояс установлен на сервере сервиса, использующего обогащение. Например, это можно сделать с помощью команды `timedatectl list-timezones`, которая показывает все установленные на сервере часовые пояса. Подробнее об установке часовых поясов смотрите в документации используемой вами операционной системы.

При обогащении события в поле события DeviceTimeZone записывается смещение времени выбранного часового пояса относительно всемирного координированного времени (UTC) в формате `+-чч:мм`. Например, если выбрать временную зону **Asia/Yekaterinburg** в поле DeviceTimeZone будет записано значение `+05:00`. Если в обогащаемом событии есть значение поля DeviceTimeZone, оно будет перезаписано.

По умолчанию, если в обрабатываемом событии не указан часовой пояс и не настроены правила обогащения по часовому поясу, событию присваивается часовой пояс сервера, на котором установлен сервис (коллектор или коррелятор), обрабатывающий событие. При изменении времени сервера сервис необходимо перезапустить.

Допустимые форматы времени при обогащении поля DeviceTimeZone

При обработке в коллекторе поступающих "сырых" событий следующие форматы времени могут быть автоматически приведены к формату +-чч:мм:

Формат времени в обрабатываемом событии	Пример
+-чч:мм	-07:00
+-ччмм	-0700
+-чч	-07

Если формат даты в поле `DeviceTimeZone` отличается от указанных выше, при обогащении события сведениями о часовом поясе в поле записывается часовой пояс серверного времени коллектора. Вы можете создать особые правила нормализации для нестандартных форматов времени.

- **геоданные**

Этот тип обогащения используется для добавления в поля событий сведений о географическом расположении IP-адресов. Подробнее о привязке IP-адресов к географическим данным.

При выборе этого типа в блоке параметров **Сопоставление геоданных с полями события** необходимо указать, из какого поля события будет считан IP-адрес, а также выбрать требуемые атрибуты геоданных и определить поля событий, в которые геоданные будут записаны:

1. В раскрывающемся списке **Поле события с IP-адресом** выберите поле события, из которого считывается IP-адрес. По этому IP-адресу будет произведен поиск соответствий по загруженным в KUMA геоданным.

   С помощью кнопки **Добавить поле события с IP-адресом** можно указать несколько полей события с IP-адресами, по которым требуется обогащение геоданными. Удалить добавленные таким образом поля событий можно с помощью кнопки **Удалить поле события с IP-адресом**.

   При выборе полей события `SourceAddress`, `DestinationAddress` и `DeviceAddress` становится доступна кнопка **Применить сопоставление по умолчанию**. С ее помощью можно добавить преднастроенные пары соответствий атрибутов геоданных и полей события.

2. Для каждого поля события, откуда требуется считать IP-адрес, выберите тип геоданных и поле события, в которое следует записать геоданные.

   С помощью кнопки **Добавить атрибут геоданных** вы можете добавить пары полей **Атрибут геоданных** – **Поле события для записи**. Так вы можете настроить запись разных типов геоданных одного IP-адреса в разные поля события. Пары полей можно удалить с помощью значка ✕.

   - В поле **Атрибут геоданных** выберите, какие географические сведения, соответствующие считанному IP-адресу, необходимо записать в событие. Доступные атрибуты геоданных: **Страна**, **Регион**, **Город**, **Долгота**, **Широта**.

- В поле **Поле события для записи** выберите поле события, в которое необходимо записать выбранный атрибут геоданных.

Вы можете записать одинаковые атрибуты геоданных в разные поля событий. Если вы настроите запись нескольких атрибутов геоданных в одно поле события, событие будет обогащено последним по очереди сопоставлением.

4. С помощью раскрывающегося списка **Отладка** укажите, следует ли включить логирование операций сервиса. По умолчанию логирование выключено.

5. В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом правила обогащения. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

   Создание фильтра в ресурсах

   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. Название должно содержать от 1 до 128 символов Юникода.

   4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

      c. В раскрывающемся списке **оператор** выберите нужный вам 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).
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

В набор ресурсов для коллектора добавлено новое правило обогащения.

Перейдите к следующему шагу мастера установки.

Шаг 7. Маршрутизация

Это необязательный шаг мастера установки. В закладке мастера установки **Маршрутизация** можно выбрать или создать ресурсы точек назначения, в параметрах которых будут определено, куда следует перенаправлять обработанные коллектором события. Обычно события от коллектора перенаправляются в две точки: в коррелятор для анализа и поиска угроз; в хранилище для хранения, а также чтобы обработанные события можно было просматривать позднее. При необходимости события можно отправлять в другие места. Точек назначения может быть несколько.

Чтобы добавить в набор ресурсов коллектора существующую точку назначения:

1. В раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, которую вы хотите добавить:

   - Выберите **Хранилище**, если хотите настроить отправку обработанных событий в хранилище.

   - Выберите **Коррелятор**, если хотите настроить отправку обработанных событий в коррелятор.

   - Выберите **Другое**, если хотите отправлять события в другие места.

     > К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях программы.

   Открывается окно **Добавить точку назначения**, где можно указать параметры пересылки событий.

2. В раскрывающемся списке **Точка назначения** выберите нужную точку назначения.

   Название окна меняется на **Изменить точку назначения**, параметры выбранного ресурса отображаются в окне. Ресурс можно открыть для редактирования в новой вкладке браузера с помощью кнопки .

3. Нажмите **Сохранить**.

Выбранная точка назначения отображается в закладке мастера установки. Точку назначения можно удалить из набора ресурсов, выбрав ее и в открывшемся окне нажав **Удалить**.

Чтобы добавить в набор ресурсов коллектора новую точку назначения:

1. В раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, которую вы хотите добавить:

   - Выберите **Хранилище**, если хотите настроить отправку обработанных событий в хранилище.

   - Выберите **Коррелятор**, если хотите настроить отправку обработанных событий в коррелятор.

   - Выберите **Другое**, если хотите отправлять события в другие места.

К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях программы.

Открывается окно **Добавить точку назначения**, где можно указать параметры пересылки событий.

2. Укажите параметры в закладке **Основные параметры**:

   - В раскрывающемся списке **Точка назначения** выберите **Создать**.
   - Введите в поле **Название** уникальное имя для точки назначения. Название должно содержать от 1 до 128 символов Юникода.
   - С помощью переключателя **Выключено**, выберите, будут ли события отправляться в эту точку назначения. По умолчанию отправка событий включена.
   - Выберите **Тип** точки назначения:
     - Выберите **storage**, если хотите настроить отправку обработанных событий в хранилище.
     - Выберите **correlator**, если хотите настроить отправку обработанных событий в коррелятор.
     - Выберите **nats**, **tcp**, **http**, **kafka** или **file**, если хотите настроить отправку событий в другие места.
   - Укажите **URL**, куда следует отправлять события, в формате hostname:<порт API>.

     Для всех типов, кроме **nats**, **file** и **diode** с помощью кнопки **URL** можно указать несколько адресов отправки.
   - Для типов **nats** и **kafka** в поле **Топик** укажите, в какой топик должны записываться данные. Топик для должен содержать символы Юникода.Топик для Kafka имеет ограничение на длину в 255 символов.

3. При необходимости укажите параметры в закладке **Дополнительные параметры**. Доступные параметры зависят от выбранного типа точки назначения:

   - **Сжатие** – раскрывающийся список, в котором можно включить сжатие Snappy. По умолчанию сжатие **Выключено**.
   - **Прокси-сервер** – раскрывающийся список для выбора ресурса прокси-сервера.

- **Размер буфера** – поле, в котором можно указать размер буфера (в байтах) для ресурса точки назначения. Значение по умолчанию: 1 МБ; максимальное: 64 МБ.

- **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. Значение по умолчанию: `30`.

- **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.

- **Идентификатор кластера** – идентификатор кластера NATS.

- **Режим TLS** – раскрывающийся список, в котором можно указать условия использование шифрования TLS:

  - **Выключено** (по умолчанию) – не использовать шифрование TLS.

  - **Включено** – использовать шифрование, но без верификации.

  - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

  При использовании TLS невозможно указать IP-адрес в качестве URL.

- **Политика выбора URL** – раскрывающийся список, в котором можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько:

  - **Любой** – события отправляются в один из доступных URL до тех пор, пока этот URL принимает события. При разрыве связи (например, при отключении принимающего узла) для отправки событий будет выбран другой URL.

  - **Сначала первый** – события отправляются в первый URL из списка добавленных адресов. Если он становится недоступен, события отправляются в следующий по очереди доступный узел. Когда первый URL снова становится доступен, события снова начинаются отправляться в него.

  - **По очереди** – пакеты с событиями по очереди отправляться в доступные URL из списка. Поскольку пакеты отправляются или при переполнении буфера точки назначения, или при срабатывании таймера очистки буфера, эта политика выбора URL не гарантирует равное распределение событий по точкам назначения.

- **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.

- **Путь** – путь к файлу, если выбран тип точки назначения **file**.

- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.

- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

- Вы можете установить проверки работоспособности, используя поля **Путь проверки работоспособности** и **Ожидание проверки работоспособности**. Вы также можете отключить проверку работоспособности, установив флажок **Проверка работоспособности отключена**.

- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.

- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах

  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. Название должно содержать от 1 до 128 символов Юникода.

  4. В блоке параметров **Условия** задайте 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, с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

c. В раскрывающемся списке **оператор** выберите нужный вам 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).
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в

правом операнде.

- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

   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**.

f. 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**.

   Параметры вложенного фильтра можно просмотреть, нажав на кнопку .

4. Нажмите **Сохранить**.

   Созданная точка назначения отображается в закладке мастера установки. Точку назначения можно удалить из набора ресурсов, выбрав ее и в открывшемся окне нажав **Удалить**.

Перейдите к следующему шагу мастера установки.

Шаг 8. Проверка параметров

Это обязательный и заключительный шаг мастера установки. На этом шаге в KUMA создается набор ресурсов для сервиса и на основе этого набора автоматически создаются сервисы:

- Набор ресурсов для коллектора отображается в разделе **Ресурсы** → **Коллекторы**. Его можно использовать для создания новых сервисов коллектора. При изменении этого набора ресурсов все сервисы, которые работают на его основе, будут использовать новые параметры, если сервисы перезапустить: для этого можно использовать кнопки **Сохранить и перезапустить сервисы** и **Сохранить и обновить параметры сервисов**.

  Набор ресурсов можно изменять, копировать, переносить из папки в папку, удалять, импортировать и экспортировать, как другие ресурсы.

- Сервисы отображаются в разделе **Ресурсы** → **Активные сервисы**. Созданные с помощью мастера установки сервисы выполняют функции внутри программы KUMA – для связи с внешними частями сетевой инфраструктуры необходимо установить аналогичные внешние сервисы на предназначенных для них серверах и устройствах. Например, внешний сервис коллектора следует установить на сервере, предназначенном для получения событий; внешние сервисы хранилища – на серверах с развернутой службой ClickHouse; внешние сервисы агентов – на тех устройствах Windows, где требуется получать и откуда необходимо пересылать события Windows.

Чтобы завершить мастер установки:

1. Нажмите **Сохранить и создать сервис**.

   В закладке мастера установки **Проверка параметров** отображается таблица сервисов, созданных на основе набора ресурсов, выбранных в мастере установки. В нижней части окна отображаются примеры команд, с помощью которых необходимо установить внешние аналоги этих сервисов на предназначенные для них серверы и устройства.

   Например:

   /opt/kaspersky/kuma/kuma collector --core https://kuma-example:<порт, используемый для связи с Ядром KUMA> --id <идентификатор сервиса> --api.port <порт, используемый для связи с сервисом> --install

Файл kuma можно найти внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

Порт для связи с Ядром KUMA, идентификатор сервиса и порт для связи с сервисом добавляются в команду автоматически. Также следует убедиться в сетевой связности системы KUMA и при необходимости открыть используемые ее компонентами порты.

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

Сервис коллектора создан в KUMA. Теперь аналогичный сервис необходимо установить на сервере, предназначенном для получения событий.

Если в коллекторы был выбран коннектор типа wmi или wec, потребуется также установить автоматически созданные агенты KUMA.

Установка коллектора в сетевой инфраструктуре KUMA

Коллектор состоит из двух частей: одна часть создается внутри веб-интерфейса KUMA, а другая устанавливается на сервере сетевой инфраструктуры, предназначенной для получения событий. В сетевой инфраструктуре устанавливается вторая часть коллектора.

Чтобы установить коллектор:

1. Войдите на сервер, на котором вы хотите установить сервис.

2. 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/.

   Убедитесь, что файл kuma имеет достаточные права для запуска.

4. Выполните следующую команду:

   ```
   sudo /opt/kaspersky/kuma/kuma collector --core https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса KUMA> --api.port <порт, используемый для связи с устанавливаемым компонентом>
   ```

Пример: `sudo /opt/kaspersky/kuma/kuma collector --core https://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 KUMA изменился на *зеленый*, остановите выполнение команды и перейдите к следующему шагу.

> Команду можно скопировать на последнем шаге мастера установщика. В ней автоматически указывается адрес и порт сервера Ядра KUMA, идентификатор устанавливаемого коллектора, а также порт, который этот коллектор использует для связи.

> При развертывании нескольких сервисов KUMA на одном хосте в процессе установки необходимо указать уникальные порты для каждого компонента с помощью параметра `--api.port <порт>`. По умолчанию используется значение `--api.port 7221`.

> Перед установкой необходимо убедиться в сетевой связности компонентов KUMA.

5. Выполните команду повторно, добавив ключ `--install`:

   `sudo /opt/kaspersky/kuma/kuma collector --core https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса KUMA> --api.port <порт, используемый для связи с устанавливаемым компонентом> --install`

   Пример: `sudo /opt/kaspersky/kuma/kuma collector --core https://kuma.example.com:7210 --id XXXX --api.port YYYY --install`

6. Добавьте порт коллектора KUMA в исключения брандмауэра.

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

Коллектор установлен. С его помощью можно получать и передавать на обработку данные из источника события.

Проверка правильности установки коллектора

Проверить готовность коллектора к получению событий можно следующим образом:

1. В веб-интерфейсе KUMA откройте раздел **Ресурсы** → **Активные сервисы**.

2. Убедитесь, что у установленного вами коллектора зеленый статус.

Если коллектор установлен правильно и вы уверены, что из источника событий приходят данные, то при поиске связанных с ним событий в таблице должны отображаться события.

*Чтобы проверить наличие ошибок нормализации с помощью раздела **События** веб-интерфейса KUMA:*

1. Убедитесь, что запущен сервис коллектора.

2. Убедитесь, что источник событий передает события в KUMA.

3. Убедитесь, что в разделе **Ресурсы** веб-интерфейса KUMA в раскрывающемся списке **Хранить исходное событие** ресурса **Нормализатор** выбрано значение **При возникновении ошибок**.

4. В разделе **События** в KUMA выполните поиск событий со следующими параметрами:

   - `ServiceID = <идентификатор коллектора, который требуется проверить>`

   - `Raw != ""`

   Если при этом поиске будут обнаружены какие-либо события, это означает, что есть ошибки нормализации, и их необходимо исследовать.

Чтобы проверить наличие ошибок нормализации с помощью панели мониторинга Grafana:

1. Убедитесь, что запущен сервис коллектора.

2. Убедитесь, что источник событий передает события в KUMA.

3. Откройте раздел Метрики и перейдите по ссылке KUMA Collectors.

4. Проверьте, отображаются ли ошибки в разделе Errors (Ошибки) виджета Normalization (Нормализация).

Если в результате обнаружены ошибки нормализации, их необходимо исследовать.

В коллекторах типа WEC и WMI необходимо убедиться, что для подключения к агенту используется уникальный порт. Этот порт указывается в разделе **Транспорт** мастера установки коллектора.

Обеспечение бесперебойной работы коллекторов

Бесперебойное поступление событий от источника событий в KUMA является важным условием защиты сетевой инфраструктуры. Бесперебойность можно обеспечить автоматическим перенаправлением потока событий на большее число коллекторов:

- На стороне KUMA необходимо установить два или больше одинаковых коллекторов.
- На стороне источника событий необходимо настроить управление потоками событий между коллекторами с помощью сторонних средств управления нагрузкой серверов, например rsyslog или nginx.

При такой конфигурации коллекторов поступающие события не будут теряться, когда сервер коллектора по какой-либо причине недоступен.

Необходимо учитывать, что при переключении потока событий между коллекторами агрегация событий будет происходить на каждом коллекторе отдельно.

Управление потоком событий с помощью rsyslog

Чтобы включить управление потоками событий на сервере источника событий с помощью rsyslog:

1. Создайте два или более одинаковых коллекторов, с помощью которых вы хотите обеспечить бесперебойный прием событий.
2. Установите на сервере источника событий rsyslog (см. документацию rsyslog).
3. Добавьте в конфигурационный файл /etc/rsyslog.conf правила перенаправления потока событий между коллекторами:

```
*.* @@<FQDN основного сервера коллектора>:<порт, на который коллектор принимает события>

$ActionExecOnlyWhenPreviousIsSuspended on

& @@<FQDN резервного сервера коллектора>:<порт, на который коллектор принимает события>

$ActionExecOnlyWhenPreviousIsSuspended off
```

Пример конфигурационного файла

Пример конфигурационного файла, где указан один основной коллектор и два резервных. Коллекторы настроены на принятие событий на порт TCP 5140.

```
*.* @@kuma-collector-01.example.com:5140
$ActionExecOnlyWhenPreviousIsSuspended on
& @@kuma-collector-02.example.com:5140
& @@kuma-collector-03.example.com:5140
$ActionExecOnlyWhenPreviousIsSuspended off
```

4. Перезапустите rsyslog, выполнив команду `systemctl restart rsyslog`.

Управление потоками событий на сервере источника событий включено.

Управление потоком событий с помощью nginx

Для управления потоком событий средствами nginx необходимо создать и настроить ngnix-сервер, который будет принимать события от источника событий, а затем перенаправлять их на коллекторы.

Чтобы включить управление потоками событий на сервере источника событий с помощью nginx:

1. Создайте два или более одинаковых коллекторов, с помощью которых вы хотите обеспечить бесперебойный прием событий.

2. Установите nginx на сервере, предназначенном для управления потоком событий.

   - Команда для установки в Oracle Linux 8.6:

     ```
     $sudo dnf install nginx
     ```

   - Команда для установки в Ubuntu 20.4:

     ```
     $sudo apt-get install nginx
     ```

     При установке из sources, необходимо собрать с параметром `-with-stream`:
     `$sudo ./configure -with-stream -without-http_rewrite_module -without-http_gzip_module`

3. На nginx-сервере в конфигурационный файл nginx.conf добавьте модуль stream с правилами перенаправления потока событий между коллекторами.

Пример модуля stream

Пример модуля, в котором поток событий распределяется между коллекторами kuma-collector-01.example.com и kuma-collector-02.example.com, которые принимают события по протоколу TCP на порт 5140 и по протоколу UPD 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.
```

4. Перезапустите nginx, выполнив команду `systemctl restart nginx`.

5. На сервере источника событий перенаправьте события на ngnix-сервер.

Управление потоками событий на сервере источника событий включено.

Для тонкой настройки балансировки может потребоваться nginx Plus, однако некоторые методы балансировки, например Round Robin и Least Connections, доступны в базовой версии ngnix.

Подробнее о настройке nginx см. в документации nginx.

Создание агента

Агент KUMA состоит из двух частей: одна часть создается внутри веб-интерфейса KUMA, а вторая устанавливается на сервере или устройстве сетевой инфраструктуры.

Создание агента производится в несколько этапов:

1. **Создание набора ресурсов агента в веб-интерфейсе KUMA**
2. **Создание сервиса агента в веб-интерфейсе KUMA**
3. **Установка серверной части агента на устройстве, с которого требуется передавать сообщения**

Агент KUMA для устройств Windows может быть создан автоматически при создании коллектора с типом транспорта wmi или wec. Набор ресурсов и сервис таких агентов создаются в мастере установки коллектора, однако их все равно требуется установить на устройстве, с которого требуется передать сообщение.

Создание набора ресурсов для агента

Сервис агента в веб-интерфейсе KUMA создается на основе набора ресурсов для агента, в котором объединяются коннекторы и точки назначения.

Чтобы создать набор ресурсов для агента в веб-интерфейсе KUMA:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Агенты** нажмите **Добавить агент**.

Откроется окно создания агента с активной закладкой **Общие параметры**.

2. Заполните параметры в закладке **Общие параметры**:

   - В поле **Название агента** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов Юникода.

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

   - При необходимости установите флажок **Отладка**, чтобы включить логирование операций сервиса.

   - В поле **Описание** можно добавить описание сервиса: до 256 символов Юникода.

3. Создайте подключение для агента с помощью кнопки + и переключитесь на добавленную закладку **Подключение <номер>**.

   Закладки можно удалять с помощью кнопки ×.

4. В блоке параметров **Коннектор** добавьте ресурс коннектора:

   - Если хотите выбрать существующий ресурс, выберите его в раскрывающемся списке.

   - Если хотите создать новый ресурс, выберите в раскрывающемся списке **Создать** и укажите его параметры:

     - В поле **Название** укажите имя коннектора. Название должно содержать от 1 до 128 символов Юникода.

     - В раскрывающемся списке **Тип** выберите тип коннектора и укажите его параметры в закладках **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа коннектора:

       - tcp

       - udp

       - nats

       - kafka

       - http

       - file

       - ftp

- nfs
- wmi
- wec
- snmp

Типом агента считается тип использованного в нем коннектора. Исключением являются агенты с точкой назначения типа diode: такие агенты считаются diode-агентами.

При использовании типа коннектора **tcp** или **upd** на этапе нормализации в поле событий DeviceAddress, если оно пустое, будут записаны IP-адреса устройств, с которых были получены события.

- В поле **Описание** можно добавить описание ресурса: до 256 символов Юникода.

Ресурс коннектора добавлен в выбранное подключение набора ресурсов агента. Созданный ресурс доступен только в этом наборе ресурсов и не отображается в разделе веб-интерфейса **Ресурсы** → **Коннекторы**.

5. В блоке параметров **Точки назначения** добавьте ресурсы точек назначения.

   - Если хотите выбрать существующий ресурс, выберите его в раскрывающемся списке.
   - Если хотите создать новый ресурс, выберите в раскрывающемся списке **Создать** и укажите его параметры:
     - В поле **Название** укажите имя точки назначения. Название должно содержать от 1 до 128 символов Юникода.
     - В раскрывающемся списке **Тип** выберите тип точки назначения и укажите ее параметры в закладках **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа точки назначения:
       - **nats** – 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.

- В поле **Описание** можно добавить описание ресурса: до 256 символов Юникода.

> 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 ✕.

6. Повторите шаги 3–5 для каждого подключения агента, которое вы хотите создать.

7. Нажмите **Сохранить**.

Набор ресурсов для агента создан и отображается в разделе **Ресурсы** → **Агенты**. Теперь можно создать сервис агента в KUMA.

Создание сервиса агента в веб-интерфейсе KUMA

Когда набор ресурсов для агента создан, можно перейти к созданию сервиса агента в KUMA.

Чтобы создать сервис агента в веб-интерфейсе KUMA:

1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** нажмите **Добавить сервис**.

2. В открывшемся окне **Выберите сервис** выберите только что созданный набор ресурсов для агента и нажмите **Создать сервис**.

Сервис агента создан в веб-интерфейсе KUMA и отображается в разделе **Ресурсы** → **Активные сервисы**. Теперь сервисы агента необходимо установить на каждом устройстве, с которого вы хотите передавать данные в коллектор. При установке используется идентификатор сервиса.

Установка агента в сетевой инфраструктуре KUMA

Когда сервис агента создан в KUMA, можно перейти к установке агента на устройствах сетевой инфраструктуры, с которых вы хотите передавать данные в коллектор.

Перед установкой убедитесь в сетевой связности системы и откройте используемые компонентами порты.

Установка агента KUMA на устройствах Linux

Чтобы установить агент KUMA на устройство Linux:

1. Войдите на сервер, на котором вы хотите установить сервис.
2. Создайте следующие директории:
   - /opt/kaspersky/kuma/
   - /opt/kaspersky/agent/
3. Поместите в директорию /opt/kaspersky/kuma/ файл kuma, расположенный внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

   Убедитесь, что файл kuma имеет достаточные права для запуска.

4. Выполните следующую команду:

   ```
   sudo /opt/kaspersky/kuma/kuma agent --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> --wd <путь к директории, где будут размещаться файлы устанавливаемого агента. Если не указывать этот флаг, файлы будут храниться в директории, где расположен файл kuma>
   ```

   Пример: `sudo /opt/kaspersky/kuma/kuma agent --core https://kuma.example.com:7210 --id XXXX --wd /opt/kaspersky/kuma/agent/XXXX`

Агент KUMA установлен на устройство Linux. Агент пересылает данные в KUMA: можно настроить коллектор для их приема.

Установка агента KUMA на устройствах Windows

Перед установкой агента KUMA на устройстве Windows администратору сервера необходимо создать на устройстве Windows учетную запись с правами EventLogReaders и Log on as a service. Эту же учетную запись необходимо использовать для запуска агента.

Чтобы установить агент KUMA на устройство Windows:

1. Скопируйте файл kuma.exe в папку на устройстве Windows. Для установки рекомендуется использовать папку `C:\Users\<имя пользователя>\Desktop\KUMA`.

   Файл kuma.exe находится внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

2. Запустите командную строку на устройстве Windows с правами администратора и найдите папку с файлом kuma.exe.

3. Выполните следующую команду:

   `kuma agent --core https://<полное доменное имя сервера ядра KUMA>:<порт, используемый сервером ядра KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса агента, созданного в KUMA> --user <имя пользователя, под которым будет работать агент, включая домен> --install`

   Пример: `kuma agent --core https://kuma.example.com:7210 --id XXXXX --user domain\username --install`

   > Справочная информация об установщике доступна по команде `kuma help agent`.

4. Введите пароль для пользователя, под которым будет работать агент.

   Создана папка `C:\Program Files\Kaspersky Lab\KUMA\agent\<Идентификатор Агента>`, в нее установлен сервис агента KUMA. Агент пересылает события Windows в KUMA: можно настроить коллектор для их приема.

Когда сервис агента установлен, он запускается автоматически. Сервис также настроен на перезапуск в случае сбоев. Агент можно перезапустить из веб-интерфейса KUMA, но только когда сервис активен. В противном случае сервис требуется перезапустить вручную на машине Windows.

Удаление агента KUMA с устройств Windows

Чтобы удалить агент KUMA с устройства Windows:

1. Запустите командную строку на компьютере Windows с правами администратора и найдите папку с файлом kuma.exe.

2. Выполните любую из команд ниже:

   - `kuma.exe agent --cfg <путь к файлу конфигурации агента> --uninstall`

   - `kuma.exe agent --id <идентификатор сервиса агента, созданного в KUMA> --uninstall`

   Указанный агент KUMA удален с устройства Windows. События Windows больше не отправляются в KUMA.

При настройке сервисов можно проверить конфигурацию на наличие ошибок до установки, запустив агент с помощью команды `kuma agent --core https://<полное доменное имя сервера ядра KUMA>:<порт, используемый сервером ядра KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса агента, созданного в KUMA> --user <имя пользователя, под которым будет работать агент, включая домен>`.

Автоматически созданные агенты

При создании коллектора с коннекторами типа wec и wmi 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 их 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.

В интерфейсе KUMA автоматически созданные агенты появляются одновременно с созданием коллектора, однако их все равно требуется установить на устройстве, с которого требуется передать сообщение.

Обновление агентов

При обновлении версий KUMA требуется обновить и установленные на удаленных машинах агенты WMI и WEC.

Чтобы обновить агент:

1. Установите на удаленной машине новый агент.

   Агент обновлен, но данные от него не поступают из-за недействительного сертификата.

2. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** сбросьте сертификат обновляемого агента.

3. На удаленной машине с установленным агентом запустите службу "KUMA Windows Agent <идентификатор сервиса>".

   Подробнее о службах Windows смотрите в документации вашей версии Windows.

Агент и его сертификаты обновлены.

Передача в KUMA событий из изолированных сегментов сети

Схема передачи данных

С помощью диодов данных можно передавать события из изолированных сегментов сети в KUMA. Передача данных организована следующим образом:

1. Установленный на изолированном сервере агент KUMA с точкой назначения **diode** принимает события и перемещает их в директорию, из которой события заберет диод данных.

   Агент накапливает события в буфере до его переполнения или в течение заданного пользователем срока после последней записи на диск. Затем события записываются в файл во временной директории агента. Файл перемещается в директорию, обрабатываемую диодом данных; в качестве его названия используется хеш-сумма (SHA-256) содержимого файла и время создания файла.

2. Диод данных перемещает файлы из директории изолированного сервера в директорию внешнего сервера.

3. Установленный на внешнем сервере коллектор KUMA с коннектором **diode** считывает и обрабатывает события из файлов той директории, в которой размещает файлы диод данных.

   После считывания из файла всех событий он автоматически удаляется. Перед считыванием событий происходит верификация содержимого файлов по хеш-сумме в названии файла. Если содержимое не проходит верификацию, файл удаляется.

В указанной выше схеме компоненты KUMA отвечают за перемещение событий в определенную директорию внутри изолированного сегмента и за прием событий из определенной директории во внешнем сегменте сети. Перемещение файлов с событиями из директории изолированного сегмента сети в директорию внешнего сегменте сети осуществляет диод данных.

Для каждого источника данных внутри изолированного сегмента сети необходимо создать свой агент и коллектор KUMA, а также настроить диод данных на работу с отдельными директориями.

Настройка компонентов KUMA

Настройка компонентов KUMA для передачи данных из изолированных сегментов сети состоит из следующих этапов:

1. Создание сервиса коллектора во внешнем сегменте сети.

   На этом этапе необходимо создать и установить коллектор для получения и обработки файлов, которые диод данных будет перемещать из изолированного сегмента сети. Создать коллектор и все требуемые для него ресурсы можно с помощью мастера установки коллектора.

   На шаге **Транспорт** требуется выбрать или создать коннектор типа **diode**. В коннекторе необходимо указать директорию, в которую диод данных будет перемещать файлы из изолированного сегмента сети.

Пользователь kuma, под которым работает коллектор, должен иметь права на чтение, запись и удаление в директории, в которую диод данных перемещает данные из изолированного сегмента сети.

2. Создание набора ресурсов агента KUMA.

   На этом этапе необходимо создать набор ресурсов агента KUMA, который будет в изолированном сегменте сети получать события и подготавливать их для передачи диоду данных. Набор ресурсов diode-агента имеет следующие особенности:

   - Ресурс точки назначения в агенте должен иметь тип **diode**. В этом ресурсе необходимо указать директорию, из которой диод данных будет перемещать файлы во внешний сегмент сети.
   - Для diode-агента невозможно выбрать коннекторы типа **sql** или **netflow**.

3. Скачивание конфигурационного файла агента в виде JSON-файла.

   a. Набор ресурсов агента с точкой назначения типа diode необходимо скачать в виде JSON-файла.

   b. Если в наборе ресурсов агента использовались ресурсы секретов, конфигурационный файл необходимо вручную дополнить данными секретов.

4. Установка сервиса агента KUMA в изолированном сегменте сети.

   На этом этапе необходимо установить агент в изолированном сегменте сети на основе конфигурационного файла агента, созданного на предыдущем этапе. Установка возможна на устройствах Linux и Windows.

Настройка диода данных

Диод данных необходимо настроить следующим образом:

- Данные необходимо передавать атомарно из директории изолированного сервера (куда их помещает агент KUMA) в директорию внешнего сервера (где их считывает коллектор KUMA).
- Переданные файлы необходимо удалять с изолированного сервера.

Сведения о настройке диода данных можно получить в документации используемого в вашей организации диода данных.

Особенности работы

При работе с изолированными сегментами сети не поддерживаются работа с SQL и NetFlow.

При использовании указанной выше схемы невозможно администрирование агента через веб-интерфейс KUMA, поскольку он располагается в изолированном сегменте сети. В списке активных сервисов KUMA такие агенты не отображаются.

Конфигурационный файл diode-агента

Созданный набор ресурсов агента с точкой назначения типа diode можно скачать в виде конфигурационного файла. Этот файл используется при установке агента в изолированном сегменте сети.

Чтобы скачать конфигурационный файл,

В веб-интерфейсе KUMA в разделе **Ресурсы** → **Агенты** выберите нужный набор ресурсов агента с точкой назначения diode и нажмите **Скачать конфигурацию**.

Конфигурация параметров агента скачивается в виде JSON-файла в соответствии с параметрами вашего браузера. Ресурсы секретов, 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 ресурса коннектора. В этом примере приводится коннектор типа kafka, но в diode-агенте можно использовать коннекторы и других типов. Если ресурс коннектора создан непосредственно в наборе ресурсов агента, значение идентификатора отсутствует.>",

"name": "<название ресурса коннектора>",

"kind": "kafka",

"connections": [

{

"kind": "kafka",

"urls": [

"localhost:9093"

],

"host": "",

"port": "",

"secretID": "<идентификатор ресурса 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 ресурса точки назначения. Если ресурс точки назначения создан непосредственно в наборе ресурсов агента, значение идентификатора отсутствует.>",

"name": "<название ресурса 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 ресурса секрета>": {
      "pfx": "<зашифрованный pfx-ключ>",
      "pfxPassword": "<пароль к зашифрованному pfx-ключу. Вместо действительного пароля из KUMA экспортируется значение changeit. В файле конфигурации необходимо вручную указать содержимое секретов>"
    }
  },
  "tenantID": "<идентификатор тенанта>"
}
```

Описание полей секретов

Поля секрета

Название поля	Тип	Описание
`user`	строка	Имя пользователя.
`password`	строка	Пароль.
`token`	строка	Токен.
`urls`	массив строк	Список URL.
`publicKey`	строка	Публичный ключ (используется в PKI).
`privateKey`	строка	Приватный ключ (используется в PKI).
`pfx`	строка, содержащая base64-закодированное содержимое pfx	Содержимое pfx файла, закодированное в base64. На Linux получить base64-кодировку файла можно при помощи команды `base64 -w0 src > dst`.
`pfxPassword`	строка	Пароль от pfx.

`securityLevel`	строка	Используется в snmp3. Возможные значения: `NoAuthNoPriv`, `AuthNoPriv`, `AuthPriv`.
`community`	строка	Используется в snmp1.
`authProtocol`	строка	Используется в snmp3. Возможные значения: `MD5`, `SHA`, `SHA224`, `SHA256`, `SHA384`, `SHA512`.
`privacyProtocol`	строка	Используется в snmp3. Возможные значения: `DES`, `AES`.
`privacyPassword`	строка	Используется в snmp3.
`certificate`	строка, содержащая base64-закодированное содержимое pem	Содержимое pem файла, закодированное в base64. На Linux получить base64-кодировку файла можно при помощи команды `base64 -w0 src > dst`.

Установка Linux-агента в изолированном сегменте сети

Чтобы установить в изолированном сегменте сети агент KUMA на устройство Linux:

1. Поместите на Linux-сервер в изолированном сегменте сети, который будет использоваться для получения агентом событий и с которого диод данных будет перемещать файлы во внешний сегмент сети, следующие файлы:

   - Конфигурационный файл агента.

     > Необходимо при помощи списка контроля доступа (ACL) настроить права доступа к конфигурационному файлу так, чтобы доступ на чтение файла был только у пользователя KUMA.

   - Исполняемый файл /opt/kaspersky/kuma/kuma (файл kuma можно найти внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/).

2. Выполните следующую команду:

   sudo ./kuma 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 KUMA на устройстве Windows администратору сервера необходимо создать на устройстве Windows учетную запись с правами EventLogReaders и Log on as a service. Эту же учетную запись необходимо использовать для запуска агента.

Чтобы установить в изолированном сегменте сети агент KUMA на устройство Windows:

1. Поместите на Window-сервер в изолированном сегменте сети, который будет использоваться для получения агентом событий и с которого диод данных будет перемещать файлы во внешний сегмент сети, следующие файлы:

   - Конфигурационный файл агента.

     Необходимо при помощи списка контроля доступа (ACL) настроить права доступа к конфигурационному файлу так, чтобы доступ на чтение файла был только у пользователя, под которым будет работать агент.

   - Исполняемый файл kuma.exe. Файл можно найти внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

   Рекомендуется использовать папку `C:\Users\<имя пользователя>\Desktop\KUMA`.

2. Запустите командную строку на устройстве Windows с правами администратора и найдите папку с файлом kuma.exe.

3. Выполните следующую команду:

   ```
   kuma.exe agent --cfg <путь к конфигурационному файлу агента> --user <имя пользователя, под которым будет работать агент, включая домен> --install
   ```

   Справочная информация об установщике доступна по команде `kuma.exe help agent`.

4. Введите пароль для пользователя, под которым будет работать агент.

Создана папка `C:\Program Files\Kaspersky Lab\KUMA\agent\<Идентификатор Агента>`, в нее установлен сервис агента KUMA. Агент перемещает события в папку для обработки диодом данных.

При установке агента конфигурационный файл агента перемещается в директорию C:\Program Files\Kaspersky Lab\KUMA\agent\<идентификатор агента, указанный в конфигурационном файле>. Файл kuma.exe перемещается в директорию C:\Program Files\Kaspersky Lab\KUMA.

При установке агента его конфигурационный файл не должен находиться в директории, в которую устанавливается агент.

Когда сервис агента установлен, он запускается автоматически. Сервис также настроен на перезапуск в случае сбоев.

Удаление агента KUMA с устройств Windows

Чтобы удалить агент KUMA с устройства Windows:

1. Запустите командную строку на компьютере Windows с правами администратора и найдите папку с файлом kuma.exe.
2. Выполните любую из команд ниже:
   - `kuma.exe agent --cfg <путь к файлу конфигурации агента> --uninstall`
   - `kuma.exe agent --id <идентификатор сервиса агента, созданного в KUMA> --uninstall`

   Указанный агент KUMA удален с устройства Windows. События Windows больше не отправляются в KUMA.

При настройке сервисов можно проверить конфигурацию на наличие ошибок до установки, запустив агент с помощью команды `kuma.exe agent --cfg <путь к конфигурационному файлу агента>`.

Передача в KUMA событий с машин Windows

Для передачи событий с машин Windows в KUMA используется связка агентов и коллекторов KUMA. Передача данных организована следующим образом:

- Установленный на машине агент KUMA получает события Window с помощью коннектора типа WEC или WMI.
- Агент передает события коллектору KUMA с помощью ресурса точки назначения.
- Коллектор принимает события от агента с помощью коннектора того же типа, который был выбран для точки назначения агента.

При создании коллектора с коннекторами типа wec и wmi автоматически создаются агенты для приема событий Windows, однако вы сможете создать все сервисы 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 в закладке **Подключение** необходимо создать или выбрать коннектор типа WEC или WMI.

   Если хотя бы одно название журнала Windows указано в коннекторе типа wec или wmi с ошибкой, агент не будет получать события их 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.

   Точка назначения агента:

   Тип точки назначения агента зависит от используемого вами способа передачи данных: nats, tcp, http, diode, kafka, file.

   В качестве разделителя в точке назначения необходимо использовать значение `\0`.

   Дополнительные параметры точки назначения агента (например, разделитель, сжатие и режим TLS) должны совпадать с дополнительными параметрами коннектора коллектора, с которым вы хотите связать агент.

2. **Создание сервиса агента в веб-интерфейсе KUMA.**

3. **Установка агента KUMA на машине Windows, с которой вы хотите получать события Windows.**

   Перед установкой убедитесь в сетевой связности системы и откройте используемые компонентами порты.

4. **Создание и установка коллектора KUMA.**

   При создании набора ресурсов коллектора на шаге **Транспорт** необходимо создать или выбрать коннектор, с помощью которого коллектор будет получать события от агента. Его тип должен совпадать с типом точки назначения агента.

   Дополнительные параметры коннектора коллектора (например, разделитель, сжатие и режим TLS) должны совпадать с дополнительными параметрами точки назначения агента, с которым вы хотите связать агент.

Аналитика

KUMA предоставляет обширную аналитику по данным, доступным программе из следующих источников:

- События в хранилище
- Алерты
- Активы
- Учетные записи, импортированные из Active Directory
- Сведения из коллекторов о количестве обработанных событий
- Метрики

Вы можете настроить и получать аналитику в разделах **Панель мониторинга**, **Отчеты**, **Состояние источников** веб-интерфейса KUMA. Для построения аналитики используются только данные из тенантов, к которым у пользователя есть доступ.

Формат даты зависит от языка локализации, выбранного в настройках программы. Возможные варианты формата даты:

- Английская локализация: ГГГГ-ММ-ДД.
- Русская локализация: ДД.ММ.ГГГГ.

Панель мониторинга

В KUMA можно настроить **Панель мониторинга** для отображения самой свежей информации (*аналитики*) о процессах KUMA. Аналитика создается с помощью *виджетов*, специализированных инструментов, которые могут отображать определенные типы информации. Если виджет отображает данные о событиях, алертах, инцидентах или активных листах, при нажатии на его заголовок открывается соответствующий раздел веб-интерфейса KUMA с активным фильтром и/или поисковым запросом, с помощью которых отображаются данные из виджета.

С помощью кнопки **CSV** данные, отображаемые на виджете, можно скачать в формате CSV в кодировке UTF-8. Название скачиваемого файла имеет формат <название виджета>_<дата скачивания (ГГГГММДД)>_<время скачивания (ЧЧММСС)>.CSV.

Коллекции виджетов называются *макетами*. Администраторы и аналитики могут создавать, редактировать и удалять макеты. Также макет можно назначить макетом по умолчанию, чтобы он отображался при открытии раздела **Панель мониторинга**.

Информация в разделе **Панель мониторинга** регулярно обновляется в соответствии с настройками макета, но вы можете принудительно обновить данные с помощью кнопки в верхней части окна. Время последнего обновления отображается рядом с заголовком окна. Если данные не обновлялись дольше 24 часов, рядом с кнопкой обновления будет отображаться значок с соответствующим предупреждением.

Данные, отображаемые на панели мониторинга, зависят от доступных вам тенантов.

Для удобства презентации данных аналитики вы можете включить режим ТВ. Это позволяет скрыть левую панель с разделами интерфейса KUMA и перейти в полноэкранный режим просмотра панели мониторинга в FullHD разрешении. В режиме ТВ вы также можете настроить показ слайд-шоу для выбранных макетов.

Создание макета панели мониторинга

Чтобы создать макет:

1. Откройте веб-интерфейс KUMA и выберите раздел **Панель мониторинга**.

2. Откройте раскрывающийся список в правом верхнем углу окна **Панель мониторинга** и выберите **Создать макет**.

   Откроется окно **Новый макет**.

3. В раскрывающемся списке **Тенанты** выберите тенантов, которым будет принадлежать создаваемый макет.

4. В раскрывающемся списке **Период** выберите период времени, по которому требуется аналитика:

   - **1 час**

- **1 день** (это значение выбрано по умолчанию)
- **7 дней**
- **30 дней**
- **В течение периода** – получать аналитику за выбранный период времени. Период времени устанавливается с помощью календаря, который отображается при выборе этого параметра.

  > Верхняя граница периода не включается в определяемый с ее помощью отрезок времени. Это означает, что, например, для получения аналитики за сутки следует настроить период День1, 00:00:00 – День 2, 00:00:00, а не День 1, 00:00:00 – День 1, 23:59:59.

5. В раскрывающемся списке **Обновлять каждые** выберите частоту обновления данных в виджетах макета:

   - **1 минута**
   - **5 минут**
   - **15 минут**
   - **1 час** (это значение выбрано по умолчанию)
   - **24 часа**

6. В раскрывающемся списке **Добавить виджет** выберите требуемый виджет и настройте его параметры.

   В макет можно добавить более одного виджета.

   Виджеты также можно перетаскивать по окну и изменять их размер с помощью кнопки , которая появляется при наведении указателя мыши на виджет.

   Добавленные в макет виджеты можно редактировать или удалять, нажав на значок , а затем выбрав требуемое действие: **Изменить** или **Удалить**.

   - Добавление виджетов

     > *Чтобы добавить виджет:*
     >
     > 1. В раскрывающемся списке **Добавить виджет** выберите требуемый виджет.

Откроется окно с параметрами виджета. С помощью кнопки **Предварительный просмотр** можно увидеть, как будет выглядеть настраиваемый виджет на макете.

2. Настройте параметры виджета и нажмите **Добавить**.

- Редактирование виджетов

Чтобы отредактировать виджет:

1. Наведите указатель мыши на нужный виджет и нажмите на появляющийся значок .

2. В раскрывающемся списке выберите значение **Изменить**.

   Откроется окно с параметрами виджета. С помощью кнопки **Предварительный просмотр** можно увидеть, как будет выглядеть настраиваемый виджет на макете.

3. Измените параметры виджета и нажмите **Сохранить**.

7. В поле **Название макета** введите уникальное имя макета. Должно содержать от 1 до 128 символов Юникода.

8. Нажмите **Сохранить**.

Новый макет создан и отображается в разделе **Панель мониторинга** веб-интерфейса KUMA.

Выбор макета панели мониторинга

Чтобы выбрать макет:

1. Откройте веб-интерфейс KUMA и выберите раздел **Панель мониторинга**.

2. Откройте раскрывающийся список в правом верхнем углу окна **Панель мониторинга** и выберите нужный макет.

Выбранный макет отображается в разделе **Панель мониторинга** веб-интерфейса KUMA.

Выбор макета панели мониторинга в качестве макета по умолчанию

Чтобы выбрать макет, который будет отображаться на панели мониторинга по умолчанию:

1. Откройте веб-интерфейс KUMA и выберите раздел **Панель мониторинга**.
2. Откройте раскрывающийся список в правом верхнем углу окна **Панель мониторинга** и наведите указатель мыши на требуемый макет.
3. Нажмите на значок ☆.

Выбранный макет теперь является макетом по умолчанию.

Редактирование макета панели мониторинга

Чтобы изменить макет:

1. Откройте веб-интерфейс KUMA и выберите раздел **Панель мониторинга**.
2. Откройте раскрывающийся список в правом верхнем углу окна **Панель мониторинга** и наведите указатель мыши на требуемый макет.
3. Нажмите на значок ✎.
4. Откроется окно **Настройка макета**.
5. Внесите необходимые изменения. Параметры, доступные для изменения, аналогичны параметрам, доступным при создании макета.
6. Нажмите **Сохранить**.

Макет изменен и отображается в разделе **Панель мониторинга** веб-интерфейса KUMA.

Если макет был удален или присвоен другому тенанту, пока вы вносили в него изменения, при нажатии на кнопку **Сохранить** отобразится ошибка. Макет сохранен не будет. Перезагрузите страницу веб-браузера, чтобы в раскрывающемся списке в правом верхнем углу просмотреть перечень доступных макетов.

Удаление макета панели мониторинга

Чтобы удалить макет:

1. Откройте веб-интерфейс KUMA и выберите раздел **Панель мониторинга**.
2. Откройте раскрывающийся список в правом верхнем углу окна **Панель мониторинга** и наведите указатель мыши на требуемый макет.

3. Нажмите на значок и подтвердите действие.

Макет удален.

Преднастроенные виджеты

KUMA поставляется с набором преднастроенных макетов с виджетами:

- Макет Alerts Overview (Обзор алертов):
  - Active alerts (Активные алерты)
  - Unassigned alerts (Неназначенные алерты)
  - Latest alerts (Последние алерты)
  - Alerts distribution (Распределение алертов)
  - Alerts by priority (Алерты по уровню важности)
  - Alerts by assignee (Алерты по исполнителю)
  - Alerts by status (Алерты по статусу)
  - Affected users in alerts (Затронутые пользователи)
  - Affected assets (Затронутые активы)
  - Affected assets categories (Затронутые категории активов)
  - Top event source by alerts number (Топ источников событий по количеству алертов)
  - Alerts by rule (Количество алертов по правилу)
- Макет Incidents Overview (Обзор инцидентов):
  - Active incidents (Активные инциденты)
  - Unassigned Incidents (Неназначенные инциденты)
  - Latest Incidents (Последние инциденты)
  - Incidents distribution (Распределение инцидентов)
  - Incidents by priority (Инциденты по уровню важности)

    - Incidents by assignee (Инциденты по исполнителю)
    - Incidents by status (Инциденты по статусам)
    - Affected assets in incidents (Активы в инцидентах)
    - Affected users in incidents (Пользователи в инцидентах)
    - Affected asset categories in incidents (Категории активов в инцидентах)
    - Active incidents by tenant (Инциденты по тенантам)
- Макет Network Overview (Обзор сетевой активности):
    - Netflow top internal IPs (Топ внутренних IP-адресов по полученному netflow-трафику)
    - Netflow top external IPs (Топ внешних IP-адресов по полученному netflow-трафику)
    - Netflow top hosts for remote control (Топ хостов, на которые были обращения на порты для удаленного управления) – отслеживаются обращения на порты 3389, 22, 135.
    - Netflow total bytes by internal ports (Топ внутренних портов по приему netflow-трафика)
    - Top Log Sources by Events count (Топ источников событий)

Включение и отключение режима ТВ

Мы рекомендуем для отображения аналитики в режиме ТВ [создать отдельного пользователя] с минимально необходимым набором прав.

Чтобы включить режим ТВ:

1. Откройте веб-интерфейс KUMA и выберите раздел **Панель мониторинга**.
2. В правом верхнем углу нажмите на кнопку ⚙.

   Откроется окно **Параметры**.
3. Переведите переключатель **Режим ТВ** в положение **Включено**.
4. Если вы хотите настроить показ макетов 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 макетов.

c. В раскрывающемся списке **Очередь** выберите макеты для просмотра. Если не выбран ни один макет, в режиме слайд-шоу будут по очереди отображаться все макеты, доступные пользователю.

d. Если требуется, измените порядок показа макетов, перетаскивая их с помощью кнопки ⣿.

5. Нажмите на кнопку **Сохранить**.

Режим ТВ будет включен. Чтобы вернуться к работе с веб-интерфейсом KUMA, нужно отключить режим ТВ.

Чтобы отключить режим ТВ:

1. Откройте веб-интерфейс KUMA и выберите раздел **Панель мониторинга**.

2. В правом верхнем углу нажмите на кнопку ⚙.

   Откроется окно **Параметры**.

3. Переведите переключатель **Режим ТВ** в положение **Выключено**.

4. Нажмите на кнопку **Сохранить**.

Режим ТВ будет отключен. В левой части экрана отобразится панель с разделами веб-интерфейса KUMA.

При внесении изменений в макеты, выбранные для слайд-шоу, эти изменения будут автоматически отображаться в активных сессиях слайд-шоу.

Отчеты

В KUMA можно настроить регулярное формирование отчетов о процессах программы.

Отчеты формируются с помощью *шаблонов отчетов*, которые созданы и хранятся в закладке **Шаблоны** раздела **Отчеты**.

Сформированные отчеты хранятся в закладке **Сформированные отчеты** раздела **Отчеты**.

Для возможности сохранять сформированные отчеты в форматах HTML и PDF необходимо установить требуемые пакеты на машине с Ядром KUMA.

При развертывании KUMA в отказоустойчивом варианте временная зона сервера Ядра программы 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.

Шаблон отчета

Шаблоны отчетов используются для указания аналитических данных, которые следует включать в отчет, а также для настройки частоты создания отчетов. Администраторы и аналитики могут создавать, редактировать и удалять шаблоны отчетов. Отчеты, созданные с использованием шаблонов отчетов, отображаются на закладке **Сформированные отчеты**.

Шаблоны отчетов доступны на закладке **Шаблоны** раздела **Отчеты**, где отображается таблица существующих шаблонов. В таблице есть **следующие столбцы**:

Вы можете настроить набор столбцов таблицы и их порядок, а также изменить сортировку данных:

- Отображение столбцов можно включить или выключить в меню, открываемом с помощью значка .
- Порядок столбцов можно изменить, перетаскивая заголовки столбцов.
- Если заголовок столбца таблицы имеет зеленый цвет, на него можно нажать, чтобы сортировать таблицу по данным этого столбца.

- **Название** – имя шаблона отчетов.

  Вы можете отсортировать таблицу по этому столбцу, нажав заголовок и выбрав **По возрастанию** или **По убыванию**.

  Вы также можете искать шаблоны отчетов, используя поле **Поиск**, которое открывается по нажатию на заголовок столбца **Название**.

- **Расписание** – периодичность, с которой отчеты должны формироваться по созданным шаблонам. Если расписание отчета не настроено, отображается значение выключено.

- **Создал** – имя пользователя, создавшего шаблон отчета.

- **Последнее обновление** – дата последнего обновления шаблона отчета.

  Вы можете отсортировать таблицу по этому столбцу, нажав заголовок и выбрав **По возрастанию** или **По убыванию**.

- **Последний отчет** – дата и время формирования последнего отчета по шаблону отчета.

- **Отправить по электронной почте** – в этом столбце отображается метка напротив шаблонов отчетов, для которых настроено уведомление пользователей по почте о сформированных отчетах.

- **Тенант** – название тенанта, которому принадлежит шаблон отчета.

Вы можете нажать имя шаблона отчета, чтобы открыть раскрывающийся список с доступными командами:

- **Создать отчет** – используйте эту команду, чтобы немедленно сформировать отчет. Созданные отчеты отображаются на закладке **Сформированные отчеты**.

- **Изменить расписание** – используйте эту команду, чтобы настроить расписание для формирования отчетов и определить пользователей, которые должны получать уведомления по электронной почте о сформированных отчетах.

- **Изменить шаблон отчета** – используйте эту команду, чтобы настроить виджеты и период времени, за который должна быть извлечена аналитика.

- **Дублировать шаблон отчета** – используйте эту команду, чтобы создать копию существующего шаблона отчета.

- **Удалить шаблон отчета** – используйте эту команду, чтобы удалить шаблон отчета.

Создание шаблона отчета

Чтобы создать шаблон отчета:

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Шаблоны**.

2. Нажмите на кнопку **Новый шаблон**.

   Откроется окно **Новый шаблон отчета**.

3. В раскрывающемся списке **Тенанты** выберите один или несколько тенантов, которым будет принадлежать создаваемый макет.

4. В раскрывающемся списке **Период** выберите период времени, по которому требуется аналитика:

   - **Сегодня** (это значение выбрано по умолчанию)

- **На этой неделе**
- **В этом месяце**
- **В течение периода** – получать аналитику за выбранный период времени.

  > Верхняя граница периода не включается в определяемый с ее помощью отрезок времени. Это означает, что, например, для получения аналитики за сутки следует настроить период День1, 00:00:00 – День 2, 00:00:00, а не День 1, 00:00:00 – День 1, 23:59:59.

- **Другой** – получать аналитику за последние N дней/недель/месяцев/лет.

5. В поле **Срок хранения** укажите, на протяжении какого времени следует хранить сформированные по этому шаблону отчеты.
6. В поле **Название шаблона** введите уникальное название шаблона отчета. Должно содержать от 1 до 128 символов Юникода.
7. В раскрывающемся списке **Добавить виджет** выберите требуемый виджет и настройте его параметры.

   В шаблон отчета можно добавить более одного виджета.

   Виджеты также можно перетаскивать по окну и изменять их размер с помощью кнопки ⤡, которая появляется при наведении указателя мыши на виджет.

   Добавленные в макет виджеты можно редактировать или удалять, наведя на них указатель мыши, нажав появившийся значок ⚙, а затем выбрав требуемое действие: **Изменить** или **Удалить**.

   - Добавление виджетов

     > *Чтобы добавить виджет:*
     >
     > 1. В раскрывающемся списке **Добавить виджет** выберите требуемый виджет.
     >
     > Откроется окно с параметрами виджета. С помощью кнопки **Предварительный просмотр** можно увидеть, как будет выглядеть настраиваемый виджет на макете.
     >
     > 2. Настройте параметры виджета и нажмите **Добавить**.

   - Редактирование виджетов

     > *Чтобы отредактировать виджет:*

1. Наведите указатель мыши на нужный виджет и нажмите на появляющийся значок ⚙.

2. В раскрывающемся списке выберите значение **Изменить**.

   Откроется окно с параметрами виджета. С помощью кнопки **Предварительный просмотр** можно увидеть, как будет выглядеть настраиваемый виджет на макете.

3. Измените параметры виджета и нажмите **Сохранить**.

8. При необходимости можно поменять логотип шаблона отчетов с помощью кнопки **Загрузить логотип**.

   Если нажать на кнопку **Загрузить логотип**, открывается окно загрузки, в котором можно указать файл изображения для логотипа. Изображение должно быть файлом .jpg, .png или .gif размером не более 3 МБ.

   Добавленный логотип будет отображаться в отчете вместо логотипа KUMA.

9. Нажмите **Сохранить**.

Новый шаблон отчета создан и отображается в закладке **Отчеты** → **Шаблоны** веб-интерфейса KUMA. Вы можете сформировать этот отчет вручную. Если вы хотите, чтобы отчеты создавались автоматически, требуется настроить расписание.

Настройка расписания отчетов

Чтобы настроить расписания отчетов:

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Шаблоны**.

2. В таблице шаблонов отчета нажмите имя шаблона отчета и в раскрывающемся списке выберите **Изменить расписание**.

   Откроется окно **Параметры отчета**.

3. Если вы хотите, чтобы отчет формировался регулярно:

   a. Включите переключатель **Расписание**.

      В группе настроек **Повторять каждый** задайте периодичность создания 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.

   b. В поле **Время** укажите время, когда должен быть сформирован отчет. Вы можете ввести значение вручную или с помощью значка часов.

4. Чтобы выбрать формат отчетов и указать адресатов для рассылки, настройте следующие параметры:

   a. В группе настроек **Отправить** нажмите **Добавить**.

   b. В открывшемся окне **Добавление адресов электронной почты** в разделе **Группы пользователей** нажмите **Добавить группу**.

   c. В появившемся поле укажите адрес электронной почты и нажмите **Enter** или щелкните вне поля ввода - адрес электронной почты будет добавлен. Можно добавить несколько адресов. 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, следует настроить SMTP-соединение.

   Если адресаты, которым отчет пришел на почту, являются пользователями KUMA, они смогут скачать отчет или просмотреть отчет по ссылкам из письма. Если адресаты не являются пользователями KUMA, переход по ссылкам будет доступен, но авторизоваться в KUMA адресаты не смогут, поэтому им будут доступны только вложения.

   Вы можете отправить письмо без вложений, тогда адресатам будут доступны отчеты только по ссылкам и только с авторизацией в KUMA, без ограничений по ролям или тенантам.

   d. В раскрывающемся списке выберите формат отчета для отправки. Доступные форматы: PDF, HTML, CSV, разделенный CSV, Excel.

5. Нажмите **Сохранить**.

Расписание отчетов настроено.

Изменение шаблона отчета

Чтобы изменить шаблон отчета:

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Шаблоны**.

2. В таблице шаблонов отчета нажмите имя шаблона отчета и в раскрывающемся списке выберите **Изменить шаблон отчета**.

   Откроется окно **Изменить шаблон отчета**.

Это окно также можно открыть на закладке **Отчеты** → **Сформированные отчеты**, нажав имя существующего отчета и выбрав в раскрывающемся списке **Изменить шаблон отчета**.

3. Внесите необходимые изменения:

- Измените список тенантов, которым принадлежит шаблон отчета.
- Обновите период времени, за который вам требуется аналитика.
- Добавьте виджеты

  Чтобы добавить виджет:

  1. В раскрывающемся списке **Добавить виджет** выберите требуемый виджет.

     Откроется окно с параметрами виджета. С помощью кнопки **Предварительный просмотр** можно увидеть, как будет выглядеть настраиваемый виджет на макете.

  2. Настройте параметры виджета и нажмите **Добавить**.

- Измените расположение виджетов, перетаскивая их.
- Измените размер виджетов с помощью кнопки , которая появляется при наведении указателя мыши на виджет.
- Отредактируйте виджеты

  Чтобы отредактировать виджет:

  1. Наведите указатель мыши на нужный виджет и нажмите на появляющийся значок .

  2. В раскрывающемся списке выберите значение **Изменить**.

     Откроется окно с параметрами виджета. С помощью кнопки **Предварительный просмотр** можно увидеть, как будет выглядеть настраиваемый виджет на макете.

  3. Измените параметры виджета и нажмите **Сохранить**.

- Удалите виджеты, наведя на них указатель мыши, а затем нажав на появившийся значок ⚙ и выбрав **Удалить**.

- В поле справа от раскрывающегося списка **Добавить виджет** введите уникальное имя шаблона отчета. Должно содержать от 1 до 128 символов Юникода.

- Измените логотип отчета, загрузив его с помощью кнопки **Загрузить логотип**. Если в шаблоне уже есть логотип, его предварительно потребуется удалить.

- Измените срок хранения отчетов, сформированных по этому шаблону.

4. Нажмите **Сохранить**.

Шаблон отчета изменен и отображается в закладке **Отчеты** → **Шаблоны** веб-интерфейса KUMA.

Копирование шаблона отчета

Чтобы создать копию шаблона отчета:

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Шаблоны**.

2. В таблице шаблонов отчета нажмите имя шаблона отчета и в раскрывающемся списке выберите **Дублировать шаблон отчета**.

   Откроется окно **Новый шаблон отчета**. Название виджета изменено на `<Шаблон отчета> - копия`.

3. Внесите необходимые изменения:

   - Измените список тенантов, которым принадлежит шаблон отчета.

   - Обновите период времени, за который вам требуется аналитика.

   - **Добавьте виджеты**

     Чтобы добавить виджет:

     1. В раскрывающемся списке **Добавить виджет** выберите требуемый виджет.

        Откроется окно с параметрами виджета. С помощью кнопки **Предварительный просмотр** можно увидеть, как будет выглядеть настраиваемый виджет на макете.

     2. Настройте параметры виджета и нажмите **Добавить**.

- Измените расположение виджетов, перетаскивая их.
- Измените размер виджетов с помощью кнопки ⤡, которая появляется при наведении указателя мыши на виджет.
- Отредактируйте виджеты

  Чтобы отредактировать виджет:

  1. Наведите указатель мыши на нужный виджет и нажмите на появляющийся значок ⚙.
  2. В раскрывающемся списке выберите значение **Изменить**.

     Откроется окно с параметрами виджета. С помощью кнопки **Предварительный просмотр** можно увидеть, как будет выглядеть настраиваемый виджет на макете.
  3. Измените параметры виджета и нажмите **Сохранить**.
- Удалите виджеты, наведя на них указатель мыши, а затем нажав на появившийся значок ⚙ и выбрав **Удалить**.
- В поле справа от раскрывающегося списка **Добавить виджет** введите уникальное имя шаблона отчета. Должно содержать от 1 до 128 символов Юникода.
- Измените логотип отчета, загрузив его с помощью кнопки **Загрузить логотип**. Если в шаблоне уже есть логотип, его предварительно потребуется удалить.

4. Нажмите **Сохранить**.

   Шаблон отчета создан и отображается в закладке **Отчеты** → **Шаблоны** веб-интерфейс KUMA.

Удаление шаблона отчета

Чтобы удалить шаблон отчета:

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Шаблоны**.
2. В таблице шаблонов отчета нажмите имя шаблона отчета и в раскрывающемся списке выберите **Удалить шаблон отчета**.

   Откроется окно подтверждения.
3. Если вы хотите удалить только шаблон отчета, нажмите на кнопку **Удалить**.

4. Если вы хотите удалить шаблон отчета и все отчеты, сформированные с помощью этого шаблона, нажмите **Удалить с отчетами**.

Шаблон отчета удален.

Сформированные отчеты

Все отчеты формируются с помощью шаблонов отчетов. Сформированные отчеты доступны на закладке **Сформированные отчеты** в разделе **Отчеты** и отображаются в таблице со **следующими столбцами**:

Вы можете настроить набор столбцов таблицы и их порядок, а также изменить сортировку данных:

- Отображение столбцов можно включить или выключить в меню, открываемом с помощью значка .
- Порядок столбцов можно изменить, перетаскивая заголовки столбцов.
- Если заголовок столбца таблицы имеет зеленый цвет, на него можно нажать, чтобы сортировать таблицу по данным этого столбца.

- **Название** – имя шаблона отчетов.

  Вы можете отсортировать таблицу по этому столбцу, нажав заголовок и выбрав **По возрастанию** или **По убыванию**.

- **Период** – период времени, за который была извлечена аналитика отчета.

- **Последний отчет** – дата и время создания отчета.

  Вы можете отсортировать таблицу по этому столбцу, нажав заголовок и выбрав **По возрастанию** или **По убыванию**.

- **Тенант** – название тенанта, которому принадлежит отчет.

- **Пользователь** – имя пользователя, который сформировал отчет вручную. Если отчет был сформирован по расписанию, значение будет пустым. Если отчет был сформирован в версии KUMA ниже 2.1, значение будет пустым.

Вы можете нажать на название отчета, чтобы открыть раскрывающийся список с доступными командами:

- **Открыть отчет** – используйте эту команду, чтобы открыть окно с данными отчета.

- **Сохранить как** – используйте эту команду, чтобы сохранить сформированный отчет в нужном формате. Доступные форматы: HTML, PDF, CSV, разделенный CSV, Excel.

- **Создать отчет** – используйте эту команду, чтобы немедленно сформировать отчет. Обновите окно браузера, чтобы увидеть вновь созданный отчет в таблице.

- **Изменить шаблон отчета** – используйте эту команду, чтобы настроить виджеты и период времени, за который должна быть извлечена аналитика.

- **Удалить отчет** – используйте эту команду, чтобы удалить отчет.

Просмотр отчетов

Чтобы просмотреть отчет:

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Сформированные отчеты**.

2. В таблице отчета нажмите имя сформированного отчета и в раскрывающемся списке выберите **Открыть отчет**.

   Откроется новая закладка браузера с виджетами, отображающими аналитику отчетов. Если виджет отображает данные о событиях, алертах, инцидентах или активных листах, при нажатии на его заголовок открывается соответствующий раздел веб-интерфейса KUMA с активным фильтром и/или поисковым запросом, с помощью которых отображаются данные из виджета. К виджетам применяются ограничения по умолчанию.

   С помощью кнопки **CSV** данные, отображаемые на каждом виджете, можно скачать в формате CSV в кодировке UTF-8. Название скачиваемого файла имеет формат <название виджета>_<дата скачивания (ГГГГММДД)>_<время скачивания (ЧЧММСС)>.CSV.

   Если вы хотите просмотреть полные данные, выгрузите отчет в формате CSV с указанными параметрами из запроса.

3. Отчет можно сохранить в выбранном формате с помощью кнопки **Сохранить как**.

Создание отчетов

Вы можете создать отчет вручную или настроить расписание, чтобы отчеты создавались автоматически.

Чтобы создать отчет вручную:

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Шаблоны**.

2. В таблице шаблонов отчета нажмите имя шаблона отчета и в раскрывающемся списке выберите **Создать отчет**.

Отчет также можно создать на закладке **Отчеты** → **Сформированные отчеты**, нажав имя существующего отчета и выбрав в раскрывающемся списке **Создать отчет**.

Отчет создается и помещается на закладку **Отчеты** → **Сформированные отчеты**.

Чтобы создавать отчеты автоматически, настройте расписание отчетов.

Сохранение отчетов

Чтобы сохранить отчет в нужном формате:

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Сформированные отчеты**.
2. В таблице отчета нажмите имя сформированного отчета и в раскрывающемся списке выберите **Сохранить как**, а затем 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.

Удаление отчетов

Чтобы удалить отчет:

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Сформированные отчеты**.
2. В таблице отчета нажмите имя сформированного отчета и в раскрывающемся списке выберите **Удалить отчет**.

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

Состояние источников

В KUMA можно контролировать состояние источников, из которых поступают данные в коллекторы. На одном сервере может быть несколько источников событий, а данные из нескольких источников могут поступать в один коллектор. Источники событий идентифицируются по следующим полям событий (данные в этих полях регистрозависимые):

- DeviceProduct

- DeviceAddress и / или DeviceHostName

Списки источников формируются в коллекторах, объединяются в Ядре KUMA и отображаются в веб-интерфейсе программы в разделе **Состояние источников** в закладке **Список источников событий**. Данные обновляются ежеминутно.

Данные о частоте и количестве поступающих событий являются важным показателем состояния наблюдаемой системы. Вы можете настроить политики мониторинга, чтобы изменения отслеживались автоматически и при достижении индикаторами определенных граничных значений автоматически создавались уведомления. Политики мониторинга отображаются в веб-интерфейсе KUMA в разделе **Состояние источников** в закладке **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**. На одной странице отображается до 250 источников. Таблицу можно сортировать, нажимая на заголовок столбца нужного параметра. При нажатии на источник событий открывается график поступления данных.

Источники событий можно искать по названию с помощью поля **Поиск**. Поиск осуществляется с помощью регулярных выражений (RE2).

При необходимости вы можете настроить период обновления данных в таблице. Доступные периоды обновления: **1 минута**, **5 минут**, **15 минут**, **1 час**. По умолчанию указано значение: **Не обновлять**. Настройка периода обновления может потребоваться для отслеживания изменений в списке источников.

Доступны следующие столбцы:

- **Статус** – статус источника:
  - зеленый – события поступают в пределах присвоенной политики мониторинга;
  - красный – частота или количество поступающих событий выходит за границы, определенные в политике мониторинга;
  - серый – источнику событий не присвоена политика мониторинга.

  Таблицу можно фильтровать по этому параметру.
- **Название** – название источника события. Название формируется автоматически из следующих полей событий:

- DeviceProduct;
- DeviceAddress и/или DeviceHostname;
- DeviceProcessName;
- Tenant.

Вы можете изменить название источника событий. Название может содержать не более 128 символов Юникода.

- **Имя хоста или IP-адрес** – название хоста или IP-адрес, откуда поступают события.
- **Политика мониторинга** – название политики мониторинга, назначенной источнику событий.
- **Поток** – частота, с которой из источника поступают события.
- **Нижний порог** – нижняя граница допустимого количества поступающих событий, указанная в политике мониторинга.
- **Верхний порог** – верхняя граница допустимого количества поступающих событий, указанная в политике мониторинга.
- **Тенант** – тенант, к которому относятся события, поступающие из источника.

Если выбрать источники событий, становятся доступны следующие кнопки:

- **Сохранить в CSV** – с помощью этой кнопки можно выгрузить данные выбранных источников событий в файл с названием event-source-list.csv в кодировке UTF-8.
- **Включить политику** и **Выключить политику** – с помощью этих кнопок для источников событий можно включить или выключить политику мониторинга. При включении требуется выбрать политику в раскрывающемся списке. При выключении требуется указать, на какой период необходимо отключить политику: временно или навсегда.

  Если для выбранного источника событий нет политики, кнопка **Включить политику** будет неактивна. Эта кнопка также будет неактивной в том случае, если выбраны источники из разных тенантов, однако у пользователя нет доступных политик в общем тенанте.

  В редких случаях из-за наложения внутренних процессов KUMA через несколько секунд после выключения политики ее статус может снова измениться с серого на зеленый. В таких случаях необходимо повторно выключить политику мониторинга.

- **Удалить источник событий** – с помощью этой кнопки источники событий можно удалить из таблицы. Статистика по этому источнику также будет удалена. Если данные из источника продолжают поступать в коллектор, источник событий снова появится в таблице, при этом его старая статистика учитываться не будет.

> По умолчанию на странице отображается и, следовательно, доступно для выбора, не больше 250 источников событий. Если источников событий больше, чтобы их можно было выбрать, необходимо загрузить дополнительные источники событий, нажав в нижней части окна на кнопку **Показать еще 250**.

Политики мониторинга

Политики мониторинга источников событий отображаются в таблице в разделе **Состояние источников** → **Политики мониторинга**. Таблицу можно сортировать, нажимая на заголовок столбца нужного параметра. При нажатии на политику открывается область данных с ее параметрами, которые можно изменить.

Доступны следующие столбцы:

- **Название** – название политики мониторинга.
- **Нижний порог** – нижняя граница допустимого количества поступающих событий, указанная в политике мониторинга.
- **Верхний порог** – верхняя граница допустимого количества поступающих событий, указанная в политике мониторинга.
- **Интервал** – период, который учитывается политикой мониторинга.
- **Тип** – тип политики мониторинга:
  - **byCount** – политикой мониторинга отслеживается количество поступающих событий.
  - **byEPS** – политикой мониторинга отслеживается частота поступающих событий.
- **Тенант** – тенант, к которому относится политика мониторинга.

Чтобы добавить политику мониторинга:

1. В веб-интерфейсе KUMA в разделе **Состояние источников** → **Политики мониторинга** нажмите **Добавить политику** и в открывшемся окне укажите параметры:

- В поле **Название политики** введите уникальное имя создаваемой политики. Название должно содержать от 1 до 128 символов Юникода.

- В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать политика. От выбора тенанта зависит, для каких источников событий можно будет включить политику мониторинга.

- В раскрывающемся списке **Тип политики** выберите, как будут отслеживаться поступающие события: по частоте или по количеству.

- 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.

- В поле **Период подсчета** укажите, за какой период в политике мониторинга должны учитываться данные из источника мониторинга. Максимальное значение: 14 дней.

- При необходимости укажите электронные адреса, на которые следует отправить уведомления о срабатывании политики мониторинга KUMA. Для добавления каждого адреса необходимо нажимать на кнопку **Адрес электронной почты**.

  Для рассылки уведомлений необходимо настроить подключение к SMTP-серверу.

2. Нажмите **Добавить**.

Политика мониторинга добавлена.

Чтобы удалить политику мониторинга,

Выберите одну или несколько политик, нажмите **Удалить политику** и подтвердите действие.

> Невозможно удалить предустановленные политики мониторинга, а также политики, назначенные источникам данных.

Виджеты

Виджеты в KUMA используются для получения аналитики для панели мониторинга и отчетов.

При нажатии на заголовки или легенду виджетов о событиях, алертах, инцидентах или активных листах открывается соответствующий раздел веб-интерфейса KUMA с данными из виджета, полученными с помощью фильтров раздела и/или поисковым запросом. Подробнее см. ниже. Этот функционал недоступен в режиме создания и редактирования макетов.

Если в виджете настроено деление периода, по которому строится аналитика, на отрезки, то значения или графики будут отображаться парами: аналитика за текущий отрезок периода (пользовательский цвет) и аналитика за предыдущий отрезок периода (серый цвет).

Виджеты организованы в группы, каждая из которых связана с типом аналитики, которую она предоставляет. В KUMA доступны следующие группы виджетов и виджеты:

- **События** – виджет для создания аналитики на основе событий.

  При нажатии на заголовок этого виджета можно перейти в раздел **События** веб-интерфейса KUMA. При этом для запроса событий из виджета применяется SQL-запрос, указанный в виджете. Запрос указывается без группировки (за исключением табличных графиков), но с учетом условий, указанных в параметре WHERE. Параметр LIMIT в запросе принимается равным 250.

- **Активные листы** – виджет для создания аналитики на основе активных листов корреляторов.

  При нажатии на заголовок этого виджета можно перейти в раздел активного листа, по которому строится аналитика виджета.

- Алерты – группа для аналитики об алертах. При нажатии на заголовок или легенду виджетов этой группы можно перейти в раздел **Алерты** веб-интерфейса KUMA для подробного просмотра данных из виджета.

  В группу входят следующие виджеты:

  - **Активные алерты** – количество незакрытых алертов.
  - **Активные алерты по тенантам** – количество незакрытых алертов, сгруппированных по тенантам.
  - **Алерты по тенантам** – количество алертов всех статусов, сгруппированных по тенантам.
  - **Неназначенные алерты** – количество алертов со статусом **Новый**.
  - **Алерты по исполнителю** – количество назначенных алертов, сгруппированных по исполнителю.
  - **Алерты по статусу** – количество алертов, сгруппированных по статусу.
  - **Алерты по уровню важности** – количество незакрытых алертов, сгруппированных по уровню важности.
  - **Алерты по правилу корреляции** – количество незакрытых алертов, сгруппированных по правилам корреляции. Для этого виджета недоступны подробные сведения по нажатию на заголовок виджета.

    - **Последние алерты** – таблица, содержащая последние 10 незакрытых алертов. Если незакрытых алертов в выбранных в виджете тенантах больше 10, часть из них отображаться не будет.

    - **Распределение алертов** – количество алертов, созданных в течение указанного в виджете периода.

- Активы – группа для аналитики об активах из обработанных событий. В эту группу входят следующие виджеты:

    - **Затронутые активы** – таблица связанных с алертами активов, в которой указан уровень важности актива и количество незакрытых алертов, с которыми он связан.

    - **Категории затронутых активов** – категории активов, привязанных к незакрытым алертам.

    - **Количество активов** – количество активов, добавленных в KUMA.

    - **Активы в инцидентах по тенантам** – количество активов в незакрытых инцидентах, сгруппированных по тенантам.

    - **Активы в алертах по тенантам** – количество активов в незакрытых алертах, сгруппированных по тенантам.

- Инциденты – группа для аналитики об инцидентах. При нажатии на заголовок или легенду виджетов этой группы можно перейти в раздел **Инциденты** веб-интерфейса KUMA для подробного просмотра данных из виджета.

  В группу входят следующие виджеты:

    - **Активные инциденты** – количество незакрытых инцидентов.

    - **Неназначенные инциденты** – количество инцидентов со статусом **Открыт**.

    - **Распределение инцидентов** – количество инцидентов, созданных в течение указанного в виджете периода.

    - **Инциденты по исполнителю** – количество инцидентов со статусом **Назначен**, сгруппированных по пользователям KUMA.

    - **Инциденты по статусам** – количество инцидентов, сгруппированных по статусам.

    - **Инциденты по уровню важности** – количество незакрытых инцидентов, сгруппированных по уровню важности. Доступные типы диаграмм: круговая, столбчатая.

- **Активные инциденты по тенантам** – количество незакрытых инцидентов, сгруппированных по тенантам, доступным пользователю.
- **Все инциденты** – количество инцидентов всех статусов.
- **Все инциденты по тенантам** – количество инцидентов всех статусов, сгруппированных по тенантам.
- **Активы в инцидентах** – количество активов в незакрытых инцидентах. Для этого виджета недоступны подробные сведения по нажатию на заголовок виджета.
- **Категории активов в инцидентах** – категории активов, которые затронуты незакрытыми инцидентами. Доступные типы диаграмм: круговая, столбчатая. Для этого виджета недоступны подробные сведения по нажатию на заголовок виджета.
- **Пользователи в инцидентах** – пользователи, затронутые в инцидентах. Доступные типы диаграмм: таблица, круговая, столбчатая. Для этого виджета недоступны подробные сведения по нажатию на заголовок виджета.
- **Последние инциденты** – последние 10 незакрытых инцидентов. Если незакрытых инцидентов в выбранных в виджете тенантах больше 10, часть из них отображаться не будет.

- Источники событий – группа для аналитики об источниках событий. В группу входят следующие виджеты:
  - **Топ источников событий по количеству алертов** – количество незакрытых алертов, сгруппированных по источникам событий.
  - **Топ источников событий по условному рейтингу** – количество событий, для которых существует незакрытый алерт, сгруппированных по источникам событий.

    > В связи с оптимизациями хранения событий в алертах в ряде случаев количество алертов созданных источниками может быть искажено. Для получения точной статистики рекомендуется в правиле корреляции указать поле события Device Product в качестве уникального, а также включить хранение всех базовых событий в корреляционном событии. Правила корреляции с такими настройками являются более ресурсоемкими.

- Пользователи – группа для аналитики о пользователях из обработанных событий. В группу входят следующие виджеты:
  - **Пользователи в алертах** – количество пользователей, связанных с незакрытыми алертами.

- **Количество пользователей AD** – количество учетных записей в Active Directory, полученных по LDAP в течение указанного в виджете периода.

В таблице событий, в области деталей событий, в окне алертов, а также в виджетах в качестве значений полей SourceAssetID, DestinationAssetID, DeviceAssetID, SourceAccountID, DestinationAccountID и ServiceID вместо идентификаторов отображаются названия активов, учетных записей или сервисов. При экспорте событий в файл идентификаторы сохраняются, однако в файл добавляются столбцы с названиями. Идентификаторы также отображаются при наведении указателя мыши на названия активов, учетных записей или сервисов.

Поиск по полям с идентификаторами возможен только с помощью идентификаторов.

Стандартные виджеты

В этом разделе описываются параметры всех виджетов, кроме виджета События и Активные листы.

Доступные параметры виджетов и стандартные ограничения по отображению данных зависят от выбранного типа виджета. Тип виджета определяется по значку:

- – круговая диаграмма.
- – счетчик.
- – таблица.
- – столбчатая диаграмма.
- – календарная диаграмма.

Параметры круговых диаграмм, счетчиков и таблиц

Параметры круговых диаграмм, счетчиков и таблиц располагаются на одной закладке. Набор параметров зависит от выбранного виджета:

- **Название** – поле для названия виджета. Должно содержать от 1 до 128 символов Юникода.
- **Описание** – поле для описания виджета. Вы можете добавить до 4000 символов Юникода, описывающих виджет.
- **Тенант** – раскрывающийся список для выбора тенантов, по данным которых будет отображаться аналитика. Выбирать можно из тенантов, для которых настроен макет. Если

не выбран ни один тенант, используется параметр по умолчанию **Как на макете**.

- **Период** – раскрывающийся список для настройки периода времени, за который должна отображаться аналитика. Доступные варианты:

  - **Как на макете** – когда выбран этот параметр, значение периода времени виджета отражает период, который был настроен для макета. Этот вариант выбран по умолчанию.

  - **1 час** – получить аналитику за предыдущий час.

  - **1 день** – получить аналитику за предыдущий день.

  - **7 дней** – получить аналитику за предыдущие 7 дней.

  - **30 дней** – получить аналитику за предыдущие 30 дней.

  - **В течение периода** – получать аналитику за выбранный период времени. Период времени устанавливается с помощью календаря, который отображается при выборе этого параметра.

    > Верхняя граница периода не включается в определяемый с ее помощью отрезок времени. Это означает, что, например, для получения аналитики за сутки следует настроить период День1, 00:00:00 – День 2, 00:00:00, а не День 1, 00:00:00 – День 1, 23:59:59.

  > Для календарных диаграмм временной отрезок по оси X строится периоду, выбранному пользователем в раскрывающемся списке **Период**. При этом данные для аналитики подбираются по датам из полей событий в SQL-запросе, а не по полю события Timestamp.

- **Хранилище** – раскрывающийся список для выбора хранилища, события которого будут использоваться для создания аналитики.

- **Цвет** – раскрывающийся список для выбора цвета отображения информации:

  - **по умолчанию** – использовать цвет шрифта, который используется в вашем браузере по умолчанию;

  - **зеленый**;

  - **красный**;

    - **синий**;
    - **желтый**.

- **Горизонтальный** – включите этот переключатель, если хотите использовать горизонтальную гистограмму вместо вертикальной. По умолчанию этот переключатель выключен.

- **Легенда** – выключите этот переключатель, если не хотите, чтобы в виджете отображалась легенда для аналитики. По умолчанию этот переключатель включен.

- **Пустые значения в легенде** – включите этот переключатель, если хотите, чтобы в легенде для аналитики отображались параметры с нулевыми значениями. По умолчанию этот переключатель выключен.

- **Десятичные знаки** – это поле используется, чтобы указать степень округления значений. Значение по умолчанию: **Авто**.

Параметры столбчатых диаграмм

Параметры столбчатых диаграмм располагаются в двух закладках. Набор параметров зависит от выбранного виджета:

- – закладка предназначена для настройки масштаба графика. Доступные параметры:

    - Поля **Минимальное значение Y** и **Максимальное значение Y** используются для определения масштаба оси Y. Поле **Десятичные знаки** слева используется для установки параметра округления для значений оси Y.

    - Поля **Минимальное значение X** и **Максимальное значение X** используются для определения масштаба оси X. Поле **Десятичные знаки** справа используется для установки параметра округления для значений 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**.

- – закладка предназначена для настройки отображения аналитики виджета.

    - **Название** – поле для названия виджета. Должно содержать от 1 до 128 символов Юникода.

- **Описание** – поле для описания виджета. Вы можете добавить до 512 символов Юникода, описывающих виджет.

- **Тенант** – раскрывающийся список для выбора тенанта, по данным которого будет отображаться аналитика.

- **Период** – раскрывающийся список для настройки периода времени, за который должна отображаться аналитика. Доступные варианты:

  - **Как на макете** – когда выбран этот параметр, значение периода времени виджета отражает период, который был настроен для макета. Этот вариант выбран по умолчанию.

  - **1 час** – получить аналитику за предыдущий час.

  - **1 день** – получить аналитику за предыдущий день.

  - **7 дней** – получить аналитику за предыдущие 7 дней.

  - **30 дней** – получить аналитику за предыдущие 30 дней.

  - **В течение периода** – получать аналитику за выбранный период времени. Период времени устанавливается с помощью календаря, который отображается при выборе этого параметра.

- **Хранилище** – раскрывающийся список для выбора хранилища, события которого будут использоваться для создания аналитики.

- **Цвет** – раскрывающийся список для выбора цвета отображения информации:

  - **по умолчанию** – использовать цвет шрифта, который используется в вашем браузере по умолчанию.

  - **зеленый**

  - **красный**

  - **синий**

  - **желтый**

- **Горизонтальный** – включите этот переключатель, если хотите использовать горизонтальную гистограмму вместо вертикальной. По умолчанию этот переключатель выключен.

При включении этого параметра горизонтальная прокрутка при большом количестве данных отображаться не будет и вся имеющаяся информация будет отражена в заданном размере виджета. Если данных для отображения много, рекомендуется увеличить размер виджета.

- **Итоговые значения** – включите этот переключатель, чтобы на виджете, кроме отдельных значений, отображались их суммы.

- **Легенда** – выключите этот переключатель, если не хотите, чтобы в виджете отображалась легенда для аналитики. По умолчанию этот переключатель включен.

- **Пустые значения в легенде** – включите этот переключатель, если хотите, чтобы в легенде для аналитики отображались параметры с нулевыми значениями. По умолчанию этот переключатель выключен.

- **Десятичные знаки** – это поле используется, чтобы указать степень округления значений. Значение по умолчанию: **Авто**.

Настраиваемая аналитика по событиям

Вы можете использовать виджет **События** для получения необходимой аналитики на основе SQL-запросов по событиям. В зависимости от выбранного значения типа графика доступны две или три закладки параметров:

- – эта закладка используется для определения типа виджета и построения поиска для аналитики.

- – закладка предназначена для настройки масштаба графика. Эта закладка доступна только для типов графиков (см. ниже) **Столбчатая диаграмма**, **Линейная диаграмма**, **Календарная диаграмма**.

- – закладка предназначена для настройки отображения аналитики виджета.

Следующие параметры доступны для закладки :

- **График** – этот раскрывающийся список используется для выбора типа графика виджета. Доступные варианты:

  - **Круговая диаграмма**

  - **Столбчатая диаграмма**

  - **Счетчик**

  - **Линейная диаграмма**

    - **Таблица**
    - **Календарная диаграмма**

- **Тенант** – раскрывающийся список для выбора тенантов, по данным которых будет отображаться аналитика. Выбирать можно из тенантов, для которых настроен макет. Если не выбран ни один тенант, используется параметр по умолчанию **Как на макете**.

- **Период** – раскрывающийся список для настройки периода времени, за который должна отображаться аналитика. Доступные варианты:

    - **Как на макете** – когда выбран этот параметр, значение периода времени виджета отражает период, который был настроен для макета. Этот вариант выбран по умолчанию.

    - **1 час** – получить аналитику за предыдущий час.

    - **1 день** – получить аналитику за предыдущий день.

    - **7 дней** – получить аналитику за предыдущие 7 дней.

    - **30 дней** – получить аналитику за предыдущие 30 дней.

    - **В течение периода** – получать аналитику за выбранный период времени. Период времени устанавливается с помощью календаря, который отображается при выборе этого параметра.

    > Верхняя граница периода не включается в определяемый с ее помощью отрезок времени. Это означает, что, например, для получения аналитики за сутки следует настроить период День1, 00:00:00 – День 2, 00:00:00, а не День 1, 00:00:00 – День 1, 23:59:59.

- **Показывать данные за предыдущий период** – переключатель, с помощью которого в виджете можно включить отображение данных сразу за два периода: за текущий и за предыдущий. Это может быть полезно для оценки динамики изменений.

- **Хранилище** – хранилище, в котором должен выполняться поиск.

- Поле SQL-запроса – в этом можно ввести поисковый запрос, аналогичный фильтрации событий с использованием синтаксиса SQL.

  Для виджетов **События** с помощью кнопки можно открыть конструктор запросов, аналогичный параметрам конструктора фильтра событий:

  [Описание параметров конструктора запросов]

- **SELECT** – используйте эти поля для определения полей событий, которые необходимо извлечь для аналитики. Количество доступных полей зависит от выбранного типа графика виджета (см. выше).

  В левом выпадающем списке вы можете выбрать поля событий из необходимых для аналитики.

  Среднее поле показывает, для чего выбранное поле используется в виджете: **metric** (метрики) или **value** (значение).

  > При выборе типа виджета **Таблица** значения в средних полях становятся доступны для редактирования и отображаются в виде названий столбцов. В качестве значений доступны только символы ANSII-ASCII.

  В правом раскрывающемся списке необходимо выбрать, как должны обрабатываться значения поля события типа **metric** (метрики) для виджета:

  - **count** – выберите этот вариант для подсчета событий. Эта опция 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** – выберите этот параметр, чтобы отобразить максимальное значение поля события из выборки событий.

  - **min** – выберите этот параметр, чтобы отображать минимальное значение поля события из выборки событий.

  - **avg** – выберите эту опцию, чтобы отображать среднее значение поля события из выборки событий.

  - **sum** – выберите этот параметр, чтобы отобразить сумму значений полей событий из выборки событий.

- **SOURCE** – этот раскрывающийся список используется для выбора типа источника данных. Для выбора доступна только опция **events** (события).

- **WHERE** – эта группа настроек используется для создания условий поиска:

  В левом раскрывающемся списке вы можете выбрать поле события, которое хотите использовать в качестве фильтра.

  В среднем выпадающем списке вы можете выбрать нужный оператор. Доступные операторы различаются в зависимости от типа значения выбранного поля события.

Справа вы можете выбрать или ввести значение поля события. В зависимости от выбранного типа значения поля события может потребоваться ввести значение вручную, выбрать его в раскрывающемся списке или выбрать в календаре.

Вы можете добавить условия поиска с помощью кнопки **Добавить условие** или удалить их с помощью кнопки со значком крестика.

Вы также можете добавить группы условий, используя кнопку **Добавить группу**. По умолчанию группы условий добавляются с оператором **AND**, однако если на него нажать, оператор можно поменять. Доступные значения: **AND**, **OR**, **NOT**. Группы условий удаляются с помощью кнопки **Удалить группу**.

- **GROUP BY** – этот раскрывающийся список используется для выбора полей событий, по которым осуществляется группировка событий. Этот параметр недоступен для типа графиков **Счетчик**.

- **ORDER BY** – этот раскрывающийся список используется для определения способа сортировки информации из результатов поиска в виджете. Этот параметр недоступен для типов графиков **Календарная диаграмма** и **Счетчик**.

  В левом раскрывающемся списке вы можете выбрать значение, метрику или поле события, которое будет использоваться для сортировки.

  В правом раскрывающемся списке можно выбрать порядок сортировки: **ASC** – для сортировки по возрастанию, **DESC** – для сортировки по убыванию.

  Для графиков типа **Таблица** можно добавить условия сортировки с помощью кнопки **Добавить столбец**.

- **LIMIT** – это поле используется для установки максимального количества точек данных для виджета. Этот параметр недоступен для типов графиков **Календарная диаграмма** и **Счетчик**.

[Пример условий поиска в конструкторе запросов](#)

Параметры условия поиска для виджета, показывающие среднее количество байтов, полученных с одного хоста

Псевдонимы metric и value в SQL-запросах недоступны для изменения для всех типов виджета с аналитикой по событиям, кроме таблиц.

Псевдонимы в виджетах 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` ``.

При отображении данных за предыдущий период сортировка по параметру `count(ID)` может работать некорректно. Рекомендуется использовать сортировку по параметру metric. Например, `SELECT count(ID) AS "metric", Name AS "value" FROM `events` GROUP BY Name ORDER BY metric ASC LIMIT 250`.

В виджетах типа **Счетчик** необходимо для значений функции `SELECT` указывать способ обработки данных: `count`, `max`, `min`, `avg`, `sum`.

Следующие параметры доступны для закладки :

- Поля **Минимальное значение Y** и **Максимальное значение Y** используются для определения масштаба оси Y. Поле **Десятичные знаки** слева используется для установки параметра округления для значений оси Y.

- Поля **Минимальное значение X** и **Максимальное значение X** используются для определения масштаба оси X. Поле **Десятичные знаки** справа используется для установки параметра округления для значений 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**.

- Поля **Толщина линии** и **Размер указателя** отображаются для типа графика **Линейная диаграмма** и используются для настройки отображения графика.

Следующие параметры доступны для закладки 🔧:

- **Название** – поле для названия виджета. Должно содержать от 1 до 128 символов Юникода.
- **Описание** – поле для описания виджета. Вы можете добавить до 512 символов Юникода, описывающих виджет.
- **Цвет** – раскрывающийся список для выбора цвета отображения информации:
  - **по умолчанию** – использовать цвет шрифта, который используется в вашем браузере по умолчанию;
  - **зеленый**;
  - **красный**;
  - **синий**;
  - **желтый**.
- **Горизонтальный** – включите этот переключатель, если хотите использовать горизонтальную гистограмму вместо вертикальной. По умолчанию этот переключатель выключен.

  При включении этого параметра горизонтальная прокрутка при большом количестве данных отображаться не будет и вся имеющаяся информация будет отражена в заданном размере виджета. Если данных для отображения много, рекомендуется увеличить размер виджета.
- **Итоговые значения** – включите этот переключатель, чтобы на виджете, кроме отдельных значений, отображались их суммы.
- **Легенда** – выключите этот переключатель, если не хотите, чтобы в виджете отображалась легенда для аналитики. По умолчанию этот переключатель включен.
- **Пустые значения в легенде** – включите этот переключатель, если хотите, чтобы в легенде для аналитики отображались параметры с нулевыми значениями. По умолчанию этот переключатель выключен.
- **Десятичные знаки** – поле для ввода количества десятичных знаков, до которых отображаемое значение должно быть округлено.
- **Длительность отрезков периода** (доступно для типов графика **Календарная диаграмма**) – раскрывающийся список для выбора длительности отрезков, на которые требуется делить период.

Настраиваемая аналитика по активным листам

Вы можете использовать виджеты **Активные листы** для получения необходимой аналитики на основе SQL-запросов активным листам. В зависимости от выбранного значения типа графика доступны две или три закладки параметров:

- – эта закладка используется для определения типа виджета и построения поиска для аналитики.
- – закладка предназначена для настройки масштаба графика. Эта закладка доступна только для типов графиков (см. ниже) **Столбчатая диаграмма**.
- – закладка предназначена для настройки отображения аналитики виджета.

Следующие параметры доступны для закладки :

- **График** – этот раскрывающийся список используется для выбора типа графика виджета. Доступные варианты:
  - **Круговая диаграмма**
  - **Столбчатая диаграмма**
  - **Счетчик**
  - **Таблица**
- **Тенант** – раскрывающийся список для выбора тенантов, по данным которых будет отображаться аналитика. Выбирать можно из тенантов, для которых настроен макет. Если не выбран ни один тенант, используется параметр по умолчанию **Как на макете**.
- **Коррелятор** – название сервиса коррелятор, по активному листу которого требуется аналитика.
- **Активный лист** – название активного листа, в котором должен выполняться поиск.

  > Один и тот же ресурс активного листа может быть использован разными сервисами корреляторов, однако при этом для каждого коррелятора создается своя сущность активного листа. Таким образом, содержимое активных листов, используемых разными корреляторами, различается, даже если идентификатор и название активных листов одинаковые.

- Поле SQL-запроса – в этом можно ввести поисковый запрос, аналогичный поиску событий с использованием синтаксиса SQL.

  Особенности SQL-запросам по активным листам:

- В отличие от поиска по событиям, в поисковых запросах по активным листам параметру **FROM** должно соответствовать значение `` `records` ``.

- С помощью SQL-запроса можно обращаться к полям активного листа, названия которых содержат пробелы и символы кириллицы. В запросах такие названия необходимо выделять кавычками.

  Если название поля активного листа начинается или заканчивается пробелами, в виджете эти пробелы не отображаются. Название поля не должно состоять только из пробелов.

  Если значения полей активного листа могут содержать пробелы в конце или в начале, поиск по ним рекомендуется осуществлять с помощью функции `LIKE '%значение поля%'`.

- Для запросов доступны служебные поля `_key` (поле с ключами записей активного листа) и `_count` (сколько раз эта запись была добавлена в активный лист), а также пользовательские поля.

- Псевдонимы metric и value в SQL-запросах недоступны для изменения для всех типов виджета с аналитикой по активным листам, кроме таблиц.

- Если в SQL-запросе используется функция преобразования даты и времени (например, fromUnixTimestamp64Milli) и при этом обрабатываемое поле не содержит даты и времени, в виджете будет отображаться ошибка. Чтобы избежать этого, используйте функции, которые могут обрабатывать нулевое значение. Пример: `SELECT _key, fromUnixTimestamp64Milli(toInt64OrNull(DateTime)) as Date FROM `records` LIMIT 250`.

- Если задать большие значения параметру LIMIT, это может привести к ошибкам в работе браузера.

- В виджетах типа **Счетчик** необходимо для значений функции `SELECT` указывать способ обработки данных: `count`, `max`, `min`, `avg`, `sum`.

Примеры SQL-запросов для получения аналитики по активным листам:

- `SELECT * FROM `records` WHERE "Источник событий" = 'Екатеринбург' LIMIT 250` – Запрос, который возвращает ключ активного листа с названием поля "Источник событий" и значением этого поля "Екатерингбург".

- `SELECT count(_key) AS metric, Status AS value FROM `records` GROUP BY value ORDER BY metric DESC LIMIT 250` – Запрос для круговой диаграммы, который возвращает количество ключей активного листа (агрегация `count` по полю `_key`) и все варианты значений пользовательского поля `Status`. В виджете отображается круговая диаграмма с общим количеством записей активного листа, пропорционально разделенным на количество вариантов значений поля `Status`.

- `SELECT Name, Status, _count AS Number FROM `records` WHERE Description ILIKE '%ftp%' ORDER BY Name DESC LIMIT 250` – Запрос для таблицы, которая возвращает значения пользовательских полей `Name` и `Status`, а также служебного поля `_count` у тех записей активного листа, в которых значения пользовательского поля `Description` соответствует запросу `ILIKE '%ftp%'`. В виджете отображается таблица со столбцами Status, Name и Number.

Следующие параметры доступны для закладки :

- Поля **Минимальное значение Y** и **Максимальное значение Y** используются для определения масштаба оси Y. Поле **Десятичные знаки** слева используется для установки параметра округления для значений оси Y.

- Поля **Минимальное значение X** и **Максимальное значение X** используются для определения масштаба оси X. Поле **Десятичные знаки** справа используется для установки параметра округления для значений 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**.

Следующие параметры доступны для закладки :

- **Название** – поле для названия виджета. Должно содержать от 1 до 128 символов Юникода.

- **Описание** – поле для описания виджета. Вы можете добавить до 512 символов Юникода, описывающих виджет.

- **Цвет** – раскрывающийся список для выбора цвета отображения информации:

  - **по умолчанию** – использовать цвет шрифта, который используется в вашем браузере по умолчанию.

  - **зеленый**

  - **красный**

  - **синий**

  - **желтый**

- **Горизонтальный** – включите этот переключатель, если хотите использовать горизонтальную гистограмму вместо вертикальной. По умолчанию этот переключатель выключен.

При включении этого параметра горизонтальная прокрутка при большом количестве данных отображаться не будет и вся имеющаяся информация будет отражена в заданном размере виджета. Если данных для отображения много, рекомендуется увеличить размер виджета.

- **Итоговые значения** – включите этот переключатель, чтобы на виджете, кроме отдельных значений, отображались их суммы.

- **Легенда** – выключите этот переключатель, если не хотите, чтобы в виджете отображалась легенда для аналитики. По умолчанию этот переключатель включен.

- **Пустые значения в легенде** – включите этот переключатель, если хотите, чтобы в легенде для аналитики отображались параметры с нулевыми значениями. По умолчанию этот переключатель выключен.

- **Десятичные знаки** – поле для ввода количества десятичных знаков, до которых отображаемое значение должно быть округлено.

Особенности отображения данных в виджетах

Ограничение отображаемых данных

Для удобства восприятия информации в KUMA заданы ограничения на отображение данных в виджетах в зависимости от их типа:

- Круговая диаграмма – отображается не более 20 отсеков.

- Столбчатая диаграмма – отображается не более 40 столбцов.

- Таблица – отображается не более 500 записей.

- Календарная диаграмма – отображается не более 365 дней.

Данные, выходящие за указанные ограничения, отображаются в виджете в категории **Остальное**.

Полные данные, по которым построена аналитика в виджете, можно скачать в формате CSV, нажав на кнопку **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.

Работа с тенантами

Доступ к тенантам регулируется в настройках пользователей. *Главный администратор* имеет доступ к данным всех тенантов. Только пользователь с этой ролью может создавать и выключать тенанты.

Тенанты отображаются в таблице раздела веб-интерфейса KUMA **Параметры** → **Тенанты**. Нажимая на столбцы, таблицу можно отсортировать.

Доступные столбцы:

- **Название** – название тенанта. Таблицу можно фильтровать по этому столбцу.

- **Ограничение EPS** – размер квоты EPS (частота обработки событий в секунду), выделенной тенанту из общей квоты EPS, которая определяется лицензией.

- **Описание** – описание тенанта.

- **Выключено** – отметка о том, является ли тенант неактивным.

  По умолчанию неактивные тенанты в таблице не отображаются. Вы можете их просмотреть, установив флажок **Показать выключенных**.

- **Создан** – дата создания тенанта.

Чтобы создать тенант:

1. В разделе веб-интерфейса KUMA **Параметры** → **Тенанты** нажмите **Добавить**.

   Откроется окно **Добавить тенант**.

2. В поле **Название** укажите название тенанта. Название должно содержать от 1 до 128 символов Юникода.

3. В поле **Ограничение EPS** укажите квоту EPS для тенанта. Сумма EPS всех тенантов не может превышать EPS лицензии.

4. При необходимости добавьте **Описание** тенанта. Описание должно содержать не более 256 символов Юникода.

5. Нажмите **Сохранить**.

Тенант добавлен и отображается в таблице тенантов.

Чтобы выключить или включить тенант:

1. В разделе веб-интерфейса KUMA **Параметры** → **Тенанты** выберите нужный тенант.

   Если тенант выключен и не отображается в таблице, установите флажок **Показать выключенных**.

2. Нажмите **Выключить** или **Включить**.

При выключении тенанта принадлежащие ему сервисы автоматически останавливаются, прием и обработка событий прекращается, EPS тенанта более не учитывается в общем количестве EPS лицензии.

При включении тенанта его сервисы требуется запустить вручную.

Выбор тенанта

Если вы имеете доступ к нескольким тенантам, в KUMA можно выбрать, данные каких тенантов будут отображаться в веб-интерфейсе KUMA.

Чтобы выбрать тенант для отображения данных:

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

   Откроется область выбора тенантов.

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

3. Требуется выбрать как минимум один тенант. Тенанты можно искать с помощью поля **Поиск**.

4. Закройте область выбора тенантов, нажав **Выбрано тенантов**.

В разделах веб-интерфейса KUMA отображаются только данные и аналитика, относящаяся к выбранным тенантам.

От выбранных для отображения данных тенантов зависит, какие тенанты можно будет указать при создании ресурсов, сервисов, макетов, шаблонов отчетов, виджетов, инцидентов, активов и других параметров KUMA, где можно выбрать тенант.

Правила принадлежности к тенантам

Правила наследования тенанта

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

- Тенант объекта (например, сервиса или ресурса) определяется пользователем при его создании.

  После создания объекта выбранный для него тенант невозможно изменить. Ресурсы, однако, можно экспортировать, а затем импортировать в другой тенант.

- Тенант алерта и корреляционного события наследуется от создавшего их коррелятора.

  Название тенанта указывается в поле события `TenantId`.

- Если события разных тенантов, обрабатываемых одним коррелятором, не смешиваются, создаваемые им корреляционные события наследуют тенант события.

- Тенант инцидента наследуется от алерта.

Примеры мультитенантных взаимодействий

Мультитенантность в KUMA дает возможность централизованно расследовать алерты и инциденты, возникающие в разных тенантах. Ниже приведены сценарии, по которым можно проследить, к каким тенантам принадлежат создаваемые объекты.

> При корреляции событий от разных тенантов в общем потоке **не следует** группировать события по тенанту: то есть не нужно в правилах корреляции в поле **Группирующие поля** указывать поле события `TenantId`. Группировка событий по тенанту необходима, только если нужно не смешивать события от разных тенантов.

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

- **Корреляция событий в рамках одного тенанта, коррелятор выделен для этого тенанта и развернут на его стороне**

  Условие:

  Коллектор и коррелятор принадлежат тенанту 2 (tenantID=2)

Сценарий:

1. Коллектор тенанта 2 получает и отправляет события в коррелятор тенанта 2.
2. При срабатывании корреляционных правил в корреляторе создаются корреляционные события с идентификатором тенанта tenantID=2.
3. Коррелятор отправляет корреляционные события в раздел хранилища для тенанта 2.
4. Создается алерт, привязанный к тенанту с идентификатором tenantID=2.
5. К алерту привязываются события, из-за которых он был создан.

Инцидент создается пользователем вручную. Тенант инцидента определяется тенантом пользователя. Алерт привязывается к инциденту вручную или автоматически.

- **Корреляция событий в рамках одного тенанта, коррелятор выделен для этого тенанта и развернут на стороне главного тенанта**

Условие:

- Коллектор развернут на тенанте 2 и принадлежат ему (tenantID=2).
- Коррелятор развернут на стороне главного тенанта.

  Принадлежность коррелятора определяется главным администратором в зависимости того, кто будет расследовать инциденты тенанта 2: сотрудники главного тенанта или тенанта 2. Принадлежность алерта и инцидента зависит от принадлежности коррелятора.

Сценарий 1. Коррелятор принадлежит тенанту 2 (tenantID=2):

1. Коллектор тенанта 2 получает и отправляет события в коррелятор.
2. При срабатывании корреляционных правил в корреляторе создаются корреляционные события с идентификатором тенанта tenantID=2.
3. Коррелятор отправляет корреляционные события в раздел хранилища тенанта 2.
4. Создается алерт, привязанный к тенанту с идентификатором tenantID=2.
5. К алерту привязываются события, из-за которых он был создан.

Результат 1:

- Созданный алерт и привязанные к нему события доступны сотрудникам тенанта 2.

Сценарий 2. Коррелятор принадлежит главному тенанту (tenantID=1):

1. Коллектор тенанта 2 получает и отправляет события в коррелятор.
2. При срабатывании корреляционных правил в корреляторе создаются корреляционные события с идентификатором тенанта tenantID=1.
3. Коррелятор отправляет корреляционные события в раздел хранилища главного тенанта.
4. Создается алерт, привязанный к тенанту с идентификатором tenantID=1.
5. К алерту привязываются события, из-за которых он был создан.

Результат 2:

- Алерт и привязанные к нему события недоступны сотрудникам тенанта 2.
- Алерт и привязанные к нему события доступны сотрудникам главного тенанта.

- **Централизованная корреляция событий, поступающих от разных тенантов**

Условие:

- Развернуто два коллектора: на тенанте 2 и тенанте 3. Оба коллектора отправляют события в один коррелятор.
- Коррелятор принадлежит главному тенанту. Правило корреляции ожидает события от обоих тенантов.

Сценарий:

1. Коллектор тенанта 2 получает и отправляет события в коррелятор главного тенанта.
2. Коллектор тенанта 3 получает и отправляет события в коррелятор главного тенанта.
3. При срабатывании корреляционного правила в корреляторе создаются корреляционные события с идентификатором тенанта tenantID=1.

4. Коррелятор отправляет корреляционные события в раздел хранилища главного тенанта.

5. Создается алерт, привязанный к главному тенанту с идентификатором tenantID=1.

6. К алерту привязываются события, из-за которых он был создан.

Результат:

- Алерт и привязанные к нему события недоступны сотрудникам тенанта 2.
- Алерт и привязанные к нему события недоступны сотрудникам тенанта 3.
- Алерт и привязанные к нему события доступны сотрудникам главного тенанта.

- **Тенант коррелирует свои события, но в главном тенанте дополнительно осуществляется централизованная корреляция событий**

Условие:

- Развернуто два коллектора: на главном тенанте и тенанте 2.
- Развернуто два коррелятора:
  - Коррелятор 1 принадлежит главному тенанту и принимает события с коллектора главного тенанта и коррелятора 2.
  - Коррелятор 2 принадлежит тенанту 2 и принимает события с коллектора тенанта 2.

Сценарий:

1. Коллектор тенанта 2 получает и отправляет события в коррелятор 2.
2. При срабатывании корреляционного правила в корреляторе тенанта 2 создаются корреляционные события с идентификатором тенанта tenantID=2.
   - Коррелятор 2 отправляет корреляционные события в раздел хранилища тенанта 2.
   - Создается алерт 1, привязанный к тенанту с идентификатором tenantID=2.
   - К алерту привязываются события, из-за которых он был создан.

- Корреляционные события от коррелятора тенанта 2 отправляются в коррелятор 1.

3. Коллектор главного тенанта получает и отправляет события в коррелятор 1.

4. В корреляторе 1 обрабатываются события обоих тенантов. При срабатывании корреляционного правила создаются корреляционные события с идентификатором тенанта tenantID=1.

   - Коррелятор 1 отправляет корреляционные события в раздел хранилища главного тенанта.

   - Создается алерт 2, привязанный к тенанту с идентификатором tenantID=1.

   - К алерту привязываются события, из-за которых он был создан.

Результат:

- Алерт 2 и привязанные к нему события недоступны сотрудникам тенанта 2.

- Алерт 2 и привязанные к нему события доступны сотрудникам главного тенанта.

- **Один коррелятор для двух тенантов**

> Если вы не хотите, чтобы при корреляции события от разных тенантов смешивались, в правилах корреляции в поле **Группирующие поля** следует указывать поле события `TenantId`. В таком случае алерт наследует тенант от коррелятора.

Условие:

- Развернуто два коллектора: на тенанте 2 и тенанте 3.

- Развернут один коррелятор, принадлежащий главному тенанту (tenantID=1). Он принимает события от обоих тенантов, но обрабатывает их независимо друг от друга.

Сценарий:

1. Коллектор тенанта 2 получает и отправляет события в коррелятор.

2. Коллектор тенанта 3 получает и отправляет события в коррелятор.

3. При срабатывании корреляционного правила в корреляторе создаются корреляционные события с идентификатором тенанта tenantID=1.

   - Коррелятор отправляет корреляционные события в раздел хранилища главного тенанта.
   - Создается алерт, привязанный к главному тенанту с идентификатором tenantID=1.
   - К алерту привязываются события, из-за которых он был создан.

Результат:

- Алерты, созданные на основе событий от тенанта 2 и 3, недоступны сотрудникам тенантов 2 и 3.
- Алерты и привязанные к ним события доступны сотрудникам главного тенанта.

Работа с инцидентами

В разделе **Инциденты** веб-интерфейса KUMA можно создавать, просматривать и обрабатывать инциденты. При необходимости вы также можете фильтровать инциденты. При нажатии на название инцидента открывается окно со сведениями о нем.

Инциденты можно экспортировать в НКЦКИ.

Срок хранения инцидентов составляет один год, однако этот параметр можно изменить.

Формат даты инцидента зависит от языка локализации, выбранного в настройках программы. Возможные варианты формата даты:

- Английская локализация: ГГГГ-ММ-ДД.
- Русская локализация: ДД.ММ.ГГГГ.

О таблице инцидентов

В основной части раздела **Инциденты** отображается таблица с информацией о зарегистрированных инцидентах. При необходимости вы можете изменить набор столбцов и порядок их отображения в таблице.

Как настроить таблицу инцидентов

1. В правом верхнем углу таблицы инцидентов нажмите на значок .

   Откроется окно настройки таблицы.

2. Установите флажки напротив тех параметров, которые требуется отображать в таблице.

   Когда вы устанавливаете флажок, таблица событий обновляется и добавляется новый столбец. При снятии флажка столбец исчезает.

   С помощью поля **Поиск** можно искать параметры таблицы.

   При нажатии на кнопку **По умолчанию** для отображения выбираются следующие столбцы:

   - **Название**.
   - **Длительность инцидента**.
   - **Назначен**.
   - **Создано**.
   - **Тенант**.
   - **Статус**.
   - **Количество алертов**.
   - **Уровень важности**.
   - **Категории затронутых активов**.

3. При необходимости измените порядок отображения столбцов, перетащив заголовки столбцов.

4. Чтобы отсортировать инциденты по определенному параметру, нажмите на заголовок нужного столбца и в раскрывающемся списке выберите один из вариантов: **По возрастанию** или **По убыванию**.

5. Чтобы отфильтровать инциденты по определенному параметру, нажмите на заголовок нужного столбца и в раскрывающемся списке выберите требуемые фильтры. Набор фильтров, доступный в раскрывающемся списке, зависит от выбранного столбца.

6. Чтобы снять фильтры, нажмите на заголовок нужного столбца и выберите **Очистить фильтр**.

Доступные столбцы таблицы инцидентов:

- **Название** – название инцидента.
- **Длительность инцидента** – время, на протяжении которого происходил инцидент (время между первым и последним событием, относящимся к инциденту).
- **Назначен** – имя сотрудника службы безопасности, которому инцидент передан для расследования или реагирования.
- **Создан** – дата и время создания инцидента. С помощью этого столбца инциденты можно фильтровать по времени их создания.
  - Доступны преднастроенные периоды: **Сегодня**, **Вчера**, **На этой неделе**, **На прошлой неделе**.
  - При необходимости можно задать произвольный период с помощью календаря, который открывается при выборе пунктов **До даты**, **После даты**, **В течение периода**.
- **Тенант** – название тенанта, которому принадлежит инцидент.
- **Статус** – текущее состояние инцидента:
  - **Открыт** – новый, еще не обработанный инцидент.
  - **Назначен** – инцидент обработан и передан сотруднику службы безопасности для расследования или реагирования.
  - **Закрыт** – инцидент закрыт, угроза безопасности устранена.
- **Количество алертов** – количество алертов, входящих в инцидент. Учитываются только алерты тех тенантов, к которым у вас есть доступ.
- **Уровень важности** – степень значимости потенциальной угрозы безопасности: **Критический** , **Высокий** , **Средний** , **Низкий** .
- **Категории затронутых активов** – категории активов с наибольшим уровнем важности, относящихся к алерту. Отображается не более трех категорий.
- **Последнее обновление** – дата и время последнего изменения, сделанного в инциденте.

- **Первое событие** и **Последнее событие** – дата и время первого и последнего события в инциденте.
- **Категория инцидента** и **Тип инцидента** – категория и тип угрозы, присвоенные инциденту.
- **Экспорт в НКЦКИ** – статус экспорта данных об инциденте в НКЦКИ:
  - **Не экспортировался** – данные не передавались в НКЦКИ.
  - **Ошибка экспорта** – попытка передать данные в НКЦКИ завершилась ошибкой, данные не переданы.
  - **Экспортирован** – данные об инциденте успешно переданы в НКЦКИ.
- **Ветвь** – данные о том, в каком узле был создан инцидент. По умолчанию отображаются инциденты вашего узла. Этот столбец отображается только при включенном режиме иерархии.
- **КИИ** – указание на то, относятся ли к инциденту активы, являющиеся объектами КИИ. Столбец скрыт от пользователей, не имеющих прав доступа к объектам КИИ.

В поле **Поиск** можно ввести регулярное выражение для поиска инцидентов по связанным с ними активами, пользователям, тенантам или корреляционным правилам. Параметры, по которым производится поиск:

- Активы: название, FQDN, IP-адрес.
- Учетные записи Active Directory: атрибуты displayName, SAMAccountName, UserPrincipalName.
- Корреляционные правила: название.
- Пользователи KUMA, которым назначены алерты: имя, логин, адрес электронной почты.
- Тенанты: название.

При фильтрации инцидентов по какому-либо параметру соответствующий столбец в таблице инцидентов подсвечивается желтым цветом.

Сохранение и выбор конфигураций фильтра инцидентов

В KUMA можно сохранять изменения параметров таблицы инцидентов в виде фильтров. Конфигурации фильтров сохраняются на сервере Ядра KUMA и доступны всем пользователям KUMA того тенанта, для которого они были созданы.

Чтобы сохранить текущие параметры конфигурации фильтра:

1. В разделе KUMA **Инциденты** откройте раскрывающийся список **Выбрать фильтр**.

2. Выберите **Сохранить текущий фильтр**.

   Откроется окно для ввода названия нового фильтра и выбора тенанта, которому он будет принадлежать.

3. Введите название конфигурации фильтра. Название должно быть уникальным для фильтров алертов, фильтров инцидентов и фильтров событий.

4. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать фильтр, и нажмите **Сохранить**.

Конфигурация фильтра сохранена.

Чтобы выбрать ранее сохраненную конфигурацию фильтра:

1. В разделе KUMA **Инциденты** откройте раскрывающийся список **Выбрать фильтр**.

2. Выберите нужную конфигурацию.

Конфигурация фильтра активна.

Вы можете выбрать фильтр, который будет использоваться по умолчанию, поставив в раскрывающемся списке **Фильтры** звездочку левее названия требуемой конфигурации фильтра.

Чтобы сбросить текущие настройки фильтра,

откройте раскрывающийся список **Фильтры** и выберите **Очистить фильтр**.

Удаление конфигураций фильтра инцидентов

Чтобы удалить ранее сохраненную конфигурацию фильтра:

1. В разделе KUMA **Инциденты** откройте раскрывающийся список **Фильтры**.

2. Нажмите значок рядом с фильтром, который требуется удалить.

3. Нажмите **OK**.

Конфигурация фильтра удалена для всех пользователей KUMA.

Просмотр информации об инциденте

Чтобы просмотреть информацию об инциденте:

1. В окне веб-интерфейса программы выберите раздел **Инциденты**.
2. Выберите инцидент, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об инциденте.

Некоторые параметры инцидентов доступны для редактирования.

В верхней части окна информации об инциденте расположена панель инструментов и указано имя пользователя, которому назначен инцидент, а также указаны разделы окна в виде закладок, при нажатии на которые можно перемещаться к нужному разделу. В этом окне вы можете обработать инцидент: назначить его пользователю, объединить его с другим инцидентом или закрыть.

Раздел **Описание** содержит следующие данные:

- **Создан** – дата и время создания инцидента.
- **Название** – название инцидента.

  Название инцидента можно изменить, введя в поле новое название и нажав **Сохранить**. Название должно содержать от 1 до 128 символов Юникода.
- **Тенант** – название тенанта, которому принадлежит инцидент.

  Тенанта можно изменить, выбрав необходимый тенант в раскрывающемся списке и нажав **Сохранить**.
- **Статус** – текущее состояние инцидента:
  - **Открыт** – новый, еще не обработанный инцидент.
  - **Назначен** – инцидент обработан и передан сотруднику службы безопасности для расследования или реагирования.
  - **Закрыт** – инцидент закрыт, угроза безопасности устранена.
- **Уровень важности** – значимость угрозы, которую представляет инцидент. Возможные значения:
  - **Критический**.
  - **Высокий**.

- **Средний**.
- **Низкий**.

Уровень важности можно изменить, выбрав нужное значение в раскрывающемся списке и нажав **Сохранить**.

- **Категории затронутых активов** – категории, к которым принадлежат связанные с инцидентом активы.
- **Появление первого события** и **Появление последнего события** – дата и время первого и последнего события в инциденте.
- **Тип инцидента** и **Категория инцидента** – тип и категория угрозы, присвоенная инциденту. Значения можно изменить, выбрав в раскрывающемся списке нужное и нажав **Сохранить**.
- **Экспорт в НКЦКИ** – сведения о том, экспортировался ли этот инцидент в НКЦКИ.
- **Описание** – описание инцидента.

  Описание можно изменить, введя в поле новый текст и нажав **Сохранить**. Описание должно содержать не более 256 символов Юникода.
- **Связанные тенанты** – тенанты, относящиеся к связанным с инцидентом алертам, активам и пользователям.
- **Доступные тенанты** – тенанты, алерты которых можно привязывать к инциденту автоматически.

  Список доступных тенантов можно изменить, установив в раскрывающемся списке флажки напротив нужных тенантов и нажав **Сохранить**.

Раздел **Связанные алерты** содержит таблицу алертов, относящихся к инциденту. При нажатии на название алерта открывается окно с подробными данными об этом алерте.

Разделы **Связанные активы** и **Связанные пользователи** содержат таблицы с данными об активах и пользователях, относящихся к инциденту. Эта информация поступает из алертов, связанных с инцидентом.

Таблицы в разделах **Связанные алерты**, **Связанные активы** и **Связанные пользователи** можно дополнить данными, нажав в нужном разделе на кнопку **Привязать** и выбрав в открывшемся окне объект, который следует привязать к инциденту. При необходимости вы можете отвязать объекты от инцидента. Для этого вам требуется выбрать необходимые объекты, нажать **Отвязать** в разделе, к которому они относятся, и сохранить изменения. Если объекты добавлены в инцидент автоматически, их нельзя отвязать, пока не отвязан алерт, в котором они упоминаются. Состав полей в таблицах этих разделов можно изменить, нажав в нужном разделе на кнопку ⚙. По данным в таблицах этих разделов можно вести поиск с помощью полей **Поиск**.

Раздел **Журнал изменений** содержит записи об изменениях, которые вы и пользователи вносили в инцидент. Изменения регистрируются автоматически, при этом есть возможность вручную добавлять комментарии.

В разделе **Интеграция с НКЦКИ** можно отслеживать статус инцидента в НКЦКИ. Кроме того, в этом разделе можно экспортировать данные об инциденте в НКЦКИ, пересылать в НКЦКИ файлы, а также обмениваться со специалистами НКЦКИ сообщениями.

Если в параметры инцидента на стороне НКЦКИ были внесены изменения, в окне инцидента в KUMA будет отображаться соответствующее уведомление. При этом для параметров, по которым есть расхождения, в окне будут отображаться варианты значений и из KUMA, и из НКЦКИ.

Создание инцидента

Чтобы создать инцидент:

1. Откройте веб-интерфейс KUMA и выберите раздел **Инциденты**.

2. Нажмите **Создать инцидент**.

   Откроется окно создания инцидента.

3. Заполните обязательные параметры инцидента:

   - В поле **Название** введите название инцидента. Название должно содержать от 1 до 128 символов Юникода.

   - В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит создаваемый инцидент.

4. При необходимости укажите другие параметры инцидента:

   - В раскрывающемся списке **Уровень важности** выберите степень угрозы, которую представляет инцидент. Доступные значения: **Низкий**, **Средний**, **Высокий**, **Критический**.

   - В полях **Появление первого события** и **Появление последнего события** укажите временной диапазон, в котором были получены события, относящиеся к инциденту.

   - В раскрывающихся списках **Категория инцидента** и **Тип инцидента** выберите категорию и тип инцидента. Доступные типы инцидента зависят от выбранной категории.

   - Добавьте **Описание** инцидента. Описание должно содержать не более 256 символов Юникода.

- В раскрывающемся списке **Доступные тенанты** выберите тенанты, алерты которых можно будет привязывать к инциденту автоматически.

- В разделе **Связанные алерты** добавьте алерты, относящиеся к инциденту.

  Привязка алертов к инцидентам

  Чтобы привязать алерт к инциденту:

  1. В разделе **Связанные алерты** окна инцидента нажмите **Привязать**.

     Откроется окно со списком непривязанных к инцидентам алертов.

  2. Выберите требуемые алерты.

     Алерты можно искать по пользователям, активам, тенантам и корреляционным правилам с помощью регулярных выражений PCRE.

  3. Нажмите **Привязать**.

  Алерты связаны с инцидентом и отображаются в разделе **Связанные алерты**.

  Чтобы отвязать алерты от инцидента:

  1. Выберите нужные алерты в разделе **Связанные алерты** и нажмите на кнопку **Отвязать**.

  2. Нажмите **Сохранить**.

  Алерты отвязаны от инцидента. Также алерт можно отвязать от инцидента в окне алерта с помощью кнопки **Отвязать**.

- В разделе **Связанные активы** добавьте активы, относящиеся к инциденту.

  Привязка активов к инцидентам

  Чтобы привязать актив к инциденту:

  1. В разделе **Связанные активы** окна инцидента нажмите **Привязать**.

     Откроется окно со списком активов.

  2. Выберите нужные активы.

     Активы можно искать с помощью поля **Поиск**.

  3. Нажмите **Привязать**.

Активы связаны с инцидентом и отображаются в разделе **Связанные активы**.

Чтобы отвязать активы от инцидента:

1. Выберите нужные активы в разделе **Связанные активы** и нажмите на кнопку **Отвязать**.
2. Нажмите **Сохранить**.

Активы отвязаны от инцидента.

- В разделе **Связанные пользователи** добавьте пользователей, относящихся к инциденту.

  Привязка пользователей к инцидентам

  Чтобы привязать пользователя к инциденту:

  1. В разделе **Связанные пользователи** окна инцидента нажмите **Привязать**.

     Откроется окно со списком пользователей.
  2. Выберите нужных пользователей.

     Пользователей можно искать с помощью поля **Поиск**.
  3. Нажмите **Привязать**.

  Пользователи связаны с инцидентом и отображаются в разделе **Связанные пользователи**.

  Чтобы отвязать пользователей от инцидента:

  1. Выберите нужных пользователей в разделе **Связанные пользователи** и нажмите на кнопку **Отвязать**.
  2. Нажмите **Сохранить**.

  Пользователи отвязаны от инцидента.

- Добавьте **Комментарий** к инциденту.

5. Нажмите **Сохранить**.

Инцидент создан.

Обработка инцидентов

Вы можете назначить инцидент пользователю, объединить инциденты или закрыть инцидент.

Чтобы обработать инцидент:

1. Выберите необходимые инциденты одним из следующих способов:

   - В разделе **Инциденты** веб-интерфейса KUMA нажмите на инцидент, который нужно обработать.

     Откроется окно инцидента, в его верхней части расположена панель инструментов.

   - В разделе **Инциденты** веб-интерфейса KUMA установите флажок рядом с требуемыми инцидентами.

     В нижней части окна отобразится панель инструментов.

2. В раскрывающемся списке **Назначить** выберите пользователя, которому вы хотите назначить инцидент.

   Вы можете назначить инцидент себе, выбрав **Мне**.

   Инциденту будет присвоен статус **Назначен**, а в раскрывающемся списке **Назначить** отобразится имя выбранного пользователя.

3. В разделе **Связанные пользователи** выберите пользователя и настройте параметры реагирования через Active Directory.

   a. После выбора связанного пользователя в открывшемся окне **Информация об учетной записи** нажмите **Реагирование через Active Directory**.

   b. В раскрывающемся списке **Команда Active Directory** выберите одно из следующих значений:

      - Добавить учетную запись в группу

        Группа Active Directory, из которой или в которую необходимо переместить учетную запись.
        В обязательном для заполнения поле **Distinguished name** необходимо указать полный путь к группе.
        Например, CN=HQ Team,OU=Groups,OU=ExchangeObjects,DC=avp,DC=ru.
        В рамках одной операции можно указать только одну группу.

      - Удалить учетную запись из группы

Группа Active Directory, из которой или в которую необходимо переместить учетную запись.
В обязательном для заполнения поле **Distinguished name** необходимо указать полный путь к группе.
Например, CN=HQ Team,OU=Groups,OU=ExchangeObjects,DC=avp,DC=ru.
В рамках одной операции можно указать только одну группу.

- Сбросить пароль учетной записи
- Блокировать учетную запись

c. Нажмите **Применить**.

4. При необходимости измените параметры инцидента.

5. После расследования закройте инцидент:

   a. Нажмите **Закрыть**.

   Откроется окно подтверждения.

   b. Укажите причину закрытия инцидента:

   - **одобрен**. Это означает, что были приняты необходимые меры по устранению угрозы безопасности.
   - **не одобрен**. Это означает, что инцидент был ложным, а полученные события не указывают на угрозу безопасности.

   c. Нажмите **Закрыть**.

   Инциденту будет присвоен статус **Закрыт**. Инциденты с таким статусом невозможно редактировать, и они отображаются в таблице инцидентов, только если при фильтрации таблицы в раскрывающемся списке **Статус** установлен флажок **Закрыт**. Изменить статус закрытого инцидента или назначить его другому пользователю невозможно, однако его можно объединить с другим инцидентом.

6. При необходимости объедините выбранные инциденты с другим инцидентом:

   a. Нажмите **Объединить** и в открывшемся окне выберите инцидент, в который следует поместить все данные из выбранных инцидентов.

   b. Подтвердите выбор, нажав **Объединить**.

   Инциденты будут объединены.

Инцидент обработан.

Изменение инцидентов

Чтобы изменить параметры инцидента:

1. В разделе **Инциденты** веб-интерфейса KUMA нажмите на инцидент, параметры которого нужно изменить.

   Откроется окно инцидента.

2. Измените нужные параметры. Для редактирования доступны все параметры инцидента, которые можно задать при его создании.

3. Нажмите **Сохранить**.

Инцидент будет изменен.

Автоматическая привязка алертов к инцидентам

В KUMA можно настроить автоматическую привязку создаваемых алертов к уже существующим инцидентам, если у алертов и инцидентов есть пересечения по относящимся к ним активам или пользователям. Если настройка включена, то при создании алерта программа выполняет поиск инцидентов за указанный период, к которым относятся активы или пользователи из алерта. Кроме того, программа проверяет, чтобы созданный алерт относился к тенантам, указанным в инцидентах в качестве параметра **Доступные тенанты**. Если удовлетворяющий условиям инцидент найден, программа связывает созданный алерт и найденный инцидент.

Чтобы настроить автоматическую привязку алертов к инцидентам:

1. Откройте раздел веб-интерфейса KUMA **Параметры** → **Инциденты** → **Автоматическая привязка алертов к инцидентам**.

2. Установите флажок **Включить** в блоках параметров **Привязка при пересечении по активам** и/или **Привязка при пересечении по пользователям**, в зависимости от того, какие связи необходимо искать между инцидентами и алертами.

3. Задайте **Срок давности создания инцидента** для параметров, по которым необходимо искать связи. Создаваемые алерты будут сравниваться с инцидентами не старше указанного срока.

Автоматическая привязка алертов к инцидентам настроена.

Чтобы выключить автоматическую привязку алертов к инцидентам,

в разделе веб-интерфейса KUMA **Параметры** → **Инциденты** → **Автоматическая привязка алертов к инцидентам** установите флажок **Выключено**.

Категории и типы инцидентов

Для удобства работы вы можете присваивать категории и типы. Если инциденту присвоена категория НКЦКИ, его можно экспортировать в НКЦКИ.

Категории и типы инцидентов, которые можно экспортировать в НКЦКИ

В таблице ниже перечислены категории и типы инцидентов, которые можно экспортировать в НКЦКИ:

Категория инцидента	Тип инцидента
Уведомление о компьютерном инциденте	Вовлечение контролируемого ресурса в инфраструктуру ВПО
	Замедление работы ресурса в результате DDoS-атаки
	Заражение ВПО
	Захват сетевого трафика
	Использование контролируемого ресурса для фишинга
	Компрометация учетной записи
	Несанкционированное изменение информации
	Несанкционированное разглашение информации
	Публикация на ресурсе запрещенной законодательством РФ информации
	Рассылка спам-сообщений с контролируемого ресурса
	Успешная эксплуатация уязвимости
Уведомление о компьютерной атаке	DDoS-атака
	Неудачные попытки авторизации
	Попытки внедрения ВПО

	Попытки эксплуатации уязвимости
	Публикация мошеннической информации
	Сетевое сканирование
	Социальная инженерия
Уведомление о наличии уязвимости	Уязвимый ресурс

Категории инцидентов можно просмотреть или изменить в разделе **Параметры** → **Инциденты** → **Типы инцидентов**, где они отображаются в виде таблицы. При нажатии на заголовки столбцов можно менять параметры сортировки таблицы. Таблица содержит следующие столбцы:

- **Категория инцидента** – общий признак инцидента или компьютерной атаки. Таблицу можно фильтровать по значениям этого столбца.
- **Тип инцидента** – класс инцидента или компьютерной атаки.
- **Категория для НКЦКИ** – соответствие типа инцидента номенклатуре НКЦКИ. Невозможно экспортировать в НКЦКИ инциденты, которым присвоены пользовательские типы и категории. Таблицу можно фильтровать по значениям этого столбца.
- **Уязвимость** – указывает ли тип инцидента на уязвимость.
- **Создан** – дата создания типа инцидента.
- **Изменен** – дата изменения типа инцидента.

Чтобы добавить тип инцидента:

1. В разделе веб-интерфейса KUMA **Параметры** → **Инциденты** → **Типы инцидентов** нажмите **Добавить**.

   Откроется окно создания типа инцидента.

2. Заполните поля **Тип** и **Категория**.
3. Если создаваемый тип инцидента соответствует номенклатуре НКЦКИ, установите флажок **Категория для НКЦКИ**.
4. Если тип инцидента указывает на уязвимость, установите флажок **Уязвимость**.
5. Нажмите **Сохранить**.

Тип инцидента создан.

Взаимодействие с НКЦКИ

В KUMA в рамках взаимодействия с Национальным координационным центром по компьютерным инцидентам (далее "НКЦКИ") можно выполнять следующие действия:

- экспортировать в НКЦКИ инциденты;
- при запросе НКЦКИ дополнять экспортированный инцидент данными;
- отправлять в НКЦКИ файлы;
- обмениваться сообщениями со специалистами НКЦКИ;
- просматривать изменения в параметрах экспортированных инцидентов, сделанных в НКЦКИ.

Данные между KUMA и НКЦКИ синхронизируются каждые 5-10 минут.

Условия взаимодействия с НКЦКИ

Для взаимодействия с НКЦКИ должны выполняться следующие условия:

- лицензия программы включает модуль GosSOPKA;
- настроена интеграция с НКЦКИ;
- в параметрах пользователей, в обязанности которых входит взаимодействие с НКЦКИ, установлен флажок **Может взаимодействовать с НКЦКИ**.

Этапы взаимодействия с НКЦКИ

В KUMA экспорт и обработка инцидентов, экспортированных в НКЦКИ, проходит через следующие этапы:

1. **Создание инцидента и проверка его на соответствие требованиям НКЦКИ**

   Вы можете создать инцидент или получить его из дочернего узла KUMA. Перед отправкой данных в НКЦКИ необходимо убедиться, что категория инцидента соответствует требованиям НКЦКИ

2. **Экспорт инцидента в НКЦКИ**

   При успешном экспорте инцидента в НКЦКИ его параметр **Экспорт в НКЦКИ** принимает значение **Экспортирован**. В нижней части окна инцидента становится доступен раздел с чатом с сотрудниками НКЦКИ.

   В НКЦКИ полученному от вас инциденту присваивается регистрационный номер и статус. Эти сведения отображаются в окне инцидента в разделе **Интеграция с НКЦКИ** и в автоматических сообщениях чата.

   Если в НКЦКИ предоставлены все необходимые данные, инциденту присваивается статус **Проверка НКЦКИ**. Параметры инцидента в таком статусе доступны для изменения, однако обновленные сведения невозможно передать из KUMA в НКЦКИ. Вы можете просмотреть разницу между данными об инциденте в KUMA и в НКЦКИ.

3. **Дополнение данных об инциденте**

   Если сотрудникам НКЦКИ не хватает сведений для обработки инцидента, они могут присвоить ему статус **Требуется дополнение**. В KUMA этот статус отображается в окне инцидента в разделе **Интеграция с НКЦКИ**. Пользователи уведомляются об изменении статуса.

   К инцидентам с таким статусом можно прикрепить файл.

   Дополнение данных завершается повторным экспортом инцидента в НКЦКИ, при котором необходимо дополнить или изменить ранее отправленные сведения. Из родительского узла KUMA невозможно вносить изменения в инциденты дочерних узлов – это необходимо сделать сотрудникам дочернего узла KUMA.

   При успешном дополнении инцидента данными ему присваивается статус **Проверка НКЦКИ**.

4. **Завершение обработки инцидента**

   Когда сотрудники НКЦКИ обработают инцидент, в НКЦКИ ему будет присвоен статус **Принято решение**. В KUMA этот статус отображается в окне инцидента в разделе **Интеграция с НКЦКИ**.

   При получении этого статуса инцидент в KUMA автоматически закрывается. Взаимодействие с НКЦКИ по данному инциденту через KUMA становится невозможным.

Особенности экспорта в НКЦКИ из иерархической структуры KUMA

Если в вашей организации развернуто несколько узлов KUMA, которые объединены в иерархическую структуру, вы можете из родительских узлов KUMA передавать в НКЦКИ инциденты, полученные из дочерних узлов KUMA. Для этого должны выполняться следующие условия:

- В родительском и дочернем узле KUMA настроена интеграция с НКЦКИ. При этом для родительского узла параметры **URL** и **Токен** в разделе **Параметры** → **НКЦКИ** являются обязательными, а для дочернего – нет.

- В обоих узлах не отключена интеграция с НКЦКИ.

При такой настройке взаимодействие с НКЦКИ осуществляется только на уровне узла, экспортировавшего инцидент в НКЦКИ.

Из родительского узла KUMA невозможно изменить параметры инцидента, полученного из дочернего узла KUMA. Если для экспорта в НКЦКИ не хватает каких-то данных, инцидент необходимо изменить на дочернем узле KUMA, а затем уже экспортировать его в НКЦКИ из родительского узла KUMA.

Экспорт данных в НКЦКИ

> Невозможно экспортировать в НКЦКИ закрытие в KUMA инциденты, если у них на момент закрытия не было заполнено поле **Описание**.

Чтобы экспортировать инцидент в НКЦКИ:

1. В разделе **Инциденты** веб-интерфейса KUMA откройте инцидент, который вы хотите экспортировать.

2. Нажмите в нижней части окна на кнопку **Экспорт в НКЦКИ**.

3. Если вы не указали категорию и тип инцидента, укажите эти сведения в открывшемся окне и нажмите на кнопку **Экспорт в НКЦКИ**.

   Откроется окно с параметрами экспорта.

4. Укажите параметры в закладке **Основные** окна **Экспорт в НКЦКИ**:

   - **Категория инцидента** и **Тип инцидента** – укажите тип и категорию инцидента. В НКЦКИ можно экспортировать только инциденты определенных категорий и типов.

   - **TLP** (обязательно) – присвойте инциденту маркер протокола Traffic Light, определяющий характер сведений об инциденте. По умолчанию используется значение **RED**. Доступные значения:

     - **WHITE** – раскрытие не ограничено;

     - **GREEN** – раскрытие только для сообщества;

     - **AMBER** – раскрытие только для организаций;

- **RED** – раскрытие только для круга лиц.

- **Название информационной системы** (обязательно) – укажите название информационного ресурса, в котором произошел инцидент. В поле можно ввести до 500 000 символов.

- **Категория КИИ системы** (обязательно) – укажите категорию критической информационной структуры (КИИ) вашей организации. Если у вашей организации нет категории КИИ, выберите пункт **Информационный ресурс не является объектом КИИ**.

- **Сфера деятельности компании** (обязательно) – укажите сферу деятельности вашей организации. По умолчанию используется значение, указанное в параметрах интеграции с НКЦКИ.

- **Местоположение** (обязательно) – выберите в раскрывающемся списке местоположение вашей организации.

- **Затронутая система имеет подключение к интернету** – установите этот флажок, если активы, относящиеся к инциденту, имеют подключение к интернету. По умолчанию этот флажок снят.

  Если этот флажок установлен, в окне становится доступна для заполнения закладка **Технические сведения**, на которой отображаются сведения об относящихся к инциденту активах. Подробнее см. ниже.

- **Сведения о продукте** (обязательно) – эта таблица становится доступна, если в качестве категории инцидента вы выбрали пункт **Уведомление о наличии уязвимости**.

  С помощью кнопки **Добавить элемент** можно добавить в таблицу строку. В столбце **Название** требуется указать название программы (например, `MS Office`), а в столбце **Версия** – версию программы (например, `2.4`).

- **Идентификатор уязвимости** – при необходимости укажите идентификатор обнаруженной уязвимости. Например, `CVE-2020-1231`.

  Это поле становится доступно, если в качестве категории инцидента вы выбрали пункт **Уведомление о наличии уязвимости**.

- **Наименование и версия уязвимого продукта** – при необходимости укажите наименование и версию уязвимого продукта. Например, `Операционные системы Microsoft и их компоненты`.

  Это поле становится доступно, если в качестве категории инцидента вы выбрали пункт **Уведомление о наличии уязвимости**.

5. При необходимости укажите параметры в закладке **Дополнительно** окна **Экспорт в НКЦКИ**.

Набор параметров в закладке зависит от выбранных категории и типа инцидента:

- **Средство обнаружения инцидента** – укажите название продукта, с помощью которого был зарегистрирован инцидент. Например, `KUMA 1.5`.
- **Требуется привлечение сил ГосСОПКА** – установите этот флажок, если вам требуется помощь сотрудников ГосСОПКА.
- **Время завершения инцидента** – укажите дату и время восстановления штатного режима работы контролируемого информационного ресурса (объекта КИИ) после компьютерного инцидента, окончания компьютерной атаки или устранения уязвимости.
- **Влияние на доступность** – оцените степень последствий инцидента для доступности системы:
  - **Высокое**
  - **Низкое**
  - **Отсутствует**
- **Влияние на целостность** – оцените степень последствий инцидента для целостности системы:
  - **Высокое**
  - **Низкое**
  - **Отсутствует**
- **Влияние на конфиденциальность** – оцените степень последствий инцидента для конфиденциальности информации:
  - **Высокое**
  - **Низкое**
  - **Отсутствует**
- **Иные последствия** – укажите иные значимые последствия инцидента.
- **Город** – укажите город, в котором находится ваша организация.

6. Если к инциденту прикреплены активы, можно указать их параметры в закладке **Технические данные**.

Эта закладка становится активной, только если вы установили флажок **Затронутая система имеет подключение к интернету**.

При необходимости изменить или дополнить сведения, ранее указанные в закладке **Технические данные**, это следует делать в вашем личном кабинете ГосСОПКА, даже если сотрудники НКЦКИ запросили у вас дополнительные сведения и у вас есть возможность изменить экспортированный инцидент.

Категории указываемых активов должны соответствовать категории затронутой КИИ системы.

7. Нажмите **Экспорт**.

8. Подтвердите экспорт.

Сведения об инциденте переданы в НКЦКИ, параметр инцидента **Экспорт в НКЦКИ** меняется на **Экспортирован**. В НКЦКИ полученному от вас инциденту присваивается регистрационный номер и статус. Эти сведения отображаются в окне инцидента в разделе **Интеграция с НКЦКИ**.

Изменить данные в экспортированном инциденте возможно, только если сотрудники НКЦКИ запросили у вас дополнительные сведения. Если дополнительные сведения запрошены не были, но вам требуется внести изменения в экспортированный инцидент, это следует делать в вашем личном кабинете ГосСОПКА.

После успешного экспорта инцидента в нижней части экрана отображается кнопка **Сравнение инцидента KUMA с данными в НКЦКИ**, при нажатии на которую открывается окно, где подсвечиваются различия в данных в инциденте между KUMA и НКЦКИ.

Дополнение данных об инциденте по запросу

Если сотрудникам НКЦКИ потребуются дополнительные сведения об инциденте, они могут их у вас запросить. В этом случае в окне инцидента в разделе **Интеграция с НКЦКИ** статус инцидента меняется на **Требуется дополнение**. При этом следующие пользователи KUMA получают по электронной почте уведомления об изменении статуса: пользователь, которому назначен инцидент, и пользователь, экспортировавший инцидент в НКЦКИ.

Если инциденту в НКЦКИ присвоен статус Требуется дополнение, в KUMA для этого инцидента становятся доступны следующие действия:

- Загрузка в НКЦКИ файлов.

- Повторный экспорт данных об инциденте в НКЦКИ с изменением или дополнением ранее указанных сведений. Выполнение этого действия завершает дополнение инцидента данными.

Отправка файлов в НКЦКИ

Если инцидент имеет статус НКЦКИ **Требуется дополнение**, вы можете приложить к нему файл. Файл будет доступен как в НКЦКИ, так и в веб-интерфейсе KUMA.

При иерархическом развертывании KUMA загружать файлы в НКЦКИ можно только из родительского узла KUMA. При этом в дочерних узлах KUMA видны журнальные записи о загрузке файла.

В журнале изменений инцидента добавляются сообщения о загрузке в НКЦКИ файлов пользователями KUMA. Сообщения о добавлении файлов со стороны НКЦКИ в журнал не заносятся.

Чтобы приложить файл к инциденту:

1. В разделе **Инциденты** веб-интерфейса KUMA откройте инцидент, к которому вы хотите приложить файл. Инцидент должен иметь статус НКЦКИ **Требуется дополнение**.

2. В разделе окна инцидента **Интеграция с НКЦКИ** выберите закладку **Файл** и нажмите на кнопку **Отправить файл в НКЦКИ**.

   Откроется окно выбора файла.

3. Выберите нужный файл размером не более 50 МБ и подтвердите выбор.

Файл приложен к инциденту. Файл доступен и для сотрудников НКЦКИ, и для пользователей KUMA.

Данные между KUMA и НКЦКИ синхронизируются каждые 5-10 минут.

Обмен сообщениями с сотрудниками НКЦКИ

После успешного экспорта инцидента в НКЦКИ в нижней части окна инцидента становится доступен чат с сотрудниками НКЦКИ. Обмениваться сообщениями можно с момента успешного экспорта инцидента до его закрытия в НКЦКИ.

Окно чата с историей сообщений и полем для ввода новых сообщений доступно в разделе окна инцидента **Интеграция с НКЦКИ** в закладке **Чат**.

Данные между KUMA и НКЦКИ синхронизируются каждые 5-10 минут.

Допустимые категории и типы инцидентов НКЦКИ

В таблице ниже перечислены категории и типы инцидентов, которые можно экспортировать в НКЦКИ:

Категория инцидента	Тип инцидента
Уведомление о компьютерном инциденте	Вовлечение контролируемого ресурса в инфраструктуру ВПО
	Замедление работы ресурса в результате DDoS-атаки
	Заражение ВПО
	Захват сетевого трафика
	Использование контролируемого ресурса для фишинга
	Компрометация учетной записи
	Несанкционированное изменение информации
	Несанкционированное разглашение информации
	Публикация на ресурсе запрещенной законодательством РФ информации
	Рассылка спам-сообщений с контролируемого ресурса
	Успешная эксплуатация уязвимости
Уведомление о компьютерной атаке	DDoS-атака
	Неудачные попытки авторизации
	Попытки внедрения ВПО
	Попытки эксплуатации уязвимости
	Публикация мошеннической информации
	Сетевое сканирование
	Социальная инженерия

Уведомление о наличии уязвимости	Уязвимый ресурс

Уведомления об изменении статуса инцидента в НКЦКИ

При некоторых изменениях статуса или данных инцидента в НКЦКИ пользователи KUMA получают следующие уведомления по электронной почте:

- Уведомление о получении сообщения от НКЦКИ.
- Уведомление о запросе дополнительных данных.
- Уведомление об изменении данных инцидента в НКЦКИ.
- Уведомление об автоматическом закрытии инцидента.

Уведомления получают следующие пользователи:

- Пользователь, которому был назначен инцидент.
- Пользователь, который экспортировал инцидент в НКЦКИ.

Работа в режиме иерархии

KUMA, развернутые в разных организациях, могут быть объединены в иерархическую структуру. Взаимодействие родительских и дочерних KUMA (или *узлов*) предоставляет следующие возможности:

- Родительские узлы KUMA получают от дочерних узлов KUMA данные о других потомках. Это позволяет родительскому узлу видеть свою ветвь иерархического дерева.
- Родительские узлы KUMA получают от потомков данные об инцидентах и, если дочерний узел включил соответствующие настройки, данные о связанных с инцидентами алертах и событиях.
- Дочерние узлы KUMA не получают данные о вышестоящих узлах, за исключением сведений о своем родительском узле KUMA.

Родительский и дочерний узлы взаимодействуют через API. Для аутентификации используются самоподписанные сертификаты, которыми администраторы родительской и дочерней организаций должны обменяться по защищенными каналам связи при подключении узлов друг к другу.

Один родительский узел может иметь более одного дочернего узла. Дочерний узел может быть подключен только к одному родительскому узлу. Родительский узел не может быть дочерним узлом своих потомков.

Пользователи с ролью главный администратор могут настроить режим иерархии в веб-интерфейсе KUMA в разделе **Параметры** → **Иерархия**:

- На закладке **Профиль узла** можно настроить профиль вашего узла, создать сертификат, а также включить и выключить режим иерархии.
- На закладке **Структура** можно просматривать доступную вам ветвь иерархического дерева, изменять подключенные узлы или отключать их.
- На обеих закладках можно подключать узлы – родительский и дочерние.

Инциденты дочерних узлов могут просматривать пользователи всех ролей в веб-интерфейсе KUMA в разделе **Инциденты**. В инцидентах можно получить сведения о связанных с ними алертах, событиях, активах и пользователях.

Первое включение режима иерархии

При первом включении режима иерархии необходимо заполнить профиль своего узла.

Чтобы заполнить профиль своего узла:

1. Откройте в веб-интерфейсе KUMA раздел **Параметры** → **Иерархия** → **Профиль узла**.
2. В поле **Название организации** укажите название своей организации (1–128 символов). Это название будет использоваться в качестве названия вашего узла в иерархии.

   Для изменения названия организации потребуется пересоздать сертификат вашего узла и заменить его на узлах, к которым вы подключены.
3. В поле **FQDN** укажите FQDN своего узла.
4. При необходимости в раскрывающемся списке **Прокси-сервер** выберите ресурс прокси-сервера, который требуется использовать для обращения к другим узлам. Прокси-сервер можно создать с помощью кнопки ＋. Выбранный прокси-сервер можно изменить, нажав на кнопку ✎.

   В URL прокси-сервера можно указывать учетные данные только с использованием следующих символов: буквы латинского алфавита, цифры, специальные символы ("-", ".", "_", ":", "~", "!", "$", "&", "\", "(", ")", "*", "+", ",", ";", "=", "%", "@"). URL в ресурсе прокси-сервера указывается с помощью ресурса секрета: он выбирается в раскрывающемся списке **Брать URL из секрета**.

5. Нажмите **Создать сертификат**.

   Профиль вашего узла KUMA заполнен и режим иерархии включен. При включении режима иерархии автоматически создается сертификат, используемый для аутентификации вашего узла. С помощью значка вы можете скачать сертификат, чтобы затем передать его по защищенному каналу связи другим узлам для создания соединения.

Создание сертификата узла

Для аутентификации узлов иерархии используются самоподписанные *сертификаты узлов*. Сертификат содержит название организации и ее FQDN.

Сертификат создается при включении режима иерархии, но вы можете пересоздать сертификат. Сертификат необходимо пересоздать при изменении названия узла или его FQDN.

Чтобы создать сертификат узла:

1. Откройте раздел веб-интерфейс KUMA **Параметры** → **Иерархия** → **Профиль узла**.

   Откроется окно с параметрами вашего узла в иерархии.

2. Нажмите на кнопку **Создать сертификат**.

   Откроется окно создания сертификата.

3. В поле **FQDN** укажите FQDN своего узла.

4. В поле **Название организации** укажите название своей организации (1–128 символов). Это название будет использоваться в качестве названия вашего узла в иерархии.

5. Закройте окно, нажав **Сохранить**.

   Сертификат узла создан. Его можно скачать, нажав на значок , и передать по защищенному каналу связи другим узлам для создания соединения.

Соединение узлов в иерархическую структуру

Перед соединением узлов следует убедиться, что на них включен режим иерархии, настроены профили узлов и созданы сертификаты узлов. Родительский и дочерний узлы должны обменяться своими сертификатами по защищенным каналам связи.

Соединение узлов иерархии состоит из следующих шагов:

- Дочерний узел подключается к родительскому узлу.

- Родительский узел подключает дочерний узел.

> Перед соединением узлов убедитесь, что системное время на машинах синхронизируется с NTP-сервером. См. подробнее для Oracle Linux и для Astra Linux Special Edition.

Когда соединение установлено, родительский узел каждые 5 минут запрашивает у дочерних узлов имеющиеся у них сведения об иерархии, выстраивая таким образом структуру доступной для себя ветви иерархического дерева. Эти данные отображаются в разделе веб-интерфейса KUMA **Параметры** → **Иерархия** → **Структура** после обновления веб-страницы.

Сведения об иерархической структуре можно принудительно обновить в помощью кнопки **Обновить структуру**. Для отображения обновленных данных необходимо обновить страницу веб-браузера.

Подключение к родительскому узлу

Чтобы подключиться к родительскому узлу:

1. Откройте раздел веб-интерфейс KUMA **Параметры** → **Иерархия** и нажмите на кнопку **Подключиться к родительскому узлу**.

   Откроется окно **Подключение к родительскому узлу**.

2. Загрузите в KUMA сертификат родительского узла с помощью кнопки **Загрузить сертификат**.

   В окне отобразится описание сертификата с указанием выпустившей его организации и ее FQDN.

3. При необходимости в поле **Порт** укажите порт для доступа к родительскому узлу.

4. Нажмите **Сохранить**.

Вы подключились к родительскому узлу. Он теперь может добавить ваш узел в качестве дочернего, чтобы получать данные о ваших дочерних узлах и просматривать ваши инциденты.

Подключение дочернего узла

Если вы подключили родительский узел, вы сможете добавить дочерние узлы только после того, как ваш родительский узел добавит вас в качестве дочернего узла. Перед подключением дочернего узла убедитесь, что он добавил ваш узел в качестве родительского.

Чтобы подключить дочерний узел:

1. Откройте раздел веб-интерфейс KUMA **Параметры** → **Иерархия** и нажмите на кнопку **Подключить дочерний узел**.

   Откроется окно **Подключение дочернего узла**.

2. Загрузите в KUMA сертификат дочернего узла с помощью кнопки **Загрузить сертификат**.

   В окне отобразится описание сертификата с указанием выпустившей его организации и ее FQDN.

3. При необходимости в поле **Порт** укажите порт для доступа к дочернему узлу.

4. Нажмите **Сохранить**.

Дочерний узел добавлен и отображается на закладке **Параметры** → **Иерархия** → **Структура**. На этой же закладке отображаются потомки дочернего узла. Вы можете просматривать инциденты своих дочерних узлов и их потомков.

Отключение от узла

Вы можете отключиться от родительского или дочернего узла. Невозможно отключиться от узлов, которые являются потомками ваших дочерних узлов.

Чтобы отключиться от узла:

1. Откройте раздел веб-интерфейс KUMA **Параметры** → **Иерархия** и перейдите на закладку **Структура**.

   Отобразится иерархическая структура.

2. Выберите узел, от которого вы хотите отключиться.

   В правой части окна отобразится область деталей со сведениями об узле.

3. Нажмите **Отключить**.

Вы отключились от узла. Если вы отключились от родительского узла, он больше не получает данные о ваших дочерних узлах и инцидентах. Если вы отключились от дочернего узла, вы больше не получаете данные о его дочерних узлах и его инцидентах.

Изменение узла

Если название и/или FQDN узла изменились, этот узел должен перевыпустить сертификат, после чего необходимо повторить процедуру соединения узлов. Устаревшие узлы необходимо отключить.

Порт подключения к узлам можно изменить в области деталей узла, не перевыпуская сертификат.

Чтобы изменить параметры подключения к узлу:

1. Откройте в веб-интерфейсе KUMA в разделе **Параметры** → **Иерархия** закладку **Структура** и выберите требуемый узел.

   В правой части окна отобразится область деталей узла.

2. В поле **Порт** укажите требуемый порт.

3. Измените настройки почтовых оповещений о появлении инцидентов на дочернем узле:

   - Если требуется выключить оповещения, снимите флажок **Отслеживание инцидентов**.

   - Если требуется включить оповещения, установите флажок **Отслеживание инцидентов** и добавьте с помощью поля ввода требуемые адреса электронной почты.

     Для отправки почтовых уведомлений требуется настроить подключение к SMTP-серверу.

4. Нажмите **Сохранить**

Параметры подключения к узлу изменены.

Ошибки при подключении узлов

Ошибки, возникающие при подключении узлов, в веб-интерфейсе KUMA могут отображаться не полностью. Полный ответ сервера можно просмотреть в консоли разработчика используемого вами браузера.

В таблице ниже перечислены ошибки, которые могут возникнуть при соединении узлов KUMA в иерархию, а также рекомендации по их устранению.

Ошибки, возникающие при установлении подключения к узлу, отображаются во всплывающих окнах в нижней части экрана. Ошибки в уже подключенных узлах можно просмотреть в разделе веб-интерфейса KUMA **Параметры** → **Иерархия** → **Структура**: текст ошибки отображается, если навести указатель мыши на значок красного треугольника рядом с узлом, в работе с которым произошла ошибка.

Сообщение об ошибке	Возможная причина возникновения ошибки	Рекомендация по устранению
`failed to exchange settings with child: <Post-запрос на адрес дочернего узла>: connect: connection refused`	Отказано в соединении. Произошла попытка добавить дочерний узел, который не добавил сертификат родительского узла.	• Подключить сначала на дочернем узле родительский узел, затем на родительском узле добавить дочерний. • Проверить включена ли иерархия на дочернем узле.
`Невозможно добавить свой узел KUMA в качестве родительского или дочернего узла`	Из узлов KUMA невозможно выстроить циклическую структуру.	Удостоверьтесь, что иерархическая структура, которую вы хотите выстроить, является древовидной.
`corrupted certificate`	Некорректный сертификат.	Необходимо проверить файл сертификата.
`failed to exchange settings with child: <Post-запрос на адрес дочернего узла>: context deadline exceeded`	Соединение не было установлено из-за превышения времени ожидания отклика.	Проверить включена ли машина дочернего узла.
`failed to exchange settings with child: <Post-запрос на адрес дочернего узла>: x509: certificate has expired or is not yet valid`	Отказано в соединении из-за недействительного сертификата.	• Убедиться в актуальности сертификата дочернего узла. • Убедиться, что системное время узлов

		синхронизируется с NTP-сервером.
failed to exchange settings with child: <Post-запрос на адрес дочернего узла>: certificate signed by unknown authority (possibly because of "x509: invalid signature: parent certificate cannot sign this kind of certificate" while trying to verify candidate authority certificate " <название узла>"	Отказано в соединении из-за недействительного сертификата.	Убедиться в актуальности сертификата родительского узла.
failed to exchange settings with child: <Post-запрос на адрес дочернего узла>: dial tcp: lookup <адрес дочернего узла> on <IP-адрес дочернего узла>: no such host	В сертификате дочернего узла несуществующий FQDN.	Убедиться в актуальности сертификата дочернего узла.
Already exists	Такой узел уже существует в структуре.	Проверьте иерархическую структуру, которую вы хотите построить.
Родительский узел уже указан в качестве дочернего узла		Не подключать родительский узел, который является дочерним узлом в этой иерархии.
Failed to query branch {"branchID":"<идентификатор ветки>","branchName":" <название узла>","branchFQDN":"<FQDN узла>","error":"Get \"<URL дочернего узла>/children\": remote error: tls: bad certificate"}	Дочерний узел удалил родителя.	Необходимо, чтобы дочерний узел подключил родительский узел.

`error: <Post-запрос на адрес дочернего узла>: read tcp <IP-адреса узлов>: read: connection reset by peer`	В настройках подключения узлов указаны неверные порты.	Убедиться, что в настройках узла указан верный порт и используется действительный сертификат.
`"error":"Get \"<URL дочернего узла>/children\": proxyconnect tcp: x509: certificate signed by unknown authority"`	Осуществляется подключение к узлу с некорректными настройками прокси-сервера.	Убедиться в корректности настроек прокси-сервера.

Просмотр своей ветви иерархии и доступных узлов

В веб-интерфейсе KUMA в разделе **Параметры** → **Иерархия** на закладке **Структура** можно просмотреть вашу ветвь иерархического дерева от родительского узла до всех потомков дочерних узлов. Ваш узел в иерархии подсвечен зеленым.

При нажатии на узел ветви в правой части окна открывается область деталей узла, в которой можно выполнить следующие действия:

- Изменить порт подключения к родительскому или дочернему узлу.
- Отключить родительский или дочерний узел.
- Изменить настройки почтовых уведомлений об инцидентах для дочерних узлов и их потомков.

Изменение профиля узла

Вы можете изменить параметры профиля своего узла.

Чтобы изменить параметры вашего узла:

1. Откройте в веб-интерфейсе KUMA раздел **Параметры** → **Иерархия** → **Профиль узла**.
2. При необходимости в раскрывающемся списке **Прокси-сервер** выберите ресурс прокси-сервера, который требуется использовать для обращения к другим узлам. Прокси-сервер можно создать с помощью кнопки ➕. Выбранный прокси-сервер можно изменить, нажав на кнопку ✎.

В URL прокси-сервера можно указывать учетные данные только с использованием следующих символов: буквы латинского алфавита, цифры, специальные символы ("-", ".", "_", ":", "~", "!", "$", "&", "\", "(", ")", "*", "+", ",", ";", "=", "%", "@"). URL в ресурсе прокси-сервера указывается с помощью ресурса секрета: он выбирается в раскрывающемся списке **Брать URL из секрета**.

3. При необходимости в поле **Порт** укажите порт, используемый для доступа к вашему узлу. Убедитесь, что доступ к порту не закрыт.

4. При необходимости в поле **Время ожидания** укажите, сколько секунд необходимо ожидать ответа узлов при попытке соединения. Значение по умолчанию – 60.

5. При необходимости установите или снимите флажки **Не включать события в инциденты, отправляемые в родительский узел** и **Не включать алерты в инциденты, отправляемые в родительский узел**. По умолчанию эти флажки сняты.

6. Нажмите **Сохранить**.

Параметры вашего узла изменены.

Если вы хотите изменить FQDN или название своего узла, пересоздайте сертификат узла.

Просмотр инцидентов от дочерних узлов

Если режим иерархии включен, вы можете просмотреть инциденты, созданные на дочерних узлах и их потомках, в разделе **Инциденты**. В таблице инцидентов отображается столбец **Ветвь**, с помощью которого можно фильтровать инциденты по узлам, в которых они были созданы. По умолчанию в таблице инцидентов отображаются инциденты, созданные на вашем узле.

Чтобы выбрать узлы, инциденты которых вы хотите просмотреть:

1. Откройте в веб-интерфейсе KUMA раздел **Инциденты**.

2. Нажмите на заголовок столбца **Ветвь** и в открывшемся окне нажмите на значок .

   В правой части окна отобразится область деталей с иерархической структурой организаций. С помощью кнопки ... можно раскрыть или скрыть все ветви структуры, а также выбрать все узлы KUMA.

3. Выберите требуемые узлы и нажмите **Сохранить**.

В таблице инцидентов отображаются инциденты, созданные на выбранных вами узлах.

При нажатии на инцидент открывается окно с подробными данными об инциденте. Данные доступны только для чтения, инцидент с другого узла невозможно изменить или обработать.

Особенности просмотра данных об инциденте, созданном на другом узле:

- Раздел окна инцидента **Связанные алерты** содержит сведения, только если на дочернем узле настроена передача в родительский узел данных об относящихся к инцидентам алертах.

  При нажатии на название относящегося к инциденту алерта открывается окно с подробными данными об этом алерте. Эти данные также доступны только для чтения, алерт другого узла невозможно изменить или обработать.

- Раздел **Связанные события** в окне алерта, относящегося к инциденту другого узла, содержит сведения, только если на дочернем узле настроена передача в родительский узел данных об относящихся к инцидентам событиях.

  В этом случае с помощью кнопки **Найти в событиях** можно открывать таблицу событий и искать нужные события. При этом вы не можете выбрать хранилище, а на SQL-запросы налагаются ограничения поиска событий в режиме детализированного анализа. В этом режиме действует обогащение данных (например, с помощью Kaspersky Threat Intelligence Portal, Kaspersky CyberTrace или Active Directory). На родительских узлах недоступны результаты обогащения данными Kaspersky Threat Intelligence Portal, сделанные на дочерних узлах.

Включение и выключение режима иерархии

Чтобы включить или выключить режим иерархии:

1. Откройте в веб-интерфейсе KUMA раздел **Параметры** → **Иерархия** → **Профиль узла**.
2. Включите или выключите режим иерархии:
   - Если вы хотите включить режим иерархии, снимите флажок **Выключено**.
   - Если вы хотите выключить режим иерархии, установите флажок **Выключено**.
3. Нажмите **Сохранить**.

Режим иерархии включен или выключен.

Работа с алертами

Алерты создаются при получении последовательности событий, запускающей правило корреляции. Подробнее об алертах вы можете посмотреть в этом разделе.

В разделе **Алерты** веб-интерфейса KUMA можно просматривать и обрабатывать алерты, зарегистрированные программой. Алерты можно фильтровать. По нажатию на название алерта открывается окно со сведениями о нем.

Формат даты алерта зависит от языка локализации, выбранного в настройках программы. Возможные варианты формата даты:

- Английская локализация: ГГГГ-ММ-ДД.
- Русская локализация: ДД.ММ.ГГГГ.

Жизненный цикл алертов

Ниже представлен жизненный цикл алерта:

1. KUMA создает алерт при срабатывании правила корреляции. Алерт именуется по породившему его правилу корреляции. Алерту присваивается статус **Новый**.

   > Алерты в статусе **Новый** продолжают обновляться данными при срабатывании правил корреляции. Если статус алерта меняется на любой другой, алерт больше не обновляется новыми событиями и, если правило корреляции срабатывает снова, создается новый алерт.

2. Сотрудник службы безопасности назначает оператора для расследования алерта. Статус алерта меняется на **Назначен**.
3. Оператор выполняет одно из следующих действий:
   - Закрывает алерт как ложно положительный (статус алерта меняется на **Закрыт**).
   - Реагирует на угрозу и закрывает алерт (статус алерта меняется на **Закрыт**).
   - Создает на основе алерта инцидент (статус алерта меняется на **В инцидент**).

Переполнение алертов

Каждый алерт и привязанные к нему события не могут превышать размер 16 МБ. Когда этот предел достигнут:

- Новые события не смогут быть привязаны к алерту.

- В столбце **Обнаружен** у алерта отображается тег **Переполнен**. Такой же тег отображается в разделе **Информация об алерте** окна сведений об алерте.

Алерты, у которых есть предупреждения о переполнении, следует обрабатывать как можно скорее, поскольку новые события не добавляются к переполненным алертам. Вы можете отфильтровать все события, которые могли быть связаны с алертом после переполнения, по ссылке **Смотреть все возможные связанные события**.

Разделение алертов

С помощью правил сегментации поток однотипных корреляционных событий можно разделять, создавая более одного алерта.

Настройка таблицы алертов

В основной части раздела **Алерты** отображается таблица с информацией о зарегистрированных алертах.

В таблице алертов отображаются следующие столбцы:

- Уровень важности ( ) – степень значимости потенциальной угрозы безопасности: критическая , высокая , средняя , низкая .
- **Название** – имя алерта.

  > Если рядом с названием алерта отображается тег **Переполнен**, это означает, что размер алерта достиг или приближается к пределу и должен быть обработан как можно скорее.

- **Статус** – текущее состояние алерта:
  - **Новый** – новый, еще не обработанный алерт.
  - **Назначен** – алерт обработан и передан сотруднику службы безопасности для расследования или реагирования.
  - **Закрыт** – алерт закрыт. Алерт был ложный или угроза безопасности устранена.
  - **Эскалирован** – на основе этого алерта был создан инцидент.
- **Назначен** – имя сотрудника службы безопасности, которому алерт передан для расследования или реагирования.

- **Инцидент** – название инцидента, к которому привязан алерт.
- **Первое появление** – дата и время создания первого корреляционного события в последовательности событий, приведшего к созданию алерта.
- **Последнее появление** – дата и время создания последнего корреляционного события в последовательности событий, приведшего к созданию или обновлению алерта.
- **Категории** – категории активов с наибольшим уровнем важности, относящихся к алерту. Отображается не более трех категорий.
- **Тенант** – название тенанта, которому принадлежит алерт.
- **КИИ** – указание на то, относятся ли к алерту активы, являющиеся объектами КИИ. Столбец скрыт от пользователей, не имеющих прав доступа к объектам КИИ.

По нажатию на заголовки столбцов вы можете просмотреть инструменты для фильтрации алертов. При фильтрации алертов по какому-либо параметру соответствующий заголовок таблицы алертов подсвечивается желтым цветом.

По кнопке вы можете настроить отображаемые столбцы таблицы алертов.

В поле **Поиск** можно ввести регулярное выражение для поиска алертов по связанным с ними активам, пользователям, тенантам или корреляционным правилам. Параметры, по которым производится поиск:

- Активы: название, FQDN, IP-адрес.
- Учетные записи Active Directory: атрибуты displayName, SAMAccountName, UserPrincipalName.
- Корреляционные правила: название.
- Пользователи KUMA, которым назначены алерты: имя, логин, адрес электронной почты.
- Тенанты: название.

Фильтрация алертов

В KUMA в разделе **Алерты** можно делать выборки алертов с помощью инструментов фильтрации и сортировки.

Конфигурацию фильтра можно сохранить. Существующие конфигурации фильтров можно удалить.

Сохранение и выбор конфигураций фильтра алертов

В KUMA можно сохранять изменения параметров таблицы алертов в виде фильтров. Конфигурации фильтров сохраняются на сервере Ядра KUMA и доступны всем пользователям KUMA того тенанта, для которого они были созданы.

Чтобы сохранить текущие параметры конфигурации фильтра:

1. В разделе KUMA **Алерты** откройте раскрывающийся список **Фильтры**.
2. Выберите **Сохранить текущий фильтр**.

   Появится поле для ввода названия нового фильтра и выбора тенанта, которому он будет принадлежать.
3. Введите название для конфигурации фильтра. Название должно быть уникальным для фильтров алертов, фильтров инцидентов и фильтров событий.
4. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать фильтр, и нажмите **Сохранить**.

Конфигурация фильтра сохранена.

Чтобы выбрать ранее сохраненную конфигурацию фильтра:

1. В разделе KUMA **Алерты** откройте раскрывающийся список **Фильтры**.
2. Выберите нужную конфигурацию.

Конфигурация фильтра активна.

Вы можете выбрать фильтр, который будет использоваться по умолчанию, поставив в раскрывающемся списке **Фильтры** звездочку левее названия требуемой конфигурации фильтра.

Чтобы сбросить текущие настройки фильтра,

откройте раскрывающийся список **Фильтры** и выберите **Очистить фильтры**.

Удаление конфигураций фильтра алертов

Чтобы удалить ранее сохраненную конфигурацию фильтра:

1. В разделе KUMA **Алерты** откройте раскрывающийся список **Фильтры**.

2. Нажмите значок на фильтре, который требуется удалить.

3. Нажмите **OK**.

Конфигурация фильтра удалена для всех пользователей KUMA.

Просмотр информации об алерте

Чтобы просмотреть информацию об алерте:

1. В окне веб-интерфейса программы выберите раздел **Алерты**.

   Отобразится таблица алертов.

2. Нажмите на название алерта, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об алерте.

В верхней части окна с информацией об алерте расположена панель инструментов, а также указаны уровень важности алерта и имя пользователя, которому назначен этот алерт. В этом окне можно обработать алерт: изменить его уровень важности, назначить его пользователю, закрыть, создать на его основе инцидент.

Раздел Информация об алерте

Этот раздел позволяет просмотреть основную информацию об алерте. Он содержит следующие данные:

- **Уровень важности правила корреляции** – уровень важности правила корреляции, в результате срабатывания которого создан алерт.
- **Наивысшая важность категории активов** – самый высокий уровень важности категории активов из тех, которые принадлежат связанным с этим алертом активам. Если с алертом связано несколько активов, отображается наибольшее значение.
- **Привязан к инциденту** – если алерт привязан к инциденту,то отображаются название и статус алерта. Если алерт не привязан к инциденту, поле не заполнено.
- **Первое появление** – дата и время создания первого корреляционного события в последовательности событий, приведшего к созданию алерта.
- **Последнее появление** – дата и время создания последнего корреляционного события в последовательности событий, приведшего к созданию или обновлению алерта.
- **Идентификатор алерта** – уникальный идентификатор алерта в KUMA.

- **Тенант** – название тенанта, которому принадлежит алерт.

- **Правило корреляции** – название правила корреляции, в результате срабатывания которого создан алерт. Название правила представлено в виде ссылки, по которой можно перейти к настройкам этого правила корреляции.

- **Переполнен** – тег, означающий, что размер алерта достиг или приближается к пределу объема в 16 МБ и алерт необходимо обработать. Новые события не добавляются к переполненным алертам, но по ссылке **Смотреть все возможные связанные события** можно отфильтровать все события, которые могли быть связаны с алертом при отсутствии переполнения.

  Быстрое переполнение алерта может означать, что неверно настроено соответствующее корреляционное правило, и это приводит к частым срабатываниям. Переполненные алерты следует обрабатывать как можно скорее, чтобы при необходимости откорректировать корреляционное правило.

Раздел Связанные события

Этот раздел содержит таблицу событий, относящихся к алерту. Если нажать на значок > рядом с правилом корреляции, отобразятся базовые события из этого правила корреляции. События можно сортировать по уровню важности и времени.

При выборе события в таблице открывается область деталей, содержащая информацию о выбранном событии. В области деталей также отображает кнопка **Подробные сведения**, при нажатии на которую открывается окно, содержащее информацию о корреляционном событии.

Ссылки **Найти в событиях** под корреляционными событиями и кнопка **Найти в событиях** справа от заголовка раздела используются для перехода к детализированному анализу.

С помощью кнопки **Скачать события** вы можете скачать информацию о связанных событиях в виде файла в формате CSV (в кодировке UTF-8). В файле доступны столбцы, заполненные хотя бы в одном связанном событии.

> Некоторые редакторы CSV-файлов воспринимают значение разделителя (например, \n) в экспортируемом из KUMA CSV-файла как перенос строки, а не как разделитель. Может быть нарушено разделение файла на строки. Если вы столкнулись с подобным, то может потребоваться дополнительное редактирование CSV-файла, полученного из KUMA.

В таблице событий, в области деталей событий, в окне алертов, а также в виджетах в качестве значений полей SourceAssetID, DestinationAssetID, DeviceAssetID, SourceAccountID, DestinationAccountID и ServiceID вместо идентификаторов отображаются названия активов, учетных записей или сервисов. При экспорте событий в файл идентификаторы сохраняются, однако в файл добавляются столбцы с названиями. Идентификаторы также отображаются при наведении указателя мыши на названия активов, учетных записей или сервисов.

Поиск по полям с идентификаторами возможен только с помощью идентификаторов.

Раздел Связанные активы

Этот раздел содержит таблицу активов, относящихся к алерту. Информация об активах поступает из событий, связанных с алертом. С помощью поля **Поиск по IP или FQDN** можно искать нужные активы. Активы можно сортировать по столбцам **Количество** и **Актив**.

В этом разделе также отображаются активы, связанные с алертом. При нажатии на название актива открывается окно **Информация об активе**.

С помощью кнопки **Скачать активы** вы можете скачать информацию о связанных активах в виде файла в формате CSV (в кодировке UTF-8). В файле доступны столбцы: **Количество**, **Название**, **IP-адрес**, **Полное доменное имя**, **Категории**.

Раздел Связанные пользователи

Этот раздел содержит таблицу пользователей, относящихся к алерту. Информация о пользователях поступает из событий, связанных с алертом. С помощью поля **Поиск пользователей** можно искать нужных пользователей. Пользователей можно сортировать по столбцам **Количество**, **Пользователь**, **User principal name** (Основное имя пользователя) и **Адрес электронной почты**.

С помощью кнопки **Скачать пользователей** вы можете скачать информацию о связанных пользователях в виде файла в формате CSV (в кодировке UTF-8). В файле доступны столбцы: **Количество**, **Пользователь**, **User principal name**, **Адрес электронной почты**, **Домен**.

Раздел Журнал изменений

Этот раздел содержит записи об изменениях, которые пользователи внесли в алерт. Изменения регистрируются автоматически, при этом есть возможность вручную добавлять комментарии. Комментарии можно сортировать по столбцу **Время**.

При необходимости в поле **Комментарий** вы можете внести комментарий к алерту и нажать **Добавить**, чтобы сохранить его.

Изменение название алертов

Чтобы изменить название алерта:

1. В окне веб-интерфейса KUMA выберите раздел **Алерты**.

   Отобразится таблица алертов.

2. Нажмите на название алерта, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об алерте.

3. В верхней части окна нажмите на значок ✎ и в открывшемся поле введите новое название алерта. Подтвердите название, нажав **ENTER** или щелкнув вне поля ввода.

Название алерта изменено.

Обработка алертов

Вы можете изменить уровень важности алерта, назначить алерт пользователю, закрыть алерт или создать на основе алерта инцидент.

Чтобы обработать алерт:

1. Выберите необходимые алерты одним из следующих способов:

   - В разделе **Алерты** веб-интерфейса KUMA нажмите на алерт, сведения о котором вы хотите просмотреть.

     Откроется окно алерта, в верхней его части расположена панель инструментов.

   - В разделе **Алерты** веб-интерфейса KUMA установите флажок рядом с требуемым алертом. Можно выбрать более одного алерта.

     > Алерты со статусом **Закрыт** не могут быть выбраны для обработки.

     В нижней части окна отобразится панель инструментов.

2. Измените уровень важности алерта с помощью раскрывающегося списка **Уровень важности**:

   - **Низкий**.

- **Средний**.
- **Высокий**.
- **Критический**.

Уровень важности алерта принимает выбранное значение.

3. Назначьте алерт пользователю с помощью раскрывающегося списка **Назначить**.

   Вы можете назначить алерт себе, выбрав **Мне**.

   Статус алерта изменится на **Назначен**, а в раскрывающемся списке **Назначить** отобразится имя выбранного пользователя.

4. В разделе **Связанные пользователи** выберите пользователя и настройте параметры реагирования через Active Directory.

   a. После выбора связанного пользователя в открывшемся окне **Информация об учетной записи** нажмите **Реагирование через Active Directory**.

   b. В раскрывающемся списке **Команда Active Directory** выберите одно из следующих значений:

   - Добавить учетную запись в группу

     Группа Active Directory, из которой или в которую необходимо переместить учетную запись.
     В обязательном для заполнения поле **Distinguished name** необходимо указать полный путь к группе.
     Например, CN=HQ Team,OU=Groups,OU=ExchangeObjects,DC=avp,DC=ru.
     В рамках одной операции можно указать только одну группу.

   - Удалить учетную запись из группы

     Группа Active Directory, из которой или в которую необходимо переместить учетную запись.
     В обязательном для заполнения поле **Distinguished name** необходимо указать полный путь к группе.
     Например, CN=HQ Team,OU=Groups,OU=ExchangeObjects,DC=avp,DC=ru.
     В рамках одной операции можно указать только одну группу.

   - Сбросить пароль учетной записи
   - Блокировать учетную запись

c. Нажмите **Применить**.

5. При необходимости создайте на основе алерта инцидент:

   a. Нажмите **Создать инцидент**.

      Откроется окно создания инцидента. В качестве названия инцидента используется название алерта.

   b. Измените нужны параметры инцидента и нажмите **Сохранить**.

   Инцидент создан, статус алерта изменен на **Эскалирован**. Алерт можно отвязать от инцидента, выбрав его и нажав **Отвязать**.

6. Закройте алерт:

   a. Нажмите **Закрыть алерт**.

      Откроется окно подтверждения.

   b. Укажите причину закрытия алерта:

      - **Отработан**. Это означает, что были приняты необходимые меры по устранению угрозы безопасности.
      - **Неверные данные**. Это означает, что алерт был ложным, а полученные события не указывают на угрозу безопасности.
      - **Неверное правило корреляции**. Это означает, что алерт был ложным, а полученные события не указывают на угрозу безопасности. Возможно, требуется коррекция правила корреляции.

   c. Нажмите **OK**.

   Статус алерта изменен на **Закрыт**. Алерты с таким статусом не обновляются новыми корреляционными событиями и отображаются в таблице алертов, только если в раскрывающемся списке **Статус** установлен флажок **Закрыт**. Изменить статус закрытого алерта или назначить его другому пользователю невозможно.

Детализированный анализ

Детализированный анализ используется, когда вам нужно получить дополнительную информацию об угрозе, из-за которой был создан алерт: реальна ли угроза, откуда она исходит, на какие элементы сетевой среды она влияет, как следует бороться с угрозой. Анализ событий, связанных с корреляционными событиями, которые в свою очередь породили алерт, может помочь вам определить курс действий.

В KUMA режим детализированного анализа включается, когда вы нажимаете ссылку **Найти в событиях** в окне алерта или в окне корреляционного события. В режиме детализированного анализа отображается таблица событий с фильтрами, автоматически настроенными на поиск событий из алерта или корреляционного события. Фильтры также соответствуют времени продолжительности алерта или времени регистрации корреляционного события. Вы можете изменить эти фильтры, чтобы найти другие события и узнать больше о процессах, связанных с угрозой.

В режиме детализированного анализа становится доступным дополнительный раскрывающийся список :

- **Все события** – просмотр всех событий.
- **События алерта** (выбрано по умолчанию) – просмотр только событий, связанных с алертом.

> При фильтрации событий, связанным с алертом, действуют ограничения на сложность поисковых SQL-запросов.

Вы можете вручную привязать к алертам событие любого типа, кроме корреляционного. К алерту можно привязать только не привязанные к нему события.

В режиме детализированного анализа можно создавать и сохранять конфигурации фильтров событий. При использовании этого фильтра в обычном режиме просмотра событий будут отображены все события, соответствующие критериям фильтра, независимо от того, привязаны ли они к алерту, выбранному для детализированного анализа.

Чтобы привязать событие к алерту:

1. В разделе **Алерты** веб-интерфейса KUMA нажмите алерт, к которому вы хотите привязать событие.

   Откроется окно алерта.

2. В разделе **Связанные события** нажмите на кнопку **Найти в событиях**.

   Откроется таблица событий с включенными фильтрами даты и времени, соответствующим дате и времени регистрации привязанных к алерту событий. В столбцах отображаются параметры, используемые правилом корреляции для создания алерта. В таблице событий также отображается столбец **Привязка к алерту**, в котором отмечаются события, привязанные к алерту.

3. В раскрывающемся списке выберите значение **Все события**.

4. При необходимости измените фильтры, чтобы найти событие, которое требуется привязать к алерту.

5. Выберите нужное событие и нажмите на кнопку **Привязать к алерту** в нижней части области деталей события.

Событие будет привязано к алерту. Вы можете отвязать это событие от алерта, нажав в области деталей **Отвязать от алерта**.

Когда событие привязывается или отвязывается от алерта, в окне алерта в разделе **Журнал изменений** добавляется запись об этом действии. По ссылке в этой записи вы можете открыть область деталей и отвязать или привязать событие к алерту, нажав на соответствующую кнопку.

Срок хранения алертов и инцидентов

По умолчанию алерты и инциденты хранятся в KUMA в течение года, но этот срок можно изменить, исправив параметры запуска программы в файле /usr/lib/systemd/system/kuma-core.service на сервере Ядра KUMA.

Чтобы изменить срок хранения алертов и инцидентов:

1. Войдите в ОС сервера, на котором установлено Ядро KUMA.

2. В файле /usr/lib/systemd/system/kuma-core.service измените следующую строку, подставив нужное количество дней:

   ```
   ExecStart=/opt/kaspersky/kuma/kuma core --alerts.retention <количество дней, в течение которых требуется хранить алерты и инциденты> --external :7220 --internal :7210 --mongo mongodb://localhost:27017
   ```

3. Перезапустите KUMA, выполнив последовательно следующие команды:

   a. `systemctl daemon-reload`

   b. `systemctl restart kuma-core`

Срок хранения алертов и инцидентов изменен.

Уведомления об алертах

При создании и назначении алертов по электронной почте рассылаются стандартные уведомления KUMA. Вы можете настроить рассылку уведомлений о создании алерта на основе пользовательского шаблона электронной почты.

Чтобы настроить рассылку уведомлений о создании алерта на основе пользовательского шаблона:

1. Откройте раздел **Параметры** → **Алерты** → **Правила уведомлений** веб-интерфейса KUMA.

2. Выберите тенант, для которого вы хотите создать правило уведомления:

   - Если у тенанта уже есть правила уведомлений, выберите его в таблице.

   - Если у тенанта нет правил уведомлений, нажмите **Добавить тенант** и в раскрывающемся списке **Тенант** выберите нужный тенант.

3. В блоке параметров **Правила уведомлений** нажмите **Добавить** и укажите параметры правила уведомлений:

   - **Название** (обязательно) – в этом поле укажите название правила уведомления.

   - **Адреса получателей** (обязательно) – в этом блоке параметров с помощью кнопки **Адрес электронной почты** можно добавить адреса электронной почты, на которые необходимо отправлять уведомления о создании алертов. Адреса добавляются по одному.

     > Кириллические домены не поддерживаются. Например, уведомление по адресу `login@домен.рф` отправлено не будет.

   - **Правила корреляции** (обязательно) – в этом блоке параметров необходимо выбрать одно или несколько правил корреляции, при срабатывании которых будут отправляться уведомления.

     В окне в виде древовидной структуры отображаются правила корреляции из общего и выбранного пользователем тенанта. Для выбора правила необходимо установить флажок рядом с ним. Можно установить флажок рядом с папкой: в таком случае будут выбраны все правила корреляции в этой папке и ее подпапках.

   - **Шаблон** (обязательно) – в этом блоке параметров необходимо выбрать шаблон электронной почты, по которому будут создаваться рассылаемые уведомления. Для выбора шаблона нажмите на значок , в открывшемся окне выберите требуемый шаблон и нажмите **Сохранить**.

     Шаблон можно создать, нажав на значок плюса, или отредактировать выбранный шаблон, нажав на значок карандаша.

   - **Выключено** – установив этот флажок вы можете выключить правило уведомления.

4. Нажмите **Сохранить**.

   Правило уведомления создано. Когда по выбранным правилам корреляции будет создаваться алерт, на указанные адреса электронной почты будут отправляться уведомления, созданные на основе пользовательских шаблонов электронной почты. Стандартные уведомления KUMA о том же событии на указанные адреса отправлены не будут.

Чтобы выключить правила уведомлений для тенанта:

1. Откройте раздел **Параметры** → **Алерты** → **Правила уведомлений** веб-интерфейса KUMA и выберите тенант, правила уведомлений которого вы хотите выключить.

2. Установите флажок **Выключено**.

3. Нажмите **Сохранить**.

   Правила уведомлений выбранного тенанта выключены.

Работа с событиями

В разделе **События** веб-интерфейса KUMA вы можете просматривать полученные программой события, чтобы расследовать угрозы безопасности или создавать правила корреляции. В таблице событий отображаются данные, полученные после выполнения SQL-запроса.

События можно отправлять в коррелятор для ретроспективной проверки.

Формат даты события зависит от языка локализации, выбранного в настройках 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 KUMA данные не отображаются. Для просмотра событий в поле поиска нужно задать SQL-запрос и нажать на кнопку 🔍. SQL-запрос можно ввести вручную или сформировать с помощью конструктора запросов.

В SQL-запросах поддерживается агрегирование и группировка данных.

Вы можете добавить условия фильтрации в уже сформированный SQL-запрос в окне просмотра статистики, таблицы событий и области деталей событий:

- Изменение запроса из окна статистики

*Чтобы изменить параметры фильтрации из окна **Статистика**:*

1. Откройте область деталей **Статистика** одним из следующих способов:

   - В правом верхнем углу таблицы событий в раскрывающемся списке ••• выберите **Статистика**.

   - В таблице событий нажмите на любое значение и в открывшемся контекстном меню выберите **Статистика**.

   В правой части окна откроется область деталей **Статистика**.

2. Откройте раскрывающийся список необходимого параметра и наведите курсор мыши на требуемое значение.

3. С помощью значков плюса и минуса измените параметры фильтрации, выполнив одно из следующих действий:

   - Если вы хотите включить в выборку событий только события с выбранным значением, нажмите +.

   - Если вы хотите исключить из выборки событий все события с выбранным значением, нажмите −.

   В результате параметры фильтрации и таблица событий будут обновлены, а в верхней части экрана отобразится измененный поисковый запрос.

- Изменение запроса из таблицы событий

Чтобы изменить параметры фильтрации из таблицы событий:

1. В разделе **События** веб-интерфейса KUMA нажмите на любое значение параметра события в таблице событий.

2. В открывшемся меню выберите один из следующих вариантов:

   - Если вы хотите оставить в таблице только события с выбранным значением, выберите **Искать события с этим значением**.

   - Если вы хотите исключить из таблицы все события с выбранным значением, выберите **Искать события без этого значения**.

В результате параметры фильтрации и таблица событий обновляются, а в верхней части экрана отображается измененный поисковый запрос.

- **Изменение запроса из области деталей события**

Чтобы изменить параметры фильтрации в области деталей события:

1. В разделе **События** веб-интерфейса KUMA нажмите на нужное событие.

   В правой части окна откроется область деталей **Информация о событии**.

2. Измените параметры фильтрации, используя значки плюса или минуса рядом с необходимыми параметрами:

   - 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.

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** 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.

Подробнее об SQL см. в справке ClickHouse. Также см. использование операторов в KUMA и поддерживаемые функции.

Формирование SQL-запроса с помощью конструктора

В KUMA вы можете сформировать SQL-запрос для фильтрации событий с помощью конструктора запросов.

Чтобы сформировать SQL-запрос с помощью конструктора:

1. В разделе **События** веб-интерфейса KUMA нажмите на кнопку .

   Откроется окно конструктора запросов.

2. Сформулируйте поисковый запрос, указав данные в следующих блоках параметров:

   SELECT – поля событий, которые следует возвращать. По умолчанию выбрано значение *, означающее, что необходимо возвращать все доступные поля события. Чтобы вам проще было просматривать результаты поиска, в раскрывающемся списке вы можете выбрать необходимые поля, тогда в таблице будут отображаться данные только для выбранных полей. Стоит учитывать, что Select * в запросе увеличивает длительность выполнения запроса, но избавляет от необходимости прописывать поля в запросе вручную.

   Выбрав поле события, вы можете в поле справа от раскрывающегося списка указать псевдоним для столбца выводимых данных, а в крайнем правом раскрывающемся списке можно выбрать операцию, которую следует произвести над данными: **count**, **max**, **min**, **avg**, **sum**.

   Если вы используете в запросе функции агрегации, настройка отображения таблицы событий, сортировка событий по возрастанию и убыванию, а также получение статистики недоступны.

   > В режиме детализированного анализа при фильтрации по событиям, связанным с алертами, невозможно производить операции над данными полей событий и присваивать названия столбцам выводимых данных.

   - **FROM** – источник данных. Выберите значение **events**.

   - **WHERE** – условия фильтрации событий.

     Условия и группы условий можно добавить с помощью кнопок **Добавить условие** и **Добавить группу**. По умолчанию в группе условий выбрано значение оператора **AND**, однако если на него нажать, оператор можно изменить. Доступные значения: **AND**, **OR**, **NOT**. 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 можно удалить с помощью кнопки ✕. Группы условий удаляются с помощью кнопки **Удалить группу**.

- **GROUP BY** – поля событий или псевдонимы, по которым следует группировать возвращаемые данные.

  Если вы используете в запросе группировку данных, настройка отображения таблицы событий, сортировка событий по возрастанию и убыванию, получение статистики, а также ретроспективная проверка недоступны.

  > В режиме детализированного анализа при фильтрации по событиям, связанным с алертами, невозможно группировать возвращаемые данные.

- **ORDER BY** – столбцы, по которым следует сортировать возвращаемые данные. В раскрывающемся списке справа можно выбрать порядок: **DESC** – по убыванию, **ASC** – по возрастанию.

- **LIMIT** – количество отображаемых в таблице строк.

  Значение по умолчанию – 250.

  Если при фильтрации событий по пользовательскому периоду количество строк в результатах поиска превышает заданное значение, вы можете отобразить в таблице дополнительные строки, нажав на кнопку **Показать больше записей**. Кнопка не отображается при фильтрации событий по стандартному периоду.

3. Нажмите на кнопку **Применить**.

   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 .

4. Для отображения данных в таблице нажмите на кнопку 🔍.

   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 KUMA и поддерживаемые функции.

Создание SQL-запроса вручную

С помощью строки поиска вы можете вручную создавать SQL-запросы любой сложности для фильтрации событий.

Чтобы сформировать SQL-запрос вручную:

1. Перейдите в раздел **События** веб-интерфейса KUMA.

   Откроется форма с полем ввода.

2. Введите SQL-запрос в поле ввода.

3. Нажмите на кнопку 🔍.

   Отобразится таблица событий, соответствующих условиям вашего запроса. При необходимости вы можете отфильтровать события по периоду.

Поддерживаемые функции и операторы

- `SELECT` – поля событий, которые следует возвращать.

  Для `SELECT` в программе поддержаны следующие функции и операторы:

  - Функции агрегации: `count, avg, max, min, sum`.
  - Арифметические операторы: `+, -, *, /, <, >, =, !=, >=, <=`.

    Вы можете комбинировать эти функции и операторы.

Если вы используете в запросе функции агрегации, настройка отображения таблицы событий, сортировка событий по возрастанию и убыванию, а также получение статистики недоступны.

- `FROM` — источник данных.

  > При создании запроса в качестве источника данных вам нужно указать значение events.

- `WHERE` — условия фильтрации событий.
  - `AND, OR, NOT, =, !=, >, >=, <, <=`
  - `IN`
  - `BETWEEN`
  - `LIKE`
  - `ILIKE`
  - `inSubnet`
  - `match` (в запросах используется синтаксис регулярных выражений re2, специальные символы требуется дополнительно экранировать с помощью обратной косой черты (\))
- `GROUP BY` — поля событий или псевдонимы, по которым следует группировать возвращаемые данные.

  Если вы используете в запросе группировку данных, настройка отображения таблицы событий, сортировка событий по возрастанию и убыванию, получение статистики, а также ретроспективная проверка недоступны.

- `ORDER BY` — столбцы, по которым следует сортировать возвращаемые данные.

  Возможные значения:

  - `DESC` — по убыванию.
  - `ASC` — по возрастанию.
- `OFFSET` — пропуск указанного количества строк перед выводом результатов запроса.
- `LIMIT` — количество отображаемых в таблице строк.

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 записей**. Кнопка не отображается при фильтрации событий по стандартному периоду.

Примеры запросов:

- `SELECT * FROM `events` WHERE Type IN ('Base', 'Audit') ORDER BY Timestamp DESC LIMIT 250`

  Все события таблицы events с типом **Base** и **Audit**, отсортированные по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

- `SELECT * FROM `events` WHERE BytesIn BETWEEN 1000 AND 2000 ORDER BY Timestamp ASC LIMIT 250`

  Все события таблицы events, для которых в поле **BytesIn** значение полученного трафика находится в диапазоне от 1000 до 2000 байт, отсортированные по столбцу **Timestamp** в порядке возрастания. Количество отображаемых в таблице строк – 250.

- `SELECT * FROM `events` WHERE Message LIKE '%ssh:%' ORDER BY Timestamp DESC LIMIT 250`

  Все события таблицы events, которые в поле **Message** содержат данные, соответствующие заданному шаблону `%ssh:%` в нижнем регистре, и отсортированы по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

- `SELECT * FROM `events` WHERE inSubnet(DeviceAddress, '00.0.0.0/00') ORDER BY Timestamp DESC LIMIT 250`

  Все события таблицы events для 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.

При переключении на конструктор параметры запроса, введенного вручную в строке поиска, не переносятся в конструктор: вам требуется создать запрос заново. При этом запрос, созданный в конструкторе, не перезаписывает запрос, введенный в строке поиска, пока вы не нажмете на кнопку **Применить** в окне конструктора.

Используемые в поисковых запросах псевдонимы не должны содержать пробелов.

Подробнее об SQL см. в справке ClickHouse. Также см. поддерживаемые функции ClickHouse.

Создание пресета

Вы можете использовать пресеты для упрощения работы с запросами, если вы регулярно хотите просматривать данные по определенному набору полей событий. 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 **Тенанта** в выпадающем списке.
5. Нажмите **Сохранить**.

   Пресет создан и сохранен.

Применение пресета

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 запрос, а столбцы будут добавлены в таблицу.

4. Нажмите на кнопку , чтобы выполнить запрос.

   После выполнения запроса столбцы будут заполнены.

Ограничение сложности запросов в режиме детализированного анализа

При детализированном анализе сложность SQL-запросов для фильтрации событий ограничена, если при расследовании алерта в раскрывающемся списке выбран пункт **События алерта**. В этом случае для фильтрации событий доступны только перечисленные ниже функции и операторы.

> При выборе в раскрывающемся списке пункта **Все события** эти ограничения не действуют.

- `SELECT`
  - В качестве символа подстановки используется `*`.
- `WHERE`
  - `AND`, `OR`, `NOT`, `=`, `!=`, `>`, `>=`, `<`, `<=`
  - `IN`
  - `BETWEEN`
  - `LIKE`
  - `inSubnet`

  Примеры:

  - `WHERE Type IN ('Base', 'Correlated')`
  - `WHERE BytesIn BETWEEN 1000 AND 2000`
  - `WHERE Message LIKE '%ssh:%'`

- `WHERE inSubnet(DeviceAddress, '10.0.0.1/24')`

- `ORDER BY`

  Сортировка возможна по столбцам.

- `OFFSET`

  Пропуск указанного количества строк перед выводом результатов запроса.

- `LIMIT`

  Значение по умолчанию – 250.

  Если при фильтрации событий по пользовательскому периоду количество строк в результатах поиска превышает заданное значение, вы можете отобразить в таблице дополнительные строки, нажав на кнопку **Показать больше записей**. Кнопка не отображается при фильтрации событий по стандартному периоду.

В режиме детализированного анализа при фильтрации по событиям, связанным с алертами, невозможно группировать возвращаемые данные. В режиме детализированного анализа при фильтрации по событиям, связанным с алертами, невозможно производить операции над данными полей событий и присваивать названия столбцам выводимых данных.

Фильтрация событий по периоду

В KUMA вы можете настроить отображение событий, относящихся к определенному временному периоду.

Чтобы отфильтровать события по периоду:

1. В разделе **События** веб-интерфейса KUMA в верхней части окна откройте раскрывающийся список **Период**.

2. Если вы хотите выполнить фильтрацию по стандартному периоду, выберите один из следующих вариантов:

   - **5 минут**

   - **15 минут**

   - **1 час**

   - **24 часа**

   - **В течение периода**

При выборе этого варианта в открывшемся календаре выберите дату начала и окончания периода и нажмите **Применить фильтр**. Формат даты и времени зависит от настроек вашей операционной системы. При необходимости вы также можете изменить значения даты вручную.

3. Нажмите на кнопку .

Если установлен фильтр по периоду, 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 ряд данных или выделить требуемый период времени и нажать на кнопку **Показать события**.

Сохранение и выбор конфигураций фильтра событий

В KUMA вы можете сохранять конфигурации фильтров для использования в будущем. Другие пользователи также могут использовать сохраненные фильтры при условии, что у них есть соответствующие права доступа. При сохранении фильтра вы сохраняете настроенные параметры сразу всех активных фильтров: фильтр по периоду, конструктору запросов и параметры таблицы событий. Поисковые запросы сохраняются на сервере Ядра KUMA и доступны всем пользователям KUMA выбранного тенанта.

Чтобы сохранить текущие настройки фильтра, запроса и периода:

1. В разделе **События** веб-интерфейса KUMA нажмите на значок рядом с выражением фильтра и выберите **Сохранить текущий фильтр**.

2. В открывшемся окне в поле **Название** введите название конфигурации фильтра. Название должно содержать до 128 символов Юникода.

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

4. Нажмите **Сохранить**.

Конфигурация фильтра сохранена.

Чтобы выбрать ранее сохраненную конфигурацию фильтра:

в разделе **События** веб-интерфейса KUMA нажмите на значок рядом с выражением фильтра и выберите нужный фильтр.

Выбранная конфигурация активна: в поле поиска отображается поисковый запрос, в верхней части окна настроенные параметры периода и частоты обновления результатов поиска. Для отправки поискового запроса нажмите на кнопку .

Если нажать на значок рядом с названием конфигурации фильтра, она станет использоваться в качестве конфигурации по умолчанию.

Удаление конфигураций фильтра событий

Чтобы удалить ранее сохраненную конфигурацию фильтра:

1. В разделе **События** веб-интерфейса KUMA нажмите на значок рядом с поисковым запросом фильтра и нажмите значок рядом с конфигурацией, которую требуется удалить.

2. Нажмите **OK**.

Конфигурация фильтра удалена для всех пользователей KUMA.

Поддерживаемые функции ClickHouse

В KUMA поддерживаются следующие функции ClickHouse:

- Арифметические функции.
- Массивы – все функции, кроме:
  - has;
  - range;
  - функций, в которых обязательны к использованию функции высшего порядка (стрелочные лямбда-выражения (->)).
- Функции сравнения: все операторы, кроме == и less.
- Логические функции: только функция not.
- Функции преобразования типов.
- Функции для работы с датами и временем: все функции, кроме date_add и date_sub.
- Функции для работы со строками.

- Функции поиска в строках – все функции, кроме:
  - position;
  - multiSearchAllPositions, multiSearchAllPositionsUTF8, multiSearchFirstPosition, multiSearchFirstIndex, multiSearchAny;
  - like и ilike;
- Условные функции: только обычный оператор if (тернарный оператор и оператор miltif не поддерживаются).
- 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 поиска и замены в строках, а также 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** раскрывается 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** вы можете просмотреть параметры сервиса, зарегистрировавшего событие.

  Вы также можете привязать событие к алерту, если программа находится в режиме детализированного анализа, и открыть окно **Информация о корреляционном событии**, если выбранное событие является корреляционным.

Экспорт событий

Из KUMA можно экспортировать информацию о событиях в TSV-файл. Выборка событий, которые будут экспортированы в TSV-файл, зависит от настроек фильтра. Информация экспортируется из столбцов, которые в данный момент отображаются в таблице событий, при этом столбцы в файле наполняются доступными данными, даже если в таблице событий в веб-интерфейсе KUMA они не отображались из-за особенностей SQL-запроса.

Чтобы экспортировать информацию о событиях:

1. В разделе **События** веб-интерфейса KUMA откройте раскрывающийся список ••• и выберите **Экспортировать в формат TSV**.

   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** отобразится 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.

Выбор хранилища

События, которые отображаются в веб-интерфейсе KUMA в разделе **События**, получены из хранилища (то есть кластера ClickHouse). В зависимости от потребностей вашей компании у вас может быть более одного хранилища, однако для получения событий необходимо указывать, события из какого именно хранилища вам требуются.

Чтобы выбрать хранилище, из которого вы хотите получать события,

В разделе **События** веб-интерфейса KUMA откройте раскрывающийся список и выберите нужный кластер хранилища.

В таблице событий отображаются события из указанного хранилища. Имя выбранного хранилища отображается в раскрывающемся списке .

В раскрывающемся списке отображаются только кластеры тенантов, доступных пользователю, а также кластер главного тенанта.

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 частотных значений. С помощью поля **Поиск** можно найти нужные параметры.

В окне **Статистика** можно менять фильтр событий.

При использовании для фильтрации событий SQL-запросов с группировкой и агрегацией данных статистика недоступна.

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:

- **Тенант**.
- **Timestamp**.
- **Name**.
- **DeviceProduct**.
- **DeviceVendor**.
- **DestinationAddress**.
- **DestinationUserName**.

В KUMA 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, в окне алертов, а также в виджетах в качестве значений полей SourceAssetID, DestinationAssetID, DeviceAssetID, SourceAccountID, DestinationAccountID и ServiceID вместо идентификаторов отображаются названия активов, учетных записей или сервисов. При экспорте событий в файл идентификаторы сохраняются, однако в файл добавляются столбцы с названиями. Идентификаторы также отображаются при наведении указателя мыши на названия активов, учетных записей или сервисов.

Поиск по полям с идентификаторами возможен только с помощью идентификаторов.

Чтобы настроить поля, отображаемые в таблице событий:

1. В правом верхнем углу таблицы событий нажмите значок .

   Откроется окно для выбора полей событий, которые требуется отображать в таблице событий.

2. Установите флажки напротив полей, которые требуется отображать в таблице. С помощью поля **Поиск** можно найти нужные поля.

   Вы можете отобразить в таблице любое поле события из модели данных событий KUMA. 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 :

- **5 секунд**
- **15 секунд**
- **30 секунд**
- **1 минута**
- **5 минут**
- **15 минут**

Таблица событий обновляется автоматически.

Чтобы выключить автоматические обновление,

Выберите **Не обновлять** в раскрывающемся списке .

Открытие окна корреляционного события

Вы можете просматривать подробные сведения о корреляционном событии в окне **Информация о корреляционном событии**.

Чтобы открыть окно корреляционного события:

1. В разделе **События** веб-интерфейса KUMA нажмите на корреляционное событие.

   Вы можете использовать фильтры для поиска корреляционных событий, присвоив значение `correlated` параметру `Type`.

   Откроется область деталей выбранного события. Если выбранное событие является корреляционным, в нижней части области деталей будет отображаться кнопка **Подробные сведения**.

2. Нажмите на кнопку **Подробные сведения**.

Откроется окно корреляционного события. Название события отображается в левом верхнем углу окна.

В разделе **Информация о корреляционном событии** окна корреляционного события отображаются следующие данные:

- **Уровень важности корреляционного события** – важность корреляционного события.
- **Правило корреляции** – название правила корреляции, которое породило корреляционное событие. Название правила представлено в виде ссылки, по которой можно перейти к настройкам этого правила корреляции.
- Уровень важности правила корреляции – важность правила корреляции, вызвавшего корреляционное событие.
- **Идентификатор правила корреляции** – идентификатор правила корреляции, которое породило корреляционное событие.
- **Тенант** – название тенанта, которому принадлежит корреляционное событие.

Раздел **Связанные события** окна корреляционного события содержит таблицу событий, относящихся к корреляционному событию. Это базовые события, в результате обработки которых было создано корреляционное событие. При выборе события в правой части окна веб-интерфейса открывается область деталей.

Ссылка **Найти в событиях** справа от заголовка раздела используется для детализированного анализа.

Раздел **Связанные активы** окна корреляционного события содержит таблицу узлов, относящихся к корреляционному событию. Эта информация поступает из базовых событий, связанных с корреляционным событием. При нажатии на название актива открывается окно **Информация об активе**.

Раздел **Связанные пользователи** окна корреляционного события содержит таблицу пользователей, относящихся к корреляционному событию. Эта информация поступает из базовых событий, связанных с корреляционным событием.

Ретроспективная проверка

Вы можете использовать функцию *Ретроспективная проверка* для "воспроизведения" событий в KUMA путем передачи выборки событий в коррелятор для их обработки определенными правилами корреляции. Можно указать, чтобы во время ретроспективной проверки событий создавались алерты. Ретроспективная проверка может быть полезна при отладке ресурсов правил корреляции или анализе исторических данных.

При ретроспективной проверке события не обогащаются данными из CyberTrace и Kaspersky Threat Intelligence Portal.

Активные листы при ретроспективной проверке обновляются.

> Ретроспективную проверку невозможно проводить на выборках событий, полученных с помощью SQL-запросов с группировкой данных и арифметическими выражениями.

Чтобы включить ретроспективную проверку:

1. В разделе **События** веб-интерфейса KUMA получите необходимую выборку событий:
   - Выберите хранилище.
   - Настройте поисковое выражение с помощью конструктора или поискового запроса.
   - Задайте необходимый временной период.
2. В раскрывающемся списке ••• выберите **Ретроспективная проверка**.

   Откроется окно ретроспективной проверки.
3. В раскрывающемся списке **Коррелятор** выберите сервис коррелятора, в который будут загружены выбранные события.
4. В раскрывающемся списке **Правила корреляции** выберите правила корреляции, с помощью которых необходимо обработать выбранные события.
5. Если вы хотите, чтобы в процессе обработки событий срабатывали правила реагирования, включите переключатель **Выполнить правила реагирования**.
6. Если вы хотите, чтобы в процессе обработки событий создавались алерты, включите переключатель **Создать алерты**.
7. Нажмите на кнопку **Создать задачу**.

В разделе **Диспетчер задач** создана задача ретроспективной проверки.

Чтобы просмотреть результаты проверки,

В разделе **Диспетчер задач** веб-интерфейса KUMA нажмите на созданную вами задачу и в раскрывающемся списке выберите **Перейти к событиям**.

Открывается новая вкладка браузера с таблицей событий, обработанных в ходе ретроспективной проверки, а также агрегированными и корреляционными событиями, созданные во время обработки.

> В зависимости от настроек вашего браузера может потребоваться ваше подтверждение на открытие новой вкладки с результатами ретроспективной проверки. Подробнее см. в документации вашего браузера.

Работа с геоданными

В KUMA можно загрузить список соответствий IP-адресов или диапазонов IP-адресов географическим данным, чтобы затем использовать эту информацию при обогащении событий.

Формат геоданных

Геоданные можно загрузить в KUMA в виде CSV-файла в кодировке UTF-8. В качестве разделителя используется запятая. В первой строке файла указаны заголовки полей: `Network,Country,Region,City,Latitude,Longitude`.

Описание CSV-файла

Имя заголовка поля в CSV	Описание поля	Пример
`Network`	IP-адрес в одном из следующих форматов: • единичный IP-адрес; • диапазон IP-адресов; • IP-адрес в формате CIDR. Допускается перемешивание ipv4- и ipv6-адресов. Обязательное поле.	• `192.168.2.24` • `192.168.2.25-192.168.2.35` • `131.10.55.70/8` • `2001:DB8::0/120`
`Country`	Принятое в вашей организации обозначение страны. Например, ее название или код. Обязательное поле.	• `Russia` • `RU`

`Region`	Принятое в вашей организации обозначение области. Например, ее название или код.	• `Sverdlovsk Oblast` • `RU-SVE`
`City`	Принятое в вашей организации обозначение города. Например, его название или код.	• `Yekaterinburg` • `65701000001`
`Latitude`	Широта описываемой точки в десятичном формате. Поле может быть пустым – в этом случае при импорте в KUMA будет использовано значение 0.	`56.835556`
`Longitude`	Долгота описываемой точки в десятичном формате. Поле может быть пустым – в этом случае при импорте в KUMA будет использовано значение 0.	`60.612778`

Конвертация геоданных из MaxMind и IP2Location

В KUMA можно использовать геоданные, полученные из MaxMind и IP2Location, однако перед использованием файлы требуется конвертировать в поддерживаемый KUMA формат. Конвертацию можно произвести с помощью приведенного ниже скрипта. Убедитесь, что файлы не содержат дублирующихся записей: например, если в файле мало колонок, в разные записи могут попадать данные одной и той же сети с теми же геоданными - такой файл конвертировать не удастся. Чтобы успешно выполнить конвертацию, убедитесь, что дублирующиеся строки отсутствуют и все строки уникальны по какому-либо полю.

Скачать скрипт

Для запуска скрипта требуется Python 2.7 или выше.

Команда запуска скрипта:

```
python converter.py --type <тип обрабатываемых геоданных: "maxmind" или "ip2location"> --out <директория, в которую будет помещен CSV-файл с геоданными в формате KUMA> --input <путь к ZIP-архиву с геоданными из MaxMind или IP2location>
```

При запуске скрипта с флагом `--help` отображается справка по доступным параметрам запуска скрипта: `python converter.py --help`

Команда для конвертации файла с российской базой диапазонов IP-адресов из ZIP-архива MaxMind:

```
python converter.py --type maxmind --lang ru --input MaxMind.zip --out
geoip_maxmind_ru.csv
```

> Без указания параметра `--lang` скрипт по умолчанию получает информацию из файла GeoLite2-City-Locations-en.csv из ZIP-архива.

Отсутствие параметра `--lang` для MaxMind равнозначно команде:

```
python converter.py --type maxmind --input MaxMind.zip --out
geoip_maxmind.csv
```

Команда для конвертации файла из ZIP-архива IP2Location:

```
python converter.py --type ip2location --input IP2LOCATION-LITE-
DB11.CSV.ZIP --out geoip_ip2location.csv
```

Команда для конвертации файла из нескольких ZIP-архивов IP2Location:

```
python converter.py --type ip2location --input IP2LOCATION-LITE-
DB11.CSV.ZIP IP2LOCATION-LITE-DB11.IPV6.CSV.ZIP --out
geoip_ip2location_ipv4_ipv6.csv
```

> Параметр `--lang` для IP2Location не используется.

Обязательные наборы полей

Исходные файлы MaxMind GeoLite2-City-Blocks-IPv4.csv и GeoLite2-City-Blocks-IPv6.csv должны содержать следующий набор полей:

network,geoname_id,registered_country_geoname_id,represented_country_geoname_id,
is_anonymous_proxy,is_satellite_provider,postal_code,latitude,longitude,accuracy_radius

Пример набора исходных данных:

```
network,geoname_id,registered_country_geoname_id,represented_country_geoname_
is_anonymous_proxy,is_satellite_provider,postal_code,latitude,longitude,accur

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_
subdivision_1_iso_code,subdivision_1_name,subdivision_2_iso_code,subdivision_
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"
```

Если исходные файлы будут содержать другой набор полей, отличный от указанного в этом разделе, или каких-то полей будет не хватать, после конвертации отсутствующие поля в итоговом файле CSV будут пустыми.

Импорт и экспорт геоданных

При необходимости в KUMA вы можете вручную импортировать и экспортировать геоданные. Геоданные импортируются и экспортируются в файле формате CSV. При успешном импорте геоданных ранее добавленные данные перезаписываются и в KUMA создается событие аудита.

Чтобы импортировать геоданные в KUMA:

1. Подготовьте CSV-файл с геоданными.

   Геоданные, полученные из MaxMind и IP2Location, требуется конвертировать в поддерживаемый KUMA формат.

2. В веб-интерфейсе KUMA откройте раздел **Параметры** → **Общие**.

3. В блоке параметров **Геоданные** нажмите на кнопку **Импортировать из файла** и выберите CSV-файл с геоданными.

   Дождитесь окончания импорта геоданных. При обновлении страницы загрузка данных прерывается.

Геоданные загружены в KUMA.

Чтобы экспортировать геоданные из KUMA,

1. В веб-интерфейсе KUMA откройте раздел **Параметры** → **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 настройками вашего браузера.

Данные экспортируются в том же формате, в каком они были загружены, за исключением диапазонов IP-адресов. Если в KUMA в импортированном файле диапазон адресов указан в формате `1.0.0.0/24`, то в файле экспорта диапазон отобразится в формате `1.0.0.0-1.0.0.255`.

Сопоставление геоданных по умолчанию

Если при настройке правила обогащения геоданными в качестве источника IP-адреса выбрать поля события `SourceAddress`, `DestinationAddress` и `DeviceAddress`, становится доступна кнопка **Применить сопоставление по умолчанию**. 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`

Управление активами

Вы можете управлять активами KUMA: просматривать информацию об активах, искать активы, добавлять активы, редактировать их и удалять, а также экспортировать данные о них в CSV-файл.

Категории активов

В KUMA активы распределены по тенантам и категориями. Активы выстроены в древовидную структуру, где в корне находятся тенанты и от них ветвятся категории активов. Вы можете просмотреть дерево тенантов и категорий в разделе **Активы** → **Все активы** веб-интерфейса KUMA. Если выбрать узел дерева, в правой части окна отображаются активы, относящиеся к соответствующей категории. Активы из подкатегорий выбранной категории не отображаются, если вы не укажете, что хотите отображать активы рекурсивно. Вы можете выделить флажками тенанты, активы которых хотите просматривать.

Категории активам можно присваивать вручную или автоматически. Автоматическая категоризация может быть реактивной, когда категории наполняются активами с помощью правил корреляции, или активной, когда категории присваиваются все активы, удовлетворяющие определенным условиям. Способ категоризации можно указать в параметрах категории при ее создании или изменении.

Если навести указатель мыши на категорию, справа от названия категории появится значок с многоточием. При нажатии на этот значок отобразится контекстное меню категорией, в котором можно выбрать следующие действия:

- **Показать активы** – просмотреть активы выбранной категории в правой части окна.
- **Отображать активы рекурсивно** – просмотреть активы из подкатегорий выбранной категории. Если вы хотите выйти из режима рекурсивного просмотра, выберите категорию для просмотра.
- **О категории** – просмотреть информации о выбранной категории в области деталей **Информация о категории**, которая отображается в правой части окна веб-интерфейса.
- **Начать категоризацию** – стартовать автоматическую привязку активов к выбранной категории. Доступно для категорий с активным способом категоризации.
- **Добавить подкатегорию** – добавление подкатегории к выбранной категории.
- **Изменить категорию** – изменение выбранной категории.
- **Удалить категорию** – удаление выбранной категории. Удалять можно только категории без активов или подкатегорий. В противном случае опция **Удалить категорию** будет неактивна.
- **Сделать закладкой** – отображение выбранной категории на отдельной закладке. Отменить это действие можно, выбрав в контекстном меню нужной категории **Убрать из закладок**.

Добавление категории активов

Чтобы добавить категорию активов:

1. Откройте раздел **Активы** веб-интерфейса KUMA.

2. Откройте окно создания категории:

   - Нажмите на кнопку **Добавить категорию**.

   - Если вы хотите создать подкатегорию, в контекстном меню родительской категории выберите **Добавить подкатегорию**.

   В правой части окна веб-интерфейса отобразится область деталей **Добавить категорию**.

3. Добавьте сведения о категории:

   - В поле **Название** введите название категории. Название должно содержать от 1 до 128 символов Юникода.

   - В поле **Родительская категория** укажите место категории в дереве категорий:

     a. Нажмите на кнопку .

     Откроется окно **Выбор категорий**, в котором отображается дерево категорий. Если вы создаете новую категорию, а не подкатегорию, то в окне может отображаться несколько деревьев категорий активов: по одному для каждого доступного вам тенанта. Выбор тенанта в этом окне невозможно отменить.

     b. Выберите родительскую категорию для создаваемой вами категории.

     c. Нажмите **Сохранить**.

     Выбранная категория отобразится в поле **Родительская категория**.

   - В поле **Тенант** отображается тенант, в структуре которого вы выбрали родительскую категорию. Тенанта категории невозможно изменить.

   - Назначьте уровень важности категории в раскрывающемся списке **Уровень важности**.

   - При необходимости в поле **Описание** добавьте примечание: до 256 символов Юникода.

4. В раскрывающемся списке **Способ категоризации** выберите, как категория будет пополняться активами. В зависимости от выбора может потребоваться указать дополнительные параметры:

   - **Вручную** – активы можно привязать к категории только вручную.

- **Активно** – активы будут с определенной периодичностью привязываться к категории, если удовлетворяют заданному фильтру.

  Активная категория активов

  1. В раскрывающемся списке **Регулярность категоризации** укажите периодичность, с которой активы будут привязываться к категории. Можно выбрать значения от одного раза в час до одного раза в сутки.

     Категоризацию можно запустить принудительно, выбрав в контекстном меню категории **Начать категоризацию**.

  2. В блоке параметров **Условия** укажите фильтр, которому должны соответствовать активы для привязывания к категории.

     Условия можно добавлять с помощью кнопок **Добавить условие**. Группы условий можно добавлять с помощью кнопок **Добавить группу**. Групповые операторы можно переключать между значениями **И**, **ИЛИ**, **НЕ**.

     Операнды и операторы фильтра категоризации

Операнд	Операторы	Комментарий
Номер сборки	>, >=, =, <=, <	
ОС	=, like	Оператор like обеспечивает регистронезависимый поиск.
IP-адрес	inSubnet, inRange	IP-адрес указывается в нотации CIDR (например: 192.168.0.0/24). При выборе оператора inRange допускается указывать только адреса из частных диапазонов IP-адресов (например: 10.0.0.0-10.255.255.255). Оба адреса должны быть из одного диапазона.
Полное доменной имя	=, like	Оператор like обеспечивает регистронезависимый поиск.
CVE	=, in	Оператор in позволяет указать массив значений.

3. С помощью кнопки **Проверить условия** убедитесь, что указанный фильтр верен: при нажатии на кнопку отображается окно **Активы, найденные по заданным условиям** с перечнем активов, удовлетворяющих условиям поиска.

- **Реактивно** – категория будет наполняться активами с помощью правил корреляции.

5. Нажмите **Сохранить**.

Новая категория добавлена в дерево категорий активов.

Настройка таблицы активов

В KUMA можно настроить содержимое и порядок отображения столбцов в таблице активов. Эти параметры хранятся локально на вашем компьютере.

Чтобы настроить параметры отображения таблицы активов:

1. В правом верхнем углу таблицы активов нажмите значок .

2. В раскрывшемся списке установите флажки напротив параметров, которые требуется отображать в таблице:

   - **Полное доменное имя**
   - **IP-адрес**
   - **Источник актива**
   - **Владелец**
   - **MAC-адрес**
   - **Создан**
   - **Последнее обновление**
   - **Тенант**

   Когда вы устанавливаете флажок, таблица активов обновляется и добавляется новый столбец. При снятии флажка столбец исчезает. Таблицу можно сортировать по некоторым столбцам.

3. Если требуется изменить порядок отображения столбцов, зажмите левую клавишу мыши на названии столбца и перетащите его в нужное место таблицы.

Параметры отображения таблицы активов настроены.

Поиск активов

В KUMA есть два режима поиска активов. Переключение между режимами поиска осуществляется с помощью кнопок в верхней левой части окна:

- – простой поиск по параметрам активов **Название**, **Полное доменное имя**, **IP-адрес**, **MAC-адрес** и **Владелец**.
- – сложный поиск активов с помощью фильтрации по условиям и группам условий.

Найденные активы можно выделить, установив напротив них флажки, и экспортировать данные о них в виде CSV-файла.

Простой поиск

Чтобы найти актив:

1. В разделе **Активы** веб-интерфейса KUMA убедитесь, что в верхней левой части окна активна кнопка .

   В верхней части окна отображается поле **Поиск**.

2. Введите поисковый запрос в поле **Поиск** и нажмите **ENTER** или значок .

В таблице отобразятся активы, у которых параметры **Название**, **Полное доменное имя**, **IP-адрес**, **MAC-адрес** и **Владелец** соответствуют критериям поиска.

Сложный поиск

Сложный поиск активов производится с помощью условий фильтрации, которые можно задать в верхней части окна:

- С помощью кнопки **Добавить условие** можно добавить строку с полями для определения условия.
- С помощью кнопки **Добавить группу** можно добавить группу фильтров. Можно переключать групповые операторы между **И**, **ИЛИ**, **НЕ**.
- Условия и группы условий можно перетягивать мышкой.
- Условия, группы и фильтры можно удалить с помощью кнопки .

- Параметры фильтрации можно отобразить в компактно, нажав на кнопку **Свернуть**. В этом случае отображается результирующее поисковое выражение. При нажатии на него условия поиска снова отображаются полностью.

- Параметры фильтрации можно обнулить с помощью кнопки **Очистить**.

- Операторы условий и доступные значения правого операнда зависят от выбранного левого операнда:

Левый операнд	Доступные операторы	Правый операнд
Номер сборки	=, >, >=, <, <=	Произвольное значение.
ОС	=, ilike	Произвольное значение.
IP-адрес	inSubnet, inRange	Произвольное значение или диапазон значений.
Полное доменное имя	=, ilike	Произвольное значение.
CVE	=, in	Произвольное значение.
Источник актива	in	• Kaspersky Security Center • KICS for Networks • Импортирован через API • Создан вручную
ОЗУ	=, >, >=, <, <=	Число.
Количество дисков	=, >, >=, <, <=	Число.
Количество сетевых карт	=, >, >=, <, <=	Число.
Свободных байт на диске	=, >, >=, <, <=	Число.
Последнее обновление антивирусных баз	>=, <=	Дата.
Последнее обновление информации	>=, <=	Дата.

Последнее обновление защиты	>=, <=	Дата.
Время начала последней сессии	>=, <=	Дата.
Расширенный статус KSC	in	• Хост с установленным Агентом администрирования подключен к сети, но Агент администрирования неактивен • Антивирусное приложение установлено, но постоянная защита не работает • Антивирусное приложение установлено, но не запущено • Количество обнаруженных вирусов слишком велико • Антивирусное приложение установлено, но статус постоянной защиты отличается от установленного администратором безопасности • Антивирусное приложение не установлено • Полная проверка на вирусы выполнялась слишком давно • Антивирусные базы обновлялись слишком давно • Агент администрирования слишком долго был неактивен • Устаревшая лицензия • Количество невылеченных объектов слишком велико • Требуется перезагрузка

		• На хосте установлено одно или несколько несовместимых приложений • Хост имеет одну или несколько уязвимостей • Последний поиск обновлений операционной системы на хосте выполнялся слишком давно • Хост не имеет надлежащего статуса шифрования • Параметры мобильного устройства не соответствуют требованиям политики безопасности • Есть необработанные инциденты • Статус хоста был предложен управляемым продуктом • На хосте недостаточно места на диске: возникают ошибки синхронизации или на диске недостаточно места
Статус постоянной защиты	=	• Приостановлена • Запускается • Выполняется (если антивирусное приложение не поддерживает категории состояния Выполняется) • Выполняется с максимальной защитой • Выполняется с максимальным быстродействием • Выполняется с рекомендуемыми параметрами

		• Выполняется с пользовательскими параметрами • Ошибка
Статус шифрования	=	• На хосте нет правил шифрования. • Шифрование выполняется. • Шифрование отменено пользователем. • Во время шифрования произошла ошибка. • Все правила шифрования хоста были выполнены. • Шифрование выполняется, на хосте требуется перезагрузка. • На хосте есть зашифрованные файлы без указанных правил шифрования.
Статус защиты от спама	=	• Неизвестно • Остановлена • Приостановлена • Запускается • Выполняется • Ошибка • Не установлено • Лицензия отсутствует
Статус антивирусной защиты почтовых серверов	=	• Неизвестно • Остановлена

		• Приостановлена • Запускается • Выполняется • Ошибка • Не установлено • Лицензия отсутствует
Статус защиты данных от утечек	=	• Неизвестно • Остановлена • Приостановлена • Запускается • Выполняется • Ошибка • Не установлено • Лицензия отсутствует
Идентификатор расширенного статуса KSC	=	• OK • Критический • Требует внимания
Статус Endpoint Sensor	=	• Неизвестно • Остановлена • Приостановлена • Запускается • Выполняется

		• Ошибка • Не установлено • Лицензия отсутствует
Последнее появление в сети	>=, <=	Дата

Чтобы найти актив:

1. В разделе **Активы** веб-интерфейса KUMA убедитесь, что в верхней левой части окна активна кнопка .

   В верхней части окна отображается блок настройки фильтрации активов.

2. Задайте параметры фильтрации активов и нажмите на кнопку **Поиск**.

В таблице отобразятся активы, которые соответствуют критериям поиска.

Экспорт данных об активах

Данные об активах, отображаемых в таблице активов, можно экспортировать в виде CSV-файла.

Чтобы экспортировать данные об активах:

1. Настройте таблицу активов.

   В файл записываются только данные, указанные в таблице. Порядок отображения столбцов таблицы активов повторяется в экспортированном файле.

2. Найдите нужные активы и выберите их, установив рядом с ними флажки.

   При необходимости вы можете выбрать сразу все активы в таблице, установив флажок в левой части заголовка таблицы активов.

3. Нажмите на кнопку **Экспортировать в CSV**.

Данные об активах будут записаны в файл assets_<дата экспорта>_<время экспорта>.csv. Файл будет скачан в соответствии с параметрами вашего браузера.

Просмотр информации об активе

Чтобы просмотреть информацию об активе, откройте окно информации об активе одним из следующих способов:

- В веб-интерфейсе KUMA выберите раздел **Активы** → выберите категорию с требуемыми активами → выберите актив.
- В веб-интерфейсе KUMA выберите раздел **Алерты** → нажмите на ссылку с требуемым алертом → в разделе **Связанные активы** выберите актив.
- В веб-интерфейсе KUMA выберите раздел **События** → выполните поиск и фильтрацию событий → выберите требуемое событие → нажмите на ссылку в одном из следующих полей: SourceAssetID, DestinationAssetID или DeviceAssetID.

В окне информации об активе может отображаться следующая информация:

- **Название** – имя актива.

  Активы, импортированные в KUMA, сохраняют имена, которые были заданы для них в источнике. Вы можете изменить эти имена в веб-интерфейсе KUMA.

- **Тенант** – название тенанта, которому принадлежит актив.
- **Источник актива** – источник информации об активе. Источников может быть несколько: сведения можно добавить в веб-интерфейсе KUMA или с помощью API, а также импортировать из Kaspersky Security Center, KICS for Networks и отчетов MaxPatrol.

  Добавляя в KUMA сведения об одном и том же активе из нескольких источников, следует учитывать правила слияния данных об активах.

- **Создано** – дата и время добавления актива в KUMA.
- **Последнее обновление** – дата и время изменения информации об активе.
- **Владелец** – владелец актива, если он указан.
- **IP-адрес** – IP-адрес актива (если есть).

  > Если в KUMA есть несколько активов с одинаковыми IP-адресами, актив, добавленный позже, возвращается во всех случаях поиска активов по IP-адресу. Если в сети вашей организации допустимо наличие активов с одинаковыми IP-адресами, разработайте и используйте дополнительные атрибуты для идентификации активов. Это может оказаться важным при корреляции.

- **Полное доменное имя** – полностью определенное имя домена актива, если указано.
- **MAC-адрес** – MAC-адрес актива (если есть).

- **Операционная система** – операционная система актива.

- **Связанные алерты** – алерты, с которыми связан актив (если есть).

  Для просмотра списка алертов, с которыми связан актив, можно перейти по ссылке **Найти в алертах**. Откроется закладка **Алерты** с поисковым выражением, позволяющим отфильтровать все активы с соответствующим идентификатором.

- **Информация о программном обеспечении** и **Информация об оборудовании** – если указаны параметры программного обеспечения и оборудования актива, они отображаются в этом разделе.

- Сведения об уязвимостях актива:

  - **Уязвимости Kaspersky Security Center** – уязвимости актива, если есть. Эта информация доступна для активов, импортированных из Kaspersky Security Center.

    Вы можете узнать больше об уязвимости, нажав на значок , открывающий портал Kaspersky Threats. Вы также можете обновить список уязвимостей, нажав на ссылку **Обновить** и запросив обновленную информацию из Kaspersky Security Center.

  - **Уязвимости KICS for Networks** – уязвимости актива, если есть. Эта информация доступна для активов, импортированных из KICS for Networks.

- Сведения об источниках актива:

  - **Последнее появление в сети** – время последнего получения сведений об активе из Kaspersky Security Center. Эта информация доступна для активов, импортированных из Kaspersky Security Center.

  - **Идентификатор хоста** – идентификатор *агента администрирования* Kaspersky Security Center, от которого получены сведения об активе. Эта информация доступна для активов, импортированных из Kaspersky Security Center. С помощью этого идентификатора определяется уникальность актива в Kaspersky Security Center.

  - **IP-адрес сервера KICS for Networks** и **Идентификатор коннектора KICS for Networks** – данные об экземпляре KICS for Networks, из которого был импортирован актив.

- **Настраиваемые поля** – данные, записанные в настраиваемые поля активов.

- Дополнительные сведения о параметрах защиты актива с установленной программой Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux:

  - **Идентификатор расширенного статуса KSC** – статус актива. Может иметь следующие значения:

    - OK.

    - Критическое.
    - Предупреждение.
  - **Расширенный статус KSC** – информация о состоянии актива. Например, "Антивирусные базы обновлялись слишком давно".
  - **Статус постоянной защиты** – статус программ "Лаборатории Касперского", установленных на активе. Например, "Выполняется (если антивирусное приложение не поддерживает категории состояния Выполняется)".
  - **Статус шифрования** – информация о шифровании актива. Например, "На хосте нет правил шифрования".
  - **Статус защиты от спама** – состояние защиты от спама. Например, "Запущена".
  - **Статус антивирусной защиты почтовых серверов** – состояние антивирусной защиты почтовых серверов. Например, "Запущена".
  - **Статус защиты данных от утечек** – состояние защиты данных от утечек. Например, "Запущена".
  - **Статус Endpoint Sensor** – состояние защиты данных от утечек. Например, "Запущена".
  - **Последнее обновление антивирусных баз** – версия загруженных антивирусных баз.
  - **Последнее обновление защиты** – время последнего обновления антивирусных баз.
  - **Время начала последней сессии** – время последнего запуска системы.

  Эти сведения отображаются, если актив был импортирован из Kaspersky Security Center.

- **Категории** – категории, к которым относится актив (если есть).
- **КИИ категория** – сведения о том, является ли актив объектом критической информационной инфраструктуры (КИИ).

По кнопке **Реагирование KSC** вы можете запустить на активе выполнение задачи Kaspersky Security Center, а по кнопке **Переместить в группу KSC** переместить просматриваемый актив между группами администрирования Kaspersky Security Center.

> Доступно при интеграции с Kaspersky Security Center.

Добавление активов

Вы можете добавлять информацию об активах следующими способами:

- Вручную.

  Вы можете добавить актив в веб-интерфейсе KUMA или с помощью API.

- Импортировать активы.

  Вы можете импортировать активы из Kaspersky Security Center, KICS for Networks и отчетов MaxPatrol.

При добавлении активы, уже существующие в KUMA, могут объединяться с добавляемыми активами.

Алгоритм объединения активов:

1. Проверка на уникальность активов в Kaspersky Security Center или KICS for Networks активов:

   - Уникальность актива импортированного из Kaspersky Security Center, проверяется по параметру **Идентификатор хоста**, в котором указан идентификатор *агента администрирования* Kaspersky Security Center. Если идентификаторы у двух активов различаются, активы считаются разными, объединения данных не происходит.

   - Уникальность актива импортированного из KICS for Networks, определяется по комбинации параметров **IP-адрес**, **IP-адрес сервера KICS for Networks** и **Идентификатор коннектора KICS for Networks**. Если любой из параметров у двух активов различается, активы считаются разными, объединения данных не происходит.

   Если активы совпадают, алгоритм выполняется далее.

2. Проверка на совпадение значений в полях **IP**, **MAC**, **FQDN**.

   Если хотя бы два из указанных полей совпадают, активы объединяются при условии, что другие поля не заполнены.

   Возможные варианты совпадений:

   - FQDN и IP-адрес активов. Поле **MAC** не заполнено.

     Проверка производится по всему массиву значений IP-адресов. Если IP-адрес актива входит в состав FQDN, значения считаются совпавшими.

   - FQDN и MAC-адрес активов. Поле **IP** не заполнено.

     Проверка производится по всему массиву значений MAC-адресов. При полном совпадении хотя бы одного значения массива с FQDN значения считаются совпавшими.

   - IP-адрес и MAC-адрес активов. Поле **FQDN** не заполнено.

Проверка производится по всему массиву значений IP- и MAC-адресов. При полном совпадении хотя бы одного значения в массивах значения считаются совпавшими.

3. Проверка на совпадение хотя бы одного из полей **IP**, **MAC**, **FQDN** при условии, что два других поля не заполнены для одного или обоих активов.

   Активы объединяются, если значения в поле совпадают. Например, если для актива KUMA указаны FQDN и IP-адрес, а для импортируемого актива только IP-адрес с тем же значением, поля считаются совпавшими. В этом случае активы объединяются.

   Для каждого поля проверка производится отдельно и завершается при первом совпадении.

Вы можете посмотреть примеры сравнения полей активов здесь.

Информация об активах может формироваться из разных источников. Если добавляемый актив и актив KUMA содержат данные, полученные из одного и того же источника, эти данные перезаписываются. Например, актив Kaspersky Security Center при импорте в KUMA получил полное доменное имя и информацию о программном обеспечении. При импорте актива из Kaspersky Security Center с аналогичным полным доменным именем эти данные будут перезаписаны при условии, что они указаны для добавляемого актива. Все поля, в которых могут обновляться данные, приведены в таблице Обновляемые данные.

Обновляемые данные

Название поля	Принцип обновления
Название	Выбирается согласно следующему приоритету: • Задано вручную. • Получено из Kaspersky Security Center. • Получено KICS for Networks.
Владелец	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Задано вручную.

IP-адрес	Данные объединяются. Если в массиве адресов есть одинаковые адреса, копия дублирующегося адреса удаляется.
Полное доменное имя	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Получено KICS for Networks. • Задано вручную.
MAC-адрес	Данные объединяются. Если в массиве адресов есть одинаковые адреса, один из дублирующихся адресов удаляется.
Операционная система	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Получено KICS for Networks. • Задано вручную.
Уязвимости	Данные активов KUMA дополняются информацией из добавляемых активов. В информации об активе данные группируются по названию источника. Устранение уязвимостей для каждого источника осуществляется отдельно.
Информация о программном обеспечении	Данные из KICS for Networks записываются всегда (при наличии). Для других источников выбирается первое значение согласно следующему приоритету: • Получено из Kaspersky Security Center. • Задано вручную.
Информация об оборудовании	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center.

- Задано через API.

Обновленные данные отображаются в информации об активе. Вы можете просмотреть информацию об активе в веб-интерфейсе KUMA.

При добавлении новых активов эти данные могут быть перезаписаны. Если данные, из которых сформирована информация об активе, не обновляются из источников более 30 дней, актив удаляется. При следующем добавлении актива из тех же источников создается новый актив.

При редактировании в веб-интерфейсе KUMA активов, информация о которых получена из Kaspersky Security Center или KICS for Networks, вы можете изменить следующие данные актива:

- Название.
- Категория.

Если информация об активе добавлена вручную, при редактировании в веб-интерфейсе KUMA этих активов вы можете изменить следующие данные актива:

- Название.
- Название тенанта, которому принадлежит актив.
- IP-адрес.
- Полное доменное имя.
- MAC-адрес.
- Владелец.
- Категория.
- Операционная система.
- Информация об оборудовании.

Редактирование данных об активах через REST API недоступно. При импорте из REST API происходит обновление данных по правилам слияния информации об активах, приведенным выше.

Добавление информации об активах в веб-интерфейсе KUMA

Чтобы добавить актив в веб-интерфейсе KUMA:

1. В разделе **Активы** веб-интерфейса KUMA нажмите на кнопку **Добавить актив**.

   В правой части окна откроется область деталей **Добавить актив**.

2. Введите параметры актива:

   - **Название актива** (обязательно).
   - **Тенант** (обязательно).
   - **IP-адрес** и/или **Полное доменное имя** (обязательно).
   - **MAC-адрес**.
   - **Владелец**.

3. При необходимости присвойте активу одну или несколько категорий:

   a. Нажмите на кнопку .

   Откроется окно **Выбор категорий**.

   b. Установите флажки рядом с категориями, которые следует присвоить активу. С помощью значков и вы можете разворачивать и сворачивать списки категорий.

   c. Нажмите **Сохранить**.

   Выбранные категории отобразятся в полях **Категории**.

4. При необходимости добавьте в раздел **Программное обеспечение** сведения об операционной системе актива.

5. При необходимости добавьте в раздел **Информация об оборудовании** сведения об оборудовании актива.

6. Нажмите на кнопку **Добавить**.

Актив создан и отображается в таблице активов в назначенной ему категории или в категории **Активы без категории**.

Импорт информации об активах из Kaspersky Security Center

В Kaspersky Security Center зарегистрированы все активы, которые находятся под защитой этой программы. Вы можете импортировать информацию об активах, защищаемых Kaspersky Security Center, в KUMA. Для этого вам требуется предварительно настроить интеграцию между программами.

В KUMA предусмотрены следующие типы импорта активов из KSC:

- Импорт информации обо всех активах всех серверов KSC.
- Импорт информации об активах выбранного сервера KSC.

Чтобы импортировать информацию обо всех активах всех серверов KSC:

1. В веб-интерфейсе KUMA выберите раздел **Активы**.
2. Нажмите на кнопку **Импортировать активы**.

   Откроется окно **Импорт активов из Kaspersky Security Center**.
3. В раскрывающемся списке выберите тенант, для которого вы хотите выполнить импорт.

   В этом случае программа загружает информацию обо всех активах всех серверов KSC, для которых настроено подключение к выбранному тенанту.

   Если вы хотите импортировать информацию обо всех активах всех серверов KSC для всех тенантов, выберите **Все тенанты**.
4. Нажмите на кнопку **OK**.

Информация об активах будет импортирована.

Чтобы импортировать информацию об активах одного сервера KSC:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center по тенантам**.
2. Выберите тенант, для которого вы хотите импортировать активы.

   Откроется окно **Интеграция с Kaspersky Security Center**.
3. Нажмите на подключение для требуемого сервера Kaspersky Security Center.

   Откроется окно с параметрами этого подключения к Kaspersky Security Center.
4. Выполните одно из следующих действий:

   - Если вы хотите импортировать все активы, подключенные к выбранному серверу KSC, нажмите на кнопку **Импортировать активы**.
   - Если вы хотите импортировать только активы, которые подключены к подчиненному серверу или включены в одну из групп (например, группу Нераспределенные устройства), выполните следующие действия:

a. Нажмите на кнопку **Загрузить иерархию**.

b. Установите флажки рядом с именами подчиненных серверов или групп, из которых вы хотите импортировать информацию об активах.

c. Установите флажок **Импортировать активы из новых групп**, если вы хотите импортировать активы из новых групп.

   Если ни один флажок не установлен, при импорте выгружается информация обо всех активах выбранного сервера KSC.

d. Нажмите на кнопку **Сохранить**.

e. Нажмите на кнопку **Импортировать активы**.

Информация об активах будет импортирована.

Импорт информации об активах из MaxPatrol

В KUMA можно импортировать сведения об активах из отчетов о результатах сканирования сетевых устройств с помощью MaxPatrol, системы контроля защищенности и соответствия стандартам. Импорт происходит через API с помощью утилиты maxpatrol-tool на сервере, где установлено Ядро KUMA. Импортированные активы отображаются в веб-интерфейсе KUMA в разделе **Активы**. При необходимости вы можете редактировать параметры активов.

Утилита входит в комплект поставки KUMA и расположена в архиве установщика в директории /kuma-ansible-installer/roles/kuma/files.

Импорт поддерживается из MaxPatrol 8.

Чтобы импортировать данные об активах из отчета MaxPatrol:

1. Сформируйте в MaxPatrol отчет сканирования сетевых активов в формате **XML file** и скопируйте файл отчета на сервер Ядра KUMA. Подробнее о задачах на сканирование и форматах выходных файлов см. в документации MaxPatrol.

   Импорт данных из отчетов в формате **SIEM integration file** не поддерживается. Требуется выбрать формат **XML file**.

2. Создайте файл с токеном для доступа к KUMA REST API. Для удобства рекомендуется разместить его в папке отчета MaxPatrol. Файл не должен содержать ничего, кроме токена.

   Требования к учетным записям, для которых генерируется API-токен:

- Роль Администратора или Аналитика.
- Доступ к тенанту, в который будут импортированы активы.
- Настроены права на использование API-запросов GET /users/whoami и POST /api/v1/assets/import.

> Мы рекомендуем для импорта активов из MaxPatrol создать отдельного пользователя с минимально необходимым набором прав на использование API-запросов.

3. Скопируйте утилиту maxpatrol-tool на сервер с Ядром KUMA и сделайте файл утилиты исполняемым с помощью команды `chmod +x <путь до файла maxpatrol-tool на сервере с Ядром KUMA>`.

4. Запустите утилиту maxpatrol-tool:

   ```
   ./maxpatrol-tool --kuma-rest <адрес и порт сервера KUMA REST API> --token <путь и имя файла с API-токеном> --tenant <название тенанта, куда будут помещены активы> <путь и имя файла с отчетом MaxPatrol> --cert <путь к файлу сертификата Ядра KUMA>
   ```

   Пример: `./maxpatrol-tool --kuma-rest example.kuma.com:7223 --token token.txt --tenant Main example.xml --cert /example-directory/ca.cert`

Вы можете использовать дополнительные флаги и команды для импорта. Например, команду для отображения полного отчета о полученных активах `--verbose, -v`. Подробное описание доступных флагов и команд приведено в таблице Флаги и команды утилиты maxpatrol-tool. Также для просмотра информации о доступных флагах и командах вы можете использовать команду --help.

Информация об активах будет импортирована из отчета MaxPatrol в KUMA. В консоли отображаются сведения о количестве новых и обновленных активов.

> Пример:
>
> inserted 2 assets;
>
> updated 1 assets;
>
> errors occured: []

Поведение утилиты при импорте активов:

- Данные импортированных в KUMA через API активов перезаписываются, а сведения об их устраненных уязвимостях удаляются.

- Активы с недействительными данными пропускаются. Сведения об ошибках отображаются при использовании флага `--verbose`.

- Если в одном отчете MaxPatrol есть активы с одинаковыми IP-адресами и полными именами домена (FQDN), эти активы объединяются. Сведения об их уязвимостях и программном обеспечении также объединяются в одном активе.

  При загрузке активов из MaxPatrol активы с аналогичными IP-адресами и полными именами доменов (FQDN), ранее импортированные из Kaspersky Security Center, перезаписываются.

  Чтобы этого избежать, вам требуется настроить фильтрацию активов по диапазону с помощью команды `--ignore <диапазоны IP-адресов> или -i <диапазоны IP-адресов>`. Активы, соответствующие условиям фильтрации, не загружаются. Описание команды вы можете просмотреть в таблице *Флаги и команды утилиты maxpatrol-tool*.

Флаги и команды утилиты maxpatrol-tool

Флаги и команды	Описание
`--kuma-rest <адрес и порт сервера KUMA REST API>, -a <адрес и порт сервера KUMA REST API>`	Адрес сервера с Ядром KUMA, куда будет производиться импорт активов, с указанием порта. Например, `example.kuma.com:7223`. По умолчанию для обращения по API используется порт 7223. При необходимости его можно изменить.
`--token <путь и имя файла с API-токеном>, -t <путь и имя файла с API-токеном>`	Путь и имя файла, содержащее токен для доступа к REST API. Файл должен содержать только токен. Учетной записи, для которой генерируется API-токен, должна быть присвоена роль Администратора или Аналитика.
`--tenant <название тенанта>, -T <название тенанта>`	Название тенанта KUMA, в который будут импортированы активы из отчета MaxPatrol.
`--dns <диапазоны IP-адресов> или -d <диапазоны IP-адресов>`	Используется для обогащения IP-адресов FQDN из указанных диапазонов с помощью DNS, если для этих адресов FQDN не был указан.

	Пример: `--dns 0.0.0.0-9.255.255.255,11.0.0.0-255.255.255,10.0.0.2`
`--dns-server <IP-адрес DNS-сервера>, -s <IP-адрес DNS-сервера>`	Адрес DNS-сервера, к которому должна обращаться утилита для получения информации о FQDN. Пример: `--dns-server 8.8.8.8`
`--ignore <диапазоны IP-адресов> или -i <диапазоны IP-адресов>`	Диапазоны адресов активов, которые при импорте следует пропустить. Пример: `--ignore 8.8.0.0-8.8.255.255, 10.10.0.1`
`--verbose, -v`	Выведение полного отчета о полученных активах и ошибках, возникших в процессе импорта.

`--help, -h`
`help`
	Получение справочной информации об утилите или команде.
	Примеры:
	`./maxpatrol-tool help`
	`./maxpatrol-tool <команда> --help`

`version`	Получение информации о версии утилиты maxpatrol-tool.
`completion`	Создание скрипта автозавершения для указанной оболочки.
`--cert <путь до файла с сертификатом Ядра KUMA>`	Путь к сертификату Ядра KUMA. По умолчанию сертификат располагается в директории с установленной программой: /opt/kaspersky/kuma/core/certificates/ca.cert.

Примеры:

- `./maxpatrol-tool --kuma-rest example.kuma.com:7223 --token token.txt --tenant Main example.xml --cert /example-directory/ca.cert` – импорт активов в KUMA из отчета MaxPatrol example.xml.
- `./maxpatrol-tool help` – получение справки об утилите.

Возможные ошибки

Сообщение об ошибке	Описание

must provide path to xml file to import assets	Не указан путь к файлу отчета MaxPatrol.
incorrect IP address format	Некорректный формат IP-адреса. Может возникнуть при указании некорректных диапазонов IP.
no tenants match specified name	Для указанного названия тенанта не было найдено подходящих тенантов с помощью REST API.
unexpected number of tenants (%v) match specified name. Tenants are: %v	Из KUMA вернулось больше одного тенанта для указанного названия тенанта.
could not parse file due to error: %w	Ошибка чтения xml-файла с отчетом MaxPatrol.
error decoding token: %w	Ошибка чтения файла с API-токеном.
error when importing files to KUMA: %w	Ошибка передачи сведений об активах в KUMA.
skipped asset with no FQDN and IP address	У одного из активов в отчете не было FQDN и IP-адреса. Сведения об этом активе не были отправлены в KUMA.
skipped asset with invalid FQDN: %v	У одного из активов в отчете был некорректный FQDN. Сведения об этом активе не были отправлены в KUMA.
skipped asset with invalid IP address: %v	У одного из активов в отчете был некорректный IP-адрес. Сведения об этом активе не были отправлены в KUMA.
KUMA response: %v	При импорте сведений об активах произошла ошибка с указанным ответом.
unexpected status code %v	При импорте сведений об активах от KUMA был получен неожиданный код HTTP.

Импорт информации об активах из KICS for Networks

После создания интеграции с KICS for Networks задачи на получение данных об активах KICS for Networks создаются автоматически. Это происходит в следующих случаях:

- Сразу после создания новой интеграции.

- Сразу после изменения параметров существующей интеграции.
- Регулярно по расписанию каждые несколько часов. По умолчанию каждые 12 часов. Расписание можно изменить.

Задачи на обновление данных об учетных записях можно создать вручную.

Чтобы запустить задачу на обновление данных об активах KICS for Networks для тенанта:

1. Откройте в веб-интерфейсе KUMA разделе **Параметры** → **Kaspersky Industrial CyberSecurity for Networks**.
2. Выберите требуемый тенант.

   Откроется окно **Интеграция с Kaspersky Industrial CyberSecurity for Networks**.
3. Нажмите на кнопку **Импортировать активы**.

   В разделе **Диспетчер задач** веб-интерфейса KUMA добавлена задача на получение данных об учетных записях выбранного тенанта.

Примеры сравнения полей активов при импорте

Каждый импортируемый актив сравнивается с активом KUMA.

Проверка на совпадение значений в полях IP, MAC, FQDN по двум полям

Сравниваемые активы	Сравниваемые поля		
	FQDN	IP	MAC
Актив KUMA	Есть	Есть	Не заполнено
Импортируемый актив 1	Есть, совпадает	Есть, совпадает	Есть
Импортируемый актив 2	Есть, совпадает	Есть, совпадает	Не заполнено
Импортируемый актив 3	Есть, совпадает	Не заполнено	Есть
Импортируемый актив 4	Не заполнено	Есть, совпадает	Есть
Импортируемый актив 5	Есть, совпадает	Не заполнено	Не заполнено
Импортируемый актив 6	Не заполнено	Не заполнено	Есть

Результаты сравнения:

- Импортируемый актив 1 и актив KUMA: для обоих активов заполнены и совпадают поля FQDN и IP, по полю MAC нет противоречия. Активы будут объединены.

- Импортируемый актив 2 и актив KUMA: для обоих активов заполнены и совпадают поля FQDN и IP. Активы будут объединены.

- Импортируемый актив 3 и актив KUMA: для обоих активов заполнены и совпадают поля FQDN и MAC, по полю IP нет противоречия. Активы будут объединены.

- Импортируемый актив 4 и актив KUMA: для обоих активов заполнено и совпадает поле IP, по полям FQDN и MAC нет противоречия. Активы будут объединены.

- Импортируемый актив 5 и актив KUMA: для обоих активов заполнено и совпадает поле FQDN, по полям IP и MAC нет противоречия. Активы будут объединены.

- Импортируемый актив 6 и актив KUMA: для активов нет ни одного совпадающего поля. Активы не объединяются.

Проверка на совпадение значений в полях IP, MAC, FQDN по одному полю

Сравниваемые активы	**Сравниваемые поля**		
	FQDN	**IP**	**MAC**
Актив KUMA	Не заполнено	Есть	Не заполнено
Импортируемый актив 1	Есть	Есть, совпадает	Есть
Импортируемый актив 2	Есть	Есть, совпадает	Не заполнено
Импортируемый актив 3	Есть	Не заполнено	Есть
Импортируемый актив 4	Не заполнено	Не заполнено	Есть

Результаты сравнения:

- Импортируемый актив 1 и актив KUMA: для обоих активов заполнено и совпадает поле IP, по полям FQDN и MAC нет противоречия. Активы будут объединены.

- Импортируемый актив 2 и актив KUMA: заполнено и совпадает поле IP, по полям FQDN и MAC нет противоречия. Активы будут объединены.

- Импортируемый актив 3 и актив KUMA: для активов нет ни одного совпадающего поля. Активы не объединяются.

- Импортируемый актив 4 и актив KUMA: для активов нет ни одного совпадающего поля. Активы не объединяются.

Назначение активу категории

Чтобы назначить категорию одному активу:

1. В веб-интерфейсе KUMA перейдите в раздел **Активы**.
2. Выберите категорию с требуемыми активами.

   Отобразится таблица активов.
3. Выберите актив.
4. В открывшемся окне нажмите на кнопку **Изменить**.
5. В поле **Категории** нажмите на кнопку .
6. Выберите категорию.

   > Если вы хотите перенести актив в раздел **Активы без категории**, вам требуется удалить существующие для актива категории, нажав на кнопку .

7. Нажмите на кнопку **Сохранить**.

Категория будет назначена.

Чтобы назначить категорию нескольким активам:

1. В веб-интерфейсе KUMA перейдите в раздел **Активы**.
2. Выберите категорию с требуемыми активами.

   Отобразится таблица активов.
3. Установите флажки рядом с активами, для которых вы хотите изменить категорию.
4. Нажмите на кнопку **Привязать к категории**.
5. В открывшемся окне выберите категорию.
6. Нажмите на кнопку **Сохранить**.

Категория будет назначена.

Не назначайте активам категорию `Categorized assets`.

Изменение параметров активов

В KUMA можно изменять параметры активов. У добавленных вручную активов можно изменять все параметры. У активов, импортированных из Kaspersky Security Center, можно изменить только название актива и его категорию.

Чтобы изменить параметры актива:

1. В разделе **Активы** веб-интерфейса KUMA нажмите на актив, который вы хотите изменить.

   В правой части окна откроется область **Информация об активе**.

2. Нажмите на кнопку **Изменить**.

   Откроется окно **Изменить актив**.

3. Внесите необходимые изменения в доступные поля:

   - **Название актива** (обязательно. Это единственное поле, доступное для редактирования у активов, импортированных из Kaspersky Security Center или KICS for Networks.)
   - **IP-адрес** и/или **Полное доменное имя** (обязательно)
   - **MAC-адрес**
   - **Владелец**
   - **Информация о программном обеспечении**:
     - **Название ОС**
     - **Версия ОС**
   - **Информация об оборудовании**:

     Параметры оборудования

     В раздел **Информация об оборудовании** можно добавить сведения об оборудовании актива:

     Доступные поля для описания CPU актива:

     - **Название процессора**

- **Частота процессора**
- **Количество ядер процессора**

  Активу можно добавить процессоры с помощью ссылки **Добавить процессор**.

Доступные поля для описания диска актива:

- **Свободных байт на диске**
- **Объем диска**

  Активу можно добавить диски с помощью ссылки **Добавить диск**.

Доступные поля для описания RAM актива:

- **Частота оперативной памяти**
- **Общий объем ОЗУ**

Доступные поля для описания сетевой карты актива:

- **Название сетевой карты**
- **Производитель сетевой карты**
- **Версия драйвера сетевой карты**

  Активу можно добавить сетевые карты с помощью ссылки **Добавить сетевую карту**.

- Настраиваемые поля.
- Категория КИИ.

4. Назначьте или измените активу категорию:

   a. Нажмите на кнопку .

   Откроется окно **Выбор категорий**.

   b. Установите флажки рядом с категориями, которые следует присвоить активу.

   c. Нажмите **Сохранить**.

Выбранные категории отобразятся в полях **Категории**.

Кроме того, можно выбрать актив и перетащить его в нужную категорию. Эта категория будет добавлена в список категорий актива.

Не назначайте активам категорию `Categorized assets`.

5. Нажмите на кнопку **Сохранить**.

Параметры актива изменены.

Удаление активов

В KUMA есть возможность удалять активы.

Чтобы удалить актив:

1. В разделе **Активы** веб-интерфейса KUMA нажмите на актив, которое вы хотите удалить.

   В правой части окна откроется область **Информация об активе**.

2. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения.

3. Нажмите **OK**.

Актив удален.

Импортированные из Kaspersky Security Center активы удаляются автоматически, если информация о них не обновлялась в течение 30 дней. Обновление актива может не происходить как из-за отсутствия данных о нем в Kaspersky Security Center, так и из-за отключения KUMA от сервера Kaspersky Security Center. Если после удаления актива в KUMA сведения о нем снова поступают из Kaspersky Security Center, актив пересоздается с тем же идентификатором. Если пересоздать автоматически удаленный актив вручную, новый актив будет иметь идентификатор, отличный от идентификатора старого актива.

Обновление программ сторонних производителей и закрытие уязвимостей на активах Kaspersky Security Center

Вы можете обновлять программы сторонних производителей, в том числе программы Microsoft, установленные на активах Kaspersky Security Center, и закрывать уязвимости этих программ.

Предварительно вам нужно создать задачу *Установка требуемых обновлений и закрытие уязвимостей* на выбранном сервере Администрирования Kaspersky Security Center со следующими параметрами:

- Программа – Kaspersky Security Center.
- Тип задачи – *Установка требуемых обновлений и закрытие уязвимостей*.
- Устройства, которым будет назначена задача – вам требуется назначить задачу корневой группе администрирования.
- Правила для установки обновлений:
  - Устанавливать только утвержденные обновления.
  - Закрывать уязвимости с уровнем критичности равным или выше (необязательный параметр).

    Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (*Средний*, *Высокий* или *Предельный*). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.
- Запуск по расписанию – расписание, в соответствии с которым выполняется задача.

О способах создания задачи см. подробнее в *справке Kaspersky Security Center*.

> Задача *Установка требуемых обновлений и закрытие уязвимостей* доступна при наличии лицензии на Системное администрирование.

Далее вам требуется установить обновления для программ сторонних производителей и закрыть уязвимости на активах в KUMA.

Чтобы установить обновления и закрыть уязвимости программ сторонних производителей на активе в KUMA:

1. Откройте окно информации об активе одним из следующих способов:
   - В веб-интерфейсе KUMA выберите раздел **Активы** → выберите категорию с требуемыми активами → выберите актив.

- В веб-интерфейсе KUMA выберите раздел **Алерты** → нажмите на ссылку с требуемым алертом → в разделе **Связанные активы** выберите актив.

- В веб-интерфейсе KUMA выберите раздел **События** → выполните поиск и фильтрацию событий → выберите требуемое событие → нажмите на ссылку в одном из следующих полей: SourceAssetID, DestinationAssetID или DeviceAssetID.

2. В окне информации об активе раскройте список **Уязвимости Kaspersky Security Center**.

3. Установите флажки рядом с программами, которые вы хотите обновить.

4. Нажмите на ссылку **Загрузить обновления**.

5. В открывшемся окне установите флажок рядом с идентификатором уязвимости, которую вы хотите закрыть.

6. Если в столбце **Лицензионное соглашение принято** для выбранного идентификатора отображается **Нет**, нажмите на кнопку **Принять обновления**.

7. Перейдите по ссылке в столбце **URL Лицензионного соглашения** и ознакомьтесь с текстом Лицензионного соглашения.

8. Если вы с ним согласны, в веб-интерфейсе KUMA нажмите на кнопку **Принять Лицензионные соглашения**.

   Напротив идентификатора уязвимости, для которого было принято Лицензионное соглашение, в столбце **Лицензионные соглашения приняты** отобразится **Да**.

9. Повторите шаги 7–10 для каждого требуемого идентификатора уязвимости.

10. Нажмите на кнопку **OK**.

Обновления будут загружены и установлены на активы, того сервера Администрирования, где была запущена задача, а также на активы всех подчиненные серверы Администрирования.

> Условия Лицензионного соглашения для обновления и закрытия уязвимостей требуется принять на каждом подчиненном сервере Администрирования отдельно.

Обновления устанавливаются на активы, на которых была обнаружена уязвимость.

Вы можете обновить список уязвимостей для актива в окне информации об активе, нажав на ссылку **Обновить**.

Перемещение активов в выбранную группу администрирования

Вы можете перемещать активы в выбранную группу администрирования Kaspersky Security Center. В этом случае на активы будут распространятся групповые политики и задачи. Подробнее о политиках и задачах Kaspersky Security Center см. *справку Kaspersky Security Center*.

Группы администрирования добавляются в KUMA при загрузке иерархии во время импорта активов из Kaspersky Security Center. Предварительно вам требуется настроить интеграцию KUMA с Kaspersky Security Center.

Чтобы переместить один актив в выбранную группу администрирования:

1. Откройте окно информации об активе одним из следующих способов:

   - В веб-интерфейсе KUMA выберите раздел **Активы** → выберите категорию с требуемыми активами → выберите актив.

   - В веб-интерфейсе KUMA выберите раздел **Алерты** → нажмите на ссылку с требуемым алертом → в разделе **Связанные активы** выберите актив.

   - В веб-интерфейсе KUMA выберите раздел **События** → выполните поиск и фильтрацию событий → выберите требуемое событие → нажмите на ссылку в поле DeviceExternalID.

2. В окне информации об активе нажмите на кнопку **Переместить в группу KSC**.

3. Нажмите на кнопку **Переместить в группу KSC**.

4. В открывшемся окне выберите группу.

   > Выбранная группа должна принадлежать тому же тенанту, которому принадлежит актив.

5. Нажмите на кнопку **Сохранить**.

Выбранный актив будет перемещен.

Чтобы переместить несколько активов в выбранную группу администрирования:

1. В веб-интерфейсе KUMA выберите раздел **Активы**.

2. Выберите категорию с требуемыми активами.

3. Установите флажки рядом с активами, которые хотите переместить в группу.

4. Нажмите на кнопку **Переместить в группу KSC**.

> Кнопка активна, если все выбранные активы принадлежат одному серверу Администрирования.

5. В открывшемся окне выберите группу.

6. Нажмите на кнопку **Сохранить**.

Выбранные активы будут перемещены.

Вы можете посмотреть, к какой группе принадлежит актив, в информации об активе.

> Сведения об активах Kaspersky Security Center обновляются в KUMA в момент импорта информации об активах из Kaspersky Security Center. Это означает, что может возникнуть ситуация, когда в Kaspersky Security Center активы были перемещены между группами администрирования, однако в KUMA эти сведения еще не отображаются. При попытке переместить такой актив в группу администрирования, в которой он уже находится, KUMA возвращает ошибку **Не удалось переместить активы в другую группу KSC**.

Аудит активов

В KUMA можно настроить создание событий аудита активов при следующих условиях:

- Актив добавлен в KUMA. Отслеживается создание актива вручную, а также создание при импорте через REST API, импорте из Kaspersky Security Center или KICS for Networks.
- Параметры актива изменены. Отслеживается изменение значение следующих полей актива:
  - Name
  - IP address
  - Mac Address
  - FQDN

- Operating system

Изменения полей может происходить при обновлении актива во время импорта.

- Актив удален из KUMA. Отслеживается удаление активов вручную, а также автоматическое удаление активов, импортированных из Kaspersky Security Center и KICS for Networks, данные о которых перестали поступать.

- Сведения об уязвимости добавлены в актив. Отслеживается появление у активов новых данных об уязвимостях. Сведения об уязвимостях могут быть добавлены в актив, например, при импорте активов из Kaspersky Security Center или KICS for Networks.

- Уязвимость актива закрыта. Отслеживается удаление из актива сведений об уязвимости. Уязвимость считается закрытой, если данные о ней перестают поступать из всех источников, из которых ранее были получены сведения о ее появлении.

- Актив добавлен в категорию. Отслеживается присвоении активу категории активов.

- Актив удален из категории. Отслеживается удаление актива из категории активов.

События аудита активов можно отправлять, например, на хранение или в корреляторы.

Настройка аудита активов

Чтобы настроить аудит активов:

1. Откройте раздел **Параметры** → **Аудит активов** веб-интерфейса KUMA.

2. Выполните одно из действий с тенантом, для которого вы хотите настроить аудит активов:

   - Добавьте тенант с помощью кнопки **Добавить тенант**, если аудит активов для требуемого тенанта настраивается впервые.

     В открывшемся окне **Аудит активов** выберите имя для нового тенанта.

   - Выберите существующий тенант в таблице, если аудит активов для требуемого тенанта уже был настроен.

     В открывшемся окне **Аудит активов** имя тенанта уже задано и редактировать его нельзя.

   - Клонируйте настройки существующего тенанта, чтобы создать копию конфигурации условий для тенанта, для которого вы хотите настроить аудит активов впервые. Для этого установите флажок напротив тенанта, конфигурацию которого требуется копировать, и нажмите **Клонировать**. В открывшемся окне **Аудит активов** выберите имя тенанта, в котором будет использована конфигурация исходного тенанта.

3. Выберите для каждого условия создания событий аудита активов, куда будут отправляться создаваемые события:

   a. В блоке параметров нужного типа событий аудита активов в раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, куда следует отправлять создаваемые события:

      - Выберите **Хранилище**, если хотите, чтобы события отправлялись в хранилище.
      - Выберите **Коррелятор**, если хотите, чтобы события отправлялись в коррелятор.
      - Выберите **Другое**, если хотите выбрать иную точку назначения.

      > К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях программы.

      Откроется окно **Добавить точку назначения**, где вам требуется параметры пересылки событий.

   b. В раскрывающемся списке **Точка назначения** выберите существующую точку назначения или выберите пункт **Создать**, если хотите создать новую точку назначения.

      При создании новой точки назначения заполните параметры, как указано в описании ресурса точки назначения.

   c. Нажмите **Сохранить**.

   Точка назначения добавлена к условию создания событий аудита активов. Для каждого условия можно добавить несколько точек назначения. Вы также можете выключить уже настроенное условие создания событий аудита активов, для этого нажмите на флажок **Выключено** напротив требуемого условия.

4. Нажмите **Сохранить**.

   Аудит активов настроен. События аудита активов будут создаваться для тех условий, для которых были добавлены точки назначения. Вы также можете выключить аудит активов для существующего тенанта. Для этого нажмите на требуемый тенант и установите флажок **Выключено** в верхней части открывшегося окна **Аудит активов**. Нажмите **Сохранить**.

Хранение и поиск событий аудита активов

События аудита активов считаются базовыми и не заменяют собой событий аудита. События аудита активов можно искать по следующим параметрам:

Поле события	Значение
DeviceVendor	`Kaspersky`
DeviceProduct	`KUMA`
DeviceEventCategory	`Audit assets`

Включение и выключение аудита активов

Можно включить или выключить аудит активов для тенанта или для определенного условия в рамках одного тенанта.

Чтобы включить или выключить аудит активов для тенанта:

1. Откройте раздел **Параметры** → **Аудит активов** веб-интерфейса KUMA и выберите тенант, для которого которого вы хотите включить или выключить аудит активов.

   Откроется окно **Аудит активов**.

2. Установите или снимите в верхней части окна флажок **Выключено**.

3. Нажмите **Сохранить**.

Чтобы включить или выключить отдельное условие создания событий аудита активов:

1. Откройте раздел **Параметры** → **Аудит активов** веб-интерфейса KUMA и выберите тенант, для которого которого вы хотите включить или выключить условие создания событий аудита активов.

   Откроется окно **Аудит активов**.

2. Установите или снимите напротив нужных условий флажок **Выключено**.

3. Нажмите **Сохранить**.

Настраиваемые поля активов

В дополнение к существующим полям модели данных актива можно создать настраиваемые поля активов. Данные из настраиваемых полей активов отображаются при просмотре информации об активе. Данные в настраиваемые поля можно записывать вручную или через API.

Вы можете создать или изменить настраиваемые поля в веб-интерфейсе KUMA в разделе **Параметры** → **Активы** в таблице **Настраиваемые поля**. Таблица имеет следующие столбцы:

- **Название** – название настраиваемого поля, которое отображается при просмотре информации об активе.

- **Значение по умолчанию** – значение, которое записывается в настраиваемое поле при добавлении актива в KUMA.

- **Маска** – регулярное выражение, которому должно соответствовать значение, записываемое в поле.

Чтобы создать настраиваемое поле активов:

1. В разделе веб-интерфейса KUMA **Параметры** → **Активы** нажмите на кнопку **Добавить поле**.

   В таблице **Настраиваемые поля** добавится пустая строка. Вы можете добавить сразу несколько строк с параметрами настраиваемого поля.

2. Заполните столбцы с параметрами настраиваемого поля: **Название** (обязательно), **Значение по умолчанию**, **Маска**.

   Допускается ввести от 1 до 1024 символов Юникода.

3. Нажмите **Сохранить**.

К модели данных активов добавлено настраиваемое поле.

Чтобы удалить или изменить настраиваемое поле активов:

1. Откройте раздел веб-интерфейса KUMA **Параметры** → **Активы**.

2. Сделайте необходимые изменения в таблице **Настраиваемые поля**:

   - Вы можете удалить настраиваемые поля, нажав на значок ✕ напротив строки с параметрами нужного поля. При удалении поля также удаляются записанные в это поле данные для всех активов.

   - Вы можете изменить значения параметров полей. При изменении значения по умолчанию уже записанные в поля активов данные не меняются.

   - Измените порядок отображения полей, перетягивая строки мышью за значок ⣿

3. Нажмите **Сохранить**.

Изменения внесены.

Активы, относящиеся к критический информационной инфраструктуре

В KUMA можно помечать активы, относящиеся к критической информационной инфраструктуре (КИИ) Российской Федерации. Это позволяет ограничивать возможности пользователей KUMA по обращению с алертами и инцидентами, к которым относятся активы, относящиеся к объектам КИИ.

> Присваивать активам КИИ-категорию можно, если в KUMA активна лицензия с модулем GosSOPKA.

Присвоить активу КИИ-категорию могут главные администраторы, а также пользователи, в профиле которых установлен флажок **Доступ к объектам КИИ**. Если ни одно из этих условий не выполнено, для пользователя действуют следующие ограничения:

- Не отображается блок параметров **Категория КИИ** в окнах **Информация об активе** и **Изменить актив**. Невозможно просмотреть или изменить КИИ-категорию актива.
- Не доступны для просмотра алерты и инциденты, к которым относятся активы с КИИ категорией. Над такими алертами и инцидентами невозможно производить никакие операции, в таблице алертов и инцидентов они не отображаются.
- Не отображается столбец **КИИ** в таблицах алертов и инцидентов.
- Недоступны операции поиска и закрытия алертов через REST API.

Категория КИИ актива отображается в окне **Информация об активе** в блоке параметров **Категория КИИ.**

Чтобы изменить КИИ-категорию актива:

1. В веб-интерфейсе KUMA в разделе **Активы** выберите нужный актив.

   Откроется окно **Информация об активе**.

2. Нажмите на кнопку **Изменить** и в раскрывающемся списке выберите одно из доступных значений:

   - **Информационный ресурс не является объектом КИИ** – значение по умолчанию, которое означает, что у актива нет категории КИИ. С таким активом, а также с алертами и инцидентами, к которым относится этот актив, могут взаимодействовать пользователи, у которых в профиле не установлен флажок **Доступ к объектам КИИ**.
   - **Объект КИИ без категории значимости**.

- **Объект КИИ третьей категории значимости**.
- **Объект КИИ второй категории значимости**.
- **Объект КИИ первой категории значимости**.

3. Нажмите **Сохранить**.

Управление пользователями

Доступ к KUMA может иметь несколько пользователей. Пользователям присваиваются роли пользователей, которые влияют на задачи, которые пользователи могут выполнять. У разных тенантов у одного и того же пользователя могут быть разные роли.

Вы можете создать или изменить учетные записи пользователя в разделе веб-интерфейса KUMA **Параметры** → **Пользователи**. Пользователи также создаются в программе автоматически, если включена интеграция KUMA с Active directory и пользователь входит в веб-интерфейс KUMA с помощью своей доменной учетной записи в первый раз.

Таблица учетных записей отображается в окне **Пользователи** веб-интерфейса KUMA. Пользователей можно искать с помощью поля **Поиск**. Вы можете отсортировать таблицу по столбцу **Данные о пользователе**, нажав заголовок и выбрав **По возрастанию** или **По убыванию**.

Учетные записи можно создать, изменить или выключить. При изменении учетных записей (как своей, так и чужих) для них можно сгенерировать API-токен.

По умолчанию выключенные учетные записи не отображаются в таблице пользователей, но их можно просмотреть, нажав на столбец **Данные о пользователе** и установив флажок **Выключенные пользователи**.

Чтобы выключить пользователя,

В разделе веб-интерфейса KUMA **Параметры** → **Пользователи** поставьте флажок напротив нужного пользователя и нажмите **Выключить пользователя**.

Роли пользователей

Пользователи KUMA могут иметь следующие роли:

- *Главный администратор* – эта роль предназначена для пользователей, отвечающих за функционирование основных систем KUMA. Например, они устанавливают системные компоненты, выполняют обслуживание, работают с сервисами, создают резервные копии и добавляют пользователей в систему. Эти пользователи имеют полный доступ к KUMA.

- *Администратор* – эта роль предназначена для пользователей, отвечающих за функционирование систем KUMA, принадлежащих определенным тенантам.

- *Аналитик* – эта роль предназначена для пользователей, ответственных за настройку системы KUMA для получения и обработки событий определенного тенанта. Они также создают и настраивают правила корреляции.

- *Аналитик первой линии* – эта роль предназначена для пользователей, ответственных за настройку системы KUMA для получения и обработки событий определенного тенанта. Они также создают и настраивают правила корреляции. Пользователи с этой ролью обладают меньшими правами, чем аналитики.

- *Оператор* – эта роль предназначена для пользователей, которые сталкиваются с непосредственными угрозами безопасности определенного тенанта. Пользователь с ролью оператор посредством REST API видит ресурсы на общем тенанте.

Права пользователей

Раздел веб-интерфейса и действия	Главный администратор	Администратор	Аналитик	Аналитик первой линии	Ог
Отчеты					
Просматривать и изменять шаблоны и отчеты	есть	есть	есть	есть	не
Формировать отчеты	есть	есть	есть	есть	не

Выгружать сформированные отчеты	есть	есть	есть	есть	не
Удалять шаблоны и сформированные отчеты	есть	есть	есть	есть	не
Изменять настройки формирования отчетов	есть	есть	есть	есть	не

Дублировать шаблон отчета	есть	есть	есть	есть	не
Получать сформированный отчет по почте	есть	есть	есть	есть	ес
Панель мониторинга					
Просматривать данные на панели мониторинга и менять макеты	есть	есть	есть	есть	ес
Просматривать универсальный макет	есть	есть	есть	есть	ес
Добавлять макеты	есть	есть	есть	есть	не
Изменять и переименовывать макеты	есть	есть	есть	only own	не

Удалять макеты	есть	есть	есть	only own	не
Включать и выключать режим ТВ	есть	есть	есть	есть	ес
Ресурсы → Сервисы и Ресурсы → Сервисы → Активные сервисы					
Просматривать список активных сервисов	есть	есть	есть	есть	не
Просматривать содержимое активного листа	есть	есть	есть	есть	не

Импортировать/ экспортировать/ очищать содержимое активного листа	есть	есть	есть	есть	не
Создавать набор ресурсов для сервисов	есть	есть	есть	нет	не
Создавать сервис в разделе Ресурсы → Сервисы → Активные сервисы	есть	есть	нет	нет	не
Удалять сервисы	есть	есть	нет	нет	не
Перезапускать сервисы	есть	есть	нет	нет	не
Обновлять параметры сервисов	есть	есть	есть	нет	не
Сбрасывать сертификаты	есть	есть	нет	нет	не
Ресурсы → Ресурсы					
Просматривать список ресурсов	есть	есть	есть	есть	не

Добавлять ресурсы	есть	есть	есть	есть	не
Дублировать ресурсы	есть	есть	есть	есть	не
Изменять ресурсы	есть	есть	есть	есть	не
Создавать/ редактировать/ удалять ресурсы в общем тенанте	есть	нет	нет	нет	не
Удалять ресурсы	есть	есть	есть	есть	не
Импортировать ресурсы	есть	есть	есть	нет	не
Просматривать репозиторий, импортировать ресурсы из репозитория	есть	есть	есть	нет	не
Экспортировать ресурсы	есть	есть	есть	нет	не

Просматривать/ редактировать черновики коллектора или коррелятора	есть	есть	есть	есть	не
Состояние источников → Список источников событий					
Просматривать источники событий	есть	есть	есть	есть	ес
Изменять источники событий	есть	есть	есть	нет	не
Удалять источники событий	есть	есть	есть	нет	не
Состояние источников → Политики мониторинга					
Просматривать политики мониторинга	есть	есть	есть	есть	ес
Создавать политики мониторинга	есть	есть	есть	нет	не
Изменять политики мониторинга	есть	есть	есть	нет	не
Удалять политики мониторинга	есть	есть	есть	нет	не
Активы					

Просматривать активы и категории активов	есть	есть	есть	есть	ес
Добавлять/ редактировать/ удалять категории активов	есть	есть	есть	есть	не
Добавлять категории активов в общем тенанте	есть	нет	нет	нет	не
Привязывать активы к категории активов общего тенанта	есть	есть	есть	есть	не
Добавлять активы	есть	есть	есть	есть	не
Изменять активы	есть	есть	есть	есть	не
Удалять активы	есть	есть	есть	есть	не
Импортировать активы из Kaspersky Security Center	есть	есть	есть	есть	не
Запускать задачи на активах в Kaspersky Security Center	есть	есть	есть	есть	не
Запускать задачи на активах Kaspersky Endpoint Detection and Response	есть	есть	есть	есть	не

Подтверждать обновления для закрытия уязвимостей активов и соглашаться с лицензионными соглашениями	есть	есть	нет	нет	не
Запускать задачи на активах в KEDR	есть	есть	есть	есть	не
Редактирование пользовательских полей активов (Параметры → Активы)	есть	есть	есть	есть	не
Алерты					
Просматривать список алертов	есть	есть	есть	есть	ес
Изменять уровень важности алертов	есть	есть	есть	есть	ес
Открывать детали алертов	есть	есть	есть	есть	ес
Назначать ответственных пользователей	есть	есть	есть	есть	ес
Закрывать алерты	есть	есть	есть	есть	ес
Добавлять комментарий к алертам	есть	есть	есть	есть	ес
Привязывать событие к алертам	есть	есть	есть	есть	ес
Отвязывать событие от алертов	есть	есть	есть	есть	ес

Изменять и удалять чужие фильтры	есть	есть	нет	нет	не
Инциденты					
Просматривать список инцидентов	есть	есть	есть	есть	ес
Создавать пустые инциденты	есть	есть	есть	есть	ес
Создавать вручную инциденты из алертов	есть	есть	есть	есть	ес
Изменять уровень важности инцидентов	есть	есть	есть	есть	ес
Открывать детали инцидентов	есть	есть	есть	есть	ес
Назначать исполнителей	есть	есть	есть	есть	ес
Закрывать инциденты	есть	есть	есть	есть	ес
Добавлять комментарии к инцидентам	есть	есть	есть	есть	ес
Привязывать алерты к инцидентам	есть	есть	есть	есть	ес
Отвязывать алерты от инцидентов	есть	есть	есть	есть	ес
Изменять и удалять чужие фильтры	есть	есть	нет	нет	не

Экспортировать инциденты в НКЦКИ	есть	есть	есть	есть	ес
Отправлять файлы в НКЦКИ	есть	есть	есть	есть	ес
Скачивать файлы, отправленные в НКЦКИ	есть	есть	есть	есть	ес
Экспортировать дополнительные данные инцидентов в НКЦКИ по запросу	есть	есть	есть	есть	ес
Отправка сообщений в НКЦКИ	есть	есть	есть	есть	ес
Просмотр сообщений от НКЦКИ	есть	есть	есть	есть	ес
Просмотр данных инцидента, экспортированного в НКЦКИ	есть	есть	есть	есть	ес
События					
Просматривать список событий	есть	есть	есть	есть	ес

Выполнять поиск событий	есть	есть	есть	есть	ес
Открывать детали событий	есть	есть	есть	есть	ес
Открывать статистику	есть	есть	есть	есть	ес
Провозить ретроспективную проверку	есть	есть	есть	нет	не
Выгружать события в TSV-файл	есть	есть	есть	есть	ес
Изменять и удалять чужие фильтры	есть	есть	нет	нет	не
Запускать ktl-обогащение	есть	есть	есть	есть	не
Запускать задачи на активах Kaspersky Endpoint Detection and Response в деталях событий	есть	есть	есть	есть	не
Создавать пресеты	есть	есть	есть	есть	ес
Удалять пресеты	есть	есть	есть	есть	ес
Просматривать и использовать пресеты	есть	есть	есть	есть	ес
Параметры → Пользователи					
Просматривать список пользователей	есть	нет	нет	нет	не

Добавлять пользователя	есть	нет	нет	нет	не
Изменять пользователя	есть	нет	нет	нет	не
Генерировать токен	есть	есть	есть	есть	ес
Изменять права доступа для токена	есть	есть	нет	нет	не
Просматривать данные своего профиля	есть	есть	есть	есть	ес
Изменять данные своего профиля	есть	есть	есть	есть	ес
Параметры → LDAP-сервер					
Просматривать параметры подключения к LDAP	есть	есть	есть	есть	не
Изменять параметры подключения к LDAP	есть	есть	нет	нет	не
Удалять конфигурацию всего тенанта из параметров	есть	есть	нет	нет	не

Импортировать активы	есть	есть	нет	нет	не
Параметры → Тенанты					
Просматривать список тенантов	есть	нет	нет	нет	не
Добавлять тенантов	есть	нет	нет	нет	не
Изменять тенантов	есть	нет	нет	нет	не
Отключать тенантов	есть	нет	нет	нет	не
Параметры → Доменная аутентификация					
Просматривать параметры подключения к Active directory	есть	нет	нет	нет	не
Изменять параметры подключения к Active directory	есть	нет	нет	нет	не
Добавлять фильтры по ролям для тенантов	есть	нет	нет	нет	не
Запускать задачи в Active directory	есть	есть	есть	нет	не
Параметры → Общие					
Просматривать параметры подключения к SMTP	есть	нет	нет	нет	не

Изменять параметры подключения к SMTP	есть	нет	нет	нет	не
Параметры → Лицензия					
Просматривать список добавленных лицензионных ключей	есть	нет	нет	нет	не
Добавлять лицензионные ключи	есть	нет	нет	нет	не
Удалять лицензионные ключи	есть	нет	нет	нет	не
Параметры → Kaspersky Security Center					
Просматривать список Kaspersky Security Center-серверов, с которыми выполнена интеграция	есть	есть	есть	есть	не
Добавлять подключения к Kaspersky Security Center	есть	есть	нет	нет	не
Удалять подключения к Kaspersky Security Center	есть	есть	нет	нет	не

Удалять конфигурацию всего тенанта из параметров	есть	есть	нет	нет	не
Запускать задачи на импорт активов Kaspersky Security Center	есть	есть	нет	нет	не
Параметры → Kaspersky Industrial CyberSecurity for Networks					
Просматривать список серверов KICS for Networks, с которыми выполнена интеграция	есть	есть	нет	нет	не
Добавлять, изменять параметры интеграции с KICS for Networks	есть	есть	нет	нет	не
Удалznm параметры интеграции с KICS for Networks	есть	есть	нет	нет	не
Запускать задачи на импорт активов из настройки для KICS for Networks	есть	есть	нет	нет	не
Параметры → Kaspersky Automated Security Awareness Platform					
Просматривать параметры интеграции с ASAP	есть	нет	нет	нет	не

Изменять параметры интеграции с ASAP	есть	нет	нет	нет	не
Просматривать сведения из ASAP в окне с данными о пользователе	есть	есть	есть	есть	ес
Назначать пользователям группу обучения ASAP	есть	есть	есть	есть	не
Параметры → Kaspersky Endpoint Detection and Response					
Просматривать параметры подключений	есть	есть	есть	есть	не
Добавлять, редактировать и отключать подключения при влюченном режиме распределенного решения	есть	нет	нет	нет	не
Включать режим распределенного решения	есть	нет	нет	нет	не
Добавлять подключения при выключенном режиме распределенного решения	есть	есть	нет	нет	не
Удалять подключения при выключенном режиме распределенного решения	есть	есть	нет	нет	не

Удалять конфигурацию всего тенанта из параметров	есть	есть	нет	нет	не
Параметры → Kaspersky CyberTrace					
Просматривать параметры интеграции с CyberTrace	есть	нет	нет	нет	не
Изменять параметры интеграции с CyberTrace	есть	нет	нет	нет	не
Параметры → IRP / SOAR					
Просматривать параметры интеграции с IRP / SOAR	есть	нет	нет	нет	не
Изменять параметры интеграции с IRP / SOAR	есть	нет	нет	нет	не
Параметры → Kaspersky Threat Lookup					
Просматривать параметры интеграции с Threat Lookup	есть	нет	нет	нет	не
Изменять параметры интеграции с Threat Lookup	есть	нет	нет	нет	не

Параметры → Алерты					
Просматривать параметры	есть	есть	есть	есть	не
Изменять параметры	есть	есть	есть	нет	не
Удалять конфигурацию всего тенанта из параметров	есть	есть	есть	нет	не
Параметры → Инциденты → Автоматическая привязка алертов к инцидентам					
Просматривать параметры	есть	есть	есть	есть	не
Изменять параметры	есть	нет	нет	нет	не
Параметры → Инциденты → Типы инцидентов					
Просматривать справочник категорий	есть	есть	есть	есть	не
Просматривать карточки категорий	есть	есть	есть	есть	не
Добавлять категории	есть	есть	нет	нет	не
Изменять категории	есть	есть	нет	нет	не
Удалять категории	есть	есть	нет	нет	не
Параметры → НКЦКИ					
Просматривать параметры	есть	нет	нет	нет	не

Изменять параметры	есть	нет	нет	нет	не
Параметры → Иерархия					
Просматривать параметры	есть	нет	нет	нет	не
Изменять параметры	есть	нет	нет	нет	не
Просматривать инциденты дочернего узла	есть	есть	есть	нет	ес
Параметры → Аудит активов					
Создавать, клонировать и редактировать параметры	есть	есть	есть	нет	не
Просматривать параметры	есть	есть	есть	есть	не
Удалять параметры	есть	есть	нет	нет	не
Параметры → Обновление репозитория					
Просматривать параметры	есть	есть	есть	нет	не
Изменять параметры	есть	нет	нет	нет	не
Запуск задачи обновление репозитория вручную	есть	есть	есть	нет	не
Параметры → Активы					

Добавлять, редактировать, удалять поля активов	есть	нет	нет	нет	не
Метрики					
Открывать метрики	есть	нет	нет	нет	не
Диспетчер задач					
Просматривать список своих задач	есть	есть	есть	есть	ес
Завершать свои задачи	есть	есть	есть	есть	ес
Перезапускать свои задачи	есть	есть	есть	есть	ес
Просматривать список всех задач	есть	нет	нет	нет	не
Завершать любые задачи	есть	нет	нет	нет	не
Перезапускать любые задачи	есть	нет	нет	нет	не
CyberTrace					
Открывать раздел	есть	нет	нет	нет	не
Доступ к данным тенантов					

Доступ к тенантам	есть	есть	есть	есть	ес
Общий тенант	есть	есть	есть	есть	ес

Главный тенант	есть	есть	есть	есть	ес

Создание пользователя

Чтобы создать учетную запись пользователя:

1. Откройте раздел веб-интерфейса KUMA **Параметры** → **Пользователи**.

   В правой части раздела **Параметры** отобразится таблица **Пользователи**.

2. Нажмите на кнопку **Добавить пользователя** и задайте параметры, как описано ниже.

   - **Имя** (обязательно) – введите имя пользователя. Длина должна быть от 1 до 128 символов Юникода.

   - **Логин** (обязательно) – 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** (обязательно) – введите уникальный адрес электронной почты пользователя. Адрес электронной почты должен быть действительным.

   - **Новый пароль** (обязательно) – введите пароль для учетной записи пользователя. Требования к паролю:

     - длина от 8 до 128 символов;

     - требуется как минимум один символ в нижнем регистре;

     - требуется как минимум один символ в верхнем регистре;

     - требуется как минимум одна цифра;

    - требуется как минимум один специальный символ: !, @, #, %, ^, &, *.

- **Подтверждение пароля** (обязательно) – повторите пароль.

- **Выключен** – установите этот флажок, если хотите выключить учетную запись пользователя. По умолчанию этот флажок снят.

- В блоке параметров **Тенанты для ролей** с помощью кнопок **Добавить поле** укажите, какие роли и в каких тенантах будет исполнять пользователь. В разных тенантах можно иметь разные роли, в одном тенанте можно иметь только одну роль.

3. Установите или снимите флажки, регулирующие права доступа и возможности пользователя:

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

    - **Скрывать ресурсы из общего тенанта** – установите этот флажок, если не хотите отображать пользователю ресурсы, расположенные в общем тенанте.

    - **Может взаимодействовать с НКЦКИ** – установите этот флажок, если хотите, чтобы пользователь мог экспортировать инциденты в НКЦКИ.

      Установить флажок может только пользователь с ролью главный администратор.

    - **Выключить уведомления о сообщениях от НКЦКИ** – установите этот флажок, если не хотите, чтобы пользователь получал уведомления о сообщениях в инцидентах, экспортированных в НКЦКИ.

    - **Группа главных администраторов** – установите этот флажок, если хотите присвоить пользователю роль главного администратора. Пользователи с ролью главного администратора могут изменять параметры других учетных записей пользователей. По умолчанию этот флажок снят.

    - **Доступ к объектам КИИ** – установите этот флажок, если хотите, чтобы пользователь мог присваивать активам категории КИИ и взаимодействовать с алертами и инцидентами, к которым относятся активы, являющиеся объектами КИИ.

4. Нажмите **Сохранить**.

Учетная запись пользователя создана и отображается в таблице **Пользователи**.

Редактирование пользователя

Чтобы отредактировать пользователя:

1. Откройте раздел веб-интерфейса KUMA **Параметры** → **Пользователи**.

В правой части раздела **Параметры** отобразится таблица **Пользователи**.

2. Выберите нужного пользователя и в открывшейся в правой части области деталей пользователя измените требуемые параметры.

   - **Имя** (обязательно) – измените имя пользователя. Длина должна быть от 1 до 128 символов Юникода.

   - **Логин** (обязательно) – 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** (обязательно) – введите уникальный адрес электронной почты пользователя. Адрес электронной почты должен быть действительным.

   - **Выключен** – установите этот флажок, если хотите выключить учетную запись пользователя. По умолчанию этот флажок снят.

   - В блоке параметров **Тенанты для ролей** с помощью кнопок **Добавить поле** укажите, какие роли и в каких тенантах будет исполнять пользователь. В разных тенантах можно иметь разные роли, в одном тенанте можно иметь только одну роль.

3. Установите или снимите флажки, регулирующие права доступа и возможности пользователя:

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

   - **Скрывать ресурсы из общего тенанта** – установите этот флажок, если не хотите отображать пользователю ресурсы, расположенные в общем тенанте.

   - **Может взаимодействовать с НКЦКИ** – установите этот флажок, если хотите, чтобы пользователь мог экспортировать инциденты в НКЦКИ.

     Установить флажок может только пользователь с ролью главный администратор.

   - **Выключить уведомления о сообщениях от НКЦКИ** – установите этот флажок, если не хотите, чтобы пользователь получал уведомления о сообщениях в инцидентах, экспортированных в НКЦКИ.

   - **Группа главных администраторов** – установите этот флажок, если хотите присвоить пользователю роль главного администратора. Пользователи с ролью главного администратора могут изменять параметры других учетных записей пользователей. По умолчанию этот флажок снят.

   - **Доступ к объектам КИИ** – установите этот флажок, если хотите, чтобы пользователь мог присваивать активам категории КИИ и взаимодействовать с алертами и

инцидентами, к которым относятся активы, являющиеся объектами КИИ.

4. Если требуется изменить пароль, нажмите на кнопку **Изменить пароль** и в открывшемся окне заполните поля, описанные ниже. По завершении нажмите **OK**.

   - **Действующий пароль** (обязательно) – введите действующий пароль своей учетной записи. Поле доступно, если вы меняете пароль своей учетной записи.

   - **Новый пароль** (обязательно) – введите новый пароль для учетной записи пользователя. Требования к паролю:

     - длина от 8 до 128 символов;

     - требуется как минимум один символ в нижнем регистре;

     - требуется как минимум один символ в верхнем регистре;

     - требуется как минимум одна цифра;

     - требуется как минимум один специальный символ: !, @, #, %, ^, &, *.

   - **Подтверждение пароля** (обязательно) – повторите пароль.

5. При необходимости сгенерируйте API-токен с помощью кнопки **Сгенерировать токен**. При нажатии на эту кнопку отображается окно создания токена.

6. При необходимости настройте доступные пользователю операции через REST API с помощью кнопки **Права доступа через API**.

7. Нажмите **Сохранить**.

Учетная запись пользователя изменена.

Редактирование своей учетной записи

Чтобы отредактировать свою учетную запись:

1. Откройте веб-интерфейс KUMA, в левом нижнем углу окна нажмите на имя учетной записи пользователя и в открывшемся меню нажмите на кнопку **Профиль**.

   Откроется окно **Пользователь** с параметрами вашей учетной записи.

2. Измените нужные параметры:

   - **Имя** (обязательно) – введите имя пользователя. Длина должна быть от 1 до 128 символов Юникода.

- **Логин** (обязательно) – 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 (обязательно) – введите уникальный адрес электронной почты пользователя. Адрес электронной почты должен быть действительным.

3. Установите или снимите флажки, регулирующие права доступа и возможности пользователя:

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

   - **Скрывать ресурсы из общего тенанта** – установите этот флажок, если не хотите отображать пользователю ресурсы, расположенные в общем тенанте.

   - **Выключить уведомления о сообщениях от НКЦКИ** – установите этот флажок, если не хотите, чтобы пользователь получал уведомления о сообщениях в инцидентах, экспортированных в НКЦКИ.

   - **Отображать непечатаемые символы** – установите этот флажок, если хотите, чтобы в веб-интерфейсе KUMA отображались непечатаемые символы: пробелы, знаки табуляции, перенос на новую строку.

     Пробелы и знаки табуляции отображаются во всех полях ввода, кроме **Описание**, в ресурсах нормализаторов, правил корреляции, фильтров и коннекторов, а также в SQL-запросах на поиск событий в разделе **События**.

     Пробелы отображаются в виде точек.

     Знак табуляции отображается в виде тире в ресурсах нормализаторов, правил корреляции, фильтров и коннекторов. В других полях знак табуляции отображается в виде одной или двух точек.

     Символ переноса на новую строку отображается во всех полях ввода, поддерживающих многострочный ввод. Например, в строке поиска событий.

     Если флажок **Отображать непечатаемые символы** установлен, отображение непечатаемых символов можно включать и выключать, нажимая клавиши **`Ctrl/Command+*`**.

4. Если требуется изменить пароль, нажмите на кнопку **Изменить пароль** и в открывшемся окне заполните поля, описанные ниже. По завершении нажмите **OK**.

   - **Действующий пароль** (обязательно) – введите действующий пароль своей учетной записи.

   - **Новый пароль** (обязательно) – введите новый пароль своей учетной записи пользователя. Требования к паролю:

    - длина от 8 до 128 символов;
    - требуется как минимум один символ в нижнем регистре;
    - требуется как минимум один символ в верхнем регистре;
    - требуется как минимум одна цифра;
    - требуется как минимум один специальный символ: !, @, #, %, ^, &, *.
  - **Подтверждение пароля** (обязательно) – повторите пароль.

5. При необходимости сгенерируйте API-токен с помощью кнопки **Сгенерировать токен**. При нажатии на эту кнопку отображается окно создания токена.
6. При необходимости настройте доступные операции через REST API с помощью кнопки **Права доступа через API**.
7. Нажмите **Сохранить**.

Ваша учетная запись отредактирована.

Управление KUMA

В этом разделе описываются общие параметры KUMA.

Вход в веб-интерфейс программы

Чтобы войти в веб-интерфейс программы:

1. В браузере введите следующий адрес:

   ```
   https://<IP-адрес или FQDN сервера Ядра KUMA>:7220
   ```

   Откроется страница авторизации веб-интерфейса с запросом на ввод логина и пароля учетной записи.
2. В поле **Логин** введите логин учетной записи.
3. В поле **Пароль** введите пароль указанной учетной записи.
4. Нажмите на кнопку **Логин**.

Откроется главное окно веб-интерфейса программы.

В режиме мультитенантности при первом входе в веб-интерфейс программы пользователю отображаются данные только для тех тенантов, которые были выбраны для него при создании его учетной записи.

Чтобы выйти из веб-интерфейса программы,

откройте веб-интерфейс KUMA, в левом нижнем углу окна нажмите на имя учетной записи пользователя и в открывшемся меню учетной записи нажмите на кнопку **Выход**.

Просмотр метрик KUMA

Полная информация о рабочих характеристиках Ядра, коллекторов, корреляторов и хранилищ KUMA доступна в разделе **Метрики** веб-интерфейса KUMA. При выборе этого раздела открывается автоматически обновляемый портал Grafana, развернутый во время установки Ядра KUMA. Если в разделе **Метрики** вы видите core:<номер порта>, это означает, что KUMA развернута в отказоустойчивой конфигурации и метрики получены с хоста, на котором было установлено Ядро. В прочих конфигурациях отображается имя хоста, с которого KUMA получает метрики.

Чтобы определить, на каком хосте работает Ядро, в терминале одного из контроллеров выполните следующую команду:

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

Логин и пароль Grafana по умолчанию: `admin` и `admin`.

Доступные показатели метрик

Показатели коллекторов:

- IO (Ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.
  - Processing EPS (Обрабатываемые события в секунду) – количество обрабатываемых событий в секунду.
  - Processing Latency (Время обработки события) – время, необходимое для обработки одного события (отображается медиана).

    - Output EPS (Вывод событий) – количество событий, отправляемых в точку назначения за секунду.
    - Output Latency (Задержка вывода) – время, необходимое для отправки пакета событий в пункт назначения и получения от него ответа (отображается медиана).
    - Output Errors (Ошибки вывода) – количество ошибок при отправке пакетов событий в пункт назначения в секунду. Сетевые ошибки и ошибки записи в дисковый буфер отображаются отдельно.
    - Output Event Loss (Потеря событий) – количество потерянных событий в секунду. События могут быть потеряны из-за сетевых ошибок или ошибок записи в дисковый буфер. События также теряются, если место назначения ответило кодом ошибки (например, если запрос был недействительным).
- Normalization (Нормализация) – показатели, относящиеся к нормализаторам.
    - Raw & Normalized event size (Размер сырых и нормализованных событий) – размер необработанного события и размер нормализованного события (отображается медиана).
    - Errors (Ошибки) – количество ошибок нормализации в секунду.
- Filtration (Фильтрация) – показатели, относящиеся к фильтрам.
    - EPS (События, обрабатываемые в секунду) – количество событий, отклоняемых Коллектором за секунду. Коллектор отклоняет события только в том случае, если пользователь добавил ресурс фильтра 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. Этот показатель помогает определить эффективность правил агрегации.
    - Buckets (Контейнеры) – количество контейнеров в правиле агрегации.
- Enrichment (Обогащение) – показатели, относящиеся к правилам обогащения.
    - Cache RPS (Запросы к кешу в секунду) – количество запросов к локальному кешу в секунду.
    - Source RPS (Запросы к источнику в секунду) – количество запросов к источнику обогащения (например, к словарю).

    - Source Latency (Задержка источника) – время, необходимое для отправки запроса к источнику обогащения и получения 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 запроса источника обогащения в секунду.

Показатели корреляторов

- IO (Ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.
    - Processing EPS (Обрабатываемые события в секунду) – количество обрабатываемых событий в секунду.
    - Processing Latency (Время обработки события) – время, необходимое для обработки одного события (отображается медиана).
    - Output EPS (Вывод событий) – количество событий, отправляемых в точку назначения за секунду.
    - Output Latency (Задержка вывода) – время, необходимое для отправки пакета событий в пункт назначения и получения от него ответа (отображается медиана).
    - Output Errors (Ошибки вывода) – количество ошибок при отправке пакетов событий в пункт назначения в секунду. Сетевые ошибки и ошибки записи в дисковый буфер отображаются отдельно.
    - Output Event Loss (Потеря событий) – количество потерянных событий в секунду. События могут быть потеряны из-за сетевых ошибок или ошибок записи в дисковый буфер. События также теряются, если место назначения ответило кодом ошибки (например, если запрос был недействительным).
- Correlation (Корреляция) – показатели, относящиеся к правилам корреляции.
    - EPS (События, обрабатываемые в секунду) – количество корреляционных событий, создаваемых за секунду.
    - Buckets (Контейнеры) – количество контейнеров в правиле корреляции (только для правил корреляции стандартного типа).
- Active Lists (Активные листы) – показатели, относящиеся к активным листам.
    - RPS (Запросы в секунду) – количество запросов (и их тип) к активному листу в секунду.
    - Records (Записи) – количество записей в активном листе.

    - WAL Size (Размер журнала Write-Ahead-Log) – размер журнала упреждающей записи. Эта метрика помогает определить размер активного листа.

Показатели хранилища

- IO (Ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.
    - RPS (Запросы в секунду) – количество запросов к Хранилищу в секунду.
    - Latency (Задержка) – время проксирования одного запроса к узлу ClickHouse (отображается медиана).

Показатели Ядра

- IO (Ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.
    - RPS (Запросы в секунду) – количество запросов к Ядру в секунду.
    - Latency (Задержка) – время обработки одного запроса (отображается медиана).
    - Errors (Ошибки) – количество ошибок запросов в секунду.
- Notification Feed (Фид уведомлений) – показатели, относящиеся к активности пользователей.
    - Subscriptions (Подписки) – количество клиентов, подключенных к Ядру через SSE для получения сообщений сервера в реальном времени. Это число обычно коррелирует с количеством клиентов, использующих веб-интерфейс KUMA.
    - Errors (Ошибки) – количество ошибок отправки сообщений в секунду.
- Schedulers (Планировщики) – показатели, относящиеся к задачам Ядра.
    - Active (Активные) – количество повторяющихся активных системных задач. Задачи, созданные пользователем, игнорируются.
    - Latency (Задержка) – время обработки одного запроса (отображается медиана).
    - Position (Позиция) – позиция (отметка времени) задачи создания алерта. Следующее сканирование ClickHouse на предмет корреляционных событий начнется с этой позиции.
    - Errors (Ошибки) – количество ошибок задач в секунду.

Метрики, общие для всех сервисов

- Process (Процесс) – общие метрики процесса.

    - CPU (ЦП) – загрузка ЦП.
    - Memory (Память) – использование RAM (RSS).
    - DISK IOPS (Операции чтения/записи диска) – количество операций чтения / записи на диск в секунду.
    - DISK BPS (Считанные/записанные байты диска) – количество байтов, считываемых / записываемых на диск в секунду.
    - Network BPS (Байты, принятые/переданные по сети) – количество байтов, полученных / отправленных в секунду.
    - Network Packet Loss (Потеря пакетов) – количество сетевых пакетов, потерянных в секунду.
    - GC Latency (Задержка сборщика мусора) – время цикла сборщика мусора GO (Garbage Collector), отображается медиана.
    - Goroutines (Гоурутины) – количество активных гоурутин. Это число отличается от количества потоков.
- OS (ОС) – показатели, относящиеся к операционной системе.
    - Load (Нагрузка) – средняя нагрузка.
    - CPU (ЦП) – загрузка ЦП.
    - Memory (Память) – использование RAM (RSS).
    - Disk (Диск) – использование дискового пространства.

Срок хранения метрик

По умолчанию данные о работе KUMA хранятся 3 месяца. Этот срок можно изменить.

Чтобы изменить срок хранения метрик KUMA:

1. Войдите в ОС сервера, на котором установлено Ядро KUMA.
2. В файле /etc/systemd/system/multi-user.target.wants/kuma-victoria-metrics.service в параметре ExecStart измените флаг `--retentionPeriod=<срок хранения метрик в месяцах>`, подставив нужный срок. Например, `--retentionPeriod=4` означает, что метрики будут храниться 4 месяца.

3. Перезапустите KUMA, выполнив последовательно следующие команды:

   a. systemctl daemon-reload

   b. systemctl restart kuma-victoria-metrics

Срок хранения метрик изменен.

Работа с задачами KUMA

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 KUMA в TSV-файл.

Просмотр таблицы задач

Таблица задач содержит список созданных задач и находится в разделе **Диспетчер задач** окна веб-интерфейса программы. Вы можете просматривать задачи, созданные вами (текущим пользователем).

Пользователь с ролью главного администратора может просматривать задачи всех пользователей.

В таблице задач содержится следующая информация:

- **Статус** – статус задачи. Задаче может быть присвоен один из следующих статусов:
  - *Мигает зеленая точка* – задача активна.
  - **Завершено** – задача выполнена.
  - **Отмена** – задача отменена пользователем.
  - **Ошибка** – задача не была завершена из-за ошибки. Сообщение об ошибке отображается при наведении курсора мыши на значок восклицательного знака.
- **Задача** – тип задачи. В программе доступны следующие типы задач:
  - **Экспорт событий** – экспорт событий KUMA.
  - **Threat Lookup** – запрос данных с портала Kaspersky Threat Intelligence Portal.
  - **Ретроспективная проверка** – задание на воспроизведение событий.
  - **Импорт активов KSC** – импорт данных об активах с серверов Kaspersky Security Center.

- **Импорт учетных записей** – импорт данных о пользователях из Active Directory.
- **Импорт активов KICS for Networks** – импорт данных об активах из KICS for Networks.
- **Обновление репозитория** - обновления репозитория KUMA для получения пакетов с ресурсами из указанного в настройках источника.

- **Создал** – пользователь, создавший задачу. Если задача создана автоматически, в столбце указано **Задача по расписанию**.

  Этот столбец отображается только для пользователей с ролями главный администратор и администратор.

- **Создана** – время создания задачи.
- **Последнее обновление** – время обновления задачи.
- **Тенант** – название тенанта, в котором была запущена задача.

Формат даты задачи зависит от языка локализации, выбранного в настройках 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 и порядок следования столбцов в таблице задач:

1. В веб-интерфейсе KUMA выберите раздел **Диспетчер задач**.

   Отобразится таблица задач.

2. В заголовочной части таблицы нажмите на кнопку .
3. В отобразившемся окне 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 настройки, нажмите на ссылку **По умолчанию**.

5. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на название столбца, зажмите левую клавишу мыши и перетащите столбец в нужное место.

Отображение столбцов в таблице задач будет настроено.

Просмотр результата выполнения задачи

Чтобы просмотреть результат выполнения задачи:

1. В веб-интерфейсе KUMA выберите раздел **Диспетчер задач**.

   Отобразится таблица задач.

2. Нажмите на ссылку с типом задачи в столбце **Задача**.

   Отобразится список доступных для этого типа задач операций.

3. Выберите **Показать результат**.

Откроется окно с результатом выполнения задачи.

Повторный запуск задачи

Чтобы перезапустить задачу:

1. В веб-интерфейсе KUMA выберите раздел **Диспетчер задач**.

   Отобразится таблица задач.

2. Нажмите на ссылку с типом задачи в столбце **Задача**.

   Отобразится список доступных для этого типа задач операций.

3. Выберите **Перезапустить**.

Задача будет запущена повторно.

Работа с задачами Kaspersky Security Center

Вы можете подключить активы Kaspersky Security Center к KUMA и загружать на эти активы обновления баз и программных модулей или запускать на них антивирусную проверку с помощью задач Kaspersky Security Center. Задачи запускаются в веб-интерфейсе KUMA.

Для запуска задач Kaspersky Security Center на активах, подключенных к KUMA, рекомендуется использовать следующий сценарий:

1. **Создание в Консоли администрирования Kaspersky Security Center учетной записи пользователя**

   Данные этой учетной записи используются при создании секрета для установки соединения с Kaspersky Security Center и могут использоваться при создании задачи.

   Подробнее о создании учетной записи и назначении прав пользователю см. в *справке Kaspersky Security Center*.

2. Создание задач в Kaspersky Security Center

3. Настройка интеграции KUMA с Kaspersky Security Center

4. Импорт информации об активах Kaspersky Security Center в KUMA

5. Назначение категории импортированным активам

   После импорта активы автоматически помещаются в группу **Устройства без категории**. Вы можете назначить импортированным активам одну из существующих категорий или создать категорию и назначить ее активам.

6. **Запуск задач на активах**

   Вы можете запускать задачи вручную в информации об активе или настроить автоматический запуск задач.

О создании задач KUMA в Kaspersky Security Center

Вы можете запустить на активах Kaspersky Security Center, подключенных к KUMA, задачу обновления антивирусных баз и модулей программы и задачу антивирусной проверки. На активах должны быть установлены программы Kaspersky Endpoint Security для Windows или Linux. Задачи создаются в Kaspersky Security Center Web Console.

Подробнее о создании задач *Обновление* и *Антивирусная проверка* на активах с Kaspersky Endpoint Security для Windows см. в справке *Kaspersky Endpoint Security для Windows*.

Подробнее о создании задач *Обновление* и *Антивирусная проверка* на активах с Kaspersky Endpoint Security для Linux см. в справке *Kaspersky Endpoint Security для Linux*.

Название задач должно начинаться с "kuma" (без учета регистра и без кавычек). Например, `KUMA antivirus check`. В противном случае задача не отображается в списке доступных задач в веб-интерфейсе KUMA.

Запуск задач Kaspersky Security Center вручную

Вы можете вручную запускать на активах Kaspersky Security Center, подключенных к KUMA, задачу обновления антивирусных баз и модулей программы и задачу антивирусной проверки. На активах должны быть установлены программы Kaspersky Endpoint Security для Windows или Linux.

Предварительно вам нужно настроить интеграцию Kaspersky Security Center с KUMA и создать задачи в Kaspersky Security Center.

Чтобы запустить задачу Kaspersky Security Center вручную:

1. В разделе **Активы** веб-интерфейса KUMA выберите актив, импортированный из Kaspersky Security Center.

   Откроется окно **Информация об активе**.

2. Нажмите на кнопку **Реагирование KSC**.

   Кнопка отображается, если подключение к Kaspersky Security Center, к которому принадлежит выбранный актив, включено.

3. В открывшемся окне **Выберите задачу** установите флажки рядом с задачами, которые вы хотите запустить, и нажмите на кнопку **Запустить**.

Kaspersky Security Center запускает выбранные задачи.

Некоторые типы задач доступны только для определенных активов.

Информация об уязвимостях и программном обеспечении доступна только для активов с операционной системой Windows.

Автоматический запуск задач Kaspersky Security Center

Вы можете настроить автоматический запуск задачи обновления антивирусных баз и модулей программы и задачи антивирусной проверки на активах Kaspersky Security Center, подключенных к KUMA. На активах должны быть установлены программы Kaspersky Endpoint Security для Windows или Linux.

Предварительно вам нужно настроить интеграцию Kaspersky Security Center с KUMA и создать задачи в Kaspersky Security Center.

Настройка автоматического запуска задач Kaspersky Security Center включает следующие этапы:

Шаг 1. Добавление правила корреляции

Чтобы добавить правило корреляции:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. Выберите **Правила корреляции** и нажмите на кнопку **Добавить правило корреляции**.
3. На закладке **Общие** укажите следующие параметры:
   a. В поле **Название** укажите название правила.
   b. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.
   c. В раскрывающемся списке **Тип** выберите **simple**.
   d. В поле **Наследуемые поля** добавьте следующие поля: DestinationAssetID.
   e. При необходимости укажите значения для следующих полей:
      - В поле **Частота срабатывания** укажите максимальное количество срабатываний правила в секунду.
      - В поле **Уровень важности** укажите уровень важности алертов и корреляционных событий, которые будут созданы в результате срабатывания правила.
      - В поле **Описание** укажите любую дополнительную информацию.
4. На закладке **Селекторы** → **Параметры** выполните следующие действия:
   a. В раскрывающемся списке **Фильтр** выберите **Создать**.
   b. В поле **Условия** нажмите на кнопку **Добавить группу**.
   c. В поле с оператором для добавленной группы выберите **И**.
   d. Добавьте условие для фильтрации по значению поля DeviceProduct:
      1. В поле **Условия** нажмите на кнопку **Добавить условие**.

2. В поле с условием выберите **Если**.

3. В поле **Левый операнд** выберите поле события.

4. В поле поле события выберите DeviceProduct.

5. В поле оператор выберите =.

6. В поле **Правый операнд** выберите **константа**.

7. В поле **значение** введите KSC.

e. Добавьте условие для фильтрации по значению поля Name:

1. В поле **Условия** нажмите на кнопку **Добавить условие**.

2. В поле с условием выберите **Если**.

3. В поле **Левый операнд** выберите поле события.

4. В поле поле события выберите Name.

5. В поле оператор выберите =.

6. В поле **Правый операнд** выберите **константа**.

7. В поле **значение** введите имя события, при обнаружении которого вы хотите автоматически запускать задачу.

   Например, если вы хотите, чтобы задача *Антивирусная проверка* запускалась при регистрации событий Kaspersky Security Center *Обнаружен вредоносный объект*, вам нужно указать в поле **значение** это имя.

   Имя события можно посмотреть в поле **Name** в информации о событии.

5. На закладке **Действия** укажите следующие параметры:

   a. В разделе **Действия** откройте раскрывающийся список **На каждом событии**.

   b. Установите флажок **Отправить на дальнейшую обработку**.

   Другие поля заполнять не требуется.

6. Нажмите на кнопку **Сохранить**.

Правило корреляции будет создано.

Шаг 2. Создание коррелятора

Вам нужно запустить мастер установки коррелятора. На шаге 3 мастера вам требуется выбрать правило корреляции, добавленное при выполнении этой инструкции.

> В поле DeviceHostName должно отображаться доменное имя (FQDN) актива. Если оно не отображается, вам нужно создать запись для этого актива в системе DNS и на шаге 4 мастера создать правило обогащения с помощью DNS.

Шаг. 3. Добавление фильтра

Чтобы добавить фильтр:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. Выберите **Фильтры** и нажмите на кнопку **Добавить фильтр**.
3. В поле **Название** укажите название фильтра.
4. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.
5. В поле **Условия** нажмите на кнопку **Добавить группу**.
6. В поле с оператором для добавленной группы выберите **И**.
7. Добавьте условие для фильтрации по значению поля DeviceProduct:
   a. В поле **Условия** нажмите на кнопку **Добавить условие**.
   b. В поле с условием выберите **Если**.
   c. В поле **Левый операнд** выберите поле события.
   d. В поле поле события выберите Type.
   e. В поле оператор выберите =.
   f. В поле **Правый операнд** выберите **константа**.
   g. В поле **значение** введите 3.
8. Добавьте условие для фильтрации по значению поля Name:
   a. В поле **Условия** нажмите на кнопку **Добавить условие**.
   b. В поле с условием выберите **Если**.

c. В поле **Левый операнд** выберите поле события.

d. В поле поле события выберите Name.

e. В поле оператор выберите =.

f. В поле **Правый операнд** выберите **константа**.

g. В поле **значение** введите имя правила корреляции, созданного на шаге 1.

Шаг 4. Добавление правила реагирования

Чтобы добавить правило реагирования:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. Выберите **Правила реагирования** и нажмите на кнопку **Добавить правило реагирования**.
3. В поле **Название** укажите название правила.
4. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.
5. В раскрывающемся списке **Тип** выберите **Реагирование через KSC**.
6. В раскрывающемся списке **Задача Kaspersky Security Center** выберите задачу Kaspersky Security Center, которую требуется запустить.
7. В раскрывающемся списке **Поле события** выберите DestinationAssetID.
8. В поле **Рабочие процессы** укажите количество процессов, которые сервис может запускать одновременно.

   По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис коррелятора.

- В поле **Описание** вы можете добавить до 4000 символов Юникода, описывающих ресурс.
- В раскрывающемся списке **Фильтр** выберите фильтр, добавленный на шаге 3 этой инструкции.

Для отправки запросов в Kaspersky Security Center необходимо убедиться, что Kaspersky Security Center доступен по протоколу UDP.

Если ресурс правила реагирования принадлежит общему тенанту, то в качестве доступных для выбора задач Kaspersky Security Center отображаются задачи от сервера Kaspersky Security Center, к которому подключен главный тенант.

Если в ресурсе правила реагирования выбрана задача, которая отсутствует на сервере Kaspersky Security Center, к которому подключен тенант, для активов этого тенанта задача не будет выполнена. Такая ситуация может возникнуть, например, когда два тенанта используют общий коррелятор.

Шаг 5. Добавление правила реагирования в коррелятор

Чтобы добавить правило реагирования в коррелятор:

1. В веб-интерфейсе KUMA выберите раздел **Ресурсы**.
2. Выберите **Корреляторы**.
3. В списке корреляторов выберите коррелятор, добавленный на шаге 2 этой инструкции.
4. В дереве шагов выберите **Правила реагирования**.
5. Нажмите на кнопку **Добавить**.
6. В раскрывающемся списке **Правило реагирование** выберите правило, добавленное на шаге 4 этой инструкции.
7. В дереве шагов выберите **Проверка параметров**.
8. Нажмите на кнопку **Сохранить и перезапустить сервисы**.
9. Нажмите на кнопку **Сохранить**.

Правило реагирования будет добавлено в коррелятор.

Автоматический запуск задачи обновления антивирусных баз и модулей программы или задачи антивирусной проверки на активах Kaspersky Security Center, подключенных к KUMA, будет настроен. Задачи запускаются при обнаружении угрозы на активах и получении KUMA соответствующих событий.

Проверка статуса задач Kaspersky Security Center

В веб-интерфейсе KUMA можно проверить, была ли запущена задача Kaspersky Security Center или завершен ли поиск событий из коллектора, который прослушивает события Kaspersky Security Center.

Чтобы выполнить проверку статуса задач Kaspersky Security Center:

1. Выберите раздел KUMA **Ресурсы** → **Активные сервисы**.

2. Выберите коллектор, настроенный на получение событий с сервера Kaspersky Security Center, и нажмите на кнопку **Перейти к событиям**.

   Откроется новая закладка браузера в разделе **События** KUMA. В таблице отобразятся события с сервера Kaspersky Security Center. Статус задач отображается в столбце **Название**.

Поля событий Kaspersky Security Center:

- **Name** (Название) – статус или тип задачи.

- **Message** (Сообщение) – сообщение о задаче или событии.

- **FlexString<номер>Label** (Заголовок настраиваемого поля <номер>) – название атрибута, полученного от Kaspersky Security Center. Например, `FlexString1Label=TaskName`.

- **FlexString<номер>** (Настраиваемое поле <номер>) – значение атрибута, указанного в поле поля FlexString<номер>Label. Например, `FlexString1=Download updates`.

- **DeviceCustomNumber<номер>Label** (Заголовок настраиваемого поля <номер>) – название атрибута, относящегося к состоянию задачи. Например, `DeviceCustomNumber1Label=TaskOldState`.

- **DeviceCustomNumber<номер>** (Настраиваемое поле <номер>) – значение, относящееся к состоянию задачи. Например, `DeviceCustomNumber1=1` означает, что задача выполняется.

- **DeviceCustomString<номер>Label** (Заголовок настраиваемого поля <номер>) – название атрибута, относящегося к обнаруженной уязвимости: например, название вируса, уязвимого приложения.

- **DeviceCustomString<номер>** (Настраиваемое поле <номер>) – значение, относящееся к обнаруженной уязвимости. Например, пары атрибут-значение `DeviceCustomString1Label=VirusName` и `DeviceCustomString1=EICAR-Test-File` означают, что обнаружен тестовый вирус EICAR.

Подключение к SMTP-серверу

В KUMA можно настроить отправку уведомлений по электронной почте с помощью SMTP-сервера. Пользователи будут получать уведомления, если в настройках их профиля установлен флажок **Получать уведомления по почте**.

Для обработки уведомлений KUMA можно добавить только один SMTP-сервер. Управление подключением к SMTP-серверу осуществляется в разделе веб-интерфейса KUMA **Параметры** → **Общие** → **Параметры подключения к SMTP-серверу**.

Чтобы настроить подключение к SMTP-серверу:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Общие**.

2. В блоке параметров **Параметры подключения к SMTP-серверу** измените необходимые параметры:

   - **Выключено** – установите этот флажок, если хотите отключить подключение к SMTP-серверу.

   - **Адрес сервера** (обязательно) – адрес SMTP-сервера в одном из следующих форматов: hostname, IPv4, IPv6.

   - **Порт** (обязательно) – порт подключения к почтовому серверу. Значение должно быть целым числом от 1 до 65 535.

   - **От кого** (обязательно) – адрес электронной почты отправителя сообщения. Например, `kuma@company.com`.

   - **Псевдоним сервера Ядра KUMA** – отличное от FQDN название сервера Ядра KUMA, которое используется в вашей сети.

   - При необходимости в раскрывающемся списке **Секрет** выберите ресурс секрета типа **credentials**, в котором записаны учетные данные для подключения к SMTP-серверу.

     Добавить секрет

     1. Если вы создали секрет ранее, выберите его в раскрывающемся списке **Секрет**.

        Если ранее не было добавлено ни одного секрета, в раскрывающемся списке отобразится **Нет данных**.

     2. Если вы хотите добавить новый секрет, справа от списка **Секрет** нажмите на кнопку +.

        Откроется окно **Секрет**.

3. В поле **Название** введите название, под которым секрет будет отображаться в списке доступных.

4. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору.

5. Если требуется, в поле **Описание** добавьте любую дополнительную информацию о секрете.

6. Нажмите на кнопку **Сохранить**.

Секрет будет добавлен и отобразится в списке **Секрет**.

- Выберите периодичность уведомлений в раскрывающемся списке **Регулярность уведомлений мониторинга**.

- Включите переключатель **Выключить уведомления мониторинга**, если не хотите получать уведомления о состоянии источников событий. По умолчанию переключатель выключен.

3. Нажмите **Сохранить**.

Соединение с SMTP-сервером настроено, пользователи могут получать сообщения электронной почты от KUMA.

Онлайн-справка KUMA

Онлайн-справка доступна на сайте "Лаборатории Касперского".

Онлайн-справка предоставляет информацию по следующим темам:

- Подготовка к установке и установка KUMA.

- Настройка и использование KUMA.

Чтобы открыть онлайн-справку для KUMA,

войдите в веб-интерфейс KUMA, в левом нижнем углу окна нажмите имя учетной записи пользователя и в открывшемся меню нажмите на кнопку **Справка**.

Журналы KUMA

Некоторые сервисы и ресурсы KUMA могут регистрировать информацию, связанную с их работой. Эта функция включается с помощью флажка или выпадающего списка **Отладка** в параметрах сервиса или ресурса.

Журналы сервисов можно скачать в веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы**, выбрав нужный сервис и нажав на кнопку **Журнал**.

Журналы хранятся на машине, на которой установлен требуемый сервис или сервис, использующий требуемый ресурс:

- Журналы на машинах Linux можно просмотреть с помощью команды `journalctl` в консоли Linux.

  Примеры:

  - `journalctl -u kuma-collector * kuma-correlator * -f` – вернет последние журналы из коллекторов и корреляторов, установленных на сервере, где была выполнена команда.

  - `journalctl -u kuma-collector-<идентификатор сервиса>` – вернет последние журналы определенного корректора, установленного на сервере, где была выполнена команда.

- Журналы на машинах Windows можно просмотреть в файле %PROGRAMDATA%\Kaspersky Lab\KUMA\<идентификатор агента>\agent.log. 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 Linux располагаются в директории с названием идентификатора агента, который был указан в команде установки агента. Например, если агент был установлен с помощью команды `sudo /opt/kaspersky/kuma/kuma agent --core https://kuma.example.com:7210 --id <идентификатор агента> --wd /opt/kaspersky/kuma/agent/<идентификатор агента>`, журналы агента будут расположены в директории `/opt/kaspersky/kuma/agent/<идентификатор агента>`.

Сервисы, где доступно ведение журнала:

- Корреляторы

- Коллекторы

- Агенты

Ресурсы, где доступно ведение журнала:

- Коннекторы

- Правила обогащения
- Точки назначения

Журнал на машинах Windows пополняется в течение месяца или пока он не достигнет размера 1 ГБ. По истечении месяца журнал архивируется, а события начинают записываться в новый журнал. Одновременно на сервере хранится не более трех заархивированных журналов. При появлении нового архива журнала, если архивов становится больше трех, самый старый архив удаляется. Также удаляются архивы с журналами старше 365 дней.

Резервное копирование KUMA

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

Резервное копирование можно осуществить следующими способами:

- с помощью REST API;
- с помощью исполняемого файла /opt/kaspersky/kuma/kuma.

> Метод резервного копирования KUMA с помощью исполняемого файла kuma будет недоступен в версиях KUMA выше 2.1.

Особенности резервного копирования KUMA

- Восстановление данных из резервной копии поддерживается только при сохранении версии KUMA.
- Резервное копирование коллекторов не требуется, за исключением коллекторов с SQL-подключением. При восстановлении таких коллекторов следует вернуть к исходному начальное значение идентификатора.
- Если после восстановления KUMA не включается, рекомендуется обнулить базу данных kuma в MongoDB.

  Как обнулить базу данных в MongoDB

  > Если после восстановления данных не включается Ядро KUMA, необходимо повторить восстановление, обнулив при этом базу данных kuma в MongoDB.
  >
  > *Чтобы восстановить данные KUMA с обнулением базы данных MongoDB:*

1. Войдите в ОС сервера, на котором установлено Ядро KUMA.

2. Остановите Ядро KUMA, выполнив следующую команду:

   ```
   sudo systemctl stop kuma-core
   ```

3. Войдите в MongoDB, выполнив следующие команды:

   a. `cd /opt/kaspersky/kuma/mongodb/bin/`

   b. `./mongo`

4. Обнулите базу данных MongoDB, выполнив следующие команды:

   a. `use kuma`

   b. `db.dropDatabase()`

5. Выйдите из базы данных MongoDB, нажав **`Ctrl+C`**.

6. Восстановите данные из резервной копии, выполнив следующую команду:

   ```
   sudo /opt/kaspersky/kuma/kuma tools restore --src <путь к директории с резервной копией> --certificates
   ```

   Флаг `--certificates` не является обязательным и используется для восстановления сертификатов.

7. Запустите KUMA, выполнив следую команду:

   ```
   sudo systemctl start kuma-core
   ```

8. Пересоздайте сервисы, используя восстановленные наборы ресурсов для сервисов.

Данные восстановлены из резервной копии.

Резервное копирование KUMA с помощью файла kuma

Чтобы выполнить резервное копирование:

1. Войдите в ОС сервера, на котором установлено Ядро KUMA.

2. Выполните следующую команду исполняемого файла kuma:

   ```
   sudo /opt/kaspersky/kuma/kuma tools backup --dst <путь к директории для резервной копии> --certificates
   ```

Резервная копия создана.

Чтобы восстановить данные из резервной копии:

1. Войдите в ОС сервера, на котором установлено Ядро KUMA.
2. Остановите Ядро KUMA, выполнив следующую команду:

   ```
   sudo systemctl stop kuma-core
   ```

3. Выполните следующую команду:

   ```
   sudo /opt/kaspersky/kuma/kuma tools restore --src <путь к директории с резервной копией> --certificates
   ```

4. Запустите KUMA, выполнив следую команду:

   ```
   sudo systemctl start kuma-core
   ```

5. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** выберите все сервисы и нажмите на кнопку **Сбросить сертификат**.
6. Установите сервисы заново с теми же портами и идентификаторами.

Данные восстановлены из резервной копии.

Уведомления KUMA

Стандартные уведомления

В KUMA можно настроить отправку уведомлений по электронной почте с помощью SMTP-сервера. Для этого необходимо настроить подключение к SMTP-серверу, а также установить флажок **Получать уведомления по почте** для пользователей, которым должны приходить уведомления.

KUMA автоматически уведомляет пользователей о следующих событиях:

- создан отчет (уведомление получают пользователи, перечисленные в параметрах расписания шаблона отчета);
- создан алерт (уведомление получают все пользователи);
- алерт назначен пользователю (уведомление получает пользователь, которому был назначен алерт);
- выполнена задача (уведомление получают пользователи, создавшие задачу).

- доступны новые пакеты с ресурсами, которые можно получить путем обновления репозитория KUMA (уведомление получают пользователи, чей адрес электронной почты указан в параметрах задачи).

Пользовательские уведомления

Вместо стандартных уведомлений KUMA о создании алертов можно рассылать уведомления на основании пользовательских шаблонов. Настройка пользовательских уведомлений взамен стандартных происходит по шагам:

- Создание ресурса шаблона электронной почты.
- Создание правила уведомления, в котором указываются правила корреляции и адреса электронной почты.

Когда по выбранным правилам корреляции будет создаваться алерт, на указанные адреса электронной почты будут отправляться уведомления, созданные на основе пользовательских шаблонов электронной почты. Стандартные уведомления KUMA о том же событии на указанные адреса отправлены не будут.

Обращение в службу технической поддержки

Если вам не удается найти решение своей проблемы в документации к программе, обратитесь к специалисту по технической поддержке в "Лабораторию Касперского".

"Лаборатория Касперского" предоставляет поддержку этой программы в течение ее жизненного цикла (см. страницу жизненного цикла программ).

REST API

В KUMA можно обращаться из сторонних решений с помощью API. KUMA REST API работает через HTTP и представляет набор методов запрос/ответ.

Запросы REST API необходимо отправлять по следующему адресу:

https://<FQDN Ядра KUMA>/api/<Версия API>/<запрос>

Пример:

https://kuma.example.com:7223/api/v1

По умолчанию для запросов используется порт 7223. При необходимости порт можно изменить.

Чтобы изменить порт, используемый для запросов REST API:

1. Войдите в ОС сервера, на котором установлено Ядро KUMA.

2. В файле /etc/systemd/system/multi-user.target.wants/kuma-core.service измените следующую строку, подставив нужный порт:

   ```
   ExecStart=/opt/kaspersky/kuma/kuma core --external :7220 --internal :7210
   --mongo mongodb://localhost:27017 --rest <требуемый номер порта для
   запросов REST API>
   ```

3. Перезапустите KUMA, выполнив последовательно следующие команды:

   a. `systemctl daemon-reload`

   b. `systemctl restart kuma-core`

Для запросов REST API используется новый порт.

> Убедитесь, что порт доступен и не закрыт межсетевым экраном.

Заголовок для аутентификации: Authorization: Bearer <токен>

Формат данных по умолчанию: JSON

Формат даты и времени: RFC 3339

Интенсивность запросов: не ограничена

Создание токена

Чтобы сгенерировать токен для пользователя:

1. Откройте раздел веб-интерфейса KUMA **Параметры** → **Пользователи**.

   В правой части раздела **Параметры** отобразится таблица **Пользователи**.

2. Выберите нужного пользователя и в открывшейся справа области деталей нажмите на кнопку **Сгенерировать токен**.

   Откроется окно **Новый токен**.

3. Если требуется, установите срок действия токена:

   a. Установите флажок **Без окончания срока действия**.

   b. В поле **Срок действия** с помощью календаря укажите дату и время истечения срока действия создаваемого токена.

4. Нажмите на кнопку **Сгенерировать токен**.

   При нажатии на эту кнопку в области деталей пользователя отображается поле с автоматически созданным токеном. При закрытии окна токен больше не отображается, и, если вы его не скопировали, потребуется сгенерировать новый токен.

5. Нажмите **Сохранить**.

Токен сгенерирован и может быть использован для API-запросов. Таким же образом можно сгенерировать токен в профиле своей учетной записи.

Настройка прав доступа к API

В KUMA для каждого пользователя можно настроить операции, которые можно выполнять от лица этого пользователя. Права можно настроить только для пользователей, созданных в KUMA.

Чтобы настроить доступные операции для пользователя:

1. Откройте раздел веб-интерфейса KUMA **Параметры** → **Пользователи**.

   В правой части раздела **Параметры** отобразится таблица **Пользователи**.

2. Выберите нужного пользователя и в открывшейся справа области деталей нажмите на кнопку **Права доступа через API**.

   Откроется окно со списком доступных операций. По умолчанию пользователю доступны все API-запросы.

3. Установите или снимите флажок напротив требуемой операции.

4. Нажмите **Сохранить**.

Доступные операции для пользователя настроены.

Доступные операции можно аналогичным образом настроить в профиле своей учетной записи.

Авторизация API-запросов

Каждый запрос REST API должен включать авторизацию с помощью токена. Пользователь, с помощью чьего токена выполняется API-запрос, должен иметь права на выполнение такого типа запросов.

К каждому запросу должен прилагаться следующий заголовок:

```
Authorization: Bearer <token>
```

Возможные ошибки:

HTTP-код	Описание	Значение поля message	Значение поля details
400	Некорректный заголовок	invalid authorization header	Example: <пример>
403	Токен не существует или пользователь-владелец выключен	access denied	

Стандартная ошибка

Возвращаемые KUMA ошибки имеют следующий формат:

```
type Error struct {
    Message    string      `json:"message"`
    Details    interface{} `json:"details"`
}
```

Операции

Описание доступных запросов и ответов.

Просмотр списка активных листов на корреляторе

GET /api/v1/activeLists

Целевой коррелятор должен быть запущен.

Доступ: администратор, аналитик.

Параметры запроса

Имя	Тип данных	Обязательный	Описание	Пример значения
correlatorID	string	Да	Идентификатор сервиса коррелятора	00000000-0000-0000-0000-000000000000

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []ActiveListInfo


type ActiveListInfo struct {
    ID      string `json:"id"`
    Name    string `json:"name"`
    Dir     string `json:"dir"`
    Records uint64 `json:"records"`
    WALSize uint64 `json:"walSize"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message	Значение поля details
400	Не указан идентификатор сервиса коррелятора	query parameter required	correlatorID
403	Пользователь не имеет необходимой роли в тенанте коррелятора	access denied	
404	Сервис с указанным идентификатором (correlatorID) не найден	service not found	
406	Сервис с указанным идентификатором (correlatorID) не является коррелятором	service is not correlator	
406	Коррелятор не выполнил первый старт	service not paired	
406	Тенант коррелятора отключен	tenant disabled	
50x	Не удалось обратиться к API коррелятора	correlator API request failed	вариативное
500	Не удалось декодировать тело ответа, полученное от коррелятора	correlator response decode failed	вариативное
500	Любые другие внутренние ошибки	вариативное	вариативное

Импорт записей в активный лист

POST /api/v1/activeLists/import

Целевой коррелятор должен быть запущен.

Доступ: администратор, аналитик.

Параметры запроса

Имя	Тип данных	Обязательный	Описание

correlatorID	string	Да	Идентификатор сервиса коррелятора	00 00 00 00
activeListID	string	Если не указан activeListName	Идентификатор активного листа	00 00 00 00
activeListName	string	Если не указан activeListID	Имя активного листа	At
format	string	Да	Формат импортируемых записей	cs
keyField	string	Только для форматов csv и tsv	Имя поля в заголовке csv или tsv файла, которое будет использовано в качестве ключевого поля записи активного листа. Значения этого поля должны быть уникальными	ip
clear	bool	Нет	Очистить активный лист перед выполнением импорта. Если параметр присутствует в URL query, его значение принимается за true. Указанные пользователем значения игнорируются. Пример: /api/v1/activeLists/import?clear	

Тело запроса

Формат	Содержимое
csv	Первая строка – заголовок, где перечислены поля, разделенные запятой. Остальные строки – значения, соответствующие полям в заголовке, разделенные запятой. Количество полей на каждой строке должно быть одинаковым.
tsv	Первая строка – заголовок, где перечислены поля, разделенные TAB. Остальные строки – значения, соответствующие полям в заголовке, разделенные TAB. Количество полей на каждой строке должно быть одинаковым.

internal	Каждая строка содержит один индивидуальный объект JSON. Данные в internal формате можно получить путем экспорта содержимого активного листа из коррелятора в WEB-консоли KUMA.

Ответ

HTTP-код: 204

Возможные ошибки

HTTP-код	Описание	Значение поля message	Значение поля details
400	Не указан идентификатор сервиса коррелятора	query parameter required	correlatorID
400	Не указан ни параметр activeListID, ни параметр activeListName	one of query parameters required	activeListID, activeListName
400	Не указан параметр format	query parameter required	format
400	Параметр format имеет неверное значение	invalid query parameter value	format
400	Параметр keyField не задан	query parameter required	keyField
400	Тело запроса имеет нулевую длину	request body required	
400	CSV или TSV файл не содержит поле, указанное в параметре keyField	correlator API request failed	line 1: header does not contain column <name>
400	Ошибка парсинга тела запроса	correlator API request failed	line <number>: <message>

403	Пользователь не имеет необходимой роли в тенанте коррелятора	access denied	
404	Сервис с указанным идентификатором (correlatorID) не найден	service not found	
404	Активный лист не найден	active list not found	
406	Сервис с указанным идентификатором (correlatorID) не является коррелятором	service is not correlator	
406	Коррелятор не выполнил первый старт	service not paired	
406	Тенант коррелятора отключен	tenant disabled	
406	Поиск активного листа выполнялся по имени (activeListName) и было найдено более одного активного листа	more than one matching active lists found	
50x	Не удалось обратиться к API коррелятора	correlator API request failed	вариативное
500	Не удалось декодировать тело ответа, полученное от коррелятора	correlator response decode failed	вариативное
500	Любые другие внутренние ошибки	вариативное	вариативное

Поиск алертов

GET /api/v1/alerts

Доступ: администратор, аналитик, оператор.

Параметры запроса

Имя	Тип данных	Обязательный	Описание	Пример зн

page	number	Нет	Номер страницы. Начинается с 1. Размер страницы – 250 записей. Если параметр не указан, то используется значение по умолчанию – 1.	1
id	string	Нет	Идентификатор алерта. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	00000000-0 0000-0000- 000000000
tenantID	string	Нет	Идентификатор тенанта алерта. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ. Если пользователь не имеет необходимой роли в указанном тенанте, то данный тенант игнорируется.	00000000-0 0000-0000- 000000000
name	string	Нет	Имя алерта. Регистронезависимое регулярное выражение (PCRE).	alert ^My alert$
timestampField	string	Нет	Имя поля алерта, по которому выполняется сортировка (DESC) и поиск по периоду (from – to). По умолчанию lastSeen.	lastSeen, firs
from	string	Нет	Нижняя границы периода в формате RFC3339. <timestampField> >= <from>	2021-09-06T00:00:00 2021-09-06T00:00:00 (UTC, с указа миллисекунд 2021-09-06T00:00:00 (MSK)

to	string	Нет	Верхняя периода в формате RFC3339. <timestampField> <= <to>	2021-09-06T00:00:00 2021-09-06T00:00:00 (UTC, с указа миллисекунд 2021-09-06T00:00:00 (MSK)
status	string	Нет	Статус алерта. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	new, assigned escalated, clo
withEvents	bool	Нет	Включить в ответ нормализованные события KUMA, связанные с найденными алертами. Если параметр присутствует в URL query, его значение принимается за true. Указанные пользователем значения игнорируются. Пример: /api/v1/alerts?withEvents	
withAffected	bool	Нет	Включить в ответ информацию об активах и аккаунтах, связанных с найденными алертами. Если параметр присутствует в URL query, его значение принимается за true. Указанные пользователем значения игнорируются. Пример: /api/v1/alerts?withAffected	

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Alert


type Alert struct {
    ID                 string            `json:"id"`
    TenantID           string            `json:"tenantID"`
    TenantName         string            `json:"tenantName"`
    Name               string            `json:"name"`
    CorrelationRuleID string            `json:"correlationRuleID"`
    Priority           string            `json:"priority"`
    Status             string            `json:"status"`
    FirstSeen          string            `json:"firstSeen"`
    LastSeen           string            `json:"lastSeen"`
    Assignee           string            `json:"assignee"`
    ClosingReason      string            `json:"closingReason"`
    Overflow           bool              `json:"overflow"`
    Events             []NormalizedEvent `json:"events"`
    AffectedAssets     []AffectedAsset   `json:"affectedAssets"`
    AffectedAccounts   []AffectedAccount `json:"affectedAccounts"`
}


type NormalizedEvent map[string]interface{}


type AffectedAsset struct {
    ID                 string           `json:"id"`
    TenantID           string           `json:"tenantID"`
```

```
    TenantName       string          `json:"tenantName"`
    Name             string          `json:"name"`
    FQDN             string          `json:"fqdn"`
    IPAddresses      []string        `json:"ipAddresses"`
    MACAddresses     []string        `json:"macAddresses"`
    Owner            string          `json:"owner"`
    OS               *OS             `json:"os"`
    Software         []Software      `json:"software"`
    Vulnerabilities  []Vulnerability `json:"vulnerabilities"`
    KSC              *KSCFields      `json:"ksc"`
    Created          string          `json:"created"`
    Updated          string          `json:"updated"`
}

type OS struct {
    Name    string `json:"name"`
    Version uint64 `json:"version"`
}

type Software struct {
    Name    string `json:"name"`
    Version string `json:"version"`
    Vendor  string `json:"vendor"`
}

type Vulnerability struct {
    KasperskyID           string   `json:"kasperskyID"`
```

```
    ProductName           string   `json:"productName"`
    DescriptionURL        string   `json:"descriptionURL"`
    RecommendedMajorPatch string   `json:"recommendedMajorPatch"`
    RecommendedMinorPatch string   `json:"recommendedMinorPatch"`
    SeverityStr           string   `json:"severityStr"`
    Severity              uint64   `json:"severity"`
    CVE                   []string `json:"cve"`
    ExploitExists         bool     `json:"exploitExists"`
    MalwareExists         bool     `json:"malwareExists"`
}

type AffectedAccount struct {
    Name             string `json:"displayName"`
    CN               string `json:"cn"`
    DN               string `json:"dn"`
    UPN              string `json:"upn"`
    SAMAccountName   string `json:"sAMAccountName"`
    Company          string `json:"company"`
    Department       string `json:"department"`
    Created          string `json:"created"`
    Updated          string `json:"updated"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message	Значение поля details
400	Неверное значение параметра page	invalid query parameter value	page
400	Неверное значение параметра status	invalid status	<status>
400	Неверное значение параметра timestampField	invalid timestamp field	
400	Неверное значение параметра from	cannot parse from	вариативное
400	Неверное значение параметра to	cannot parse to	вариативное
400	Значение параметра from больше значения параметра to	from cannot be greater than to	
500	Любые другие внутренние ошибки	вариативное	вариативное

Закрытие алертов

POST /api/v1/alerts/close

Целевой коррелятор должен быть запущен.

Доступ: администратор, аналитик, оператор.

Тело запроса

Формат: JSON

Имя	Тип данных	Обязательный	Описание	Пример значения
id	string	Да	Идентификатор алерта	00000000-0000-0000-0000-000000000000
reason	string	Да	Причина закрытия алерта	responded, incorrect data, incorrect correlation rule

Ответ

HTTP-код: 204

Возможные ошибки

HTTP-код	Описание	Значение поля message	Значение поля details
400	Не указан идентификатор алерта (id)	id required	
400	Не указана причина закрытия алерта (reason)	reason required	
400	Неверное значение параметра reason	invalid reason	
403	Пользователь не имеет необходимой роли в тенанте алерта	access denied	
404	Алерт не найден	alert not found	
406	Тенант алерта отключен	tenant disabled	
406	Алерт уже закрыт	alert already closed	
500	Любые другие внутренние ошибки	вариативное	вариативное

Поиск активов

GET /api/v1/assets

Доступ: администратор, аналитик, оператор.

Параметры запроса

Имя	Тип данных	Обязательный	Описание	Пример значения

page	number	Нет	Номер страницы. Начинается с 1. Размер страницы – 250 записей. Если параметр не указан, то используется значение по умолчанию – 1.	1
id	string	Нет	Идентификатор актива. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	00000000-0000-0000-0000-000000000000
tenantID	string	Нет	Идентификатор тенанта актива. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ. Если пользователь не имеет необходимой роли в указанном тенанте, то данный тенант игнорируется.	00000000-0000-0000-0000-000000000000
name	string	Нет	Название актива. Регистронезависимое регулярное выражение (PCRE).	asset ^My asset$
fqdn	string	Нет	FQDN актива. Регистронезависимое регулярное выражение (PCRE).	^com$
ip	string	Нет	IP-адрес актива. Регистронезависимое регулярное выражение (PCRE).	10.10 ^192.168.1.2$
mac	string	Нет	MAC-адрес актива. Регистронезависимое регулярное выражение (PCRE).	^00:0a:95:9d:68:16$

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Asset


type Asset struct {
    ID                      string          `json:"id"`
    TenantID                string          `json:"tenantID"`
    TenantName              string          `json:"tenantName"`
    Name                    string          `json:"name"`
    FQDN                    string          `json:"fqdn"`
    IPAddresses             []string        `json:"ipAddresses"`
    MACAddresses            []string        `json:"macAddresses"`
    Owner                   string          `json:"owner"`
    OS                      *OS             `json:"os"`
    Software                []Software      `json:"software"`
    Vulnerabilities         []Vulnerability `json:"vulnerabilities"`
    KSC                     *KSCFields      `json:"ksc"`
    Created                 string          `json:"created"`
    Updated                 string          `json:"updated"`
}


type KSCFields struct {
    NAgentID          string `json:"nAgentID"`
    KSCInstanceID     string `json:"kscInstanceID"`
```

```
    KSCMasterHostname string `json:"kscMasterHostname"`
    LastVisible       string `json:"lastVisible"`
}

type OS struct {
    Name    string `json:"name"`
    Version uint64 `json:"version"`
}

type Software struct {
    Name    string `json:"name"`
    Version string `json:"version"`
    Vendor  string `json:"vendor"`
}

type Vulnerability struct {
    KasperskyID           string   `json:"kasperskyID"`
    ProductName           string   `json:"productName"`
    DescriptionURL        string   `json:"descriptionURL"`
    RecommendedMajorPatch string   `json:"recommendedMajorPatch"`
    RecommendedMinorPatch string   `json:"recommendedMinorPatch"`
    SeverityStr           string   `json:"severityStr"`
    Severity              uint64   `json:"severity"`
    CVE                   []string `json:"cve"`
    ExploitExists         bool     `json:"exploitExists"`
    MalwareExists         bool     `json:"malwareExists"`
```

```
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message	Значение поля details
400	Неверное значение параметра page	invalid query parameter value	page
500	Любые другие внутренние ошибки	вариативное	вариативное

Импорт активов

Особенности идентификации, создания и обновления активов

Активы импортируются в соответствии с правилами слияния данных об активах.

POST /api/v1/assets/import

Массовое создание или обновление активов.

Доступ: администратор, аналитик.

Тело запроса

Формат: JSON

```
type Request struct {
    TenantID string  `json:"tenantID"`
    Assets   []Asset `json:"assets"`
}
```

```
type Asset struct {
    Name            string          `json:"name"`
    FQDN            string          `json:"fqdn"`
    IPAddresses     []string        `json:"ipAddresses"`
    MACAddresses    []string        `json:"macAddresses"`
    Owner           string          `json:"owner"`
    OS              *OS             `json:"os"`
    Software        []Software      `json:"software"`
    Vulnerabilities []Vulnerability `json:"vulnerabilities"`
}

type OS struct {
    Name    string `json:"name"`
    Version uint64 `json:"version"`
}

type Software struct {
    Name    string `json:"name"`
    Version string `json:"version"`
    Vendor  string `json:"vendor"`
}

type Vulnerability struct {
    KasperskyID           string   `json:"kasperskyID"`
    ProductName           string   `json:"productName"`
    DescriptionURL        string   `json:"descriptionURL"`
```

```
    RecommendedMajorPatch string   `json:"recommendedMajorPatch"`
    RecommendedMinorPatch string   `json:"recommendedMinorPatch"`
    SeverityStr           string   `json:"severityStr"`
    Severity              uint64   `json:"severity"`
    CVE                   []string `json:"cve"`
    ExploitExists         bool     `json:"exploitExists"`
    MalwareExists         bool     `json:"malwareExists"`
}
```

Обязательные поля Request

Имя	Тип данных	Обязательный	Описание	Пример значения
tenantID	string	Да	Идентификатор тенанта	00000000-0000-0000-0000-000000000000
assets	[]Asset	Да	Массив импортируемых активов	

Обязательные поля Asset

Имя	Тип данных	Обязательный	Описание	Пример значе

fqdn	string	Если не указан ipAddresses	FQDN актива. Рекомендуется указывать именно FQDN, а не просто имя хоста. Приоритетный признак для идентификации актива.	my-asset-1.example.com my-asset-1
ipAddresses	[]string	Если не указан fqdn	Массив IP-адресов актива. IPv4 или IPv6. Первый элемент массива используется как второстепенный признак для идентификации актива.	["192.168.1.1", "192.168.2.2"] ["2001:0db8:85a3:0000:0000

Ответ

HTTP-код: 200

Формат: JSON

```
type Response struct {
    InsertedIDs  map[int64]interface{} `json:"insertedIDs"`
    UpdatedCount uint64                `json:"updatedCount"`
    Errors       []ImportError         `json:"errors"`
}

type ImportError struct {
    Index   uint64 `json:"index"`
```

```
    Message string `json:"message"`

}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message	Значение поля details
400	Не указан идентификатор тенанта (tenantID)	tenantID required	
400	Попытка импорта активов в общий тенант	import into shared tenant not allowed	
400	В теле запроса не указан ни один актив	at least one asset required	
400	Не указано ни одно из обязательных полей	one of fields required	asset[<index>]: fqdn, ipAddresses
400	Неверный FQDN	invalid value	asset[<index>].fqdn
400	Неверный IP address	invalid value	asset[<index>].ipAddresses[<index>]
400	Дублируется IP адрес	duplicated value	asset[<index>].ipAddresses
400	Неверный MAC адрес	invalid value	asset[<index>].macAddresses[<inde
400	Дублируется MAC адрес	duplicated value	asset[<index>].macAddresses
403	Пользователь не имеет необходимой роли в указанном тенанте	access denied	
404	Указанный тенант не найден	tenant not found	
406	Указанный тенант отключен	tenant disabled	

500	Любые другие внутренние ошибки	вариативное	вариативное

Удаление активов

POST /api/v1/assets/delete

Доступ: администратор, аналитик.

Тело запроса

Формат: JSON

Имя	Тип данных	Обязательный	Описание	Пример значе
tenantID	string	Да	Идентификатор тенанта	00000000-0000-0000-00 000000000000
ids	[]string	Если не указаны ни fqdns, ни ipAddresses	Список идентификаторов активов	["00000000-0000-0000-0 000000000000"]
fqdns	[]string	Если не указаны ни ids, ни ipAddresses	Массив FQDN активов	["my-asset-1.example.com", "
ipAddresses	[]string	Если не указаны ни ids, ни fqdns	Массив основных IP-адресов активов	["192.168.1.1", "2001:0db8:85a3:0000:000

Ответ

HTTP-код: 200

Формат: JSON

```
type Response struct {
    DeletedCount uint64 `json:"deletedCount"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message	Значение поля details
400	Не указан идентификатор тенанта (tenantID)	tenantID required	
400	Попытка удаления актива из общего тенанта	delete from shared tenant not allowed	
400	Не указано ни одно из обязательных полей	one of fields required	ids, fqdns, ipAddresses
400	Указан неверный FQDN	invalid value	fqdns[<index>]
400	Указан неверный IP адрес	invalid value	ipAddresses[<index>]
403	Пользователь не имеет необходимой роли в указанном тенанте	access denied	
404	Указанный тенант не найден	tenant not found	
406	Указанный тенант отключен	tenant disabled	
500	Любые другие внутренние ошибки	вариативное	вариативное

Поиск событий

POST /api/v1/events

Доступ: администратор, аналитик, оператор.

Тело запроса

Формат: JSON

Request

Имя	Тип данных	Обязательный	Описание	Пример значения
period	Period	Да	Период поиска	
sql	string	Да	SQL запрос	SELECT * FROM events WHERE Type = 3 ORDER BY Timestamp DESC LIMIT 1000 SELECT sum(BytesOut) as TotalBytesSent, SourceAddress FROM events WHERE DeviceVendor = 'netflow' GROUP BY SourceAddress LIMIT 1000 SELECT count(Timestamp) as TotalEvents FROM events LIMIT 1
clusterID	string	Нет, если кластер единственный	Идентификатор Storage кластера. Можно найти запросив список сервисов с kind = storage. Идентификатор кластера будет в поле resourceID.	00000000-0000-0000-0000-000000000000

rawTimestamps	bool	Нет	Отображать timestamp'ы в исходном виде - Milliseconds since EPOCH. По умолчанию false.	true или false
emptyFields	bool	Нет	Отображать пустые поля нормализованных событий. По умолчанию false.	true или false

Period

Имя	Тип данных	Обязательный	Описание	Пример значения
from	string	Да	Нижняя граница периода в формате RFC3339. Timestamp >= <from>	2021-09-06T00:00:00Z (UTC) 2021-09-06T00:00:00.000Z (UTC, с указанием миллисекунд) 2021-09-06T00:00:00Z+00:00 (MSK)
to	string	Да	Верхняя граница периода в формате RFC3339. Timestamp <= <to>	2021-09-06T00:00:00Z (UTC) 2021-09-06T00:00:00.000Z (UTC, с указанием миллисекунд) 2021-09-06T00:00:00Z+00:00 (MSK)

Ответ

HTTP-код: 200

Формат: JSON

Результат выполнения SQL-запроса

Возможные ошибки

HTTP-код	Описание	Значение поля message	Значение поля details
400	Нижняя граница диапазона не указана	period.from required	
400	Нижняя граница диапазона указана в неподдерживаемом формате	cannot parse period.from	вариативное
400	Нижняя граница диапазона равна нулю	period.from cannot be 0	
400	Верхняя граница диапазона не указана	period.to required	
400	Верхняя граница диапазона указана в неподдерживаемом формате	cannot parse period.to	вариативное
400	Верхняя граница диапазона равна нулю	period.to cannot be 0	
400	Нижняя граница диапазона больше верхней	period.from cannot be greater than period.to	
400	Неверный SQL запрос	invalid sql	вариативное
400	В SQL запросе фигурирует неверная таблица	the only valid table is `events`	
400	В SQL запросе отсутствует LIMIT	sql: LIMIT required	
400	LIMIT в SQL запросе превышает максимальный (1000)	sql: maximum LIMIT is 1000	
404	Storage cluster не найден	cluster not found	
406	Параметр clusterID не был указан и в KUMA зарегистрировано множество кластеров	multiple clusters found, please provide clusterID	
500	Нет доступных нод кластера	no nodes available	
50x	Любые другие внутренние ошибки	event search failed	вариативное

Просмотр информации о кластере

GET /api/v1/events/clusters

Доступ: администратор, аналитик, оператор.

Кластеры главного тенанта доступны всем пользователям.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательный	Описание	Пример значения
page	number	Нет	Номер страницы. Начинается с 1. Размер страницы – 250 записей. Если параметр не указан, то используется значение по умолчанию – 1.	1
id	string	Нет	Идентификатор кластера. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ	00000000-0000-0000-0000-000000000000
tenantID	string	Нет	Идентификатор тенанта. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ. Если пользователь не имеет необходимой роли в указанном тенанте, то данный тенант игнорируется.	00000000-0000-0000-0000-000000000000
name	string	Нет	Имя кластера. Регистронезависимое регулярное выражение (PCRE).	cluster ^My cluster$

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Cluster


type Cluster struct {
    ID         string `json:"id"`
    Name       string `json:"name"`
    TenantID   string `json:"tenantID"`
    TenantName string `json:"tenantName"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message	Значение поля details
400	Неверное значение параметра page	invalid query parameter value	page
500	Любые другие внутренние ошибки	вариативное	вариативное

Поиск ресурсов

GET /api/v1/resources

Доступ: администратор, аналитик, оператор.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательный	Описание	
page	number	Нет	Номер страницы. Начинается с 1. Размер страницы – 250 записей. Если параметр не указан, то используется значение по умолчанию – 1.	1
id	string	Нет	Идентификатор ресурса. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	00000000-0000-0000-0
tenantID	string	Нет	Идентификатор тенанта ресурса. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ. Если пользователь не имеет необходимой роли в указанном тенанте, то данный тенант игнорируется.	00000000-0000-0000-0
name	string	Нет	Имя ресурса. Регистронезависимое регулярное выражение (PCRE).	resource ^My resource$

kind	string	Нет	Тип ресурса. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ	collector, correlator, storag enrichmentRule, destinatio

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Resource


type Resource struct {
    ID          string `json:"id"`
    Kind        string `json:"kind"`
    Name        string `json:"name"`
    Description string `json:"description"`
    TenantID    string `json:"tenantID"`
    TenantName  string `json:"tenantName"`
    UserID      string `json:"userID"`
    UserName    string `json:"userName"`
    Created     string `json:"created"`
    Updated     string `json:"updated"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message	Значение поля details
400	Неверное значение параметра page	invalid query parameter value	page
400	Неверное значение параметр kind	invalid kind	<kind>
500	Любые другие внутренние ошибки	вариативное	вариативное

Загрузка файла с ресурсами

POST /api/v1/resources/upload

Доступ: администратор, аналитик.

> Пользователи с ролью аналитик первой линии не могут использовать этот метод.

Тело запроса

Зашифрованное содержимое файла с ресурсами в бинарном формате.

Ответ

HTTP-код: 200

Формат: JSON

Идентификатор файла. Следует указать его в теле запросов на просмотр содержимого файла и на импорт ресурсов.

```
type Response struct {
    ID string `json:"id"`
```

```
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message	Значение поля details
400	Размер файла превышает максимально допустимый (64 МБ)	maximum file size is 64 MB	
403	Пользователь не имеет необходимых ролей ни в одном из тенантов	access denied	
500	Любые другие внутренние ошибки	вариативное	вариативное

Просмотр содержимого файла с ресурсами

POST /api/v1/resources/toc

Доступ: администратор, аналитик, оператор.

> Пользователи с ролью аналитик первой линии не могут использовать этот метод.

Тело запроса

Формат: JSON

Имя	Тип данных	Обязательный	Описание	Пример значения
fileID	string	Да	Идентификатор файла, полученный в результате выполнения загрузки файла с ресурсами.	00000000-0000-0000-0000-000000000000
password	string	Да	Пароль файла с ресурсами.	SomePassword!88

Ответ

HTTP-код: 200

Формат: JSON

Версия файла, список ресурсов, категорий, папок.

Идентификатор полученных ресурсов необходимо использовать при импорте.

```
type Package struct {
    Version         string                        `json:"version"`
    AssetCategories []*categories.Category        `json:"assetCategories"`
    Folders         []*folders.Folder             `json:"folders"`
    Resources       []*resources.ExportedResource `json:"resources"`
}
```

Импорт ресурсов

POST /api/v1/resources/import

Доступ: администратор, аналитик.

Тело запроса

Имя	Тип данных	Обязательный	Описание	Пример значения
fileID	string	Да	Идентификатор файла, полученный в результате выполнения загрузки файла с ресурсами.	00000000-0000-000 0000-00000000000

password	string	Да	Пароль файла с ресурсами.	SomePassword!88
tenantID	string	Да	Идентификтор целевого тенанта	00000000-0000-000 0000-00000000000

actions	map[string]uint8	Да	Маппинг идентификатора ресурса к действию, которое нужно предпринять в отношении него.	0 – не импортировать (используется при разрешении конфликт
				1 – импортировать (изначально должно б присвоено каждому ресурсу)
				2 – заменить (используется при разрешении конфликт
				
				{
				"00000000-0000-0000-0000-000000000000": 0
				"00000000-0000-0000-0000-000000000001": 1
				"00000000-0000-0000-0000-000000000002": 2
				}

Ответ

HTTP-код	Тело
204	

409	Идентификаторы импортируемых ресурсов, конфликтующих с уже существующими по ID. В этом случае необходимо повторить операцию импорта, указав для данных ресурсов следующие действия:
	0 – не импортировать
	2 – заменить
	`type ImportConflictsError struct {`
	`HardConflicts []string `json:"conflicts"``
	`}`

Экспорт ресурсов

POST /api/v1/resources/export

Доступ: администратор, аналитик.

> Пользователи с ролью аналитик первой линии не могут использовать этот метод.

Тело запроса

Формат: JSON

Имя	Тип данных	Обязательный	Описание	Пример значения
ids	[]string	Да	Идентификаторы ресурсов, которые необходимо экспортировать	["00000000-0000-0000-0000-000000000000"]
password	string	Да	Пароль файла с экспортированными ресурсами	SomePassword!88

tenantID	string	Да	Идентификатор тенанта, которому принадлежат экспортируемые ресурсы	00000000-0000-0000-0000-000000000000

Ответ

HTTP-код: 200

Формат: JSON

Идентификатор файла с экспортированными ресурсами. Следует использовать его в запросе на скачивание файла с ресурсами.

```
type ExportResponse struct {
    FileID string `json:"fileID"`
}
```

Скачивание файла с ресурсами

GET /api/v1/resources/download/<id>

Здесь id – идентификатор файла, полученный в результате выполнения запроса на экспорт ресурсов.

Доступ: администратор, аналитик.

> Пользователи с ролью аналитик первой линии не могут использовать этот метод.

Ответ

HTTP-код: 200

Зашифрованное содержимое файла с ресурсами в бинарном формате.

Возможные ошибки

HTTP-код	Описание	Значение поля message	Значение поля details
400	Не указан идентификатор файла	route parameter required	id
400	Идентификатор файла не является валидным UUID	id is not a valid UUID	
403	Пользователь не имеет необходимых ролей ни в одном из тенантов	access denied	
404	Файл не найден	file not found	
406	Файл является директорией	not regular file	
500	Любые другие внутренние ошибки	вариативное	вариативное

Поиск сервисов

GET /api/v1/services

Доступ: администратор, аналитик.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательный	Описание	Пример значен
page	number	Нет	Номер страницы. Начинается с 1. Размер страницы – 250 записей. Если параметр не указан, то используется значение по умолчанию – 1.	1

id	string	Нет	Идентификатор сервиса. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	00000000-0000-000(000000000000
tenantID	string	Нет	Идентификатор тенанта сервиса. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ. Если пользователь не имеет необходимой роли в указанном тенанте, то данный тенант игнорируется.	00000000-0000-000(000000000000
name	string	Нет	Имя сервиса. Регистронезависимое регулярное выражение (PCRE).	service ^My service$
kind	string	Нет	Тип сервиса. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	collector, correlator, sto
fqdn	string	Нет	FQDN сервиса. Регистронезависимое регулярное выражение (PCRE).	hostname ^hostname.example.com

paired	bool	Нет	Выводить только те сервисы, которые выполнили первый запуск. Если параметр присутствует в URL query, его значение принимается за true. Указанные пользователем значения игнорируются. Пример: /api/v1/services?paired

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Service


type Service struct {
    ID         string `json:"id"`
    TenantID   string `json:"tenantID"`
    TenantName string `json:"tenantName"`
    ResourceID string `json:"resourceID"`
    Kind       string `json:"kind"`
    Name       string `json:"name"`
    Address    string `json:"address"`
    FQDN       string `json:"fqdn"`
    Status     string `json:"status"`
    Warning    string `json:"warning"`
    APIPort    string `json:"apiPort"`
```

```
    Uptime     string `json:"uptime"`
    Version    string `json:"version"`
    Created    string `json:"created"`
    Updated    string `json:"updated"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message	Значение поля details
400	Неверное значение параметра page	invalid query parameter value	page
400	Неверное значение параметр kind	invalid kind	<kind>
500	Любые другие внутренние ошибки	вариативное	вариативное

Поиск тенантов

GET /api/v1/tenants

Выводятся только доступные пользователю тенанты.

Доступ: администратор, аналитик.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательный	Описание	Пример значения

page	number	Нет	Номер страницы. Начинается с 1. Размер страницы – 250 записей. Если параметр не указан, то используется значение по умолчанию – 1.	1
id	string	Нет	Идентификатор тенанта. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	00000000-0000-0000-0000-000000000000
name	string	Нет	Название тенанта. Регистронезависимое регулярное выражение (PCRE).	tenant ^My tenant$
main	bool	Нет	Вывести только основной тенант. Если параметр присутствует в URL query, его значение принимается за true. Указанные пользователем значения игнорируются. Пример: /api/v1/tenants?main	

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Tenant


type Tenant struct {
    ID          string `json:"id"`
    Name        string `json:"name"`
```

```
    Main        bool   `json:"main"`
    Description string `json:"description"`
    EPS         uint64 `json:"eps"`
    EPSLimit    uint64 `json:"epsLimit"`
    Created     string `json:"created"`
    Updated     string `json:"updated"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message	Значение поля details
400	Неверное значение параметра page	invalid query parameter value	page
500	Любые другие внутренние ошибки	вариативное	вариативное

Просмотр информации о предъявителе токена

GET /api/v1/users/whoami

Ответ

HTTP-код: 200

Формат: JSON

```
type Response struct {
    ID      string         `json:"id"`
    Name    string         `json:"name"`
```

```
    Login   string         `json:"login"`
    Email   string         `json:"email"`
    Tenants []TenantAccess `json:"tenants"`
}

type TenantAccess struct {
    ID   string `json:"id"`
    Name string `json:"name"`
    Role string `json:"role"`
}
```

Обновление словаря в сервисах

POST /api/v1/dictionaries/update

Обновить можно только словари в ресурсах словарей типа таблица.

Доступ: администратор, аналитик.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательный	Описание	Пример значения
collectorID	string	Нет	ID коллекторов, на которых будет обновлен словарь. Возможно указать несколько значений, тогда словарь будет обновлен на каждом из сервисов.	00000000-0000-0000-0000-000000000000

correlatorID	string	Нет	ID корреляторов, на которых будет обновлен словарь. Возможно указать несколько значений, тогда словарь будет обновле на каждом из сервисов.	00000000-0000-0000-0000-000000000000
dictionaryID	string	Да	ID словаря, который будет обновлен.	00000000-0000-0000-0000-000000000000

Если обновление на одном из сервисов заканчивается ошибкой, это не прерывает обновления на других сервисах.

Тело запроса

Имя поля multipart	Тип данных	Обязательный	Описание	Пример значения
file	CSV-файл	Да	Запрос содержит CSV-файл. Данные существующего словаря заменяются на данные этого файла. Первая строка CSV-файла с названиями столбцов не должна меняться.	key columns,column1,column2 key1,k1col1,k1col2 key2,k2col1,k2col2

Ответ

HTTP-код: 200

Формат: JSON

```
type Response struct {
```

```
ServicesFailedToUpdate []UpdateError `json:"servicesFailedToUpdate"`

}

type UpdateError struct {

ID string `json:"id"`

Err error `json:"err"`

}
```

Возвращает только ошибки для сервисов, на которых словари не были обновлены.

Возможные ошибки

HTTP-код	Описание	Значение поля message	Значение поля details
400	Неверное тело запроса	request body decode failed	возникшая ошибка
400	Нулевое количество строк словаря	request body required	
400	Не указан ID словаря	invalid value	dictionaryID
400	Некорректное значение строки словаря	invalid value	rows или rows[i]
400	Словарь с указанным ID имеет неверный вид (не таблица)	can only update table dictionary	
400	Попытка изменить столбцы словаря	columns must not change with update	
403	Нет доступа к запрашиваемому ресурсу	access denied	
404	Сервис не найден	service not found	
404	Словарь не найден	dictionary not found	идентификатор сервиса
500	Любые другие внутренние ошибки	вариативное	вариативное

Получение словаря

GET /api/v1/dictionaries

Получить можно только словари в ресурсах словарей типа таблица.

Доступ: администратор, аналитик.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательный	Описание	Пример значения
dictionaryID	string	Да	ID словаря, который будет получен	00000000-0000-0000-0000-000000000000

Ответ

HTTP-код: 200

Формат: text/plain; charset=utf-8

Возвращается CSV-файл с данными словаря в теле ответа.

Просмотр пользовательских полей активов

GET /api/v1/settings/id/:id

Пользователь может просматривать список пользовательских полей, сделанных пользователем KUMA в веб-интерфейсе программы.

Пользовательское поле представляет из себя контейнер для ввода текста. При необходимости может использоваться значение по умолчанию и маска для проверки корректности вводимого текста в формате https://pkg.go.dev/regexp/syntax. Все символы косой черты в маске необходимо дополнительно экранировать.

Доступ: администратор, аналитик, оператор.

Параметры запроса

Имя	Тип данных	Обязательный	Описание	Пример значения
id	string	Да	Идентификатор конфигурации пользовательских полей	00000000-0000-0000-0000-000000000000

Ответ

HTTP-код: 200

Формат: JSON

```
type Settings struct {
    ID           string         `json:"id"`
    TenantID     string         `json:"tenantID"`
    TenantName   string         `json:"tenantName"`
    Kind         string         `json:"kind"`
    UpdatedAt    int64          `json:"updatedAt"`
    CreatedAt    int64          `json:"createdAt"`
    Disabled     bool           `json:"disabled"`
    CustomFields []*CustomField `json:"customFields"`
}

type CustomField struct {
    ID      string `json:"id"`
    Name    string `json:"name"`
    Default string `json:"default"`
```

```
    Mask    string `json:"mask"`

}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message	Значение поля details
404	Параметры не найдены: неверный идентификатор или параметров нет	Not found in database	null
500	Любые другие внутренние ошибки	вариативное	вариативное

Создание резервной копии Ядра KUMA

GET /api/v1/system/backup

Доступ: главный администратор.

Запрос не имеет параметров.

В ответ на запрос возвращается архив tar.gz, содержащий резервную копию Ядра KUMA. На хосте, где установлено Ядро, резервная копия не сохраняется. Сертификаты включаются в состав резервной копии.

Если операция выполнена успешно, создается событие аудита со следующими параметрами:

- `DeviceAction = "Core backup created"`
- `SourceUserID = "<user-login>"`

Восстановить Ядра KUMA из резервной копии можно с помощью API-запроса `POST /api/v1/system/restore`.

Восстановление Ядра KUMA из резервной копии

POST /api/v1/system/restore

Доступ: главный администратор.

Запрос не имеет параметров.

Тело запроса должно содержать архив с резервной копией Ядра KUMA, полученный в результате выполнения API-запроса `GET /api/v1/system/backup`.

После получения архива с резервной копией KUMA выполняет следующие действия:

1. Распаковывает архив с резервной копией Ядра KUMA во временную директорию.
2. Сравнивает версию текущей KUMA и с версией резервной копии KUMA. Восстановление данных из резервной копии доступно только при сохранении версии KUMA.

   Если версии соответствуют друг другу, создается событие аудита со следующими параметрами:

   - `DeviceAction = "Core restore scheduled"`
   - `SourceUserID = "<имя пользователя инициировавшего восстановление KUMA из резервной копии"`
3. Если версии не различаются, выполняет восстановление данных из резервной копии Ядра KUMA.
4. Удаляет временную директорию и стартует в штатном режиме.

   В журнале Ядра KUMA появится запись "WARN: restored from backup".

После восстановления Ядра KUMA веб-интерфейсе программы в разделе **Ресурсы** → **Активные сервисы** необходимо выбрать все сервисы и нажать на кнопку **Сбросить сертификат**, а затем установить сервисы заново с теми же портами и идентификаторами.

Приложения

В этом разделе представлены приложения к основному тексту документа.

Команды для запуска и установки компонентов вручную

В этом разделе описаны параметры исполняемого файла KUMA /opt/kaspersky/kuma/kuma, с помощью которого можно вручную запустить или установить компоненты KUMA. Это может пригодиться в случае, если вам нужно увидеть выходные данные в консоли операционной системы сервера.

Параметры команд

Команды	Описание

`tools`	Запуск инструментов управления KUMA.
`collector`	Установка, запуск или удаление сервиса коллектора.
`core`	Установка, запуск или удаление сервиса Ядра.
`correlator`	Установка, запуск или удаление сервиса коррелятора.
`agent`	Установка, запуск или удаление сервиса агента.
`help`	Получение информации о доступных командах и параметрах.
`license`	Получение информации о лицензии.
`storage`	Запуск или установка Хранилища.
`version`	Получение информации о версии 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 KUMA.
- `kuma core -h` – получение справки по команде `core` установщика KUMA.
- `kuma collector --core <адрес сервера, где должен получить свои параметры коллектор> --id <идентификатор устанавливаемого сервиса> --api.port <порт>` используется для запуска установки сервиса коллектора.

Проверка целостности файлов KUMA

Целостность компонентов KUMA проверяется с помощью набора скриптов, основанных на инструменте integrity_checker, расположенных в директории /opt/kaspersky/kuma/integrity/bin. При проверке целостности используются xml-файлы манифестов из директории /opt/kaspersky/kuma/integrity/manifest/*, подписанные криптографической сигнатурой "Лаборатории Касперского".

Для запуска инструмента проверки целостности необходима учетная запись с правами не ниже прав учетной записи kuma.

Проверка целостности выполняется раздельно для компонентов KUMA и должна выполняться раздельно на серверах с соответствующими компонентами. При проверке целостности также проверяется целостность использованного xml-файла.

Чтобы проверить целостность файлов компонентов:

1. Перейдите в директорию, содержащую набор скриптов с помощью следующей команды:

   `cd /opt/kaspersky/kuma/integrity/bin`

2. Выполните команду из таблицы ниже, в зависимости от того, целостность какого компонента KUMA вы хотите проверить:

   - `./check_all.sh` – компоненты Ядра KUMA и хранилища;
   - `./check_core.sh` – компоненты Ядра KUMA;
   - `./check_collector.sh` – компоненты коллектора KUMA;
   - `./check_correlator.sh` – компоненты коррелятора KUMA;
   - `./check_storage.sh` – компоненты хранилища;
   - `./check_kuma_exe.sh <полный путь к файлу kuma.exe без указания имени файла> –` агент KUMA для Windows. Стандартное расположение исполняемого файла агента на устройстве Window: C:\Program Files\Kaspersky Lab\KUMA\.

   Целостность файлов компонентов будет проверена.

Результат проверки каждого компонента отображается в следующем формате:

- Блок Summary описывает количество проверенных объектов со статусом проверки: целостность не подтверждена/объект пропущен/целостность подтверждена:
  - Manifests – количество обработанных файлов манифеста.
  - Files – количество обработанных файлов KUMA.
  - Directories – при проверке целостности KUMA не используется.
  - Registries – при проверке целостности KUMA не используется.
  - Registry values – при проверке целостности KUMA не используется.
- Результат проверки целостности компонента:
  - SUCCEEDED – целостность подтверждена.
  - FAILED – целостность нарушена.

Модель данных нормализованного события

В этом разделе вы можете найти модель данных нормализованного события KUMA. Все события, которые обрабатываются корреляторами KUMA с целью обнаружения алертов, должны соответствовать этой модели.

События, несовместимые с этой моделью данных, необходимо преобразовывать в этот формат (нормализовать) с помощью коллекторов.

Модель данных нормализованного события

Название поля	Тип значения	Описание
Поля внутреннего стандарта		
ID	Строка	Уникальный идентификатор события типа UUID. Никогда не меняет своего значения Для базового события, генерируемого на коллекторе, идентификатор генерируется коллектором. Идентификатор корреляционного события генерируется коррелятором.
Timestamp	Число, timestamp	Время создания базового и корреляционного событий в коллекторе. Время создания корреляционного события в корреляторе. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
TenantID	Строка	Идентификатор тенанта.
ServiceID	Строка	Идентификатор экземпляра сервиса: коррелятора, коллектора, хранилища.
ServiceName	Строка	Название экземпляра сервиса, задается администратором KUMA при создании сервиса.

AggregationRuleName	Строка	Название правила агрегации, которое обработало событие.
AggregationRuleID	Строка	Идентификатор правила агрегации, которое обработало событие.
CorrelationRuleName	Строка	Название правила корреляции, по которому было создано корреляционное событие. Заполняется только для корреляционного события.
CorrelationRuleID	Строка	Идентификатор правила корреляции, по которому было создано корреляционное событие. Заполняется только для корреляционного события.
GroupedBy	Вложенный список строк	Список названий полей, по которым была группировка в корреляционном правиле. Заполняется только для корреляционного события.
Priority	Число	Уровень важности события.
Code	Строка	В базовом событии это код возврата процесса, функции или операции из источника. В корреляционном событии в это поле записывается код алерта для первой линии поддержки, либо код шаблона уведомления, которое будет отправлено.
Tactic	Строка	Название тактики из MITRE.
Technique	Строка	Название техники из MITRE.

ReplayID	Строка	Идентификатор ретроспективной проверки, в процессе которой было создано событие.
Raw	Строка	Неизмененный текст исходного, "сырого" события.
SourceAssetID	Строка	Идентификатор целевого актива.
DestinationAssetID	Строка	Идентификатор актива-источника.
DeviceAssetID	Строка	Идентификатор актива.
SourceAccountID	Строка	Идентификатор целевой учетной записи.
DestinationAccountID	Строка	Идентификатор учетной записи-источника.
SpaceID	Строка	Идентификатор пространства.
BaseEvents	Вложенный список [Event]	Вложенная структура со списком базовых событий. Поле может быть заполнено у корреляционных событий.
TI	Вложенный словарь [строка:строка]	Поле, в котором в формате словаря содержатся категории, полученные от внешнего источника Threat Intelligence по индикаторам из события.
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.

AffectedAssets	Вложенная структура [Affected]	Вложенная структура, из которой можно обратиться к связанным с алертам активам и учетным записям, а также узнать, сколько раз они фигурируют в событиях алерта.
Поля по стандарту CEF		
DeviceVendor	Строка	Название производителя источника журнала. Значение берется из "сырого" события. DeviceVendor, DeviceProduct и DeviceVersion однозначно идентифицируют источник журнала.
DeviceProduct	Строка	Название продукта из источника журнала. Значение берется из "сырого" события. DeviceVendor, DeviceProduct и DeviceVersion однозначно идентифицируют источник журнала.
DeviceVersion	Строка	Версия продукта из источника журнала. Значение берется из "сырого" события. DeviceVendor, DeviceProduct и DeviceVersion однозначно идентифицируют источник журнала.
DeviceEventClassID	Строка	Уникальный идентификатор типа события из источника журнала. Некоторые источники журнала определяют категорию событий.
Name	Строка	Название события в "сыром" событии.
Severity	Строка	Уровень важности ошибки из "сырого" события.

DeviceAction	Строка	Действие, совершенное устройством или предпринятое источником журнала. Например, blocked, detected.
ApplicationProtocol	Строка	Протокол уровня приложений, например HTTP, Telnet.
DeviceCustomIPv6Address1	Строка	Поле для отображения значения адреса IPv6, которое не может быть сопоставлено любому другому элементу модели данных. Может использоваться для обработки журналов сетевых устройств, где необходимо отличать IP-адреса разных устройств (например, для брандмауэров). Поле настраивается.
DeviceCustomIPv6Address1Label	Строка	Описание назначения поля DeviceCustomIPv6Address1.
DeviceCustomIPv6Address2	Строка	Поле для отображения значения адреса IPv6, которое не может быть сопоставлено любому другому элементу модели данных. Может использоваться для обработки журналов сетевых устройств, где необходимо отличать IP-адреса разных устройств (например, для брандмауэров). Поле настраивается.
DeviceCustomIPv6Address2Label	Строка	Описание назначения поля DeviceCustomIPv6Address2.

DeviceCustomIPv6Address3	Строка	Поле для отображения значения адреса IPv6, которое не может быть сопоставлено любому другому элементу модели данных. Может использоваться для обработки журналов сетевых устройств, где необходимо отличать IP-адреса разных устройств (например, для брандмауэров). Поле настраивается.
DeviceCustomIPv6Address3Label	Строка	Описание назначения поля DeviceCustomIPv6Address3.
DeviceCustomIPv6Address4	Строка	Поле для отображения значения адреса IPv6, которое не может быть сопоставлено любому другому элементу модели данных. Может использоваться для обработки журналов сетевых устройств, где необходимо отличать IP-адреса разных устройств (например, для брандмауэров). Поле настраивается.
DeviceCustomIPv6Address4Label	Строка	Описание назначения поля DeviceCustomIPv6Address4.
DeviceEventCategory	Строка	Категория "сырого" события из схемы определения категорий событий источника журнала.
DeviceCustomFloatingPoint1	Число	Поле для значения типа Float, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.

DeviceCustomFloatingPoint1Label	Строка	Описание назначения поля DeviceCustomFloatingPoint1.
DeviceCustomFloatingPoint2	Число	Поле для значения типа Float, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomFloatingPoint2Label	Строка	Описание назначения поля DeviceCustomFloatingPoint2.
DeviceCustomFloatingPoint3	Число	Поле для значения типа Float, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomFloatingPoint3Label	Строка	Описание назначения поля DeviceCustomFloatingPoint3.
DeviceCustomFloatingPoint4	Число	Поле для значения типа Float, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomFloatingPoint4Label	Строка	Описание назначения поля DeviceCustomFloatingPoint4.
DeviceCustomNumber1	Число	Поле для целочисленного значения, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomNumber1Label	Строка	Описание назначения поля DeviceCustomNumber1.
DeviceCustomNumber2	Число	Поле для целочисленного значения, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.

DeviceCustomNumber2Label	Строка	Описание назначения поля DeviceCustomNumber2.
DeviceCustomNumber3	Число	Поле для целочисленного значения, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomNumber3Label	Строка	Описание назначения поля DeviceCustomNumber3.
BaseEventCount	Число	Количество базовых событий, объединенных в агрегированном событии.
DeviceCustomString1	Строка	Поле для строкового значения, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomString1Label	Строка	Описания назначения поля DeviceCustomString1.
DeviceCustomString2	Строка	Поле для строкового значения, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomString2Label	Строка	Описания назначения поля DeviceCustomString2.
DeviceCustomString3	Строка	Поле для строкового значения, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomString3Label	Строка	Описания назначения поля DeviceCustomString3.

DeviceCustomString4	Строка	Поле для строкового значения, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomString4Label	Строка	Описания назначения поля DeviceCustomString4.
DeviceCustomString5	Строка	Поле для строкового значения, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomString5Label	Строка	Описания назначения поля DeviceCustomString5.
DeviceCustomString6	Строка	Поле для строкового значения, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomString6Label	Строка	Описания назначения поля DeviceCustomString6.
DestinationDnsDomain	Строка	DNS-часть полного доменного имени (FQDN) точки назначения, если "сырое" событие содержит сведения об отправителе и получателе данных. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationServiceName	Строка	Название сервиса на стороне приемника трафика. Например, "sshd". Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.

DestinationTranslatedAddress	Строка	IP-адрес устройства приемника трафика (после трансляции). Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationTranslatedPort	Число	Номер порта на устройстве приемника трафика (после трансляции адреса приемника). Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DeviceCustomDate1	Число, timestamp	Поле для значения типа Timestamp, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
DeviceCustomDate1Label	Строка	Поле для описания назначения поля DeviceCustomDate1.
DeviceCustomDate2	Число, timestamp	Поле для значения типа Timestamp, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.

DeviceCustomDate2Label	Строка	Поле для описания назначения поля DeviceCustomDate2.
DeviceDirection	Число	Поле для описания направления соединения из "сырого" события. • 0 – входящее соединение. • 1 – исходящее соединение.
DeviceDnsDomain	Строка	DNS-часть полного доменного имени (FQDN) IP-адреса устройства, с которого пришло "сырое" событие.
DeviceExternalID	Строка	Внешний уникальный идентификатор устройства, если такой передается в "сыром" событии.
DeviceFacility	Строка	Facility из "сырого" события, если есть. Например, в Syslog в поле Facility может передаваться название компоненты ОС, в которой произошла ошибка.
DeviceInboundInterface	Строка	Название интерфейса входящего соединения.
DeviceNtDomain	Строка	Доменное имя Windows устройства.
DeviceOutboundInterface	Строка	Название интерфейса исходящего соединения.
DevicePayloadID	Строка	Уникальный идентификатор полезной нагрузки, который ассоциирован с "сырым" событием.

DeviceProcessName	Строка	Название процесса из "сырого" события.
DeviceTranslatedAddress	Строка	Ретранслированный IP-адрес устройства, с которого пришло "сырого" событие.
DestinationHostName	Строка	Название хоста приемника трафика. Полное доменное имя приемника трафика, если доступно. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationMacAddress	Строка	MAC-адрес устройства приемника трафика. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationNtDomain	Строка	Доменное имя Windows устройства приемника трафика. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationProcessID	Число	Идентификатор системного процесса, ассоциированного с приемником трафика в "сыром" событии. Например, если в событии указано Process ID 105, то DestinationProcessId=105. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.

DestinationUserPrivileges	Строка	Названия пользовательских ролей, которые идентифицируют пользовательские привилегии на стороне точки назначения. Например, "User", "Guest", "Administrator". Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationProcessName	Строка	Название системного процесса в точке назначения. Например, "sshd", "telnet". Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationPort	Число	Номер порта на стороне точке назначения. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationAddress	Строка	IPv4-адрес точки назначения. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DeviceTimeZone	Строка	Часовой пояс устройства, на котором было сгенерировано событие.

		По умолчанию указывается часовой пояс системного времени коллектора или коррелятора. Если настроено обогащение события сведениями о часовом поясе, в поле указывается часовой пояс из правила обогащения. Если в "сыром" событии был указан часовой пояс источника события и при нормализации эти данные были сохранены, в поле события сохраняются сведения о часовом поясе источника события. Формат значения поля: +-чч:мм.
DestinationUserID	Строка	Идентификатор пользователя на стороне точки назначения. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationUserName	Строка	Имя пользователя на стороне точки назначения. Может содержать адрес электронной почты пользователя. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DeviceAddress	Строка	IPv4-адрес устройства, с которого получено событие.
DeviceHostName	Строка	Название хоста устройства, с которого было получено событие. Полное доменное имя устройства, если доступно.

DeviceMacAddress	Строка	MAC-адрес устройства, с которого было получено событие. Полное доменное имя устройства, если доступно.
DeviceProcessID	Число	Идентификатор системного процесса устройства, которое создало событие.
EndTime	Число	Время завершения события. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
ExternalID	Строка	Идентификатор устройства, которое создало событие.
FileCreateTime	Число	Время создания файла из события. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
FileHash	Строка	Хеш-код файла.
FileID	Строка	Идентификатор файла.
FileModificationTime	Число	Время последней модификации файла. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
FilePath	Строка	Путь к файлу, включая имя файла.
FilePermission	Строка	Список разрешений к файлу.
FileType	Строка	Тип файла. Например, application, pipe, socket.

FlexDate1	Число, timestamp	Поле для значения типа Timestamp, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
FlexDate1Label	Строка	Описание назначения поля flexDate1.
FlexString1	Строка	Поле для значения типа String, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
FlexString1Label	Строка	Описание назначения поля flexString1.
FlexString2	Строка	Поле для значения типа String, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
FlexString2Label	Строка	Описание назначения поля flexString2.
FlexNumber1	Число	Поле для целочисленного типа, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
FlexNumber1Label	Строка	Описание назначения поля flexNumber1.
FlexNumber2	Число	Поле для целочисленного типа, которое не может быть сопоставлено любому другому полю модели данных.

		Поле настраивается.
FlexNumber2Label	Строка	Описание назначения поля flexNumber2.
FileName	Строка	Имя файла, без указания пути к файлу.
FileSize	Число	Размер файла.
BytesIn	Число	Количество полученных источником и переданных получателю байтов. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
Message	Строка	Краткое описание ошибки или проблемы из "сырого" события.
OldFileCreateTime	Число	Время создания OLD-файла из события. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
OldFileHash	Строка	Хеш-код OLD-файла.
OldFileID	Строка	Идентификатор OLD-файла.
OldFileModificationTime	Число	Время последней модификации OLD-файла. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
OldFileName	Строка	Имя OLD-файла (без пути).

OldFilePath	Строка	Путь к OLD-файлу, включая имя файла.
OldFilePermission	Строка	Путь к OLD-файлу, включая имя файла.
OldFileSize	Число	Размер OLD-файла.
OldFileType	Строка	Тип файла. Например, application, pipe, socket.
BytesOut	Число	Количество отправленных байтов. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
EventOutcome	Строка	Результат выполнения действия. Например, "success", "failure".
TransportProtocol	Строка	Название протокола 4-уровня OSI (например, TCP, UDP).
Reason	Строка	Краткое описание причины аудита в сообщениях аудита.
RequestUrl	Строка	URL запроса.
RequestClientApplication	Строка	Агент, который обрабатывал запрос.
RequestContext	Строка	Описание контекста запроса.
RequestCookies	Строка	Файлы cookie, связанные с запросом.
RequestMethod	Строка	Метод, который использовался для доступа к веб-адресу (например, POST, GET).
DeviceReceiptTime	Число	Время получения события.

		Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
SourceHostName	Строка	Название хоста источника трафика. Полное доменное имя источника трафика, если доступно. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceDnsDomain	Строка	Доменное имя Windows-устройства источника трафика. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceServiceName	Строка	Название сервиса на стороне источника трафика. Например, "sshd". Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceTranslatedAddress	Строка	IPv4-адрес перехода источника. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceTranslatedPort	Число	Номер порта перехода на стороне источника. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.

SourceMacAddress	Строка	MAC-адрес устройства источника трафика. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceNtDomain	Строка	Доменное имя Windows устройства источника трафика. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceProcessID	Число	Идентификатор системного процесса, ассоциированного с источником трафика в "сыром" событии. Например, если в событии указано Process ID 105, то SourceProcessId=105. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceUserPrivileges	Строка	Названия пользовательских ролей, которые идентифицируют пользовательские привилегии на стороне источника. Например, "User", "Guest", "Administrator". Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceProcessName	Строка	Название системного процесса на стороне источника. Например, "sshd", "telnet".

		Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourcePort	Число	Номер порта на стороне источника. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceAddress	Строка	IPv4-адрес источника. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
StartTime	Число	Время, когда началось связанное с событием действие. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
SourceUserID	Строка	Идентификатор пользователя на стороне источника. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceUserName	Строка	Имя пользователя на стороне источника. Может содержать адрес электронной почты пользователя. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
Type	Число	Тип события. Доступны следующие значения: • 1 – базовое событие.

		• 2 – агрегированное событие. • 3 – корреляционное событие. • 4 – событие аудита. • 5 – событие мониторинга.
Поля с геоданными		
SourceCountry	Строка	Страна, соответствующая IPv4-адресу источника из поля SourceAddress.
SourceRegion	Строка	Регион, соответствующий IPv4-адресу источника из поля SourceAddress.
SourceCity	Строка	Город, соответствующий IPv4-адресу источника из поля SourceAddress.
SourceLatitude	Число	Долгота, соответствующая IPv4-адресу источника из поля SourceAddress.
SourceLongitude	Число	Широта, соответствующая IPv4-адресу источника из поля SourceAddress.
DestinationCountry	Строка	Страна, соответствующая IPv4-адресу точки назначения из поля DestinationAddress.
DestinationRegion	Строка	Регион, соответствующий IPv4-адресу точки назначения из поля DestinationAddress.
DestinationCity	Строка	Город, соответствующий IPv4-адресу точки назначения из поля DestinationAddress.

DestinationLatitude	Число	Долгота, соответствующая IPv4-адресу точки назначения из поля DestinationAddress.
DestinationLongitude	Число	Широта, соответствующая IPv4-адресу точки назначения из поля DestinationAddress.
DeviceCountry	Строка	Страна, соответствующая IPv4-адресу устройства из поля DeviceAddress.
DeviceRegion	Строка	Регион, соответствующий IPv4-адресу устройства из поля DeviceAddress.
DeviceCity	Строка	Город, соответствующий IPv4-адресу устройства из поля DeviceAddress.
DeviceLatitude	Число	Долгота, соответствующая IPv4-адресу устройства из поля DeviceAddress.
DeviceLongitude	Число	Широта, соответствующая IPv4-адресу устройства из поля DeviceAddress.

Вложенная структура `Affected`

Поле	Тип данных	Описание
`Assets`	Вложенный список `[AffectedRecord]`	Перечень и количество связанных с алертом активов.
`Accounts`	Вложенный список `[AffectedRecord]`	Перечень и количество связанных с алертом учетных записей.

Вложенная структура `AffectedRecord`

Поле	Тип данных	Описание
`Value`	Строка	Идентификатор актива или учетной записи.
`Count`	Число	Количество раз актив или учетная запись фигурирует в связанных с алертом событиях.

Модель данных алерта

В этом разделе описана модель данных алерта KUMA. Алерты создаются корреляторами при выявлении с помощью правил корреляции угроз безопасности информации. Алерты необходимо расследовать для устранения этих угроз.

Поле алерта	Тип данных	Описание
`ID`	Строка	Уникальный идентификатор алерта.
`TenantID`	Строка	Идентификатор тенанта, которому принадлежит алерт. Значение наследуется от коррелятора, создавшего алерт.
`TenantName`	Строка	Название тенанта.
`CorrelationRuleID`	Строка	Идентификатор правила, на основании которого был создан алерт.
`CorrelationRuleName`	Строка	Название правила корреляции, на основании которого был создан алерт.
`Status`	Строка	Статус алерта. Возможные значения: • `New` – новый алерт. • `Assigned` – алерт назначен пользователю. • `Closed` – алерт закрыт. • `Exported to IRP` – алерт выгружен IRP-систему для дальнейшего расследования.

		• `Escalated` – на основе алерта создан инцидент.
`Priority`	Число	Уровень важности алерта. Возможные значения: • 1–4 – Низкий. • 5–8 – Средний. • 9–12 – Высокий. • 13–16 – Критический.
`ManualPriority`	Строка `TRUE/FALSE`	Параметр, показывающий, как был определен уровень важности алерта. Возможные значения: • `true` – задан пользователем. • `false` (значение по умолчанию) – рассчитан автоматически.
`FirstSeen`	Число	Время создания первого корреляционного события из алерта.
`LastSeen`	Число	Время создания последнего корреляционного события из алерта.
`UpdatedAt`	Число	Дата последнего изменения параметров алерта.
`UserID`	Строка	Идентификатор пользователя KUMA, которому алерт назначен на рассмотрение.
`UserName`	Строка	Имя пользователя KUMA, которому алерт назначен на рассмотрение.
`GroupedBy`	Вложенный список строк	Перечень полей событий, по которым группировались событий в правиле корреляции.

`ClosingReason`	Строка	Причина закрытия алерта. Возможные значения: • `Incorrect Correlation Rule` – алерт был ложным, а полученные события не указывают на угрозу безопасности. Возможно, требуется коррекция правила корреляции. • `Incorrect Data` – алерт был ложным, а полученные события не указывают на угрозу безопасности. • `Responded` – были приняты необходимые меры по устранению угрозы безопасности.
`Overflow`	Строка `TRUE/FALSE`	Признак, обозначающий что алерт переполнен, то есть размер алерта и привязанных к нему событий превышает 16 МБ. Возможные значения: • `true` • `false`
`MaxAssetsWeightStr`	Строка	Максимальный уровень важности категорий активов, связанных с алертом.
`IntegrationID`	Строка	Идентификатор алерта в программе IRP / SOAR, если в KUMA настроена интеграция с такой программой.
`ExternalReference`	Строка	Ссылка на раздел в программе IRP / SOAR, в котором отображаются сведения об импортированном из KUMA алерте.

`IncidentID`	Строка	Идентификатор инцидента, к которому привязан алерт.
`IncidentName`	Строка	Название инцидента, к которому привязан алерт.
`SegmentationRuleName`	Строка	Название правила сегментации, по которому корреляционные события сгруппированы в алерте.
`BranchID`	Строка	Идентификатор ветви иерархии, в которой был создан алерт. Указывается при иерархическом развертывании KUMA.
`BranchName`	Строка	Название ветви иерархии, в которой был создан алерт. Указывается при иерархическом развертывании KUMA.
`Actions`	Вложенная структура `[Action]`	Вложенная структура со строками, в которых указаны изменения статусов и назначений алерта, пользовательские комментарии.
`Events`	Вложенная структура `[EventWrapper]`	Вложенная структура, из которой можно обратиться к связанным с алертом корреляционным событиям.
`Assets`	Вложенная структура `[Asset]`	Вложенная структура, из которой можно обратиться к связанным с алертом активам.
`Accounts`	Вложенная структура `[Account]`	Вложенная структура, из которой можно обратиться к связанным с алертом учетным записям.
`AffectedAssets`	Вложенная структура `[Affected]`	Вложенная структура, из которой можно обратиться к связанным с алертам активам и учетным записям, а также узнать, сколько раз они фигурируют в событиях алерта.

Вложенная структура `Affected`

Поле	Тип данных	Описание
`Assets`	Вложенный список `[AffectedRecord]`	Перечень и количество связанных с алертом активов.
`Accounts`	Вложенный список `[AffectedRecord]`	Перечень и количество связанных с алертом учетных записей.

Вложенная структура `AffectedRecord`

Поле	Тип данных	Описание
`Value`	Строка	Идентификатор актива или учетной записи.
`Count`	Число	Количество раз актив или учетная запись фигурирует в связанных с алертом событиях.

Вложенная структура `EventWrapper`

Поле	Тип данных	Описание
`Event`	Вложенная структура `[Event]`	Поля события.
`Comment`	Строка	Комментарий, добавленный при добавлении событий к алерту.
`LinkedAt`	Число	Дата добавления событий к алерту.

Вложенная структура `Action`

Поле	Тип данных	Описание
`CreatedAt`	Число	Дата, когда действие над алертом было произведено.
`UserID`	Строка	Идентификатор пользователя.
`Kind`	Строка	Тип действия.

`Value`	Строка	Значение.
`Event`	Вложенная структура [`Event`]	Поля события.
`ClusterID`	Строка	Идентификатор кластера.

Модель данных актива

Структура актива представлена полями, в которых содержатся значения. Поля также могут содержать вложенные структуры.

Поле актива	Тип значения	Описание
`ID`	Строка	Идентификатор актива.
`TenantName`	Строка	Название тенанта.
`DeletedAt`	Число	Дата удаления актива.
`CreatedAt`	Число	Дата создания актива.
`TenantID`	Строка	Идентификатор тенанта.
`DirectCategories`	Вложенный список строк	Категории актива.
`CategoryModels`	Вложенная структура [`Category`]	Изменение категорий актива.
`AffectedByIncidents`	Вложенный словарь: [`строка:строка TRUE/FALSE`]	Идентификаторы инцидентов.
`IPAddress`	Вложенный список строк	IP-адреса актива.
`FQDN`	Строка	FQDN актива.
`Weight`	Число	Уровень важности актива.
`Deleted`	Строка со значениями `TRUE/FALSE`	Помечен ли актив на удаление из KUMA.
`UpdatedAt`	Число	Дата последнего обновления актива.
`MACAddress`	Вложенный список строк	MAC-адреса актива.
`IPAddressInt`	Вложенный список чисел	IP-адрес в виде числа.

`Owner`	Вложенная структура `[OwnerInfo]`	Сведения о владельце актива.
`OS`	Вложенная структура `[OS]`	Сведения об операционной системы актива.
`DisplayName`	Строка	Название актива.
`APISoft`	Вложенная структура `[Software]`	ПО, установленное на активе.
`APIVulns`	Вложенная структура `[Vulnerability]`	Уязвимости актива.
`KICSServerIp`	Строка	IP-адрес сервера KICS for Networks.
`KICSConnectorID`	Число	Идентификатор коннектора KICS for Networks.
`KICSDeviceID`	Число	Идентификатор актива в KICS for Networks.
`KICSStatus`	Строка	Статус актива актива в KICS for Networks.
`KICSHardware`	Вложенная структура `[KICSSystemInfo]`	Аппаратные сведения об активе, полученные из KICS for Networks.
`KICSSoft`	Вложенная структура `[KICSSystemInfo]`	Сведения о ПО актива, полученные из KICS for Networks.
`KICSRisks`	Вложенная структура `[KICSRisk]`	Сведения об уязвимостях актива, полученные из KICS for Networks.
`Sources`	Вложенная структура `[Sources]`	Основные сведения об активе, поступавшие из разных источников.
`FromKSC`	Строка со значениями `TRUE/FALSE`	Индикатор, указывающий, что сведения об активе импортированы из KSC.
`NAgentID`	Строка	Идентификатор агента KSC, от которого получены сведения об активе.

`KSCServerFQDN`	Строка	FQDN сервера KSC.
`KSCInstanceID`	Строка	Идентификатор экземпляра KSC.
`KSCMasterHostname`	Строка	Имя хоста сервера KSC.
`KSCGroupID`	Число	Идентификатор группы KSC.
`KSCGroupName`	Строка	Название группы KSC.
`LastVisible`	Число	Дата, когда от KSC в последний раз были получены сведения об активе.
`Products`	Вложенный словарь: `[строка:вложенная структура [ProductInfo]]`	Сведения об установленных на активе приложениях Kaspersky, полученные из KSC.
`Hardware`	Вложенная структура `[Hardware]`	Аппаратные сведения об активе, полученные из KSC.
`KSCSoft`	Вложенная структура `[Software]`	Сведения о ПО актива, полученные из KSC.
`KSCVulns`	Вложенная структура `[Vulnerability]`	Сведения об уязвимостях актива, полученные из KSC.

Вложенная структура `Category`

Поле	Тип значения	Описание
`ID`	Строка	Идентификатор категории.
`TenantID`	Строка	Идентификатор тенанта.
`TenantName`	Строка	Название тенанта.
`Parent`	Строка	Родительская категория.
`Path`	Вложенный список строк	Структура категорий.
`Name`	Строка	Название категории.

`UpdatedAt`	Число	Последнее обновление категории.
`CreatedAt`	Число	Дата создания категории.
`Description`	Строка	Описание категории.
`Weight`	Число	Уровень важности категории.
`CategorizationKind`	Строка	Тип присвоения категории активам.
`CategorizationAt`	Число	Дата категоризации.
`CategorizationInterval`	Строка	Интервал присвоения категорий.

Вложенная структура `OwnerInfo`

Поле	Тип значения	Описание
`DisplayName`	Строка	Имя владельца актива.

Вложенная структура `OS`

Поле	Тип значения	Описание
`Name`	Строка	Название операционной системы.
`BuildNumber`	Число	Версия операционной системы.

Вложенная структура `Software`

Поле	Тип значения	Описание
`DisplayName`	Строка	Название ПО.
`DisplayVersion`	Строка	Версия ПО.
`Publisher`	Строка	Издатель ПО.

`InstallDate`	Строка	Дата установки.
`HasMSIInstaller`	Строка `TRUE/FALSE`	Признак, имеет ли ПО MSI-установщик.

Вложенная структура `Vulnerability`

Поле	Тип значения	Описание
`KasperskyID`	Строка	Идентификатор уязвимости, присвоенный Kaspersky.
`ProductName`	Строка	Название ПО.
`DescriptionURL`	Строка	URL с описанием уязвимости.
`RecommendedMajorPatch`	Строка	Рекомендуемое обновление.
`RecommendedMinorPatch`	Строка	Рекомендуемое обновление.
`SeverityStr`	Строка	Уровень важности уязвимости.
`Severity`	Число	Уровень важности уязвимости.
`CVE`	Вложенный список строк	Идентификатор уязвимости CVE.
`ExploitExists`	Строка `TRUE/FALSE`	Существует ли эксплойт.
`MalwareExists`	Строка `TRUE/FALSE`	Существует ли вредоносная программа.

Вложенная структура `KICSSystemInfo`

Поле	Тип значения	Описание
`Model`	Строка	Модель устройства.
`Version`	Строка	Версия устройства.
`Vendor`	Строка	Производитель.

Вложенная структура `KICSRisk`

Поле	Тип значения	Описание
`ID`	Число	Идентификатор риска KICS for Networks.
`Name`	Строка	Название риска.
`Category`	Строка	Тип риска.
`Description`	Строка	Описание риска.
`DescriptionUrl`	Строка	Ссылка на описание риска.
`Severity`	Число	Уровень важности риска.
`Cvss`	Число	Оценка CVSS.

Вложенная структура `Sources`

Поле	Тип значения	Описание
`KSC`	Вложенная структура `[SourceInfo]`	Сведения об активе, поступившие из KSC.
`API`	Вложенная структура `[SourceInfo]`	Сведения об активе, поступившие через REST API.
`Manual`	Вложенная структура `[SourceInfo]`	Сведения об активе, введенные вручную.
`KICS`	Вложенная структура `[SourceInfo]`	Сведения об активе, поступившие из KICS for Networks.

Вложенная структура `Sources`

Поле	Тип значения	Описание
`MACAddress`	Вложенный список строк	MAC-адреса актива.
`IPAddressInt`	Вложенный список чисел	IP-адрес в виде числа.

`Owner`	Вложенная структура `[OwnerInfo]`	Сведения о владельце актива.
`OS`	Вложенная структура `[OS]`	Сведения об операционной системы актива.
`DisplayName`	Строка	Название актива.
`IPAddress`	Вложенный список строк	IP-адреса актива.
`FQDN`	Строка	FQDN актива.
`Weight`	Число	Уровень важности актива.
`Deleted`	Строка со значениями `TRUE/FALSE`	Помечен ли актив на удаление из KUMA.
`UpdatedAt`	Число	Дата последнего обновления актива.

Вложенная структура `ProductInfo`

Поле	Тип значения	Описание
`ProductVersion`	Строка	Версия ПО.
`ProductName`	Строка	Название ПО.

Вложенная структура `Hardware`

Поле	Тип значения	Описание
`NetCards`	Вложенная структура `[NetCard]`	Перечень сетевых карт актива.
`CPU`	Вложенная структура `[CPU]`	Перечень процессоров актива.
`RAM`	Вложенная структура `[RAM]`	Перечень ОЗУ актива.
`Disk`	Вложенная структура `[Disk]`	Перечень дисков актива.

Вложенная структура `NetCard`

Поле	Тип значения	Описание
`ID`	Строка	Идентификатор сетевой карты.
`MACAddresses`	Вложенный список строк	MAC-адреса сетевой карты.
`Name`	Строка	Название сетевой карты.
`Manufacture`	Строка	Производитель сетевой карты.
`DriverVersion`	Строка	Версия драйвера.

Вложенная структура `RAM`

Поле	Тип значения	Описание
`Frequency`	Строка	Частота ОЗУ.
`TotalBytes`	Число	Объем ОЗУ в байтах.

Вложенная структура `CPU`

Поле	Тип значения	Описание
`ID`	Строка	Идентификатор процессора.
`Name`	Строка	Название процессора.
`CoreCount`	Строка	Количество ядер.
`CoreSpeed`	Строка	Частота.

Вложенная структура `Disk`

Поле	Тип значения	Описание
`FreeBytes`	Число	Свободное пространство на диске.
`TotalBytes`	Число	Общее пространство на диске.

Модель данных учетной записи

К полям учетной записи можно обращаться из шаблонов электронной почты, а также при корреляции событий.

Поле	Тип значения	Описание
`ID`	Строка	Идентификатор учетной записи.
`ObjectGUID`	Строка	Атрибут Active Directory. Идентификатор учетной записи в Active Directory.
`TenantID`	Строка	Идентификатор тенанта.
`TenantName`	Строка	Название тенанта.
`UpdatedAt`	Число	Последнее обновление учетной записи.
`Domain`	Строка	Домен.
`CN`	Строка	Атрибут Active Directory. Имя пользователя.
`DisplayName`	Строка	Атрибут Active Directory. Отображаемое имя пользователя. По этому атрибуту события можно искать при корреляции.
`DistinguishedName`	Строка	Атрибут Active Directory. Название объекта LDAP. По этому атрибуту события можно искать при корреляции.
`EmployeeID`	Строка	Атрибут Active Directory. Идентификатор сотрудника.
`Mail`	Строка	Атрибут Active Directory. Электронная почта пользователя. По этому атрибуту события можно искать при корреляции.

`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. По этому атрибуту события можно искать при корреляции.
`TelephoneNumber`	Строка	Атрибут Active Directory. Номер телефона.
`UserPrincipalName`	Строка	Атрибут Active Directory. Имя участника-пользователя. По этому атрибуту события можно искать при корреляции.
`Archived`	Строка `TRUE/FALSE`	Признак, определяющий, является ли учетная запись устаревшей.
`MemberOf`	Список строк	Атрибут Active Directory. Группы AD, в которые внесен пользователь. По этому атрибуту события можно искать при корреляции.
`PreliminarilyArchived`	Строка `TRUE/FALSE`	Признак, определяющий, требуется ли обозначить учетную запись как устаревшую.
`CreatedAt`	Число	Дата создания учетной записи.
`SN`	Строка	Атрибут Active Directory. Фамилия пользователя. По этому атрибуту события можно искать при корреляции.
`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. По этому атрибуту события можно искать при корреляции.
`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.

Поля событий аудита

События аудита создаются при выполнении в KUMA определенных действий, связанных с безопасностью, и используются для обеспечения целостности системы. Этот раздел содержит информацию о полях событий аудита.

Поля событий с общей информацией

Каждое событие аудита имеет поля событий, описанные ниже.

Название поля события	Значение поля
ID	Уникальный идентификатор события в виде UUID.
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 KUMA в формате `+-чч:мм`.
Type	Тип события аудита. Событию аудита соответствует значение `4`.
TenantID	Идентификатор главного тенанта.
DeviceVendor	`Kaspersky`
DeviceProduct	`KUMA`
EndTime	Время создания события.

Пользователь успешно вошел в систему или не смог войти

Название поля события	Значение поля
DeviceAction	`user login`
EventOutcome	`succeeded` или `failed` – статус зависит от исхода операции.
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.
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 успешно 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, 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.
SourceUserID	ID пользователя, который использовался для изменения данных.
DestinationUserName	Логин пользователя, данные которого были изменены.
DestinationUserID	ID пользователя, данные которого были изменены.
DeviceCustomString1	Текущее значение логина.

DeviceCustomString1Label	`new login`
DeviceCustomString2	Значение логина до его изменения.
DeviceCustomString2Label	`old login`

Роль пользователя успешно 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, 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.
SourceUserID	ID пользователя, который использовался для изменения данных.
DestinationUserName	Логин пользователя, данные которого были изменены.
DestinationUserID	ID пользователя, данные которого были изменены.
DeviceCustomString1	Текущее значение роли.
DeviceCustomString1Label	`new role`
DeviceCustomString2	Значение роли до ее изменения.
DeviceCustomString2Label	`old role`

Другие данные пользователя успешно 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, 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.
SourceUserID	ID пользователя, который использовался для изменения данных.
DestinationUserName	Логин пользователя, данные которого были изменены.
DestinationUserID	ID пользователя, данные которого были изменены.

Пользователь успешно 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.

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, 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.
SourceUserID	Идентификатор пользователя.

Пароль пользователя успешно 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, 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.
SourceUserID	ID пользователя, который использовался для изменения данных.
DestinationUserName	Логин пользователя, данные которого были изменены.
DestinationUserID	ID пользователя, данные которого были изменены.

Пользователь успешно 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, 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 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 успешно 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, 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, 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 успешно 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, 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 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`

Токен доступа пользователя успешно 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, 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.
SourceUserID	Идентификатор пользователя, который использовался для изменения данных.
DestinationUserName	Логин пользователя, данные которого были изменены.
DestinationUserID	Идентификатор пользователя, данные которого были изменены.

Сервис успешно 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, 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	ID сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Сервис успешно 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, 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 удаления сервиса.
SourceUserID	Идентификатор пользователя, который использовался для удаления сервиса.
DeviceExternalID	ID сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.
DestinationAddress	Адрес машины, с которой 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 успешно 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, 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 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 успешно 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, 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 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 успешно 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, который сообщил информацию о запуске сервиса. Это может быть адрес прокси-сервера, если информация передается через прокси.
SourcePort	Порт, передавший информацию о запуске сервиса. Это может быть порт прокси-сервера, если информация передается через прокси.
DeviceExternalID	ID сервиса.
DeviceProcessName	Название сервиса.

DeviceFacility	Тип сервиса.
DestinationAddress	Адрес машины, на которой был запущен сервис.
DestinationHostName	Полное доменное имя машины, на которой был запущен сервис.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Сервис успешно 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 был отправлен запрос на сопряжение сервисов. Это может быть адрес прокси-сервера, если запрос передается через прокси.
SourcePort	Порт, отправивший запрос на сопряжение сервисов. Это может быть порт прокси-сервера, если запрос передается через прокси.
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 машины, на которой был запущен сервис.
DestinationHostName	Полное доменное имя машины, на которой 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`

Раздел хранилища 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, 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 удаления.
SourceUserID	Идентификатор пользователя, который использовался для удаления.
Name	Имя индекса.
Message	`deleted by user`

Раздел хранилища автоматически удален в связи с истечением срока действия

Название поля события	Значение поля
DeviceAction	`partition deleted`
EventOutcome	`succeeded`
Name	Имя индекса
SourceServiceName	`scheduler`
Message	`deleted by retention period settings`

Активный лист успешно очищен или операция завершилась с ошибкой

Событию может быть присвоен статус `succeeded` или `failed`.

Поскольку запрос на очистку активного листа осуществляется через удаленное соединение, ошибка передачи данных может возникнуть в любой момент: до удаления или после удаления.

Это означает, что активный лист может быть очищен успешно, но событие все равно будет иметь статус `failed`, поскольку EventOutcome возвращает статус TCP/IP-соединения запроса, а не статус проверки, был ли очищен активные лист.

Название поля события	Значение поля

DeviceAction	`active list cleared`
EventOutcome	`succeeded` или `failed`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для очистки активного листа.
SourceUserID	Идентификатор пользователя, который использовался для очистки активного листа.
DeviceExternalID	Идентификатор сервиса, активные лист которого был очищен.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
Message	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Элемент активного листа успешно изменен или операция завершилась с ошибкой

Событию может быть присвоен статус `succeeded` или `failed`.

Поскольку запрос на изменение элемента активного листа осуществляется через удаленное соединение, ошибка передачи данных может возникнуть в любой момент: до изменения или после изменения.

Это означает, что элемент активного листа может быть изменен успешно, но событие все равно будет иметь статус `failed`, поскольку EventOutcome возвращает статус TCP/IP-соединения запроса, а не статус проверки, был ли изменен элемент активного листа.

Название поля события	Значение поля
DeviceAction	`active list item changed`
EventOutcome	`succeeded` или `failed`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, 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 элемента активного листа.
SourceUserID	Идентификатор пользователя, который использовался для изменения элемента активного листа.
DeviceExternalID	Идентификатор сервиса, активный лист которого был изменен.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
DeviceCustomString1	Название ключа.
DeviceCustomString1Label	`key`
Message	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	`tenant ID`

DeviceCustomString6	название тенанта
DeviceCustomString6Label	`tenant name`

Элемент активного листа успешно удален или операция завершилась с ошибкой

Событию может быть присвоен статус `succeeded` или `failed`.

Поскольку запрос на удаление элемента активного листа осуществляется через удаленное соединение, ошибка передачи данных может возникнуть в любой момент: до удаления или после удаления.

Это означает, что элемент активного листа может быть удален успешно, но событие все равно будет иметь статус `failed`, поскольку EventOutcome возвращает статус TCP/IP-соединения запроса, а не статус проверки, был ли удален элемент активного листа.

Название поля события	Значение поля
DeviceAction	`active list item deleted`
EventOutcome	`succeeded` или `failed`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, 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 удаления элемента активного листа.
SourceUserID	Идентификатор пользователя, который использовался для удаления элемента активного листа.
DeviceExternalID	Идентификатор сервиса, активный лист которого был очищен.
ExternalID	Идентификатор активного листа.

Name	Название активного листа.
DeviceCustomString1	Название ключа.
DeviceCustomString1Label	`key`
Message	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Активный лист успешно импортирован или операция завершилась с ошибкой

Импорт элементов активного листа выполняется по частям через удаленное подключение.

Поскольку импорт осуществляется через удаленное соединение, ошибка передачи данных может произойти в любой момент: когда данные частично или полностью импортированы. EventOutcome возвращает статус подключения, а не статус проверки импорта.

Название поля события	Значение поля
DeviceAction	`active list imported`
EventOutcome	`succeeded` или `failed`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, 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 выполнения импорта.

SourceUserID	Идентификатор пользователя, который использовался для импорта.
DeviceExternalID	Идентификатор сервиса, для которого был выполнен импорт.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
Message	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	название тенанта
DeviceCustomString6Label	`tenant name`

Активный лист успешно экспортирован

Название поля события	Значение поля
DeviceAction	`active list exported`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, 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 выполнения экспорта.
SourceUserID	Идентификатор пользователя, который использовался для экспорта.

DeviceExternalID	Идентификатор сервиса, для которого был выполнен экспорт.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	название тенанта
DeviceCustomString6Label	`tenant name`

Ресурс успешно 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, 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 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 успешно 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, 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 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 успешно 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, 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 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`

Актив успешно создан

Название поля события	Значение поля
DeviceAction	`asset created`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, 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 добавления актива.
SourceUserID	Идентификатор пользователя, который использовался для добавления актива.
DeviceExternalID	Идентификатор актива.
SourceHostName	Идентификатор актива.
Name	Название актива.
DeviceCustomString1	Разделенные запятыми IP-адреса актива.
DeviceCustomString1Label	`addresses`
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Актив успешно удален

Название поля события	Значение поля
DeviceAction	`asset deleted`
EventOutcome	`succeeded`

SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, 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 добавления актива.
SourceUserID	Идентификатор пользователя, который использовался для добавления актива.
DeviceExternalID	Идентификатор актива.
SourceHostName	Идентификатор актива.
Name	Название актива.
DeviceCustomString1	Разделенные запятыми IP-адреса актива.
DeviceCustomString1Label	`addresses`
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Категория актива успешно добавлена

Название поля события	Значение поля
DeviceAction	`category created`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.

SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, 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 добавления категории.
SourceUserID	Идентификатор пользователя, который использовался для добавления категории.
DeviceExternalID	Идентификатор категории.
Name	Название категории.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Категория актива успешно удалена

Название поля события	Значение поля
DeviceAction	`category deleted`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, 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 удаления категории.

SourceUserID	Идентификатор пользователя, который использовался для удаления категории.
DeviceExternalID	Идентификатор категории.
Name	Название категории.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Параметры успешно 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, 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 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 успешно 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, 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 тенанта.
SourceUserID	Идентификатор пользователя, который использовался для создания тенанта.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Тенант успешно 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 успешно 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 успешно 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

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	`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, 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.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`
Message	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке.

Ответ в Active Directory

Название поля события	Значение поля
DeviceAction	`ad response`
DeviceFacility	`manual response` или `automatic response`
EventOutcome	`succeeded` или `failed`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для изменения данных тенанта.

SourceUserID	Идентификатор пользователя, который использовался для изменения данных тенанта.
DeviceCustomString3	Наименование правила ответа: CHANGE_PASSWORD, ADD_TO_GROUP, REMOVE_FROM_GROUP, BLOCK_USER.
DeviceCustomString3Label	`response rule name`
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`
DestinationUserName	Учетная запись пользователя Active Directory, на которую вызван ответ (sAMAccountName).
DestinationNtDomain	Домен учетной записи пользователя Active Directory, на которую вызван ответ.
DestinatinUserID	UUID учетной записи в KUMA.
FlexString1	Информация о группе, куда был добавлен или удален пользователь.
FlexString1Label	`group DN`

Реагирование через KICS for Networks

Название поля события	Значение поля
DeviceAction	`KICS responce`
DeviceFacility	`manual response` или `automatic response`
EventOutcome	`succeeded` или `failed`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.

SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который отправил запрос.
SourceUserID	Идентификатор пользователя, который отправил запрос.
DeviceCustomString3	Наименование правила ответа: `Authorized`, `Not Authorized`.
DeviceCustomString3Label	`response rule name`
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`
DeviceExternalID	Идентификатор актива.
SourceHostName	FQDN актива.
Name	Название актива.
DeviceCustomString1	Перечень ip-адресов актива.
DeviceCustomString1Label	`addresses`

Реагирование через Kaspersky Automated Security Awareness Platform

Название поля события	Значение поля
DeviceAction	`KASAP response`
DeviceFacility	`manual response`
EventOutcome	`succeeded` или `failed`
Message	Описание ошибки, если произошла ошибка, иначе поле будет пустое.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.

SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который отправил запрос.
SourceUserID	Идентификатор пользователя, который отправил запрос.
DeviceCustomString1	Менеджер пользователя, на которого назначен курс.
DeviceCustomString1Label	`manager`
DeviceCustomString3	Информация о группе, где был пользователь. Отсутствует в случае `failed`.
DeviceCustomString3Label	`manager`
DeviceCustomString4	Информация о группе, куда добавили пользователя.
DeviceCustomString4Label	`new kasap group`
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`
DestinationUserID	Идентификатор учетной записи пользователя Active Directory, на которую происходит реагирование.
DestinationUserName	Имя учетной записи (sAMAccountName).
DestinationNtDomain	Домен учетной записи пользователя Active Directory, на которую происходит реагирование.

Реагирование через KEDR

Название поля события	Значение поля
DeviceAction	`KEDR response`
DeviceFacility	`manual response` или `automatic response`

EventOutcome	`succeeded` или `failed`
Message	Описание ошибки, если произошла ошибка, иначе поле будет пустое.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который отправил запрос.
SourceUserID	Идентификатор пользователя, который отправил запрос.
SourceAssetID	Идентификатор актива в KUMA, для которого производится реагирование. Значение не указывается, если реагирование производится по хешу или для всех активов.
DeviceExternalID	Параметр external ID, присвоенный KUMA в KEDR. Если external id один, при запуске по пользовательским хостам не заполняется.
DeviceCustomString1	Перечисление IP/FQDN-адресов актива для правила запрета для хоста по выбранному хешу из карточки события.
DeviceCustomString1Label	`user defined list of ips or hostnames`
DeviceCustomString2	Параметр sensor ID в KEDR (UUIDv4 | 'all' | 'custom').
DeviceCustomString2Label	`sensor id of asset in KATA/EDR`
ServiceID	Идентификатор сервиса, который вызвал реагирование. Заполняется только при автоматическом реагировании.
DeviceCustomString3	Наименование типа задачи: `enable_network_isolation`, `disable_network_isolation`, `enable_prevention`, `disable_prevention`, `run_process`.
DeviceCustomString3Label	`kedr response kind`

DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Настройка получения событий Auditd с помощью rsyslog

KUMA позволяет осуществлять мониторинг и проводить аудит событий Auditd на устройствах Linux с помощью rsyslog.

Перед настройкой получения событий убедитесь, что вы создали коллектор KUMA для событий Auditd.

Настройка получения событий состоит из следующих этапов:

1. Установка коллектора KUMA в сетевой инфраструктуре.
2. Настройка сервера источника событий.
3. Проверка поступления событий Auditd в веб-интерфейс KUMA.

Установка коллектора KUMA для получения событий Auditd

После создания коллектора для настройки получения событий с помощью rsyslog требуется установитьколлектор на сервере сетевой инфраструктуры, предназначенной для получения событий.

Подробнее о процедуре установки коллектора KUMA см. в разделе Установка коллектора в сетевой инфраструктуре.

Настройка сервера источника событий

Для передачи событий от сервера в коллектор KUMA используется 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. В папке /etc/rsyslog.d создайте файл audit.conf со следующим содержанием:

```
$ModLoad imfile
$InputFileName /var/log/audit/audit.log
$InputFileTag tag_audit_log:
$InputFileStateFile audit_log
$InputFileSeverity info
$InputFileFacility local6
$InputRunFileMonitor
*.* @<ip адрес коллектора KUMA>:<порт коллектора KUMA>
```

> Если вы хотите отправлять события по протоколу TCP, вместо последней строки в файле вставьте следующую:
> `*.* @@<ip адрес коллектора KUMA>:<порт коллектора KUMA>`.

3. Сохраните изменения в файле audit.conf.

4. Перезапустите сервис rsyslog, выполнив следующую команду:

```
systemctl restart rsyslog.service
```

Сервер источника событий настроен. Данные о событиях передаются с сервера в коллектор KUMA.

Проверка поступления событий Auditd в коллектор

Вы можете проверить, что настройка сервера источника событий Auditd выполнена правильно с помощью веб-интерфейса KUMA.

Подробнее о проверке поступления событий см. в разделе Поиск связанных событий.

Настройка получения событий KATA/EDR с помощью Syslog

KUMA позволяет передавать информацию о событиях из программы Kaspersky Anti Targeted Attack Platform в SIEM-систему KUMA с помощью Syslog.

В этом разделе описывается настройка передачи событий Kaspersky Anti Targeted Attack Platform с помощью Syslog, а именно настройка пересылки событий KATA, создание коллектора <PRODUCT_NAME_NOV> для сбора событий, установка коллектора <PRODUCT_NAME_NOM и проверка поступления событий в веб-интерфейсе KUMA.

Настройка передачи событий KATA/EDR в KUMA

Чтобы настроить передачу событий из программы Kaspersky Anti Targeted Attack Platform в KUMA:

1. В браузере на любом компьютере, на котором разрешен доступ к серверу Central Node, введите IP-адрес сервера с компонентом Central Node.

   Откроется окно ввода учетных данных пользователя Kaspersky Anti Targeted Attack Platform.

2. В окне ввода учетных данных пользователя установите флажок **Локальный администратор** и введите данные Администратора.

3. Выберите раздел **Параметры**, подраздел **SIEM-система**.

4. Укажите следующие параметры:

   a. Установите флажки **Журнал активности** и **Обнаружения**.

   b. В поле **Хост/IP** введите IP-адрес или имя хоста коллектора KUMA.

   c. В поле **Порт** укажите номер порта подключения к коллектору KUMA.

   d. В поле **Протокол** выберите из списка **TCP** или **UDP**.

   e. В поле **ID хоста** укажите идентификатор хоста сервера, который будет указан в журнале SIEM-систем как источник обнаружения.

   f. В поле **Периодичность сигнала** введите интервал отправки сообщений.

   g. Нажмите на кнопку **Применить**.

Передача событий Kaspersky Anti Targeted Attack Platform в KUMA настроена.

Настройка интеграции Kaspersky Anti Targeted Attack Platform с KUMA

Создание коллектора KUMA для получения событий KATA/EDR

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий Kaspersky Anti Targeted Attack Platform.

Подробнее о процедуре создания коллектора KUMA см. в разделе Создание коллектора.

> При создании коллектора в веб-интерфейсе KUMA убедитесь, что номер порта соответствует порту, указанному в пункте 4c настроек для передачи событий Kaspersky Anti Targeted Attack Platform в KUMA, а тип коннектора соответствует пункту 4d.

> Для получения событий Kaspersky Anti Targeted Attack Platform с помощью Syslog в мастере установки коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] KATA**.

Установка коллектора KUMA для получения событий KATA/EDR

После создания коллектора для настройки получения событий Kaspersky Anti Targeted Attack Platform с помощью Syslog требуется установить новый коллектор на сервере сетевой инфраструктуры, предназначенной для получения событий.

Подробнее о процедуре установки коллектора KUMA см. в разделе Установка коллектора в сетевой инфраструктуре.

Проверка поступления событий KATA/EDR в KUMA

Вы можете проверить, что настройка сервера источника событий Kaspersky Anti Targeted Attack Platform выполнена правильно с помощью веб-интерфейса KUMA.

Подробнее о проверке поступления событий см. в разделе Поиск связанных событий.

События Kaspersky Anti Targeted Attack Platform отображаются в таблице с результатами поиска как KATA.

Настройка получения событий Kaspersky Security Center в формате CEF

KUMA позволяет получать и передавать события в формате CEF от Сервера администрирования Kaspersky Security Center в SIEM-систему KUMA.

В этом разделе описывается процедура настройки получения событий от Сервера администрирования Kaspersky Security Center в формате CEF, а именно настройка передачи событий Kaspersky Security Center, создание коллектора KUMA для сбора событий, установка коллектора KUMA и проверка поступления событий Kaspersky Security Center в формате CEF в веб-интерфейс KUMA.

Настройка передачи событий Kaspersky Security Center в формате CEF

Kaspersky Security Center позволяет настроить параметры экспорта событий в SIEM-систему в формате CEF.

> Функция экспорта событий Kaspersky Security Center в SIEM-системы в формате CEF доступна при наличии лицензии Kaspersky Endpoint Security для бизнеса Расширенный или выше.

Чтобы настроить передачу событий от Сервера администрирования Kaspersky Security Center в SIEM-систему KUMA:

1. В дереве консоли Kaspersky Security Center выберите узел **Сервер администрирования**.
2. В рабочей области узла выберите вкладку **События**.
3. Перейдите по ссылке **Настроить параметры уведомлений и экспорта событий** и в раскрывающемся списке выберите **Настроить экспорт в SIEM-систему**.

   Откроется окно **Свойства: События**.
4. Установите флажок **Автоматически экспортировать события в базу SIEM-системы**.

5. В раскрывающемся списке **SIEM-система** выберите **ArcSight (CEF-формат)**.

6. Укажите адрес сервера SIEM-системы KUMA и порт для подключения к серверу в соответствующих полях.

   По кнопке **Экспортировать архив** Kaspersky Security Center экспортирует уже созданные события в базу SIEM-системы KUMA с указанной даты. По умолчанию Kaspersky Security Center экспортирует события с текущей даты.

7. Нажмите на кнопку **OK**.

В результате Сервер администрирования Kaspersky Security Center будет автоматически экспортировать все события в SIEM-систему KUMA.

Настройка экспорта событий Kaspersky Security Center в SIEM-систему KUMA

Настройка коллектора KUMA для сбора событий Kaspersky Security Center

После завершения настройки экспорта событий из Сервера администрирования Kaspersky Security Center в формате CEF вам нужно настроить коллектор в веб-интерфейсе KUMA.

Чтобы настроить коллектор KUMA для событий Kaspersky Security Center, выполните следующие действия:

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **Коллекторы**.

2. В списке коллекторов найдите коллектор с нормализатором **[OOTB] KSC** и откройте его для редактирования.

3. На вкладке **Транспорт** в поле **URL** укажите порт, по которому коллектор будет получать события Kaspersky Security Center.

   Порт должен совпадать с портом сервера SIEM-системы KUMA.

4. На вкладке **Парсинг событий** проверьте, что выбран нормализатор **[OOTB] KSC**.

5. На вкладке **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:

   - **Хранилище**. Для отправки обработанных событий в хранилище.
   - **Коррелятор**. Для отправки обработанных событий в коррелятор.

   Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

6. На вкладке **Проверка параметров** нажмите **Сохранить и создать сервис**.

7. Скопируйте появившуюся команду для установки коллектора KUMA.

Установка коллектора KUMA для сбора событий Kaspersky Security Center

После завершения настройки коллектора для сбора событий Kaspersky Security Center в формате CEF необходимо установить коллектор KUMA на сервере сетевой инфраструктуры, предназначенной для получения событий.

Подробнее о процедуре установки коллектора KUMA см. в разделе Установка коллектора в сетевой инфраструктуре.

Проверка поступления событий Kaspersky Security Center в KUMA

Вы можете проверить, что экспорт событий из Сервера администрирования Kaspersky Security Center в формате CEF в SIEM-систему KUMA выполнен правильно с помощью веб-интерфейса KUMA.

Подробнее о проверке поступления событий см. в разделе Поиск связанных событий.

Чтобы отобразить события Kaspersky Security Center в формате CEF в таблице, введите следующее поисковое выражение:

```
SELECT * FROM `events` WHERE DeviceProduct = 'KSC' ORDER BY Timestamp DESC
LIMIT 250
```

Настройка получения событий Kaspersky Security Center из БД MS SQL

KUMA позволяет получать информацию о событиях Kaspersky Security Center из базы данных MS SQL (далее БД MS SQL).

Перед настройкой убедитесь, что вы создали коллектор KUMA для событий Kaspersky Security Center из БД MS SQL.

Настройка получения событий состоит из следующих этапов:

1. Создание учетной записи в БД MS SQL.
2. Настройка службы SQL Server Browser.
3. Создание секрета.
4. Настройка коннектора.
5. Настройка коллектора для получения событий из БД MS SQL.
6. Установка коллектора в сетевой инфаструктуре.
7. Проверка поступления событий из БД MS SQL в веб-интерфейс KUMA.

Создание учетной записи в БД MS SQL

Для получения событий Kaspersky Security Center из БД MS SQL требуется учетная запись, которая имеет права, необходимые для подключения и работы с базой данных.

Чтобы создать учетную запись для работы с БД MS SQL:

1. Войдите на сервер с установленной БД MS SQL для Kaspersky Security Center.
2. С помощью **SQL Server Management Studio** подключитесь к БД 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 БД MS SQL и сделайте выборку по таблице.

Настройка службы SQL Server Browser

После создания учетной записи в БД MS SQL требуется настроить службу SQL Server Browser.

Чтобы настроить службу SQL Server Browser:

1. Откройте **SQL Server Configuration Manager**.

2. В левой панели выберите **SQL Server Services**.

   Откроется список служб.

3. Откройте свойства службы **SQL Server Browser** одним из следующих способов:

- Дважды нажмите на название службы **SQL Server Browser**.
- Нажмите правой кнопкой мыши на название службы **SQL Server Browser** и в контекстном меню выберите **Properties**.

4. В открывшемся окне **SQL Server Browser Properties** выберите вкладку **Service**.
5. В поле **Start Mode** выберите **Automatic**.
6. Выберите вкладку **Log On** и нажмите на кнопку **Start**.

   Автоматический запуск службы **SQL Server Browser** включен.
7. Включите и настройте протокол **TCP/IP**, выполнив следующие действия:
   a. В левой панели раскройте раздел **SQL Server Network Configuration** и выберите подраздел **Protocols for <Имя SQL-сервера>**.
   b. Нажмите правой кнопкой мыши на протокол **TCP/IP** и в контекстом меню выберите **Enable**.
   c. В появившемся окне **Warning** нажмите **OK**.
   d. Откройте свойства протокола **TCP/IP** одним из следующих способов:
      - Дважды нажмите на протокол **TCP/IP**.
      - Нажмите правой кнопкой мыши на протокол **TCP/IP** и в контекстном меню выберите **Properties**.
   e. Выберите вкладку **IP Addresses**, а затем в разделе **IPALL** в поле **TCP Port** укажите порт 1433.
   f. Нажмите на кнопку **Apply**, чтобы сохранить внесенные изменения.
   g. Нажмите на кнопку **OK**, чтобы закрыть окно.
8. Перезагрузите службу **SQL Server (<Имя SQL-сервера>)**, выполнив следующие действия:
   a. В левой панели выберите **SQL Server Services**.
   b. В списке служб справа нажмите правой кнопкой мыши на службу **SQL Server (<Имя SQL-сервера>)** и в контекстном меню выберите **Restart**.
9. В **Брандмауэре защитника Windows в режиме повышенной безопасности** разрешите на сервере входящие подключения по порту TCP 1433.

Создание секрета в KUMA

После создания и настройки учетной записи в MS SQL требуется добавить секрет в веб-интерфейсе KUMA. Этот ресурс используется для хранения учетных данных для подключения к БД MS SQL.

Чтобы создать секрет в в KUMA:

1. Откройте раздел веб-интерфейса KUMA **Ресурсы** → **Секреты**.

   Отобразится список доступных секретов.

2. Нажмите на кнопку **Добавить секрет**, чтобы создать новый секрет.

   Откроется окно секрета.

3. Введите данные секрета:

   a. В поле **Название** выберите имя для добавляемого секрета.

   b. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать создаваемый ресурс.

   c. В раскрывающемся списке **Тип** выберите **urls**.

   d. В поле **URL** укажите строку вида:

   ```
   sqlserver://[< domain >%5C]< username >:
   < password >@< server >:1433/< database_name >
   ```

   где:

   - `domain` – имя домена.
   - `5%C` – разделитель домена и пользователя. Представляет собой знак "\" в URL-формате.
   - `username` – имя созданной учетной записи БД MS SQL.
   - `password` – пароль созданной учетной записи БД MS SQL.
   - `server` – имя или IP-адрес сервера с БД MS SQL, установленной для Kaspersky Security Center.
   - `database_name` – имя БД Kaspersky Security Center. Имя по умолчанию: KAV.

   Например,

   ```
   sqlserver://test.local%5Cuser:password123@10.0.0.1:1433/KAV
   ```

Если в пароле учетной записи БД MS SQL используются специальные символы (@ # $ % & * ! + = [ ] : ' , ? / \ ` ( ) ;), переведите их в формат URL.

4. Нажмите **Сохранить**.

Из соображений безопасности после сохранения секрета строка, указанная в поле URL, скрывается.

Настройка коннектора

Для подключения KUMA к БД MS SQL требуется настроить коннектор.

Чтобы настроить коннектор:

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **Коннекторы**.
2. В списке коннекторов справа найдите коннектор **[OOTB] KSC SQL** и откройте его для редактирования.

   Если коннектор недоступен для редактирования, скопируйте его и откройте для редактирования копию коннектора.

   Если коннектор **[OOTB] KSC SQL** отсутствует, обратитесь к системному администратору.

3. На вкладке **Основные параметры** в выпадающих списках **URL** выберите секрет, созданный для подключения к БД MS SQL.
4. Нажмите **Сохранить**.

Настройка коллектора KUMA для получения событий Kaspersky Security Center из БД MS SQL

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий Kaspersky Security Center из БД MS SQL.

Подробнее о процедуре создания коллектора KUMA см. в разделе Создание коллектора.

При создании коллектора в веб-интерфейсе KUMA на вкладке **Транспорт** выберите коннектор **[OOTB] KSC SQL**.

Для получения событий Kaspersky Security Center из БД MS SQL на вкладке **Парсинг событий** выберите нормализатор **[OOTB] KSC from SQL**

Установка коллектора KUMA для сбора событий Kaspersky Security Center из БД MS SQL

После завершения настройки коллектора для получения событий Kaspersky Security Center из БД MS SQL требуется установить коллектор KUMA на сервере сетевой инфраструктуры, предназначенной для получения событий.

Подробнее о процедуре установки коллектора KUMA см. в разделе Установка коллектора в сетевой инфраструктуре.

Проверка поступления событий Kaspersky Security Center из БД MS SQL

Проверьте корректность настройки получения событий Kaspersky Security Center, выполнив поиск связанных событий в веб-интерфейсе KUMA.

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 feather logo – товарные знаки Apache Software Foundation.

Ubuntu, LTS являются зарегистрированными товарными знаками Canonical Ltd.

Cisco, IOS являются зарегистрированными товарными знаками или товарными знаками Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

Citrix – товарный знак Citrix Systems, Inc. и/или дочерних компаний, зарегистрированный в патентном офисе США и других стран.

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.

Firebird – зарегистрированный товарный знак Firebird Foundation.

FortiGate – товарный знак или зарегистрированный в США и/или других странах товарный знак Fortinet Corporation.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

Google, Chrome – товарные знаки Google LLC.

Huawei является товарным знаком Huawei Technologies Co., Ltd.

Intel, Core – товарный знак Intel Corporation, зарегистрированный в Соединенных Штатах Америки и в других странах.

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.

OpenAPI – товарный знак компании The Linux Foundation.

Kubernetes является зарегистрированным товарным знаком Linux Foundation в США и других странах.

Microsoft, Active Directory, Excel, Hyper-V, Windows и Windows Server являются товарными знаками группы компаний Microsoft.

CVE – зарегистрированный товарный знак MITRE Corporation.

Mozilla и Firefox являются товарными знаками Mozilla Foundation в США и других странах.

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.

Ansible, CentOS – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

Symantec – товарный знак или зарегистрированный в США и других странах товарный знак Symantec Corporation или аффилированных компаний.

ClickHouse – товарный знак компании YANDEX LLC.

ViPNet является зарегистрированным товарным знаком компании "ИнфоТеКС".

Глоссарий

SELinux (Security-Enhanced Linux)

Система контроля доступа процессов к ресурсам операционной системы на основе использования политик безопасности.

SIEM

Security Information and Event Management system – система управления информацией о безопасности и событиями безопасности. Решение для управления информацией и событиями в системе безопасности компании.

STARTTLS

Расширение обычного протокола текстового обмена, которое позволяет создать зашифрованное соединение (TLS или SSL) прямо поверх обычного TCP-соединения вместо открытия для шифрованного соединения отдельного порта.

userPrincipalName

UserPrincipalName (UPN) – это имя пользователя в формате адреса электронной почты, например `username@domain.com`.

UPN-имя необязательно должно соответствовать фактическому адресу электронной почты пользователя. В этом примере `username` – это имя пользователя в домене Active Directory (user logon name), а `domain.com` – это UPN-суффикс. Между ними используется разделитель `@`. По умолчанию в Active Directory в качестве UPN-суффикса используется DNS-имя домена Active Directory.

Агрегация

Объединение нескольких однотипных сообщений из источника события в одно событие.

Веб-интерфейс KUMA

Служба KUMA, которая предоставляет пользовательский интерфейс для настройки и отслеживания операций KUMA.

Кластер

Группа серверов, на которых установлена программа KUMA и которые были сгруппированы для централизованного управления с помощью веб-интерфейса программы.

Коллектор

Сервис KUMA, который принимает события из источников событий, преобразует их и передает их другим программным компонентам для дальнейшей обработки.

Коннектор

Ресурс KUMA, обеспечивающий транспорт для приема данных из внешних систем.

Нормализация

Процесс приведения данных, составляющих событие, в соответствие с полями модели данных события KUMA. Во время нормализации могут выполняться определенные преобразования данных по заданным правилам (например, символы верхнего регистра могут заменяться на символы нижнего регистра, определенные последовательности символов могут перезаписываться другими и т.п.).

Обогащение

Преобразование текстовых данных события с использованием словарей, констант, вызовов службы DNS и других инструментов.

Парсинг

Процесс организации данных и приведения поступающих событий в формат KUMA.

Роль

Набор прав доступа, установленных для предоставления пользователю веб-интерфейса KUMA полномочий для выполнения задач.

Сетевой порт

Параметр протокола TCP и UDP, который определяет место назначения пакетов данных в формате IP, которые передаются на узел по сети, и позволяет различным программам, работающим на одном узле, получать данные независимо друг от друга. Каждая программа обрабатывает данные, отправленные на определенный порт (иногда говорят, что программа прослушивает этот номер порта).

Стандартной практикой является присвоение стандартных номеров портов определенным распространенным сетевым протоколам (например, веб-серверы обычно получают данные через HTTP на TCP-порт 80), хотя в целом программа может использовать любой протокол на любом порту. Возможные значения: от 1 до 65 535.

Событие

Случай активности сетевых устройств и служб, связанных с безопасностью, который можно увидеть и записать. Например, к событиям относятся нарушения политики информационной безопасности, отключение мер безопасности, возникновение беспрецедентной ситуации и т.п.

Фильтр

Набор условий, которые программа использует для выбора событий для дальнейшей