kaspersky

Kaspersky Unified Monitoring and Analysis Platform

Руководство по эксплуатации

Версия программы: 1.5

Содержание

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 поддержка мультитенантности для поставщиков услуг управляемой безопасности (MSSP) и крупных предприятий. Это нововведение позволяет компаниям с несколькими филиалами и поставщикам услуг обнаруживать и приоритизировать угрозы для нескольких отделений из единой централизованной среды, а также закрывать доступ к данным других филиалов за счет создания тенантов на основе источников событий. Главный администратор платформы может назначать пользователям каждого тенанта определенные роли, четко определяющие, какую информацию каждый пользователь может просматривать, создавать или изменять.
- Поддерживается аутентификация пользователей KUMA средствами Microsoft Active Directory. Для каждого тенанта можно отдельно настроить роли пользователей Active Directory.
- KUMA включает пакет стандартных правил корреляции, разработанный специалистами «Лаборатории Касперского». Все правила сопоставлены с матрицей MITRE ATTACK и могут использоваться в качестве основы для разработки собственных правил мониторинга угроз. Обратите внимание, что правила корреляции необходимо проверять и настраивать для корректной работы в определенных средах.
- Значительно расширены возможности управления инцидентами. Эта функция в KUMA помогает расследовать инциденты, определять их первопричины и координировать совместную работу нескольких аналитиков.
  - Добавлены карточки инцидентов. Аналитик может создавать инциденты с нуля или на основе одного или нескольких алертов. Инцидент создается, если подтверждаются подозрения о возникновении нарушения политик безопасности. Карточка инцидента позволяет собрать в одном месте все признаки инцидента: подозрительные алерты и другие данные (например, информацию о затронутых устройствах и пользователях).
  - Поддерживается интеграция с российской инфраструктурой НКЦКИ (Национальный координационный центр по компьютерным инцидентам), что упрощает для пользователей платформы процесс информирования НКЦКИ об инцидентах, обязательный в рамках соблюдения нормативных требований.
  - Добавлен готовый макет панели мониторинга Incidents Overview (Обзор инцидентов).
  - Поддерживается категоризация инцидентов.

    - Добавлена гибкая группировка алертов и инцидентов для снижения нагрузки на аналитиков. Она позволяет точно настраивать критерии для автоматического объединения корреляционных событий с алертами и алертов с инцидентами.

- Добавлен мониторинг состояния источников событий для своевременного уведомления администраторов о проблемах, из-за которых значительно сокращается объем поступающих из источника событий данных или поток прерывается совсем. После настройки ожидаемого минимального количества событий в политике мониторинга и назначения этой политики источнику событий, указанные в параметрах политики пользователи будут получать уведомления об отклонениях от заданных параметров.

- Реализована поддержка новых коннекторов для приема событий по следующим протоколам.

    - WMI (через RPC) – позволяет получать события Windows с удаленных компьютеров с помощью методов на основе протокола дистанционного вызова процедур (RPC). WMI работает без агента, в отличие от WEC, который позволяет принимать события Windows только с локального компьютера или с WEC-сервера, на котором установлен агент.

    - SNMP версии 1, 2 и 3 – позволяет в активном режиме запрашивать данные по протоколу SNMP.

    - NFS – позволяет получать события из файлов в общей папке NFS.

    - FTP – позволяет получать события из файлов, доступных по протоколу FTP.

- Поддерживается автоматическая категоризация устройств (динамическая категоризация). Проактивная категоризация позволяет пользователю платформы задавать критерии для каждой категории (например, включать в категорию активы с ОС Windows, расположенные в подсети 10.10.0.0/16). В то же время реактивная категоризация позволяет изменять категории устройств по итогам корреляции. Как и ранее, динамические категории можно учитывать при корреляции и сортировке алертов.

- Поддерживается полное резервное копирование данных Ядра KUMA для повышения отказоустойчивости платформы.

- Добавлен REST API HTTP для управления устройствами и активными листами.

- Значительно улучшена функциональность агента KUMA. Теперь он поддерживает все коннекторы, поддерживаемые KUMA (ранее поддерживал только коннектор WEC), и может использоваться для маршрутизации событий.

- Поддерживается обновление с версий 1.0 и 1.1. Ресурсы (правила корреляции, нормализаторы и прочие) сохраняются во время обновления. По вопросам переноса накопленных данных (событий, алертов) при обновлении обратитесь к специалистам «Лаборатории Касперского».

- Добавлены мастеры установки для подключения источников событий и создания корреляторов. Они упрощают эти процессы и предотвращают возможные ошибки. Мастеры обеспечивают интерактивное прохождение пользователем платформы всех необходимых шагов и помогают проверить настройки.

Комплект поставки

В комплект поставки входят следующие файлы:

- kuma-ansible-installer-<номер сборки>.tar.gz для установки компонентов KUMA;

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

Комплект поставки версии KUMA, сертифицированной государственными органами Российской Федерации

В комплект поставки версии KUMA, сертифицированной государственными органами Российской Федерации, входят два диска со следующими файлами:

- Диск 1:
  - kuma-ansible-installer-<номер сборки>-certified.tar.gz для установки компонентов KUMA.
- Диск 2 (вспомогательный):
  - kuma-ansible-installer-<номер сборки>-env.tar.gz – архив, содержащий следующие компоненты:
    - clickhouse.tar.gz для установки СУБД ClickHouse на серверах хранилища KUMA.
    - mongodb.tar.gz для установки СУБД MongoDB, используемой для хранения конфигураций и настроек сервисов и тенантов.
    - каталог ansible\ для автоматизации настройки и развертывания KUMA.

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.
  - Диск: 500 ГБ доступного места на диске, смонтированного в разделе /opt.
- Серверы для установки коррелляторов:
  - 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 2 ядер (4 потока) с поддержкой набора инструкций SSE 4.2 или 4 vCPU (виртуальных процессоров).
- ОЗУ: 12 ГБ.
- 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.

  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.

- 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 (20H1, 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 8.4.

Требования к программному обеспечению

На каждом сервере, который используется для установки сервисов KUMA, необходимо установить операционную систему Oracle Linux 8.4.

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

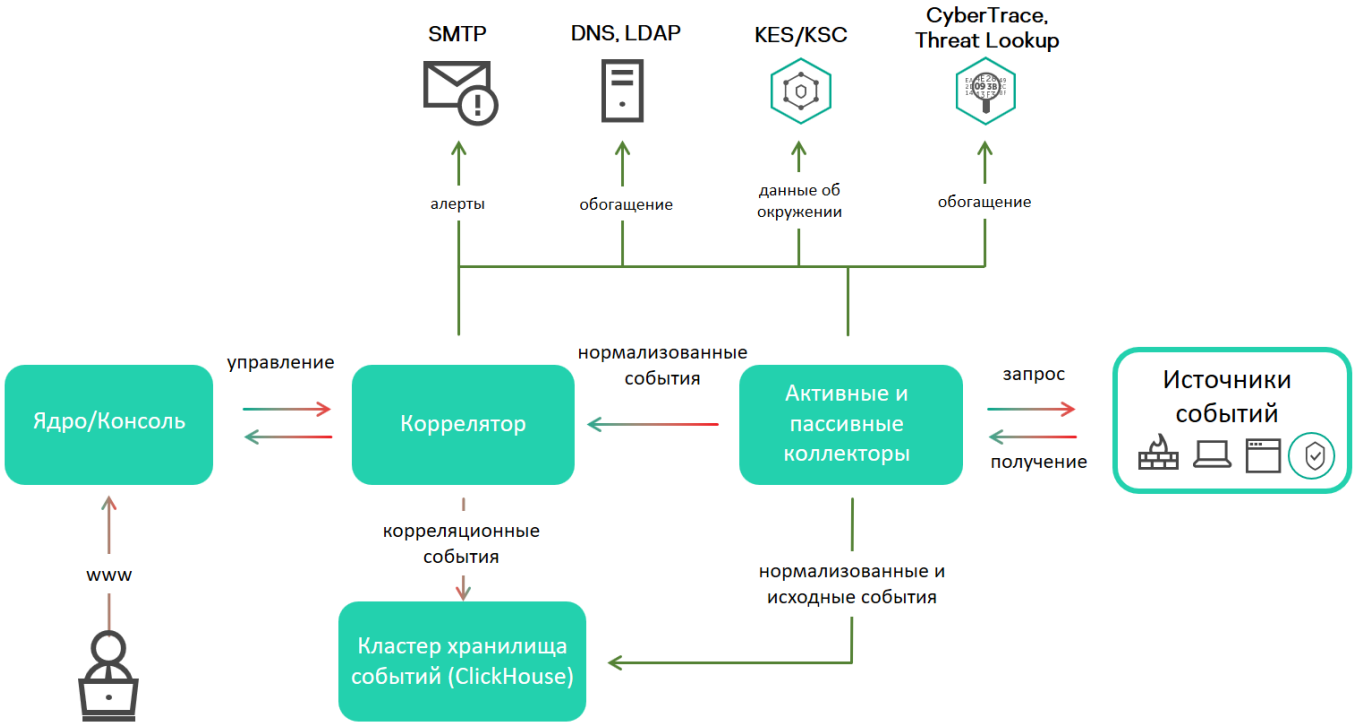
На компьютерах, используемых для веб-интерфейса KUMA, необходимо установить браузер Google™ Chrome™ 93 или более поздней версии либо Mozilla™ Firefox™ 92 или более поздней версии.

Архитектура программы

Стандартная установка программы включает следующие компоненты:

- 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.
- *Ядро*, включающее графический интерфейс для мониторинга и управления настройками компонентов системы.
- *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;
   - nats;
   - kafka;
   - http;
   - sql;
   - file;
   - 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 отбирать для дальнейшей обработки только события, удовлетворяющие заданным условиям. События, не удовлетворяющие условиям фильтрации, на этом этапе отсеиваются и далее не обрабатываются.

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:

   - constant;
   - cybertrace;
   - dictionary;
   - dns;
   - event;
   - ldap;
   - template.

   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.

Компоненты хранилища: кластеры, шарды, реплики, киперы

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

Шард (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 (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 (keeper) – опциональная роль реплики, подразумевающая ее участие в **координации** репликации данных на уровне **всего** кластера. На весь кластер требуется хотя бы одна реплика с этой ролью. Рекомендуемое количество таких реплик – 3. Число реплик, участвующих в координации репликации, должно быть **нечетным**.

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 устройств 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)
- 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 этап жизненного цикла события проходит 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 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*, создаваемые 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 событий корреляции, 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.

Ниже представлен жизненный цикл алерта:

1. KUMA создает алерт при срабатывании правила корреляции. Алерт обновляется, если правило корреляции срабатывает снова. Алерту присваивается статус **Новый**.

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**).

   После этого алерт больше не обновляется новыми событиями, и, если правило корреляции срабатывает снова, создается новый алерт.

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 устройствах

Устройства – это сетевые устройства, зарегистрированные в KUMA. Сетевые устройства 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 устройство с определенными параметрами (например, конкретным IP-адресом), формируется связь между этим устройством и всеми событиями, в которых указаны эти параметры (в нашем случае IP-адрес).

Устройства 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 привязано устройство, категория этого устройства также принимается во внимание. Например, если вы присвоите высокий уровень важности определенной категории устройств, то связанные с этими устройствами 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 устройства в KUMA, поскольку их использование позволяет формулировать четкие и универсальные правила корреляции для более эффективного анализа событий.

Работа с устройствами 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®.
- udp – используются для получения данных по протоколу UDP. Устанавливается на устройства Linux.
- nats – используются для коммуникации через NATS. Устанавливается на устройства Linux.
- kafka – используются для коммуникации с помощью kafka. Устанавливается на устройства Linux.
- http – используются для связи по протоколу HTTP. Устанавливается на устройства Linux.
- 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.
- nfs – используются для получения данных по протоколу Network File System. Устанавливается на устройства Linux.

- snmp – используются для получения данных с помощью Simple Network Management Protocol. 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 устройств, связанных с обработанными событиями, так как правила корреляции принимают во внимание уровень важности категории этих устройств. Если к алерту или корреляционному событию не привязаны устройства с уровнем важности или не привязаны устройства 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. KUMA можно установить на одном сервере для ознакомления с возможностями программы. KUMA также можно установить в производственной среде.

Установка для демонстрации

Для демонстрации вы можете развернуть компоненты KUMA на одном сервере. Установка KUMA происходит в несколько этапов:

Имя сервера, на котором запускается установщик, должно отличаться от `localhost` или `localhost.<домен>`. Установщик можно запустить из любой папки, но RPM-пакеты должны находится в одной папке с файлом kuma-installer. Вы можете получить больше информации о kuma-installer, запустив его с параметром `--help`.

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).

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.

При установке версии KUMA, сертифицированной государственными органами Российской Федерации, файлы с обоих дисков из комплекта поставки необходимо распаковать в папку `kuma-ansible-installer`.

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:

   - 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 в производственной среде и имеете отдельную контрольную машину, присвойте параметру ansible_connection значение ssh:

     ```
     ansible_connection: ssh
     ```

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.

Для запуска установщика необходимы root-права.

Чтобы установить KUMA для демонстрации:

1. На контрольной машине войдите в ОС как пользователь root и перейдите в папку с распакованным установщиком.
2. Подложите в папку <папка установщика>/roles/kuma/files/ файл с лицензионным ключом.
3. Запустите установщик, выполнив следующую команду:

   ```
   ./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 `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 `/opt/kaspersky/kuma/kuma <collector/correlator/storage> --id <идентификатор сервиса> --uninstall`. Повторите команду удаления для каждого сервиса.

3. **Пересоздание сервисов на нужных машинах**

Установка KUMA в производственной среде

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).

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.

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	Доступ пользователей к веб-интерфейса KUMA
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.
TCP	9200	От коллектора и коррелятора до серверов хранилища	Отправка нормализованных и корреляционных событий в хранилище

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 Oracle Linux 8.4, выбрав вариант установки Server. Образ диска для установки доступен на официальном сайте Oracle.

2. Войдите в операционную систему как пользователь root.

3. Настройте сетевой интерфейс.

   Для удобства можно воспользоваться утилитой с графическим интерфейсом nmtui.

4. 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:

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

   c. Выждите несколько секунд и выполните следующую команду:

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

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

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

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

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

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

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

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

   При установке версии KUMA, сертифицированной государственными органами Российской Федерации, файлы с обоих дисков из комплекта поставки необходимо распаковать в папку `kuma-ansible-installer`.

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 Oracle Linux 8.4, выбрав вариант установки Server. Образ диска для установки доступен на официальном сайте Oracle.

2. Войдите в операционную систему как пользователь root.

3. Настройте сетевой интерфейс.

   Для удобства можно воспользоваться утилитой с графическим интерфейсом nmtui.

4. 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:

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

   c. Выждите несколько секунд и выполните следующую команду:

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

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

5. 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.

6. 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.

7. 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 5–7 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.

При установке версии KUMA, сертифицированной государственными органами Российской Федерации, файлы с обоих дисков из комплекта поставки необходимо распаковать в папку `kuma-ansible-installer`.

Чтобы создать файл инвентаря:

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

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

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

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

3. Отредактируйте параметры файла инвентаря:

   - 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 машины не зарегистрированы в DNS-зоне вашей организации, присвойте параметру generate_etc_hosts значение true, а также для каждой машины в инвентаре замените значения параметра `ip (0.0.0.0)` на актуальные IP-адреса.

     ```
     generate_etc_hosts: true
     ```

     При использование этого параметра установщик автоматически дополнит файлы /etc/hosts на машинах, куда устанавливаются компоненты KUMA, IP-адресами машин из файла инвентаря.

   - Если вы устанавливаете KUMA в производственной среде и имеете отдельную контрольную машину, присвойте параметру ansible_connection значение ssh:

     ```
     ansible_connection: ssh
     ```

4. Укажите в файле инвентаря хост целевых машин, на которых следует установить компоненты KUMA. Если машины не зарегистрированы в DNS-зоне вашей организации, замените значения параметра `ip (0.0.0.0)` на актуальные IP-адреса.

   Хосты указываются в следующих разделах файла инвентаря:

   - `core` – раздел для указания хоста и IP-адреса целевой машины, на которой будет установлено Ядро KUMA. В этом разделе можно указать только один хост.

   - `collector` – раздел для указания хоста и IP-адреса целевой машины, на которой будет установлен коллектор. В этом разделе можно указать один или более хостов.

   - `correlator` – раздел для указания хоста и IP-адреса целевой машины, на которой будет установлен коррелятор. В этом разделе можно указать один или более хостов.

   - `storage` – раздел для указания хостов и IP-адресов целевых машин, на которых будут установлены компоненты хранилища. В этом разделе можно указать один или более хостов.

     Компоненты хранилища: кластеры, шарды, реплики, киперы

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

Шард (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 (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 (keeper) – опциональная роль реплики, подразумевающая ее участие в **координации** репликации данных на уровне **всего** кластера. На весь кластер требуется хотя бы одна реплика с этой ролью. Рекомендуемое количество таких реплик – 3. Число реплик, участвующих в координации репликации, должно быть **нечетным**.

Каждая машина в разделе `storage` 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**.

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.

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.

Для запуска установщика необходимы root-права.

Чтобы установить KUMA:

1. На контрольной машине войдите в ОС как пользователь root и перейдите в папку с распакованным установщиком.
2. Подложите в папку <папка установщика>/roles/kuma/files/ файл с лицензионным ключом.
3. Запустите установщик, выполнив следующую команду:

   ```
   ./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 целевых машинах. 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.

Создание сервисов

Сервисы KUMA следует устанавливать только после завершения развертывания 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>`.

Ниже перечислены разделы, в которых описано создание сервисов:

- Создание хранилища
- Создание коррелятора
- Создание коллектора
- Создание агентов KUMA

Изменение корневого сертификата

После установки Ядра KUMA создается уникальный самоподписанный корневой сертификат с соответствующим ключом. Этот сертификат используется для подписи всех других сертификатов, используемых для внутренней связи между компонентами KUMA, а также для запросов REST API. Корневой сертификат хранится на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

Вы можете использовать сертификат и ключ своей компании вместо самоподписанного корневого сертификата и ключа KUMA.

Для изменения конфигурации компонентов KUMA требуются root-права.

Перед изменением сертификата KUMA обязательно сделайте резервную копию предыдущего сертификата и ключа с именами backup_external.cert и backup_external.key.

Чтобы изменить корневой сертификат KUMA:

1. Переименуйте файлы сертификата и ключа вашей компании в external.cert и external.key.

   Ключи должны быть в PEM-формате.

2. Поместите external.cert и external.key в папку /opt/kaspersky/kuma/core/certificates/.
3. Перезапустите службу kuma-core, выполнив команду `systemctl restart kuma-core`.
4. Перезапустите браузер, с помощью которого вы работаете в веб-интерфейсе KUMA.

   Сертификат и ключ вашей компании используются для внутренней связи между компонентами KUMA и для запросов REST API.

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:

   ```
   ./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.

Обновление предыдущих версий KUMA

KUMA версии 1.5.x можно установить поверх версий 1.x.x. Для этого следуйте инструкции по установке программы в производственной среде и на этапе подготовке файла инвентаря перечислите в нем хосты уже развернутой системы KUMA.

При обновлении накопленные события не переносятся из старой версии программы в новую.

Старые сервисы коллекторов и корреляторов в новой программе при настройке точек назначения отображаются в разделе **Другое**.

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.

Предусмотрены следующие типы лицензий:

- *Пробная* – бесплатная лицензия, предназначенная для ознакомления с программой.

  Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии KUMA прекращает выполнять все свои функции. Чтобы продолжить использование программы, вам нужно приобрести коммерческую лицензию.

  Вы можете активировать программу по пробной лицензии только один раз.

- *Коммерческая* – платная лицензия, предоставляемая при приобретении программы.

По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью (например, недоступно обновление баз KUMA). Чтобы продолжить использование KUMA в режиме полной функциональности, вам нужно продлить срок действия коммерческой 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, устройств, на которых можно использовать программу по предоставляемой лицензии);
- 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 одним из следующих способов: применить *файл ключа* или ввести *код активации*. 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 дополнительным (или 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.

Дополнительный (или 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 расширением 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 или после заказа пробной версии 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 кнопку **Добавить активный лицензионный ключ**. Эта кнопка не отображается, если в программу уже был добавлен лицензионный ключ.
   - Если вы хотите добавить резервный ключ, нажмите кнопку **Добавить резервный лицензионный ключ**. Эта кнопка неактивна, пока не будет добавлен основной ключ.

     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

Программа Kaspersky Security Center предназначена для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации и предоставляет администратору доступ к детальной информации об уровне безопасности сети. KUMA можно интегрировать с Kaspersky Security Center, чтобы получать информацию об устройствах. С помощью коррелляторов можно также отправлять в KUMA команды на создание задач, относящихся к устройствам.

Задачи Kaspersky Security Center — это функции, выполняемые данной программой, например Полная проверка компьютера, Обновление баз. Более подробная информация о задачах Kaspersky Security Center приведена в онлайн-справке Kaspersky Security Center.

Подготовка Kaspersky Security Center к интеграции с KUMA

Чтобы обеспечить взаимодействие Kaspersky Security Center и KUMA:

- Убедитесь, что со стороны KUMA есть доступ к Kaspersky Security Center по протоколу UDP.
- Создайте в Kaspersky Security Center пользователя с необходимыми разрешениями.
- Создайте задачи Kaspersky Security Center для всех устройств во всех программах, подключенных к Kaspersky Security Center.
- Настройте Kaspersky Security Center для отправки событий в KUMA. Это необходимо для получения информации о задачах Kaspersky Security Center в KUMA.

Создание пользователя KUMA в Kaspersky Security Center

Чтобы создать пользователя в Kaspersky Security Center для интеграции с KUMA:

1. В Консоли администрирования Kaspersky Security Center выберите узел с именем требуемого Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Безопасность**.
4. В поле **Имена групп или пользователей** нажмите кнопку **Внутренний пользователь**.

   Откроется окно выбора пользователей.
5. Нажмите кнопку **Добавить пользователя** и добавьте пользователя.

Требуется указать только имя пользователя и пароль. После создания пользователь отобразится в окне **Выбор пользователей**.

6. Выберите созданного пользователя и нажмите **OK**.

   Пользователь будет отображаться в поле **Имена групп или пользователей**.

7. В рабочей области в разделе **Разрешения для веб** на закладке **Права** выберите пользователя и настройте права пользователя KUMA:

   - Получение сведений об устройствах из Kaspersky Security Center: в узле **Базовые функции** установите флажок **Разрешить** рядом с правами на **Чтение**.
   - Стартовать задачи Kaspersky Endpoint Security для Linux: в узле **Базовые функции** установите флажки **Разрешить** рядом с правами на **Чтение** и **Изменение**.
   - Стартовать задачи сканирования в Kaspersky Endpoint Security для Windows: в узлах Базовые функции и Компоненты защиты установите флажки Разрешить рядом с правами на Чтение и Изменение.
   - Стартовать задачи обновления в Kaspersky Endpoint Security для Windows: в узлах Базовые функции и Компоненты защиты установите флажки Разрешить рядом с правами на Чтение и Изменение.

8. Нажмите **OK**.

Пользователь KUMA добавлен в Kaspersky Security Center. Теперь его можно использовать для создания подключения к Kaspersky Security Center.

Настройка Kaspersky Security Center для отправки событий в KUMA

Для просмотра информации о задачах из Kaspersky Security Center в KUMA необходимо настроить экспорт событий Kaspersky Security Center в формате CEF и выбрать типы событий, которые будут экспортироваться из Kaspersky Security Center.

Чтобы экспортировать события Kaspersky Security Center в KUMA:

1. В дереве консоли Kaspersky Security Center выберите узел с именем Сервера администрирования, события которого необходимо экспортировать.
2. В рабочей области выбранного Сервера администрирования перейдите на закладку **События**.
3. Нажмите на стрелку рядом со ссылкой **Настроить параметры уведомлений и экспорта событий** и в раскрывающемся списке выберите значение **Настроить экспорт в SIEM-систему**.
4. Откроется окно свойств событий в разделе **Экспорт событий**.
5. В разделе **Экспорт событий** укажите следующие параметры:

   a. Установите флажок **Автоматически экспортировать события в базу SIEM-системы**.

   b. В раскрывающемся списке **SIEM-система** выберите **ArcSight (формат CEF)**.

   c. В поле **Адрес сервера SIEM-системы** введите веб-адрес сервера коллектора KUMA, используемого для приема событий из Kaspersky Security Center.

   d. В поле **Порт сервера SIEM-системы** введите порт, через который сервер коллектора KUMA ожидает приема событий из Kaspersky Security Center.

e. В раскрывающемся списке **Протокол** выберите **TCP/IP**.

6. Нажмите **OK**.

Автоматический экспорт событий из Kaspersky Security Center будет включен. Подробнее об экспорте событий из Kaspersky Security Center в SIEM-системы см. онлайн-справку Kaspersky Security Center.

Чтобы выбрать типы событий для экспорта для каждой политики Kaspersky Security Center:

1. В дереве консоли Kaspersky Security Center выберите узел **Политики**.
2. Откройте контекстное меню требуемой политики по правой клавише мыши и выберите пункт **Свойства**.
3. В открывшемся окне свойств политики выберите раздел **Настройка событий**.
4. На закладке **Информация** выберите типы событий **Задача запущена** и **Задача выполнена** и нажмите кнопку **Свойства**.
5. В появившемся окне свойств событий установите флажок **Экспортировать в SIEM-систему по протоколу Syslog**, чтобы включить экспорт для выбранных событий.
6. Нажмите на кнопку **OK**, чтобы сохранить изменения.
7. В окне свойств политики нажмите на кнопку **OK**.

Выбранные события будут отправляться в KUMA по протоколу Syslog. Подробнее об экспорте событий из Kaspersky Security Center по протоколу Syslog см. в онлайн-справке Kaspersky Security Center.

Необходимо настроить коллектор KUMA на прием событий Kaspersky Security Center. Для событий из Kaspersky Security Center установлено значение поля `DeviceProduct = SecurityCenter`, по которому их можно искать в KUMA.

Пример коллектора для получения событий Kaspersky Security Center включен в установочный пакет KUMA. Он называется `[Example] KSC`. Он состоит из коннектора, выполняющего прослушивание TCP-порта 5141, и, что более важно, нормализатора `[Example] KSC`, который используется для обработки событий Kaspersky Security Center в ваших собственных коллекторах.

Создание задач KUMA в Kaspersky Security Center

Для запуска задач, связанных с устройствами, в Kaspersky Security Center из KUMA необходимо заранее создать эти задачи в Kaspersky Security Center.

Для каждой программы Лаборатории Касперского, не совместимой с другими программами, необходимо создать отдельную задачу. Например, создайте отдельные задачи для продуктов Linux и Windows или, если у вас установлена программа Kaspersky Endpoint Security для Windows версии 10 и 11, создайте отдельные задачи для каждой из версий. Для совместимых продуктов создайте задачи для последней версии.

Если у вас несколько иерархически объединенных Серверов администрирования Kaspersky Security Center, необходимо создавать задачи только на основном Сервере администрирования. В противном случае создайте задачи на каждом вторичном Сервере администрирования Kaspersky Security Center.

Чтобы создать задачу в Kaspersky Security Center:

1. В дереве консоли Kaspersky Security Center выберите группу администрирования, для которой нужно создать задачу.
2. В рабочей области выберите закладку **Задачи**.
3. Запустите мастер создания задачи по кнопке **Создать задачу**.

   Запустится **мастер создания задачи**.
4. Следуйте указаниям мастера, чтобы создать требуемую задачу.

   Название задания должно начинаться с "`kuma `". Например, "`kuma asset virus scan`".

Созданная задача отобразится в разделе **Задачи** дерева консоли Kaspersky Security Center. Эту задачу можно запустить из KUMA.

Управление подключениями к Kaspersky Security Center

В этом разделе описана работа с подключениями Kaspersky Security Center, необходимыми для интеграции Kaspersky Security Center и KUMA.

Подключения к Kaspersky Security Center создаются и управляются в разделе **Параметры** веб-интерфейса KUMA в закладке **Интеграции** → **KSC**. В правой части раздела **Параметры** веб-интерфейса KUMA отображается список тенантов, для которых настроены подключения Kaspersky Security Center. При нажатии на тенант открывается окно **Подключения к Kaspersky Security Center** со списком созданных подключений к Kaspersky Security Center. При нажатии на подключение открывается область деталей с параметрами выбранного подключения. Можно создать более одного подключения с Kaspersky Security Center.

Чтобы включить или отключить интеграцию с Kaspersky Security Center:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры**.
2. В левой части раздела **Параметры** выберите закладку **Параметры** → **KSC**.

   В правой части раздела **Параметры** отобразится таблица **Подключения к Kaspersky Security Center**.
3. Выберите тенанта, для которого вы хотите включить или отключить интеграцию с Kaspersky Security Center.

   В правой части раздела **Параметры** отобразится таблица **Подключение к Kaspersky Security Center**.
4. Включите или отключите интеграцию с Kaspersky Security Center:

   - Снимите флажок **Выключено**, если хотите, чтобы KUMA получал информацию об устройствах Kaspersky Security Center и отправлял в Kaspersky Security Center команды.
   - Установите флажок **Выключено**, если не хотите, чтобы KUMA получал информацию об устройствах Kaspersky Security Center и отправлял в Kaspersky Security Center команды.

По умолчанию этот флажок снят.

5. Нажмите **Сохранить**.

Создание подключения к Kaspersky Security Center

Чтобы создать подключение к Kaspersky Security Center:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры**.
2. В левой части раздела **Параметры** выберите закладку **Параметры → KSC**.

   В правой части раздела **Параметры** отобразится таблица **Подключения к Kaspersky Security Center**.
3. Выберите тенанта, для которого вы хотите создать подключение к Kaspersky Security Center.

   В правой части раздела **Параметры** отобразится таблица **Подключение к Kaspersky Security Center**.
4. Нажмите на кнопку **Добавить подключение к KSC** и задайте параметры, как описано ниже.

   - **Название** (обязательно) – введите уникальное имя подключения к Kaspersky Security Center. Длина должна быть от 1 до 128 символов Юникода.
   - **URL** (обязательно) – введите URL сервера Kaspersky Security Center в формате hostname:port или IPv4:port.
   - **Выключено** – снимите этот флажок, если хотите использовать это подключение к Kaspersky Security Center. По умолчанию этот флажок снят.
5. В раскрывающемся списке **Секрет** выберите ресурс секрета с необходимыми учетными данными Kaspersky Security Center или создайте новый ресурс секрета, нажав кнопку с плюсом.

   Создание ресурса с учетными данными Kaspersky Security Center

Учетные данные сервера Kaspersky Security Center хранятся в ресурсе секрета.

Чтобы создать ресурс секрета с учетными данными сервера Kaspersky Security Center:

1. В разделе **Ресурсы** веб-интерфейса KUMA выберите **Секреты**.

   Отобразится список доступных секретов.

2. В левой части окна **Секреты** выберите тенанта, в котором будет использоваться подключение к Kaspersky Security Center с этими учетными данными.

3. При необходимости выберите папку, в которой вы хотите создать секрет.

4. Нажмите кнопку **Добавить секрет**, чтобы создать новый секрет. Этот ресурс используется для хранения учетных данных для подключения к серверу Kaspersky Security Center.

   Откроется окно секрета.

5. Введите данные секрета:

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

   b. В раскрывающемся списке **Тенант** выберите тенанта, 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.

6. Нажмите **Сохранить**.

   Учетные данные сервера Kaspersky Security Center сохранены и могут использоваться в других ресурсах KUMA.

6. Нажмите **Сохранить**.

Подключение к Kaspersky Security Center создано. Его можно использовать для импорта информации об устройствах из Kaspersky Security Center в KUMA и для создания задач, связанных с устройствами, 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**.

2. В левой части раздела **Параметры** выберите закладку **Параметры → KSC**.

   В правой части раздела **Параметры** отобразится таблица **Подключения к Kaspersky Security Center**.

3. Выберите тенанта, для которого вы хотите изменить подключение к Kaspersky Security Center.

   В правой части раздела **Параметры** отобразится таблица **Подключение к Kaspersky Security Center**.

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

   Откроется окно с параметрами выбранного подключения к Kaspersky Security Center.

5. Измените нужные параметры:

   - **Название** (обязательно) – введите уникальное имя подключения к Kaspersky Security Center. Длина должна быть от 1 до 128 символов Юникода.
   - **URL** (обязательно) – введите URL сервера Kaspersky Security Center в формате hostname:port или IPv4:port.
   - **Секрет** (обязательно) – выберите ресурс секрета с необходимыми учетными данными Kaspersky Security Center.
   - **Выключено** – установите этот флажок, если не хотите использовать это подключение к Kaspersky Security Center. По умолчанию этот флажок снят.

6. Нажмите **Сохранить**.

Подключение к Kaspersky Security Center изменено.

Удаление подключения к Kaspersky Security Center

Чтобы удалить подключение к Kaspersky Security Center:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры**.
2. В левой части раздела **Параметры** выберите закладку **Параметры → KSC**.

   В правой части раздела **Параметры** отобразится таблица **Подключения к Kaspersky Security Center**.
3. Выберите тенанта, для которого вы хотите удалить подключение к Kaspersky Security Center.

   В правой части раздела **Параметры** отобразится таблица **Подключение к Kaspersky Security Center**.
4. Нажмите на подключение Kaspersky Security Center, которое вы хотите удалить, а затем нажмите кнопку **Удалить**.

Подключение к Kaspersky Security Center удалено.

Работа с задачами Kaspersky Security Center

После настройки Kaspersky Security Center для интеграции с KUMA и установки подключения к Kaspersky Security Center из KUMA можно запускать задачи Kaspersky Security Center из KUMA. Это можно делать вручную из раздела **Устройства** веб-интерфейса или автоматически, с помощью правил реагирования в процессе корреляции.

Запуск задач Kaspersky Security Center вручную

Чтобы запустить задачи Kaspersky Security Center вручную:

1. В разделе **Устройства** веб-интерфейса KUMA выберите устройства, импортированные из Kaspersky Security Center.

   В правой части окна отобразится область **Информация об устройстве** с кнопкой **Запустить задачу KSC**.

2. Нажмите кнопку **Запустить задачу KSC**.

   Откроется окно **Выбрать задачу KSC**.

3. Выберите задачи, которые вы хотите выполнить, и нажмите кнопку **Запустить**.

Kaspersky Security Center запускает выбранные задачи для выбранных устройств.

Некоторые типы задач доступны только для определенных устройств. Информация об уязвимостях и программном обеспечении доступна только для устройств с операционной системой Windows.

Запуск задач Kaspersky Security Center автоматически

Корреляторы могут запускать задачи Kaspersky Security Center автоматически. При выполнении определенных условий коррелятор активирует правила реагирования, содержащие список задач Kaspersky Security Center для запуска и определения соответствующих устройств.

Чтобы настроить ресурс реагирования, который может использоваться корреляторами для автоматического запуска задач Kaspersky Security Center:

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

2. Нажмите кнопку **Добавить реагирование** и задайте параметры, как описано ниже:

   - В поле **Имя** введите имя ресурса для его идентификации.
   - В раскрывающемся списке **Тип** выберите **ksctasks** (задачи Kaspersky Security Center).
   - В раскрывающемся списке **Задача Kaspersky Security Center** выберите задачи, запускаемые при срабатывании коррелятора, связанного с этим ресурсом реагирования.

     Вы можете выбрать несколько задач. При активации реагирования из списка задач выбирается только первая задача, соответствующая выбранному устройству. Остальные подходящие задачи игнорируются. Если требуется запустить несколько задач при выполнении одного условия, необходимо создать несколько правил реагирования.

   - В поле **Поле события** выберите поля события, вызывающие срабатывание коррелятора, в которых определены устройства, для которых должна быть запущена задача. Возможные значения:

     - SourceAssetID
     - DestinationAssetID
     - DeviceAssetID

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

   Создание фильтра в ресурсах

1. В раскрывающемся меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, включите переключатель **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию переключатель выключен.

3. Если вы включили переключатель **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.

       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.
       - **inActiveList** – этот фильтр имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
       - **inCategory** – устройству в левом операнде назначается по крайней мере одна из категорий устройств 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).

С помощью флажка **с учетом регистра** в раскрывающемся списке **оператор** можно указать, требуется ли учитывать регистр значений, переданных в фильтр. По умолчанию флажок снят.

- 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 ×.

4. При необходимости в поле **Рабочие процессы** укажите количество процессов реагирования, которые можно запускать одновременно.

5. Нажмите **Сохранить**.

Ресурс реагирования создан. Теперь его можно связать с коррелятором, который будет вызывать его, запуская тем самым задачу Kaspersky Security Center.

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. Войдите в веб-интерфейс KUMA.

2. Откройте раздел **Ресурсы** → **Активные сервисы**.

3. 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.

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 [Example] KSC SQL и нормализатора [Example] KSC from SQL.

Чтобы создать коллектор для получения событий Kaspersky Security Center,

Следуйте инструкциям в разделе Создание коллектора, выбирая в мастере установки преднастроенные ресурсы:

- На шаге 2 мастера установки выберите коннектор [Example] KSC SQL:
  - В поле **URL** укажите строку 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())
```

- На шаге 3 мастера установки выберите нормализатор [Example] KSC from SQL.
- Остальные параметры укажите в соответствии вашими требованиями к коллектору.

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 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 меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, включите переключатель **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию переключатель выключен.

3. Если вы включили переключатель **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.

       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.
       - **inActiveList** – этот фильтр имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
       - **inCategory** – устройству в левом операнде назначается по крайней мере одна из категорий устройств 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).

С помощью флажка **с учетом регистра** в раскрывающемся списке **оператор** можно указать, требуется ли учитывать регистр значений, переданных в фильтр. По умолчанию флажок снят.

- 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 ×.

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** → **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 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** → **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, IPv4 или IPv6.
   - **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.

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 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 тенанта, 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 **KTL**.

   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**.

    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 хэшах 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 KTL**.

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 KTL** 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 KTL**.

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 KTL** 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 KTL**.

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, появление 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.

Интеграции R-Vision IRP и KUMA настраивается в обоих приложениях.

Сопоставление полей алерта KUMA и инцидента R-Vision IRP

Поле алерта KUMA	Поле инцидента R-Vision IRP
`firstSeen`	`detection`

`priority`	`level`
`correlationRuleName`	`description`
`events` (в виде json-файла)	`files`

R-Vision IRP и KUMA: сторона KUMA

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

Интеграция в KUMA настраивается в разделе **Параметры** веб-интерфейса KUMA на закладке **Параметры** → **R-Vision**.

Чтобы настроить интеграцию с R-Vision IRP:

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

   Отобразится список доступных секретов.

2. Нажмите 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** выберите имя для добавляемого секрета. Длина названия должна быть от 1 до 128 символов Юникода.

   b. В раскрывающемся списке **Тенант** выберите тенанта, 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. В поле **Описание** можно добавить 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** → **R-Vision**.

   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.
- **Название компании** – название компании (удобно использовать при работе с несколькими клиентами).
- **Категория** (обязательно) – категория алерта R-Vision IRP, который создается при получении данных об алерте от KUMA.
- **Поля событий KUMA для отправки в R-Vision** (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**.

KUMA теперь настроена для интеграции 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.

R-Vision IRP и KUMA: сторона R-Vision IRP

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

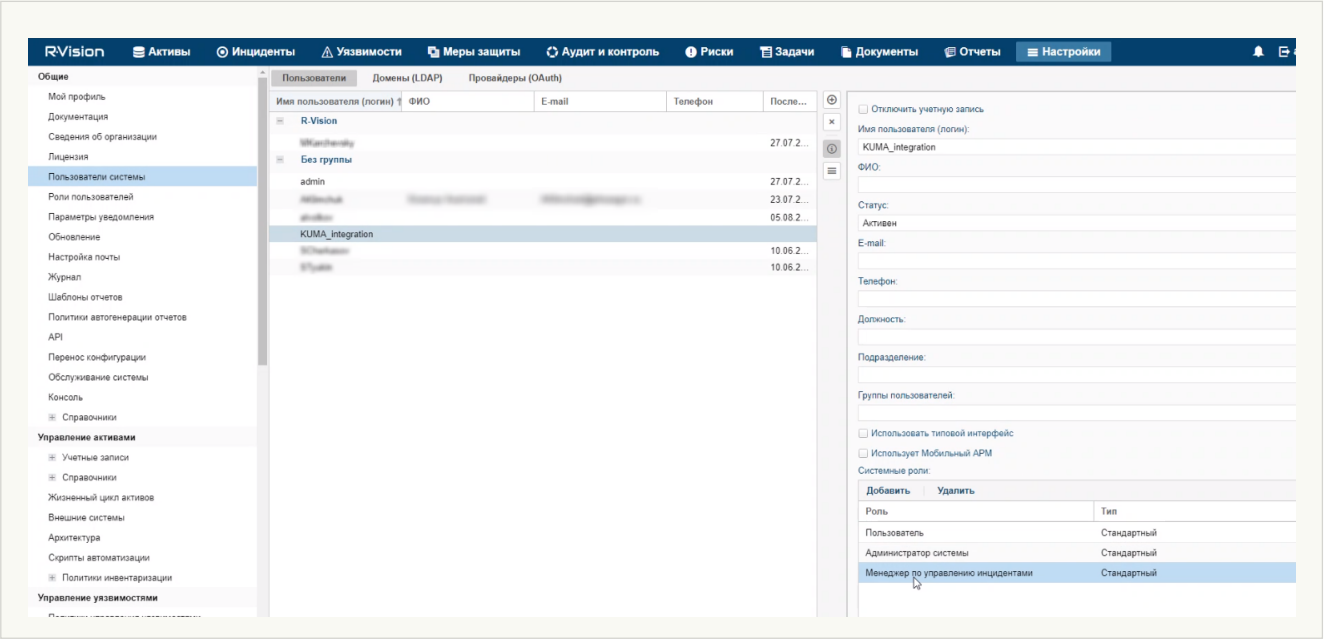
Интеграция в R-Vision IRP настраивается в разделе **Настройки** веб-интерфейса R-Vision IRP. Подробнее о настройке R-Vision IRP см. в документации этой программы.

Настройка интеграции с KUMA состоит из следующих этапов:

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

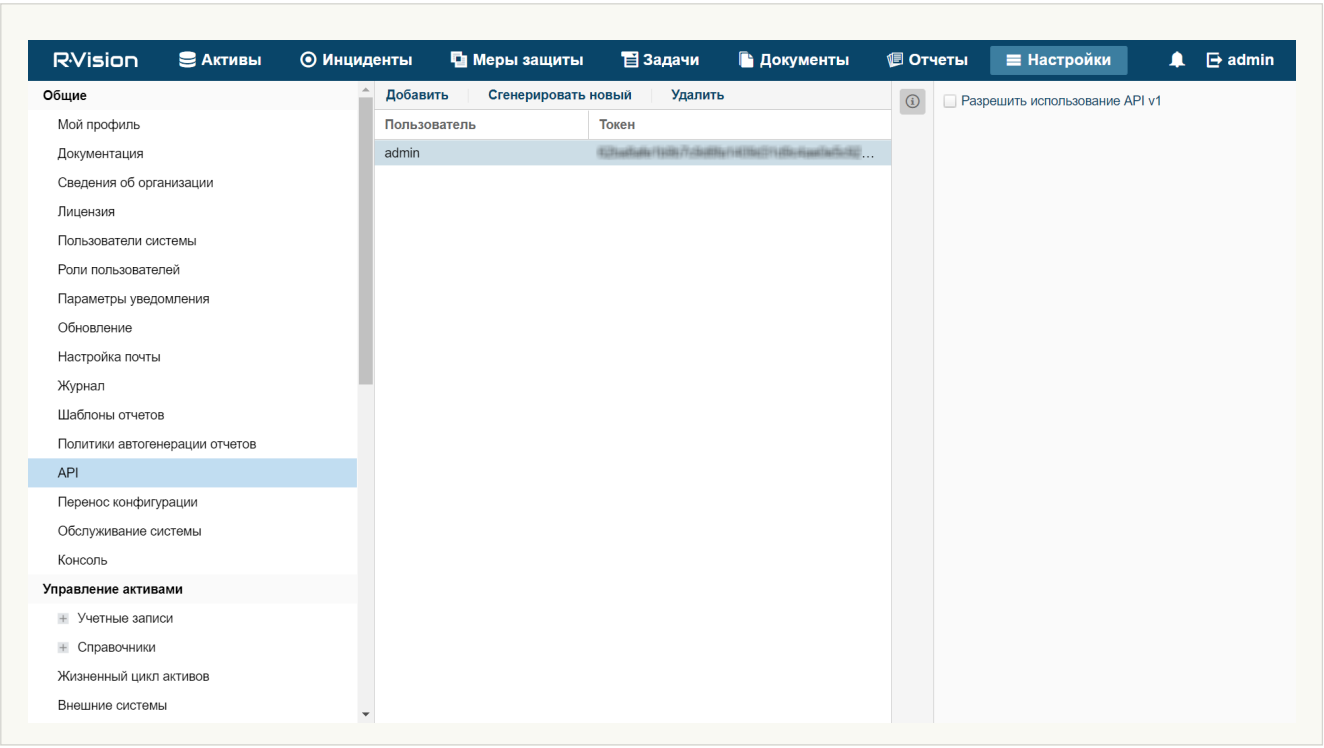
  1. Присвойте используемому для интеграции пользователю R-Vision IRP системную роль **Менеджер по управлению инцидентами**. Роль можно присвоить в веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Общие** → **Пользователи системы**, выбрав нужного пользователя. Роль добавляется в блоке параметров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

     Пользователь R-Vision IRP 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

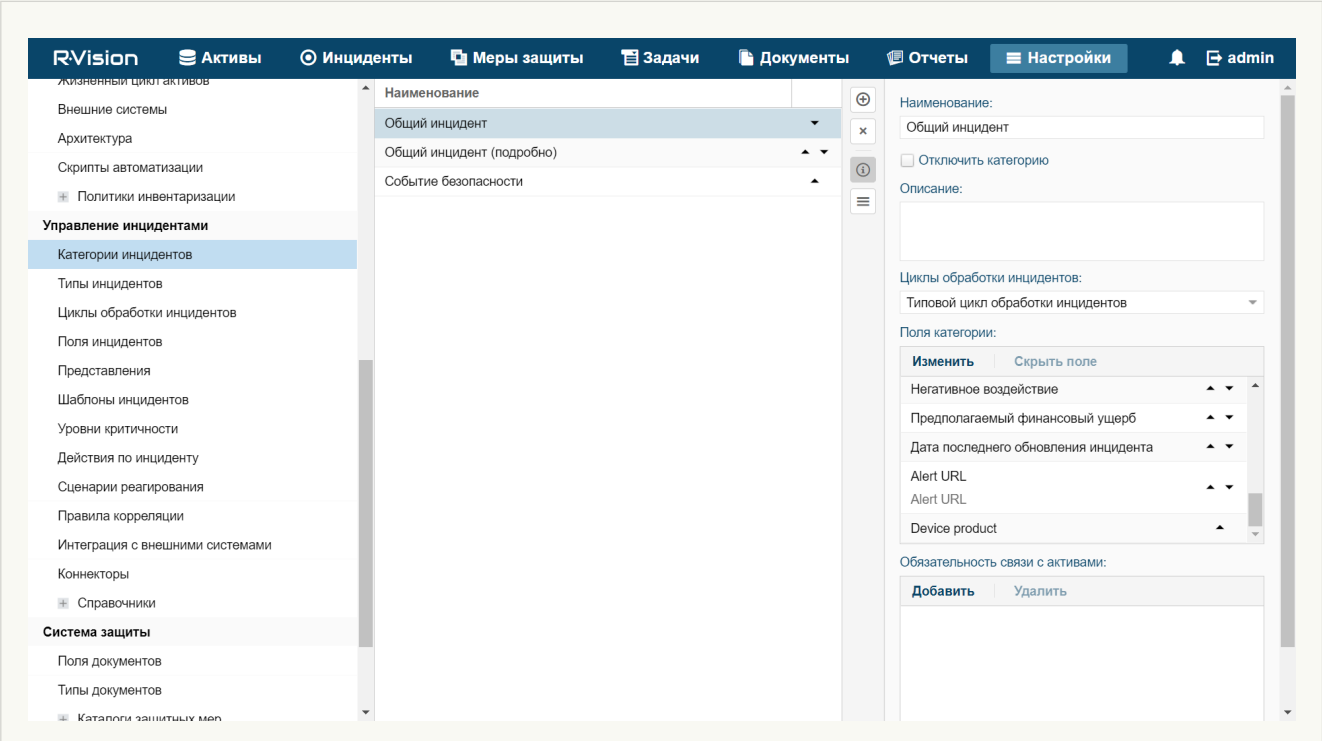


- **Настройка полей инцидентов R-Vision IRP и алертов KUMA**

  1. Добавьте поля инцидента ALERT_ID и ALERT_URL.

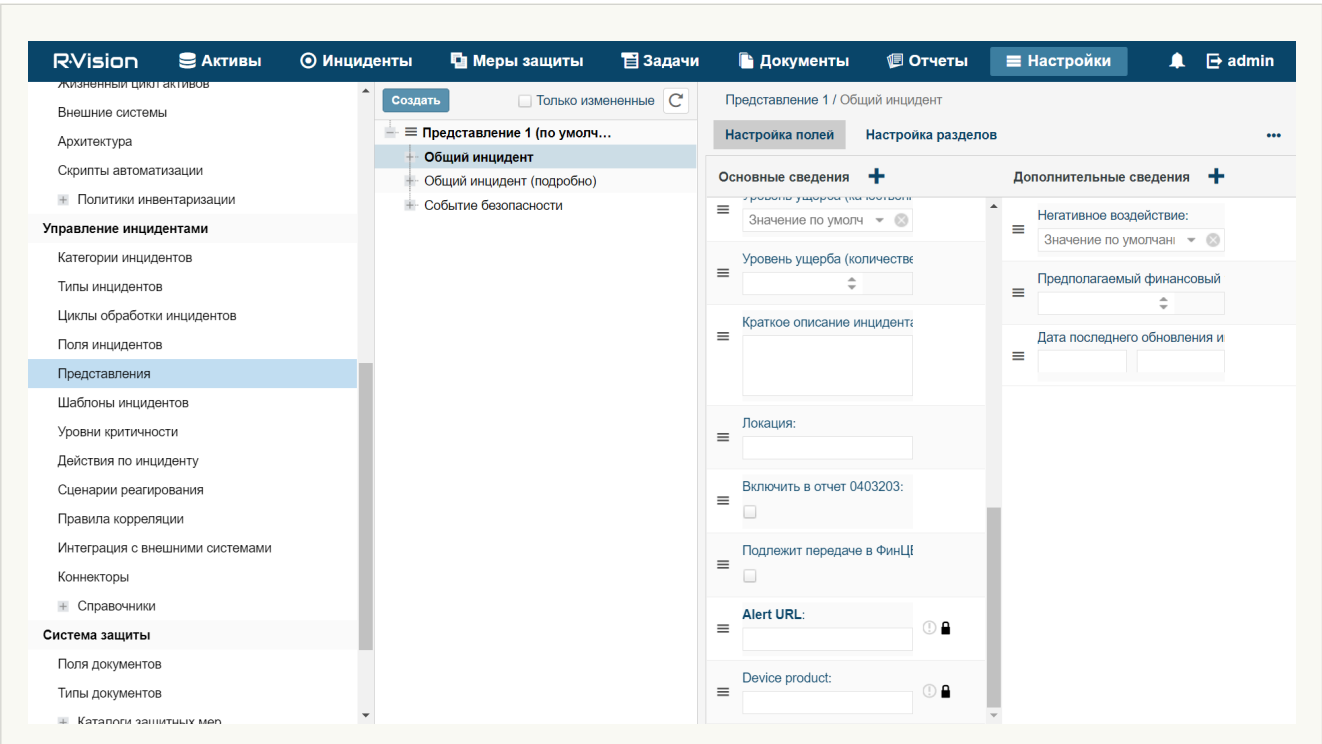
  2. Настройте категорию инцидентов R-Vision IRP, создаваемых по алертам KUMA. Это можно сделать в веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Управление инцидентами** → **Категории инцидентов**. Добавьте новую или измените существующую категорию инцидентов, указав в блоке параметров **Поля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

     Категории инцидентов с данными из алертов KUMA



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 закрыто для редактирования



- **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.

R-Vision IRP теперь настроена для интеграции 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

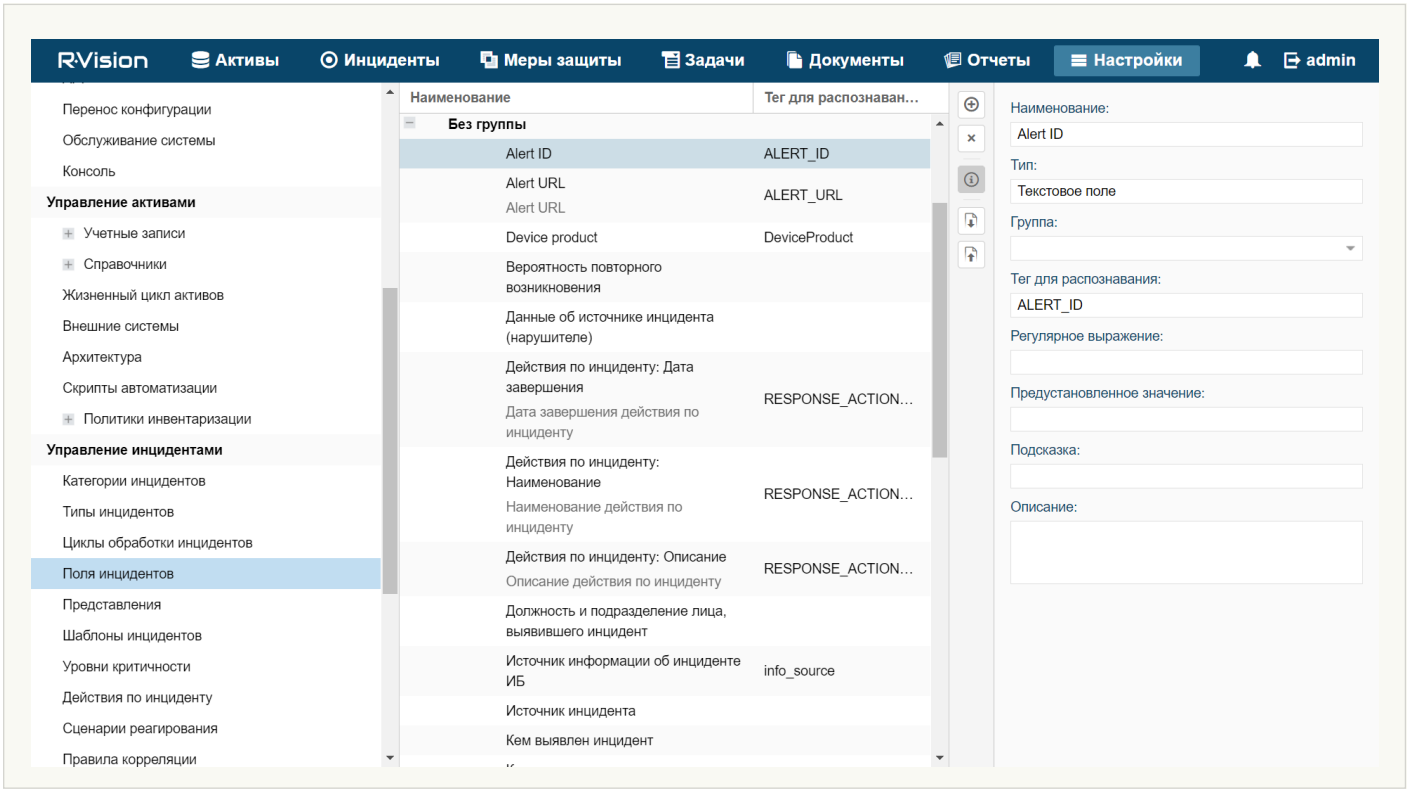
Чтобы добавить в R-Vision IRP поле инцидента ALERT_ID:

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



Чтобы добавить в R-Vision IRP поле инцидента ALERT_URL:

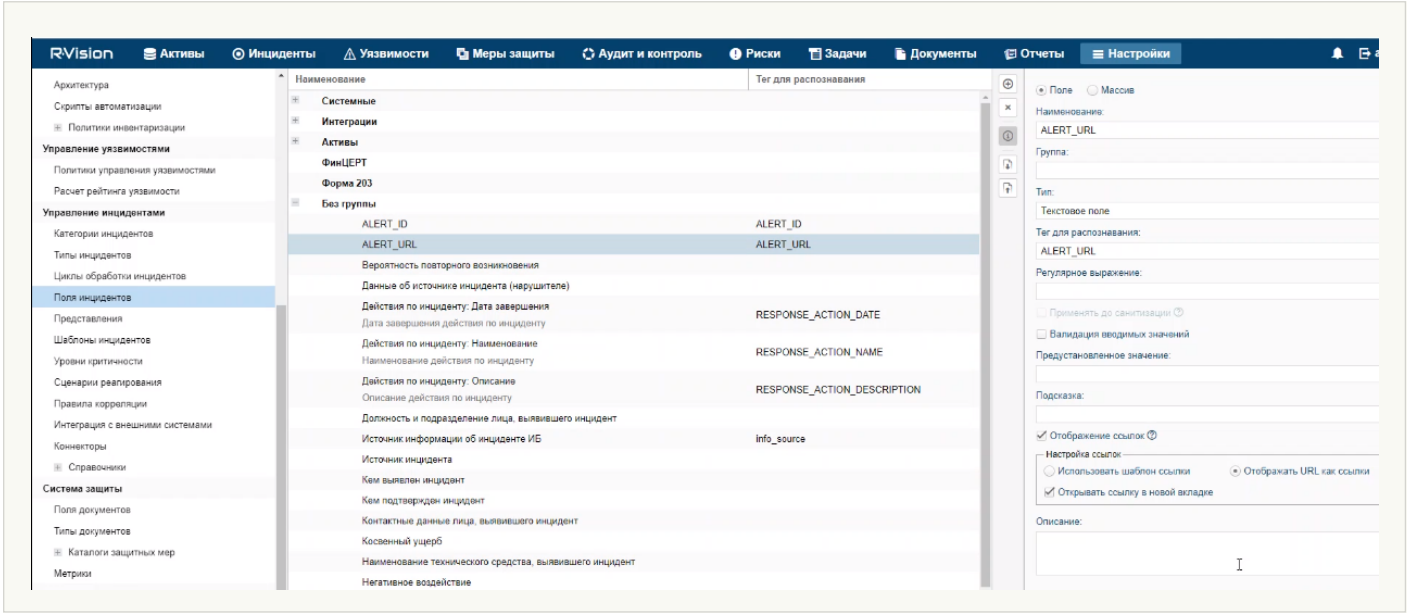
1. В веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Управление инцидентами** → **Поля инцидентов** выберите группу полей **Без группы**.
2. Нажмите на значок плюса в правой части экрана.

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



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** → **Asset Management** → **System components** 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. Установите флажки **Default collector** и **Use for reaction**.
6. Нажмите **Добавить**.

Коллектор R-Vision IRP создан.

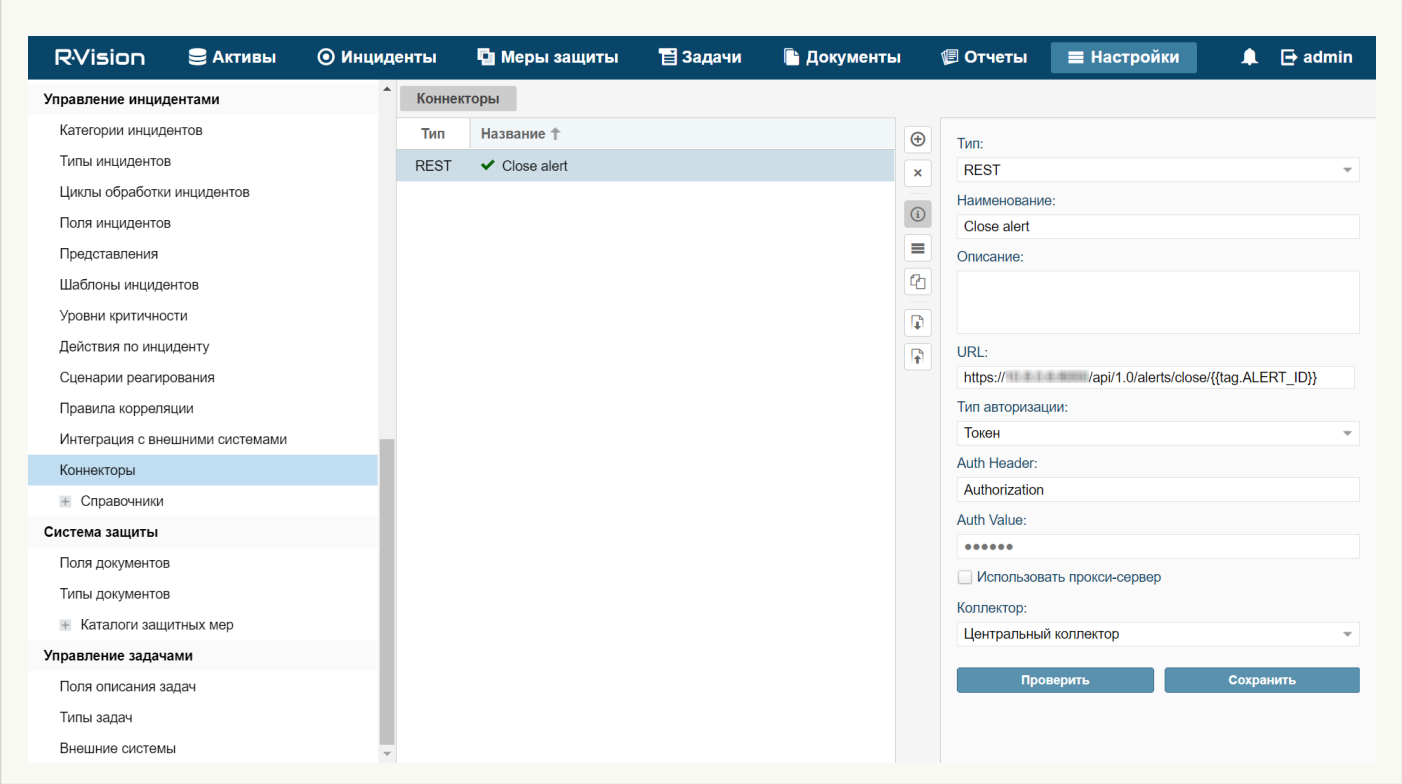
Создание коннектора в R-Vision IRP

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`. Например, `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.
8. Токен главного администратора KUMA можно можно получить в веб-интерфейсе KUMA в разделе **Параметры** → **Пользователи**.
9. В раскрывающемся списке **Коллектор** выберите ранее созданный коллектор.
10. Нажмите **Сохранить**.

Коннектор R-Vision IRP создан, теперь необходимо настроить API-запрос.

Коннектор R-Vision IRP создан



Чтобы настроить коннектор в R-Vision IRP:

1. В веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Управление инцидентами** → **Коннекторы** откройте только что 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`. Например, `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 можно получить в веб-интерфейсе KUMA в разделе **Параметры** → **Пользователи**.

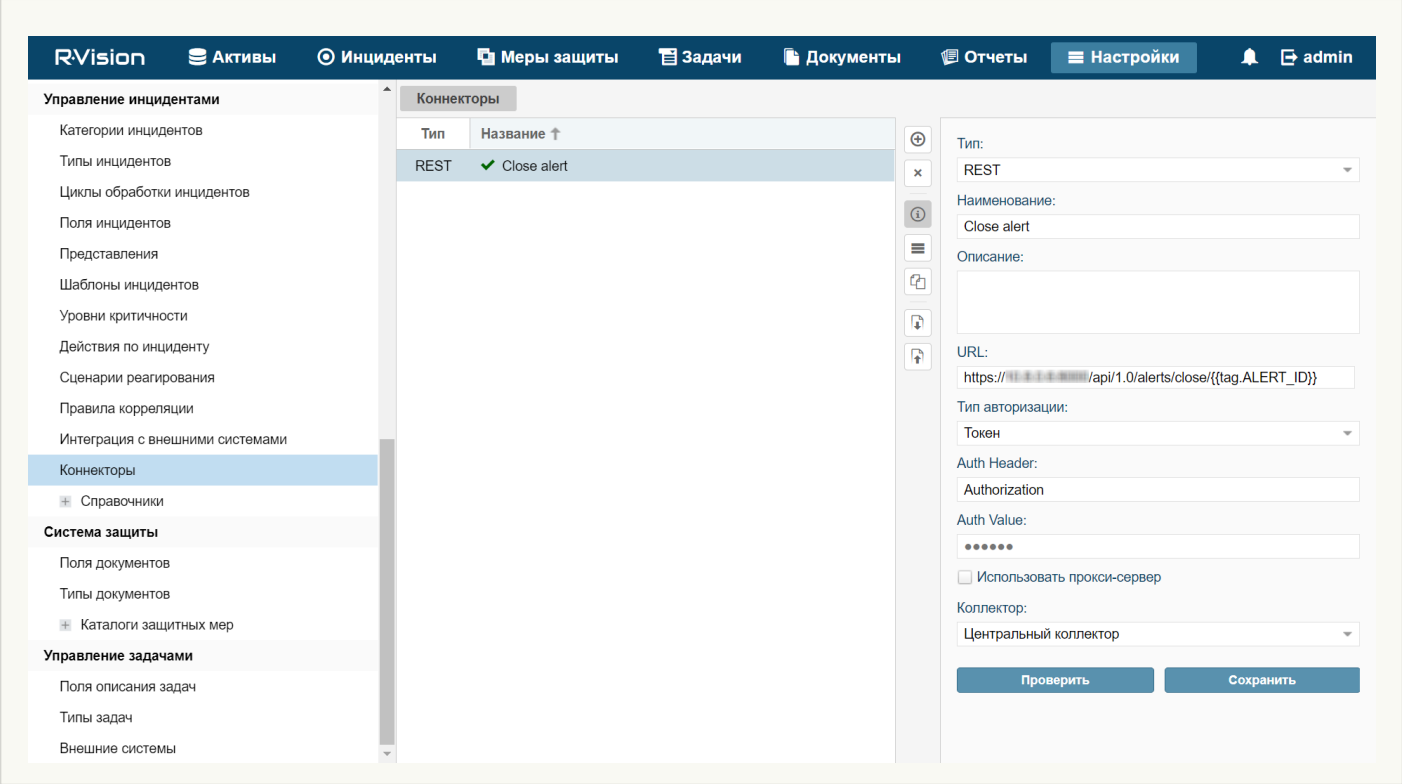
5. На закладке **BODY** → **Raw** введите содержание тела API-запроса:

   ```
   {
       "id":"{{tag.ALERT_ID}}"
       "reason":"<комментарий, который будет добавлен к алерту в KUMA при закрытии. Например, Responded to alert from R-Vision>"
   }
   ```

6. Нажмите **Сохранить**.

Коннектор R-Vision IRP настроен для отправки API-запросов на закрытие алертов в KUMA.

Коннектор R-Vision IRP создан



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: оно будет срабатывать при закрытии инцидента.

5. В блоке параметров **Действия по инциденту** нажмите **Добавить** → **Run connector** и в открывшемся окне выберите коннектор, который следует выполнить при срабатывании правила:

   a. В раскрывающемся списке **Коннектор** выберите ранее созданный коннектор.

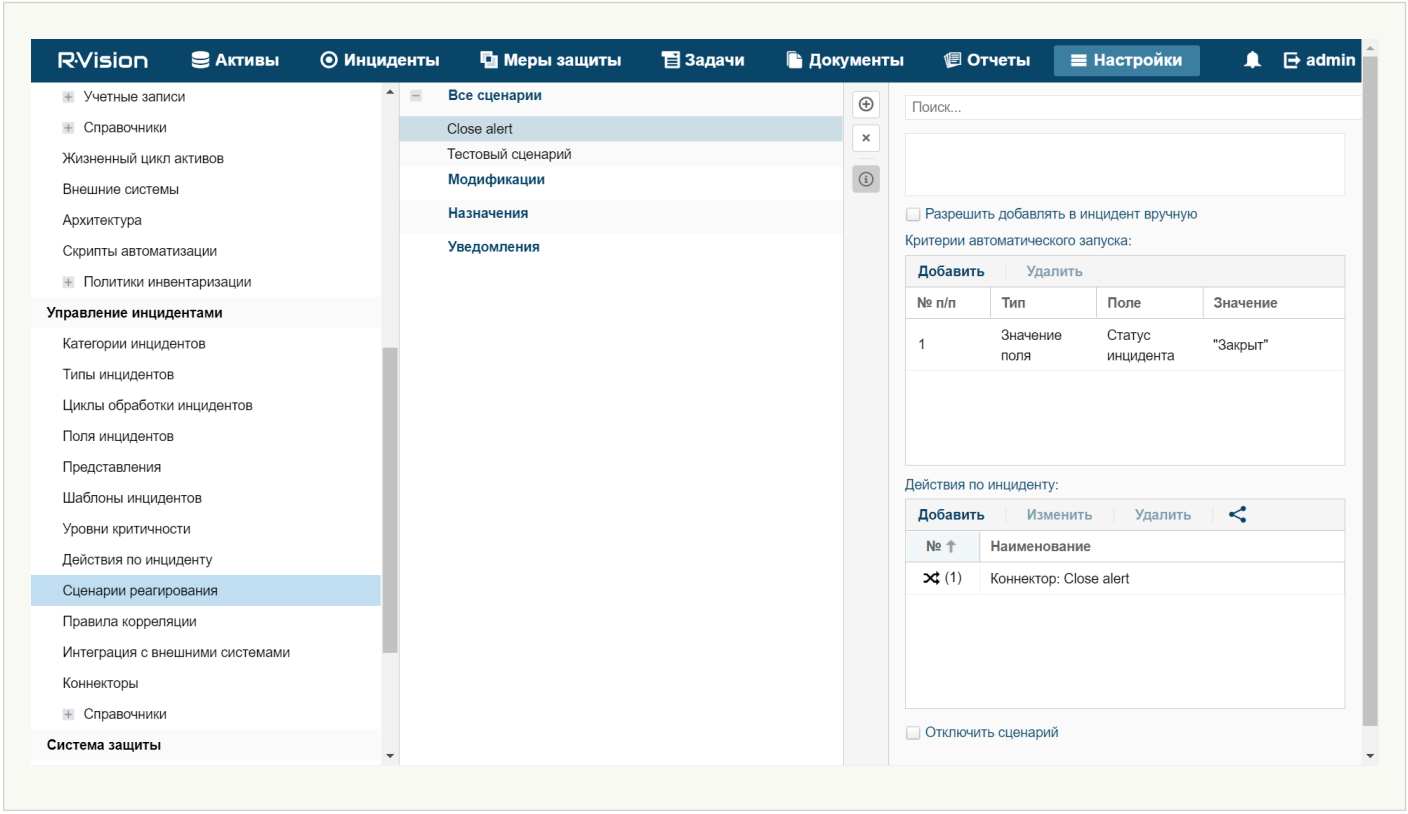
b. Нажмите **Добавить**.

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]



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.

Сценарии работы с алертами в условиях интеграции KUMA и R-Vision IRP:

- **Передача сведений 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 спеиалиста по безопасности, назначенного для обработки алерта.
- Уровень важности алерта.
- Категория инцидента R-Vision IRP, соответствующего алерту KUMA.
- Иерархический список событий, связанных с алертом.
- Список устройств, как внутренних так и внешних, связанных с алертом.
- Список пользователей, связанных с алертом.
- Журнал изменений алерта.
- Ссылка на алерт в KUMA.

- **Расследование киберугроз в KUMA**

  Первоначальная обработка алерта производится в KUMA. Специалист по безопасности может уточнять и менять любые параметры алерта, кроме идентификатора и названия. Сделанные изменения отражаются в карточке инцидента R-Vision IRP.

  Если киберугроза признается ложной и алерт закрываются в KUMA, соответствующий ему инцидент R-Vision IRP также автоматически закрывается.

- **Закрытие инцидента 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.

- **Открытие ранее закрытого инцидента**

  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. Сделанные 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 соответствующий алерт в KUMA остается закрытым.

- **Запрос дополнительных сведений из системы-источника в рамках сценария реагирования или вручную**

  В процессе анализа в R-Vision IRP возникает необходимость получить дополнительные сведения из KUMA. В R-Vision IRP формируется 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.

  Такая же последовательность действий происходит на этапе автоматической обработки, если нет возможности сразу сохранить всю информацию по инциденту при импорте.

Интеграция с Active Directory

KUMA можно интегрировать с используемыми в вашей организации службами Active Directory®.

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 Active Directory 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 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** веб-интерфейса KUMA. В разделе таблице **LDAP** отображаются тенанты, для которых созданы подключения по протоколу LDAP. При выборе тенанта отображаются сами подключения.

*Чтобы добавить в раздел **LDAP** тенанта:*

1. В разделе **Параметры** → **LDAP** веб-интерфейса KUMA нажмите **Добавить**.
2. В открывшемся окне **Подключения по протоколу LDAP** в раскрывающемся списке **Тенант** выберите нужного тенанта и нажмите **Сохранить**.

Тенант добавлен и отображается в таблице раздела **LDAP**.

Если выбрать тенанта, откроется окно **Подключения по протоколу LDAP**, в котором отображается таблица с существующими LDAP-подключениями. Подключения можно создать или выбрать для редактирования.

После включения интеграции информация об учетных записях Active Directory становится доступной в окне алертов, в окне с подробной информацией о событиях корреляции, 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`

В поле **Время хранения данных** можно указать, сколько дней сведения, полученные из LDAP, будут храниться в KUMA после того, как они перестанут поступать от сервера Active Directory.

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** веб-интерфейса KUMA и выберите тенанта, у которого вы хотите включить или выключить все подключения к LDAP.

   Откроется окно **Подключения по протоколу LDAP**.

2. Установите или снимите флажок **Выключить**.

3. Нажмите **Сохранить**.

Чтобы включить или отключить определенное LDAP-подключение:

1. Откройте раздел **Параметры** → **LDAP** веб-интерфейса KUMA и выберите тенанта, у которого вы хотите включить или выключить подключение к LDAP.

   Откроется окно **Подключения по протоколу LDAP**.

2. Выберите нужное подключение и в открывшемся окне установите или снимите флажок **Выключить**.

Создание подключения

Чтобы создать LDAP-подключение к Active Directory:

1. Откройте раздел **Параметры** → **LDAP** веб-интерфейса KUMA и выберите тенанта, для которого хотите создать подключение к LDAP.

   Откроется окно **Подключения по протоколу LDAP**.

2. Нажмите на кнопку **Добавить подключение по протоколу LDAP** и задайте параметры, как описано ниже.

   - **Название** (обязательно) – введите уникальное имя LDAP-подключения. Длина должна быть от 1 до 128 символов Юникода.
   - **URL** (обязательно) – введите URL сервера Active Directory.
   - **Режим TLS** – укажите, нужно ли включить режим TLS для LDAP-подключения. При использовании TLS вы не можете указывать IP-адрес в качестве URL.
   - **Время ожидания в секундах** – укажите время ожидания ответа от сервера Active Directory.
   - **Запросов в секунду** – количество запросов в секунду в формате cron. По умолчанию данные запрашиваются один раз в день.
   - **Фильтр** – укажите фильтр LDAP. Например, `"(&(sAMAccountType=805306368)(!(userAccountControl:1.2.840.113556.1.4.803:=2))"`.

     Фильтр `sAMAccountType=805306368` является обязательным. Если он отсутствует в выражении для пользовательского фильтра, он автоматически добавляется в запрос Active Directory.

   - **База поиска (Base DN)** – введите базовое отличительное имя каталога, в котором должен выполняться поисковый запрос.
   - **Ограничение размера запроса** – введите максимальный размер запроса.
   - **Выключено** – установите этот флажок, если не хотите использовать это LDAP-подключение. По умолчанию этот флажок снят.

3. В блоке параметров **Секрет** создайте или выберите существующий ресурс секрета (тип **credentials**) с учетными данными для подключения к серверу Active Directory:

   - Существующий секрет можно выбрать в раскрывающемся списке. Выбранный секрет можно изменить, нажав на кнопку .
   - Новый секрет можно создать, нажав на кнопку +, указав параметры ниже и нажав **Сохранить**.
     - **Название** (обязательно) – название ресурса: от 1 до 128 символов Юникода.
     - **Пользователь** и **Пароль** (обязательно) – учетные данные для подключения к серверу Active Directory.
     - **Описание** – описание ресурса: до 256 символов Юникода.

4. Нажмите **Сохранить**.

LDAP-подключение к Active Directory создано и отображается в окне **Подключение по протоколу LDAP**.

Информация об учетных записях из Active Directory будет запрошена в течение 12 часов. Чтобы данные стали доступны сразу, перезапустите сервер Ядра KUMA. Информация об учетных записях обновляется каждые 12 часов.

Удаление подключения

Чтобы удалить LDAP-подключения к Active Directory:

1. Откройте раздел **Параметры** → **LDAP** веб-интерфейса KUMA и выберите тенанта, которому принадлежит нужное подключение к LDAP.

   Откроется окно **Подключения по протоколу LDAP**.

2. Нажмите на подключение LDAP, которое вы хотите удалить, а затем нажмите кнопку **Удалить**.

LDAP-подключение к Active Directory будет удалено.

Авторизация с помощью доменных учетных записей

Для того чтобы пользователи могли проходить авторизацию в веб-интерфейсе KUMA с помощью своих доменных учетных данных, требуется выполнить следующие этапы настройки.

1. **Включить доменную авторизацию, если она отключена**

   По умолчанию доменная авторизация включена, но подключение к домену не настроено.

2. **Настроить соединение с контроллером домена**

   Вы можете подключиться только к одному домену.

3. **Добавить фильтры для ролей пользователей**

   Вы можете указать для каждой роли KUMA группу Active Directory. Пользователи из этой группы, пройдя авторизацию 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 в Active Directory указанному фильтру в порядке следования ролей в веб-интерфейсе KUMA: оператор → аналитик → администратор → главный администратор. При первом совпадении пользователю присваивается роль и дальнейшая проверка фильтров не осуществляется. Если для пользователя указано два фильтра в одном тенанте, то будет использована роль с наименьшими правами. Если указано несколько фильтров для разных тенантов, то на каждом тенанте пользователь будет иметь указанную роль.

Включение и выключение доменной авторизации

По умолчанию доменная авторизация включена, но подключение к домену Active Directory не настроено. Если после настройки подключения вы хотите временно приостановить доменную авторизацию, вы можете отключить ее в веб-интерфейсе KUMA, не удаляя заданные ранее значения параметров. При необходимости вы сможете в любой момент включить авторизацию снова.

Чтобы включить или отключить доменную авторизацию пользователей в веб-интерфейсе KUMA:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Active directory**.

2. Выполните одно из следующих действий:

   - Если вы хотите выключить доменную авторизацию, в верхней части рабочей области установите флажок **Выключено**.
   - Если вы хотите включить доменную авторизацию, в верхней части рабочей области снимите флажок **Выключено**.

3. Нажмите на кнопку **Сохранить**.

Доменная авторизация будет включена или отключена.

Настройка соединения с контроллером домена

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** → **Active directory**.
2. В блоке параметров **Подключение** в поле **База поиска (Base DN)** введите DistinguishedName корневой записи для поиска групп доступа в службе каталогов Active Directory.
3. В поле **URL** укажите адрес контроллера домена в формате `<hostname или IP-адрес сервера>:<порт>`.

   Вы можете указать через запятую адреса нескольких (но не более 3) серверов с контроллерами домена на случай, если один из них будет недоступен. Все указанные серверы должны находиться в одном домене.

4. Если вы хотите использовать TLS-шифрование для соединения с контроллером домена, в раскрывающемся списке **Режим TLS** выберите пункт **Включено**.

   По умолчанию TLS-шифрование отключено. При использовании TLS вы не можете указывать IP-адрес в качестве URL.

5. 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 **Секрет**.

      Если ранее не было добавлено ни одного сертификата, в раскрывающемся списке отобразится **Нет данных**.

   b. Если вы хотите загрузить новый сертификат, справа от списка **Секрет** 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 нужный файл.

   e. Если требуется, в поле **Описание** укажите любую информацию о сертификате.

f. Нажмите на кнопку **Сохранить**.

Сертификат будет загружен и отобразится в списке **Секрет**.

6. 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.

7. Если вы хотите настроить доменную авторизацию для пользователя с ролью главного администратора KUMA, в поле **Главный администратор** укажите DistinguishedName группы Active Directory, в которой состоит пользователь.

   > Если для учетной записи найдено совпадение по фильтру для роли главного администратора, то другие фильтры ролей не проверяются.

   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 будет настроено. Для работы доменной авторизации требуется также добавить фильтры для ролей пользователей KUMA.

Добавление фильтров ролей пользователей

> Вы можете заполнить фильтры только для тех ролей, для которых требуется настроить доменную авторизацию. Остальные поля можно оставить пустыми.

Чтобы добавить фильтры ролей пользователей:

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Active directory**.

2. В блоке параметров **Фильтры ролей** нажмите на кнопку **Добавить фильтры ролей**.

3. В раскрывающемся списке **Тенант** выберите, для пользователей какого тенанта вы хотите настроить доменную авторизацию.

4. Укажите DistinguishedName группы Active Directory, пользователи которой должны иметь возможность пройти авторизацию со своими доменными учетными данными, в полях для следующих ролей:

   - **Оператор**.
   - **Аналитик**.
   - **Администратор**.

   Пример ввода фильтра: `CN=KUMA team,OU=Groups,OU=Clients,DC=test,DC=domain`.

Вы можете указать для каждой роли только одну группу Active Directory. 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 авторизацию с ролями оператор, аналитик или администратор тенанта.

6. Нажмите на кнопку **Сохранить**.

Фильтры ролей пользователей будут добавлены. Заданные параметры будут применены после следующего входа пользователя в веб-интерфейс KUMA. После первой авторизации пользователя информация о нем отобразится в разделе **Параметры** → **Пользователи**. Поле **Логин** и **Пароль**, полученные из Active Directory, недоступны для редактирования. Роль пользователя также будет недоступна для редактирования: для изменения роли потребуется изменить фильтры ролей пользователей.

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.

Интеграцию можно включить или выключить с помощью флажка **Выключено**.

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.

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.
- **Реагирование** – ресурсы этого типа используются в корреляторах для выполнения скриптов или запуска задач Kaspersky Security Center при выполнении определенных условий.
- **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.
- **Время обновления** – дата и время последнего обновления ресурса. Может использоваться для сортировки ресурсов.
- **Создан** – имя пользователя, создавшего ресурс.

- **Описание** – описание ресурса.

Ресурсы можно расположить по папкам. В левой части каждой 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.

Инструменты ресурсов

В этом разделе содержится информация об инструментах, доступных в KUMA для организации ресурсов и работы с ними.

Работа с папками ресурсов

Папки можно создавать, переименовывать, перемещать и удалять.

Чтобы создать папку:

Выберите в дереве папку, в которой требуется новая папка.

Нажмите на кнопку **Добавить папку**.

Новая папка 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 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 **ОК**.

Папка удалена. Невозможно удалить папку с файлами или подпапками.

Работа с ресурсами

Ресурсы можно создавать, перемещать, копировать, редактировать и удалять.

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 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 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 находятся в новых папках. Ресурсы невозможно переместить между папками разных тенантов.

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 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 обновлен. Если этот ресурс используется в сервисе, перезапустите сервис, чтобы он задействовал новые настройки.

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 **ОК**.

Ресурс удален.

Экспорт и импорт ресурсов

Вы можете экспортировать и импортировать ресурсы.

Чтобы экспортировать ресурсы:

1. В разделе **Ресурсы** → **<тип ресурса>** нажмите на значок ⋯.

2. В раскрывающемся списке выберите **Экспортировать ресурсы**.

   Откроется окно **Экспортировать ресурсы** с деревом всех доступных ресурсов.

3. В поле **Пароль** введите пароль, который необходимо использовать для защиты экспортируемых данных.

4. В раскрывающемся списке **Тенант** выберите тенанта, ресурсы которого вы хотите экспортировать.

5. Установите флажки рядом с ресурсами, которые вы хотите экспортировать.

   Если выбранные ресурсы связаны с другими ресурсами, эти ресурсы также будут экспортированы.

6. Нажмите на кнопку **Экспортировать**.

Ресурсы в защищенном паролем файле сохранятся на вашем компьютере в зависимости от настроек вашего браузера. Ресурсы секретов экспортируются пустыми.

Чтобы импортировать ресурсы:

1. В раскрывающемся списке ••• выберите **Импортировать ресурсы**.

   Откроется окно **Импорт ресурсов**.

2. В поле **Пароль** введите пароль для файла, который вы хотите импортировать.

3. В раскрывающемся списке **Тенант** выберите тенанта, которому будут принадлежать импортируемые ресурсы.

4. Нажмите на кнопку **Выбрать файл** и укажите файл с ресурсами, которые вы хотите импортировать.

   В окне **Импорт ресурсов** отображается дерево всех доступных ресурсов в выбранном файле.

5. Выберите ресурсы, которые хотите импортировать.

6. Нажмите на кнопку **Импортировать**.

7. Разрешите конфликты (см. ниже) между импортированными и существующими ресурсами, если они возникли. Подробнее о конфликтах ресурсов см. ниже.

   a. Если имя любого из импортированных ресурсов совпадает с именем уже 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, 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, для ресурса коннектора требуется ресурс подключения): такие 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**.

Коннекторы

Ресурсы коннекторов используются для установления соединений между сервисами KUMA, сетевыми устройствами и / или другими службами. Параметры коннекторов отображаются на двух вкладках: **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа коннектора.

Доступные параметры коннекторов:

- **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. Набор доступных параметров зависит от выбранного типа коннектора.

  Доступные типы:

  - **internal**

    Тип **internal** используется для установления связи между сервисами KUMA.

    Доступные параметры:

    - Закладка **Основные параметры**:
      - **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.
    - Закладка **Дополнительные параметры**:
      - **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**.

- **tcp**

  Тип **tcp** используется для связи по протоколу TCP.

  Доступные параметры:

  - Закладка **Основные параметры**:
    - **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. По умолчанию используется `\n`.
  - 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.

      При использовании TLS вы не можете указывать 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**.

- **udp**

Тип **udp** используется для связи по протоколу UDP.

Доступные параметры:

- Закладка **Основные параметры**:
  - **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. По умолчанию используется `\n`.
- 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**.

- **netflow**

Тип **netflow** используется для установления соединений NetFlow.

Доступные параметры:

- Закладка **Основные параметры**:
  - **URL** (обязательно) – URL, с которым необходимо установить связь.
- 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**.

- **nats**

Тип **nats** используется для коммуникации через NATS.

Доступные параметры:

- Закладка **Основные параметры**:
  - **URL** (обязательно) – URL, с которым необходимо установить связь.
  - **Топик** (обязательно) – тема сообщений NATS. Должно содержать от 1 до 255 символов Юникода.
  - **Разделитель** – используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.
- 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: `io.nats`.
  - **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 хранилища** – идентификатор хранилища NATS.
  - **Режим TLS** – использование шифрования TLS:
    - **Выключено** (по умолчанию) – не использовать шифрование TLS.
    - **Включено** – использовать шифрование, но без верификации.
    - **С верификацией** – использовать шифрование с верификацией.

    При использовании TLS вы не можете указывать 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**.

- kafka

Тип **kafka** используется для коммуникации с помощью kafka.

Доступные параметры:

- Закладка **Основные параметры**:
  - **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port.
  - **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`.
- Закладка **Дополнительные параметры**:
  - **Идентификатор группы** – параметр GroupID для сообщений Kafka. Должен содержать от 1 до 255 следующих символов: a–z, A–Z, 0–9, "." `,` `"_",` "-".
  - **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.

    При использовании TLS вы не можете указывать IP-адрес в качестве URL.
  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

- **http**

Тип **http** используется для связи по протоколу HTTP.

Доступные параметры:

- Закладка **Основные параметры**:
  - **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. По умолчанию используется `\n`.
- 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.

    При использовании TLS вы не можете указывать 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**.

- **sql**

Тип **sql** используется для связи с SQL. Поддерживаются следующие типы SQL:

- MSSQL
- MySQL
- PostgreSQL
- CockroachDB
- SQLite3

Доступные параметры:

- Закладка **Основные параметры**:
  - **URL** (обязательно) – раскрывающийся список для выбора ресурса секрета, в котором хранится список строк с запросами на SQL-подключения. Формат строки может зависеть от конкретной базы данных. Ниже приведены примеры строк подключения для MSSQL (две нотации):
    - `sqlserver://username:password@host/instance?param1=value&param2=value`
    - `server=localhost\\SQLExpress;user id=sa;database=master;app name=MyAppName`

    При создании подключений могут некорректно обрабатываться строки с учетными данными, содержащими специальные символы. Если подключение не создается, но вы уверены в правильности параметров, укажите специальные символы в процентной кодировке.

    Коды специальных символов

!	#	$	%	&	'	(	)	*	+
%21	%23	%24	%25	%26	%27	%28	%29	%2A	%2B
,	/	:	;	=	?	@	[	]	
%2C	%2F	%3A	%3B	%3D	%3F	%40	%5B	%5D	

    Следующие специальные символы не поддерживаются в паролях доступа к базам SQL: пробел, [,], :, /, #, %, \.

    Доступные форматы адресов сервера: hostname:port, IPv4:port, IPv6:port.

    При необходимости секрет можно создать в окне создания коннектора с помощью кнопки +. Выбранный секрет можно изменить, нажав на кнопку .
  - **Столбец идентификатора** (обязательно) – параметр столбца идентификаторов для SQL-запросов.
  - **Начальное значение идентификатора** (обязательно) – параметр идентификатора для SQL-запросов.

С помощью параметров **URL**, **Столбец идентификатора** и **Начальное значение идентификатора** определяется одно SQL-подключение. Таких подключений в одном коннекторе можно создать несколько, добавляя новые с помощью кнопки **Добавить подключение**. Удалить подключения можно с помощью кнопки .

- **Запрос** (обязательно) – поле для SQL-запросов.

  Примеры SQL-запросов

  ```
  MySQL – select * from table_name where id > ?

  MSSQL – select * from table_name where id > @p1

  SQLite – select * from table_name where id > ?

  PostgreSQL (и Cockroach) – select * from table_name where id > $1
  ```

- **Интервал запросов, сек.** – время между SQL-запросами в секундах. Значение по умолчанию: 10 секунд.

- 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**.

Оператор UNION не поддерживается коннекторами типа SQL.

KUMA может обрабатывать ответы SQL в кодировке UTF-8. Настройте SQL-сервер на отправку сообщений в кодировке UTF-8 или принудительно меняйте кодировку входящих сообщений на UTF-8, выбрав этот вариант в раскрывающемся списке **Кодировка символов** в настройках коннектора.

- file

Тип **file** используется для получения данных из файла.

Доступные параметры:

- Закладка **Основные параметры**:
  - **URL** (обязательно) – полный путь до файла, с которым требуется выполнять взаимодействие. Например, `/var/*som?[1-9].log`.

    Шаблоны масок для файлов и директорий

    Маски:
    - '*' – соответствует любой последовательности символов;
    - '[' ['^'] { диапазон символов } ']' – класс символов (не должен быть пустым);
    - c – соответствует символу c (c != '*', '?', '\\', '[');
    - '\\' c – соответствует символу c.

    Диапазоны символов:
    - c – соответствует символу c (c != '\\', '-', ']');
    - '\\' c – соответствует символу c;
    - lo '-' hi – соответствует символу c для lo <= c <= hi.

    Примеры:
    - /var/*som?[1-9].log
    - /mnt/dns_logs/*/dns.log
    - /mnt/proxy/access*.log
- 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**.

- ftp

Тип **ftp** используется для получения данных по протоколу File Transfer Protocol.

Доступные параметры:

- Закладка **Основные параметры**:
  - **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);
    - c – соответствует символу c (c != '*', '?', '\\', '[');
    - '\\' c – соответствует символу c.

    Диапазоны символов:
    - c – соответствует символу c (c != '\\', '-', ']');
    - '\\' c – соответствует символу c;
    - lo '-' hi – соответствует символу c для lo <= c <= hi.

    Примеры:
    - /var/*som?[1-9].log
    - /mnt/dns_logs/*/dns.log
    - /mnt/proxy/access*.log

    Если в URL не содержится порт ftp сервера, подставляется 21 порт.
- 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**.

- nfs

Тип **nfs** используется для получения данных по протоколу Network File System.

Доступные параметры:

- Закладка **Основные параметры**:
  - **URL** (обязательно) – путь до удаленной директории в формате nfs://host/path.
  - **Запрос** (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.
- 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**.

- wmi

Тип **wmi** используется для получения данных с помощью Windows Management Instrumentation.

Доступные параметры:

- Закладка **Основные параметры**:
  - **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**.
  - **Учетные данные, используемые по умолчанию** – раскрывающийся список для выбора ресурса секрета, в котором хранятся учетные данные для подключения к удаленным устройствам Windows. При необходимости секрет можно создать в окне создания коннектора с помощью кнопки +. Выбранный секрет можно изменить, нажав на кнопку .
  - В таблице **Удаленные хосты** перечисляются удаленные устройства Windows, к которым требуется установить подключение. Доступные столбцы:
    - **Сервер** – удобочитаемое для пользователя имя устройства, с которой необходимо принимать данные. Например, "src.test.local".
    - **Хост** (обязательно) – IP-адрес или доменное имя устройства, с которого необходимо принимать данные.
    - **Журналы Windows** (обязательно) – 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.

      Преднастроенные журналы:
      - Application
      - ForwardedEvents
      - Security
      - System
      - HardwareEvents
    - **Секрет** – учетные данные для доступа к удаленному устройству Windows с правами на чтение журналов. Можно выбрать ресурс секрета в раскрывающемся списке или создать его с помощью кнопки +. Выбранный секрет можно изменить, нажав на кнопку .

      Если оставить это поле пустым, то будут использоваться учетные данные из секрета, выбранного в раскрывающемся списке **Учетные данные, используемые по умолчанию**.
- 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**.

Изменение параметров на удаленной машине

Чтобы с удаленной машины можно было получать события с помощью WMI:

- На удаленных машинах требуется создать учетные записи 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 требуется открыть следующие TCP-порты: 135, 445, 49152-65535.
- На удаленных машинах требуется запустить следующие службы:
  - Remote Procedure Call (RPC)
  - RPC Endpoint Mapper

- **wec**

Тип **wec** используется для получения данных с помощью Windows Event Collector.

Доступные параметры:

- Закладка **Основные параметры**:
  - **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**.
  - **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
- 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**.

- **snmp**

Тип **snmp** используется для получения данных с помощью Simple Network Management Protocol. Поддерживаемые версии протокола:

- snmpV1
- snmpV2
- snmpV3

Доступные параметры:

- Закладка **Основные параметры**:
  - **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.
- 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**.

- **Описание** – описание ресурса: до 256 символов Юникода.

Нормализаторы

Ресурсы нормализатора используются для приведения "сырых" событий из различных форматов к модели данных событий KUMA. Это превращает "сырые" события в нормализованные, которые уже могут обрабатываться другими ресурсами и сервисами KUMA.

Ресурс нормализатора состоит из *основного* и необязательных *дополнительных нормализаторов*. Данные передаются по древовидной структуре нормализаторов в зависимости от заданных *условий*, что позволяет настроить сложную логику обработки событий.

Ресурс нормализатора создается в несколько этапов:

1. **Создание основного нормализатора**

   Основной нормализатор создается с помощью кнопки **Добавить парсинг событий**. Ввод параметров нормализатора завершается нажатием кнопки **ОК**.

   Созданный основной нормализатор отображается 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.

2. **Создание условий для использования дополнительного нормализатора**

   При нажатии на нормализаторе значка плюса откроется окно **Добавление дополнительного нормализатора**, в котором вы можете определить условия, при которых данные будут поступать в новый нормализатор.

3. **Создание дополнительного нормализатора**

   При завершении предыдущего этапа открывается окно создания дополнительного нормализатора. Ввод параметров нормализатора завершается нажатием кнопки **ОК**.

   Созданный дополнительный нормализатор отображается в виде темного блока, на котором указаны условия, при котором этот нормализатор будет задействован (см. этап 2). Условия можно изменить, редактируя значения в нужных полях.

   Если навести указатель мыши на дополнительный нормализатор, отобразится кнопка со значком плюса, с помощью которой можно создать новый дополнительный нормализатор. С помощью кнопки со значком корзины нормализатор можно удалить.

   Если требуется создать больше дополнительных нормализаторов, повторите этапы 2 и 3.

4. **Завершение создания ресурса нормализатора**

   Создание ресурса нормализатора завершается нажатием кнопки **Сохранить**.

Параметры нормализатора

Окно нормализатора содержит две закладки: **Схема нормализации** и **Обогащение**.

Схема нормализации

Эта закладка используются для указания основных параметров нормализатора, а также определения правил приведения событий к формату KUMA.

Доступные параметры:

- **Название** (обязательно) – имя нормализатора. Должно содержать от 1 до 128 символов Юникода. Название основного нормализатора будет использоваться в качестве названия ресурса нормализатора.

- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

  Этот параметр недоступен для дополнительных нормализаторов.

- **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.

  - **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 один из возможных разделителей значений:

  - `\n` (используется по умолчанию)
  - `\t`
  - `\0`

- **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. По умолчанию используется символ перевода строки, однако 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. По умолчанию используется символ "=", однако 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.

  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 **netflow** 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 **netflow** 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 **netflow** 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.

- **Хранить исходное событие** (обязательно) – с помощью этого раскрывающегося списка можно указать, надо ли сохранять исходное "сырое" событие во вновь созданном нормализованном событии. Доступные значения:

  - **Не хранить** – 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.

Этот параметр недоступен для дополнительных нормализаторов.

- **Сохранить дополнительные поля** (обязательно) – в этом раскрывающемся списке можно выбрать, 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.

- **Описание** – описание ресурса: до 256 символов Юникода.

  Этот параметр недоступен для дополнительных нормализаторов.

- **Примеры событий** – в это поле можно поместить пример данных, которые вы хотите обработать. Пример событий можно также загрузить из файла формата tsv, csv или txt с помощью кнопки **Загрузить из файла**.

- 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.

    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 применения к значению регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для удаления 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 с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования.
- **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.

- **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*.

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

Эта закладка используются для 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. Правил обогащения может быть несколько. Обогащения создаются с помощью кнопки **Добавить обогащение**.

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.

    При выборе этого типа необходимо указать в поле **Константа** 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.

  - **словарь**

    Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря.

    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.

При выборе этого типа в раскрывающемся списке **Исходное поле** необходимо выбрать 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 применения к значению регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для удаления 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 с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования.
- **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.

- **шаблон**

  Этот тип обогащения используется, если в поле события необходимо записать в поле события значение, полученное при обработке шаблонов Go.

  При выборе этого типа в поле **Шаблон** требуется поместить 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}}`.

- **Целевое поле** (обязательно) – раскрывающийся список для выбора поля события KUMA, в которое следует поместить данные.

Условие передачи данных в дополнительный нормализатор

Окно **Добавление дополнительного нормализатора** используется для определения условий, при которых данные будут попадать в дополнительный нормализатор.

Доступные параметры:

- **Поля, которые следует передать в нормализатор** – используется для указания полей события в том случае, если вы хотите отправлять в дополнительный нормализатор только события с определенными полями. Оставьте поле пустым, если хотите передать в дополнительный нормализатор все данные.

- **Нормализовать, если поле события имеет определенное значение** – используется для указания полей события, если вы хотите отправлять в дополнительный нормализатор только события, в которых определенным полям присвоены определенные значения. Значение указывается в поле **Значение условия**.

  Обрабатываемые этими условиями 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 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 применения к значению регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для удаления 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 с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования.
- **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.

Предустановленные нормализаторы

В поставку KUMA включены перечисленные в таблице ниже нормализаторы.

Наименование нормализатора	Источник событий	Тип	Комментарий
[Example] Apache Access Syslog (Common or	Apache access.log в формате Common or Combined Log Format), с Syslog заголовком	syslog	

Combined Log Format)			
[Example] Apache Access file (Common or Combined Log Format)	Apache access.log в формате Common or Combined Log Format)	regexp	Чтение файла
[Example] BIND Syslog	Журналы DNS сервера BIND, с заголовком Syslog	syslog	
[Example] BIND file	Журналы DNS сервера BIND	regexp	Чтение файла
[Example] Bastion SKDPU-GW	ИТ Бастион Система СКДПУ	syslog	
[Example] CEF	События в формате CEF от произвольных источников	cef	
[Example] Checkpoint Syslog CEF by CheckPoint	Checkpoint, нормализация на основании вендорской схемы представления событиий в формат CEF	syslog	
[Example] Checkpoint Syslog basic	Кастомный мапинг полей Checkpoint, нормализация в зависимости от типа устройства	syslog	
[Example] Cisco Basic	Cisco ASA базовый набор событий	syslog	
[Example] Cisco ASA Extended v 0.1	Cisco ASA базовый расширенный набор событий	syslog	
[Example] Cisco WSA AccessFile	Прокси-сервер Cisco WSA, файл access.log	regexp	Чтение файла
[Example] Continent DB AlertLog	Континент АПКШ, запрос к БД, таблица AlertLog	sql	
[Example] Continent DB PacketLog	Континент АПКШ, запрос к БД, таблица PacketLog	sql	
[Example] Continent DB ServerAccessLog	Континент АПКШ, запрос к БД, таблица ServerAccessLog	sql	
[Example] Continent DB SystemLog	Континент АПКШ, запрос к БД, таблица SystemLog	sql	
[Example] CyberTrace	События Kaspersky CyberTrace	regexp	
[Example] DNS Windows	Журналы DNS сервера Windows	regexp	Чтение файла
[Example] Dovecot Syslog	Журналы POP3/IMAP сервера dovecpt	syslog	
[Example] Exchange CSV	Журналы MTA сервера Exchange	csv	Чтение файла
[Example] Fortimail	Журналы почтовой системы Fortimail	regexp	Только KUMA v 1.5
[Example] IIS Log File	Журналы Microsoft IIS	regexp	Чтение файла

Format			
[Example] IPFIX	события Netflow формата IPFIX	ipfix	
[Example] InfoWatch Traffic Monitor	DLP система Traffic Monitor компании Инфовоч	sql	
[Example] KATA	Kaspersky Atri Target Attack	cef	
[Example] KICS4Net v2.x	Kaspersky Industrial Cyber Security v 2.x	cef	
[Example] KICS4Net v3.x	Kaspersky Industrial Cyber Security v 3.x	syslog	
[Example] KSC	Kaspersky Security Center	cef	Пассивное получение событий от KSC: KUMA прослушивает порт, KSC отправляет события
[Example] KSC from SQL	Kaspersky Security Center	sql	Активное получение событий из KSC: KUMA получает события из БД KSC
[Example] KSMG	Kaspersky Security Mail Gateway	syslog	
[Example] Linux audit and iptables Syslog	События Linux	syslog	
[Example] Linux audit.log file	События Linux	regexp	Чтение файла
[Example] Syslog	События в формате Syslog от произвольных источников	syslog	
[Example] Syslog-CEF	События в формате CEF от произвольных источников, с заголовком Syslog	syslog	
[Example] VipNet Coordinator Syslog	Журналы VipNet Coordinator	syslog	На основании примеров журналов отдного из заказчиков
[Example] Windows Basic	Базовый набор событий Windows Security	xml	
[Example] Windows Extended v.0.1	Расширенный набор событий Windows	xml	
[Example] pfSense Syslog	События pfSence	syslog	
[Example] pfSense w/o hostname	Кастомный нормализатор события pfSence (некорректный формат Syslog заголовка)	regexp	
[Example][Syslog] Continent IPS/IDS & TLS	Континент COB, TSL	syslog	Получение по Syslog
[Example][regexp] Continent IPS/IDS & TLS	Континент COB, TSL	regexp	Чтение файла
[Example] NetFlow v5	События Netflow v5	netflow5	
[Example] NetFlow	События Netflow v9	netflow9	

v9			
[Example] MS DHCP file	Журналы DHCP сервера Windows	csv	Чтение файла
[Example] Nginx regexp	Журнал Nginx	regexp	
[Example] 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
[Example] PT WAF	Web Application Firewall компании Positive Technologies	syslog	
[Example] Squid access Syslog	Журналы access.log прокси-сервера Squid	syslog	
[Example] Squid access.log file	Журналы access.log прокси-сервера Squid	regexp	Чтение файла
[Example] Unbound Syslog	Журналы DNS сервера unbount	syslog	

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.

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** (обязательные) – это список полей событий, используемых для создания записи активного листа и служащих ключом записи активного листа.
  - **Поле события** (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:
  - **Название** (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.
- **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 **Не учитывать регистр**, если требуется, чтобы оператор игнорировал регистр значений. Флажок игнорируется, если выбраны операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

  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.
- **inActiveList** – этот фильтр имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inCategory** – устройству в левом операнде назначается по крайней мере одна из категорий устройств 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).

Доступные типы операндов зависят от того, является ли операнд левым (L) или правым (R).

Доступные типы операндов для левого (L) и правого (R) операндов

	тип поле события	тип активный лист	тип словарь	тип константа	тип список	тип TI
оператор =	L,R	L,R	L,R	R	R	L,R
> оператор	L,R	L,R	L,R	R		L,R
оператор >=	L,R	L,R	L,R	R		L,R
< оператор	L,R	L,R	L,R	R		L,R
оператор <=	L,R	L,R	L,R	R		L,R
оператор contains	L,R	L,R	L,R	R	R	L,R
оператор startsWith	L,R	L,R	L,R	R	R	L,R
оператор endsWith	L,R	L,R	L,R	R	R	L,R
оператор match	L	L	L	R	R	L

оператор inSubnet	L,R	L,R	L,R	R	R	L,R
оператор inCategory	L	L	L	R	R	
оператор inActiveDirectoryGroup	L	L	L	R	R	
оператор inActiveList		L				
оператор TIDetect						

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.

    При выборе этого типа необходимо указать в поле **Константа** 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.

  - **словарь**

    Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря.

    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.

При выборе этого типа в раскрывающемся списке **Исходное поле** необходимо выбрать 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 применения к значению регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для удаления 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 с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования.
- **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.

- шаблон

Этот тип обогащения используется, если в поле события необходимо записать в поле события значение, полученное при обработке шаблонов Go.

При выборе этого типа в поле **Шаблон** требуется поместить 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}}`.

- 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 кэша** – время жизни значений, хранящихся в кеше. Значение по умолчанию: `60`.
  - **Кэш 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 **Поля 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.

- **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 ресурсом правила агрегации. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах

1. В раскрывающемся меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, включите переключатель **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию переключатель выключен.

3. Если вы включили переключатель **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.

       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.
       - **inActiveList** – этот фильтр имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
       - **inCategory** – устройству в левом операнде назначается по крайней мере одна из категорий устройств 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).

С помощью флажка **с учетом регистра** в раскрывающемся списке **оператор** можно указать, требуется ли учитывать регистр значений, переданных в фильтр. По умолчанию флажок снят.

- 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 ×.

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 ресурсом правила агрегации. 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** и **inActiveDirectoyGroup**.

  Создание фильтра в ресурсах

1. В раскрывающемся меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, включите переключатель **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию переключатель выключен.

3. Если вы включили переключатель **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.

       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.
       - **inActiveList** – этот фильтр имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
       - **inCategory** – устройству в левом операнде назначается по крайней мере одна из категорий устройств 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).

С помощью флажка **с учетом регистра** в раскрывающемся списке **оператор** можно указать, требуется ли учитывать регистр значений, переданных в фильтр. По умолчанию флажок снят.

- 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 ×.

Точки назначения

Ресурсы точек назначения 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.

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) – раскрывающийся список для выбора типа точки назначения:

  - **nats** – используется для коммуникации через NATS.

  - **tcp** – используется для связи по протоколу TCP.

  - **http** – используется для связи по протоколу HTTP.

  - **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.

- **URL** (обязательно) – URL, куда следует отправлять события. В URL требуется указывать вместе с портом. Например: `hostname:port`.

  Для всех типов, кроме **nats** и **file** с помощью кнопки **URL** можно указать несколько адресов отправки, если в вашу лицензию KUMA включен модуль High Level Availability.

  Если в качестве типа точки назначения выбраны **storage** или **correlator**, поле **URL** можно заполнить автоматически с помощью раскрывающегося списка **Копировать URL сервиса**, в котором отображаются активные сервисы выбранного типа.

- **Топик** (обязательно) – параметр типов точек назначения **nats** и **kafka**. Топик, в который должны записываться данные. Топик должен содержать от 1 до 255 символов Юникода.

- **Описание** – описание ресурса: до 256 символов Юникода.

Дополнительные параметры

- **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 хранилища** – идентификатор хранилища 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.

  При использовании TLS вы не можете указывать 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**
  - **Сначала первый**
  - **По очереди**

- **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**.

- **Очистка 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 ресурсом правила агрегации. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах

1. В раскрывающемся меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, включите переключатель **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию переключатель выключен.

3. Если вы включили переключатель **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.

       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.
       - **inActiveList** – этот фильтр имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
       - **inCategory** – устройству в левом операнде назначается по крайней мере одна из категорий устройств 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).

С помощью флажка **с учетом регистра** в раскрывающемся списке **оператор** можно указать, требуется ли учитывать регистр значений, переданных в фильтр. По умолчанию флажок снят.

- 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 ×.

Словари

Словари – это ресурсы, в которых хранятся пары ключей и значений, которые могут использоваться другими ресурсами и сервисами KUMA. Информация, содержащаяся в словаре, отображается в виде таблицы.

Доступные параметры:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.

- **Тенант** (обязательно) – имя тенанта, которому принадлежит ресурс.

- **Описание** – вы можете добавить до 256 символов Юникода, описывающих ресурс.

- Блок параметров **Значения** – содержит таблицу пар **Ключ** – **Значение**. В таблицу можно добавлять новые строки с помощью кнопки **Пустые поля** или удалять строки с помощью кнопки ×.

Данные словаря можно импортировать или экспортировать в формате CSV с помощью ссылок **Импортировать CSV** и **Экспортировать CSV**.

Импорт CSV

Вы можете импортировать информацию в словарь в формате CSV `{КЛЮЧ}[,|;]{ЗНАЧЕНИЕ}\n`, где:

- `{КЛЮЧ}` – уникальный ключ как для CSV-файла, так и для словаря, в который импортируется CSV-файл.

- `[, |;]` – разделитель. Запятая или точка с запятой. Если строка содержит оба символа, в качестве разделителя используется запятая.
- `{ЗНАЧЕНИЕ}` – значение ключа.

Когда файл CSV импортируется, имя словаря изменяется, чтобы отразить имя импортированного файла. Импортированные ключи и значения добавляются в словарь. Вы можете импортировать данные в словарь несколько раз.

Экспорт CSV

Вы можете экспортировать информацию из словаря в формате CSV `{КЛЮЧ},{ЗНАЧЕНИЕ}\n`, где:

- `{КЛЮЧ}` – уникальный ключ как для CSV-файла, так и для словаря, в который импортируется CSV-файл.
- Запятая используется как разделитель.
- `{ЗНАЧЕНИЕ}` – значение ключа.

Если ключ или значение содержат символы запятой или кавычек (, и "), они заключаются в кавычки ("). Кроме того, символ кавычки (") экранируется дополнительной кавычкой (").

Правила корреляции

Ресурсы правила корреляции используются в сервисах коррелляторов 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 событий корреляции при обнаружении определенного события.
- operational – используется для операций с активными листами. Этот тип ресурсов не может создавать корреляционные события.

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.
- **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 быть 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`.
- **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 следующие параметры:

- **Название** (обязательно) – уникальное имя группы событий, удовлетворяющее 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 меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, включите переключатель **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию переключатель выключен.

3. Если вы включили переключатель **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.

       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.
       - **inActiveList** – этот фильтр имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
       - **inCategory** – устройству в левом операнде назначается по крайней мере одна из категорий устройств 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).

С помощью флажка **с учетом регистра** в раскрывающемся списке **оператор** можно указать, требуется ли учитывать регистр значений, переданных в фильтр. По умолчанию флажок снят.

- 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 ×.

- **Обнуление** – этот флажок должен быть установлен, если правило корреляции НЕ должно срабатывать при получении селектором определенного количества событий. По умолчанию этот флажок снят.

Если к ресурсу правила корреляции добавлено более одного селектора, становится доступной группа параметров **Объединяющий фильтр**. Этот фильтр используется для сравнения полей разных событий. Объединяющий фильтр настраивается с помощью раскрывающегося списка **Фильтр**, как описано выше.

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.

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, используемые для создания записи активного листа. Этот список также используется в качестве ключа записи активного листа.

  - **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. 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:

    - **constant**

      > Этот тип обогащения используется, если в поле события необходимо добавить константу.
      >
      > При выборе этого типа необходимо указать в поле **Константа** 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.

- **dictionary**

  Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря.

  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.

- **event**

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события.

При выборе этого типа в раскрывающемся списке **Исходное поле** необходимо выбрать 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 применения к значению регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для удаления 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 с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования.
- **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.

- template

Этот тип обогащения используется, если в поле события необходимо записать в поле события значение, полученное при обработке шаблонов Go.

При выборе этого типа в поле **Шаблон** требуется поместить 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}}`.

- **Целевое поле** – в этом раскрывающемся списке можно выбрать 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 устройств, указанных в событии. Правил категоризации может быть несколько: их можно добавить или удалить с помощью кнопок **Добавить категоризацию** или **Удалить категоризацию**. Устройствам можно добавлять или удалять только реактивные категории.
  - **Действие** – этот раскрывающийся список используется для выбора операции над категорией:
    - **Добавить** – присвоить категорию устройству.
    - **Удалить** – отвязать устройство от категории.
  - **Поле события** – поле события, в котором указано устройство, 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.
- **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.
- **Частота срабатываний** – максимальное количество срабатываний правила корреляции в секунду.
- **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 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 меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, включите переключатель **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию переключатель выключен.

3. Если вы включили переключатель **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.

       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.
       - **inActiveList** – этот фильтр имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
       - **inCategory** – устройству в левом операнде назначается по крайней мере одна из категорий устройств 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).

С помощью флажка **с учетом регистра** в раскрывающемся списке **оператор** можно указать, требуется ли учитывать регистр значений, переданных в фильтр. По умолчанию флажок снят.

- 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 ×.

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.

- **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. 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:

    - constant

      Этот тип обогащения используется, если в поле события необходимо добавить константу.

      При выборе этого типа необходимо указать в поле **Константа** 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.

    - dictionary

      Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря.

      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.

    - event

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события.

При выборе этого типа в раскрывающемся списке **Исходное поле** необходимо выбрать 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 применения к значению регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для удаления 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 с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования.
- **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.

- template

Этот тип обогащения используется, если в поле события необходимо записать в поле события значение, полученное при обработке шаблонов Go.

При выборе этого типа в поле **Шаблон** требуется поместить 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}}`.

- **Целевое поле** – в этом раскрывающемся списке можно выбрать 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 устройств, указанных в событии. Правил категоризации может быть несколько: их можно добавить или удалить с помощью кнопок **Добавить категоризацию** или **Удалить категоризацию**. Устройствам можно добавлять или удалять только реактивные категории.
  - **Действие** – этот раскрывающийся список используется для выбора операции над категорией:
    - **Добавить** – присвоить категорию устройству.
    - **Удалить** – отвязать устройство от категории.
  - **Поле события** – поле события, в котором указано устройство, 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 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 **operational**, если хотите создать правило корреляции типа operational.
- **Частота срабатываний** – максимальное количество срабатываний правила корреляции в секунду.
- **Описание** – описание ресурса. До 256 символов Юникода.

Закладка **Селекторы**

В ресурсе типа **operational** может быть один селектор. В селекторе доступен только блок 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 меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, включите переключатель **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию переключатель выключен.

3. Если вы включили переключатель **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.

       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.
       - **inActiveList** – этот фильтр имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
       - **inCategory** – устройству в левом операнде назначается по крайней мере одна из категорий устройств 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).

С помощью флажка **с учетом регистра** в раскрывающемся списке **оператор** можно указать, требуется ли учитывать регистр значений, переданных в фильтр. По умолчанию флажок снят.

- 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 ×.

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.

- **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. Средний раскрывающийся список используется для выбора полей событий. Правое поле можно использовать для назначения константы полю активного листа, если была выбрана операция **Установить**.

Активные листы

Ресурсы активных листов – это динамически обновляемые контейнеры данных, используемые корреляторами KUMA для чтения и записи информации при анализе событий по правилам корреляции.

Параметры ресурса активный лист:

- **Идентификатор** – идентификатор активного листа. Этот параметр отображается у созданных активных листов. Значение можно скопировать с помощью кнопки .
- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – имя тенанта, которому принадлежит ресурс.
- **Срок жизни** – время в секундах, в течение которого в активном листе будет храниться добавленная в него запись. Значение по умолчанию: `0`. Максимальный срок жизни: `31536000` (один год). При истечении срока жизни запись удаляется, при этом создается событие удаления записи из активного листа (см. ниже).
- **Описание** – вы можете добавить до 256 символов Юникода, описывающих ресурс.

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

Правила реагирования

Ресурсы правил реагирования используются для автоматической отправки сообщений при выполнении определенных условий. Ресурсы этого типа используются в коррелляторах.

Доступные параметры ресурсов правил реагирования:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – имя тенанта, которому принадлежит ресурс.
- **Тип** (обязательно) – доступные типы реагирования:
  - **ksctasks** – если настроена интеграция KUMA и Kaspersky Security Center, можно настроить правила реагирования на запуск задач Kaspersky Security Center, связанных с устройствами. Например, можно запустить антивирусную проверку или обновление базы данных. Такие задачи можно стартовать только для устройств, импортированных из Kaspersky Security Center.

    Параметры реагирования типа ksctasks

    - **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`".
    - **Поле события** (обязательно) – определяет поле события для устройства, 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.

    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 устройств этого тенанта задача не будет выполнена. Такая ситуация может возникнуть, например, когда два тенанта используют общий коррелятор.

  - **script** – используется для выполнения последовательности команд, записанных в файл. Файл скрипта хранится на сервере, где установлен сервис коррелятора, использующий ресурс реагирования:

/opt/kaspersky/kuma/correlator/<Идентификатор коррелятора>/scripts. Пользователь `kuma` этого сервера должен иметь права на запуск скрипта.

Параметры реагирования типа script

- **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}}"`

- **Описание** – вы можете добавить до 256 символов Юникода, описывающих ресурс.
- **Рабочие процессы** – количество рабочих процессов, которые одновременно могут быть заняты задачами реагирования.
- **Фильтр** – используется для определения условий, при соответствии которым события 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 меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, включите переключатель **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию переключатель выключен.

3. Если вы включили переключатель **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.

       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.
       - **inActiveList** – этот фильтр имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
       - **inCategory** – устройству в левом операнде назначается по крайней мере одна из категорий устройств 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).

С помощью флажка **с учетом регистра** в раскрывающемся списке **оператор** можно указать, требуется ли учитывать регистр значений, переданных в фильтр. По умолчанию флажок снят.

- 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 ×.

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) – имя тенанта, которому принадлежит ресурс.

- **URL** (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 *секрет* 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) – имя 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.

Доступные параметры, зависящие от типа секрета:

- **credentials** – этот тип секретов используется для хранения данных учетных записей, с помощью которых осуществляется подключение к другим службам, например к SMTP-серверам.
  - **Пользователь** и **Пароль** (обязательные поля) – имя пользователя и пароль, которые используются для подключения к внешней службе.
- **token** – используется для хранения токенов для API-запросов. Токены используются, например, при подключении к R-Vision IRP.
  - **Токен** (обязательно) – это поле используется для хранения токена.
- **ktl** – используется для хранения данных учетной записи Kaspersky Threat Intelligence Portal.
  - **Имя** и **Пароль** (обязательные поля) – имя пользователя и пароль вашей учетной записи Kaspersky Threat Intelligence Portal.
  - **PFX** (обязательно) – этот раздел используется для загрузки ключа сертификата Kaspersky Threat Intelligence Portal.
  - **Пароль PFX** (обязательно) – в этом поле вводится пароль для доступа к ключу сертификата Kaspersky Threat Intelligence Portal.
- **urls** – используется для хранения URL. Поля URL можно добавлять с помощью кнопки **Добавить** и удалять с помощью кнопки ×.

  Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.
- **snmpV1** – используется для хранения значения **Уровень доступа** (например, `public` или `private`), требуемое при взаимодействии по протоколу Simple Network Management Protocol.
- **snmpV3** – используется для хранения данных, требуемое при взаимодействии по протоколу Simple Network Management Protocol:
  - **Пользователь** – имя пользователя, указывается без домена.
  - **Уровень безопасности** – уровень безопасности пользователя:
    - **NoAuthNoPriv** – сообщения посылаются без аутентификации и без обеспечения конфиденциальности.
    - **AuthNoPriv** – 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 пользователя. 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 уровней безопасности AuthPriv.
- **Пароль обеспечения безопасности** – пароль шифрования, который был указан при создании пользователя. Это поле становится доступно при выборе уровней безопасности AuthPriv.

- **cetrificate** – используется для хранения файлов сертификатов. Файлы загружаются в ресурс с помощью кнопки **Загрузить файл сертификата**.

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`.

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 с устройств Windows.

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:

- **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.
- **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.

- **Время работы** – как долго сервис работает.

С помощью кнопки **Добавить сервис** можно создавать новые сервисы на основе существующих наборов ресурсов для сервисов. В этом окне также можно перезапустить сервис или удалить его сертификат, скопировать идентификатор сервиса или удалить сервис. Кроме того, в этом разделе можно просмотреть разделы хранилищ и активные листы коррелляторов.

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 наборе ресурсов. Изменения сохраняются с помощью кнопки **Сохранить** и вступают в силу после перезапуска сервиса.

Инструменты сервисов

В этом разделе описываются инструменты по работе с сервисами, доступные в раздел веб-интерфейса KUMA **Ресурсы → Активные сервисы**.

Получение идентификатора сервиса

Идентификатор сервиса используется для связи частей сервиса – расположенной внутри KUMA и установленной 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. Этот вариант используется для изменения таких параметров, как порт или тип коннектора.
   - **Сбросить сертификат** – удалить сертификаты, используемые сервисом для внутренней связи. Например, этот вариант подойдет при обновлении сертификата Ядра.

Сервис будет перезапущен.

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.

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.
- **Дата** – дата создания раздела.

- **Пространство** – название раздела.
- **Размер** – размер раздела.
- **События** – количество хранимых событий.
- **Истекает** – дата, когда истекает срок действия пространства.

Вы можете удалять пространства.

Чтобы удалить пространство:

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

   Откроется окно подтверждения.
4. Нажмите **ОК**.

Пространство удалено.

Окно активных листов коррелятора

В таблице **Активные листы коррелятора** можно просмотреть список активных листов, которые использует определенный коррелятор.

*Чтобы открыть таблицу **Активные листы коррелятора**:*

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

   Откроется таблица **Активные листы коррелятора**.

В таблице есть следующие столбцы:

- **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.

Активные листы можно просматривать, импортировать, экспортировать или очищать.

Чтобы просмотреть активный лист:

Откройте таблицу **Активные листы коррелятора** (см. выше) и нажмите название требуемого активного листа.

Откроется таблица с содержимым активного листа. Если вы хотите просмотреть содержимое записи, нажмите на значение ее ключа (столбец **Ключ**). Если запись следует удалить, нажмите на значок . С помощью поля **Поиск** можно искать нужные записи.

Чтобы экспортировать активный лист:

1. Откройте таблицу **Активные листы коррелятора** (см. выше).
2. Открой раскрывающийся список ... слева от необходимого активного листа.
3. Нажмите **Экспортировать**.

   Активный лист будет загружен в формате JSON используя настройки вашего браузера. Название загруженного файла соответствует названию активного листа.

Чтобы импортировать данные в активный лист:

1. Откройте таблицу **Активные листы коррелятора** (см. выше).
2. Открой раскрывающийся список ... слева от необходимого активного листа.
3. Нажмите **Импортировать**.

   Откроется окно импорта активного листа.
4. В поле **Файл** выберите файл, который требуется импортировать.
5. В раскрывающемся списке **Формат** выберите формат файла:
   - **csv**
   - **tsv**
   - **internal**
6. В поле **Ключевое поле** введите значение ключа активного листа.
7. Нажмите **Импортировать**.

   Данные из файла импортированы в активный лист.

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**, в котором будет отображаться таблица с событиями, отобранными по поисковому выражению `ServiceID = <идентификатор выбранного сервиса>`.

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.
- **Время обновления** – дата и время последнего обновления набора ресурсов. Может использоваться для сортировки.
- **Создан** – имя пользователя, создавшего набор ресурсов.
- **Описание** – описание набора ресурсов.

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 **Подключить источник событий**.

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

Установка коллектора на сервер, предназначенный для получения событий, на сервере 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 событий**.
- В веб-интерфейсе KUMA в разделе **Ресурсы** → **Коллекторы** нажмите **Добавить коллектор**.

Следуйте указаниям мастера.

Шаги мастера, кроме первого и последнего, можно выполнять в произвольном порядке. Переключаться между шагами можно с помощью кнопок **Вперед** и **Назад**, а также нажимая на названия шагов в левой части окна.

По завершении мастера в веб-интерфейсе KUMA в разделе **Ресурсы** → **Коллекторы** создается набор ресурсов для коллектора, а в разделе **Ресурсы** → **Активные сервисы** добавляется сервис коллектора.

Шаг 1. Подключение источников событий

Это обязательный шаг мастера установки. На этом шаге указывается основные параметры коллектора: название и тенант, которому он будет принадлежать.

Чтобы задать основные параметры коллектора:

- В поле **Название** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов Юникода.
- В раскрывающемся списке **Тенант** выберите тенанта, 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 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 коллектора 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**

  Тип **internal** используется для установления связи между сервисами KUMA.

  Доступные параметры:

  - Закладка **Основные параметры**:
    - **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.
  - Закладка **Дополнительные параметры**:
    - **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**.

- **tcp**

  Тип **tcp** используется для связи по протоколу TCP.

  Доступные параметры:

  - Закладка **Основные параметры**:
    - **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. По умолчанию используется `\n`.
  - 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.

      При использовании TLS вы не можете указывать 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**.

- udp

  Тип **udp** используется для связи по протоколу UDP.

  Доступные параметры:

  - Закладка **Основные параметры**:
    - **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. По умолчанию используется `\n`.
  - 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**.

- netflow

  Тип **netflow** используется для установления соединений NetFlow.

  Доступные параметры:

  - Закладка **Основные параметры**:
    - **URL** (обязательно) – URL, с которым необходимо установить связь.
  - 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**.

- nats

Тип **nats** используется для коммуникации через NATS.

Доступные параметры:

- Закладка **Основные параметры**:
  - **URL** (обязательно) – URL, с которым необходимо установить связь.
  - **Топик** (обязательно) – тема сообщений NATS. Должно содержать от 1 до 255 символов Юникода.
  - **Разделитель** – используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.
- 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: `io.nats`.
  - **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 хранилища** – идентификатор хранилища NATS.
  - **Режим TLS** – использование шифрования TLS:
    - **Выключено** (по умолчанию) – не использовать шифрование TLS.
    - **Включено** – использовать шифрование, но без верификации.
    - **С верификацией** – использовать шифрование с верификацией.

    При использовании TLS вы не можете указывать 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**.

- kafka

Тип **kafka** используется для коммуникации с помощью kafka.

Доступные параметры:

- Закладка **Основные параметры**:
  - **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port.
  - **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`.
- Закладка **Дополнительные параметры**:
  - **Идентификатор группы** – параметр GroupID для сообщений Kafka. Должен содержать от 1 до 255 следующих символов: a–z, A–Z, 0–9, "." `,` `"_",` "-".
  - **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.

    При использовании TLS вы не можете указывать IP-адрес в качестве URL.
  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

- **http**

Тип **http** используется для связи по протоколу HTTP.

Доступные параметры:

- Закладка **Основные параметры**:
  - **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. По умолчанию используется `\n`.
- 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.

    При использовании TLS вы не можете указывать 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**.

- **sql**

Тип **sql** используется для связи с SQL. Поддерживаются следующие типы SQL:

- MSSQL
- MySQL
- PostgreSQL
- CockroachDB
- SQLite3

Доступные параметры:

- Закладка **Основные параметры**:
  - **URL** (обязательно) – раскрывающийся список для выбора ресурса секрета, в котором хранится список строк с запросами на SQL-подключения. Формат строки может зависеть от конкретной базы данных. Ниже приведены примеры строк подключения для MSSQL (две нотации):
    - `sqlserver://username:password@host/instance?param1=value&param2=value`
    - `server=localhost\\SQLExpress;user id=sa;database=master;app name=MyAppName`

    При создании подключений могут некорректно обрабатываться строки с учетными данными, содержащими специальные символы. Если подключение не создается, но вы уверены в правильности параметров, укажите специальные символы в процентной кодировке.

    Коды специальных символов

!	#	$	%	&	'	(	)	*	+
%21	%23	%24	%25	%26	%27	%28	%29	%2A	%2B
,	/	:	;	=	?	@	[	]	
%2C	%2F	%3A	%3B	%3D	%3F	%40	%5B	%5D	

    Следующие специальные символы не поддерживаются в паролях доступа к базам SQL: пробел, [,], :, /, #, %, \.

    Доступные форматы адресов сервера: hostname:port, IPv4:port, IPv6:port.

    При необходимости секрет можно создать в окне создания коннектора с помощью кнопки +. Выбранный секрет можно изменить, нажав на кнопку .
  - **Столбец идентификатора** (обязательно) – параметр столбца идентификаторов для SQL-запросов.
  - **Начальное значение идентификатора** (обязательно) – параметр идентификатора для SQL-запросов.

С помощью параметров **URL**, **Столбец идентификатора** и **Начальное значение идентификатора** определяется одно SQL-подключение. Таких подключений в одном коннекторе можно создать несколько, добавляя новые с помощью кнопки **Добавить подключение**. Удалить подключения можно с помощью кнопки .

- **Запрос** (обязательно) – поле для SQL-запросов.

  Примеры SQL-запросов

  ```
  MySQL – select * from table_name where id > ?

  MSSQL – select * from table_name where id > @p1

  SQLite – select * from table_name where id > ?

  PostgreSQL (и Cockroach) – select * from table_name where id > $1
  ```

- **Интервал запросов, сек.** – время между SQL-запросами в секундах. Значение по умолчанию: 10 секунд.

- 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**.

Оператор UNION не поддерживается коннекторами типа SQL.

KUMA может обрабатывать ответы SQL в кодировке UTF-8. Настройте SQL-сервер на отправку сообщений в кодировке UTF-8 или принудительно меняйте кодировку входящих сообщений на UTF-8, выбрав этот вариант в раскрывающемся списке **Кодировка символов** в настройках коннектора.

- file

Тип **file** используется для получения данных из файла.

Доступные параметры:

- Закладка **Основные параметры**:
  - **URL** (обязательно) – полный путь до файла, с которым требуется выполнять взаимодействие. Например, `/var/*som?[1-9].log`.

    Шаблоны масок для файлов и директорий

    Маски:
    - '*' – соответствует любой последовательности символов;
    - '[' ['^'] { диапазон символов } ']' – класс символов (не должен быть пустым);
    - c – соответствует символу c (c != '*', '?', '\\', '[');
    - '\\' c – соответствует символу c.

    Диапазоны символов:
    - c – соответствует символу c (c != '\\', '-', ']');
    - '\\' c – соответствует символу c;
    - lo '-' hi – соответствует символу c для lo <= c <= hi.

    Примеры:
    - /var/*som?[1-9].log
    - /mnt/dns_logs/*/dns.log
    - /mnt/proxy/access*.log
- 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**.

- ftp

Тип **ftp** используется для получения данных по протоколу File Transfer Protocol.

Доступные параметры:

- Закладка **Основные параметры**:
  - **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);
    - c – соответствует символу c (c != '*', '?', '\\', '[');
    - '\\' c – соответствует символу c.

    Диапазоны символов:
    - c – соответствует символу c (c != '\\', '-', ']');
    - '\\' c – соответствует символу c;
    - lo '-' hi – соответствует символу c для lo <= c <= hi.

    Примеры:
    - /var/*som?[1-9].log
    - /mnt/dns_logs/*/dns.log
    - /mnt/proxy/access*.log

    Если в URL не содержится порт ftp сервера, подставляется 21 порт.
- 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**.

- nfs

Тип **nfs** используется для получения данных по протоколу Network File System.

Доступные параметры:

- Закладка **Основные параметры**:
  - **URL** (обязательно) – путь до удаленной директории в формате nfs://host/path.
  - **Запрос** (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.
- 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**.

- wmi

Тип **wmi** используется для получения данных с помощью Windows Management Instrumentation.

Доступные параметры:

- Закладка **Основные параметры**:
  - **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**.
  - **Учетные данные, используемые по умолчанию** – раскрывающийся список для выбора ресурса секрета, в котором хранятся учетные данные для подключения к удаленным устройствам Windows. При необходимости секрет можно создать в окне создания коннектора с помощью кнопки +. Выбранный секрет можно изменить, нажав на кнопку .
  - В таблице **Удаленные хосты** перечисляются удаленные устройства Windows, к которым требуется установить подключение. Доступные столбцы:
    - **Сервер** – удобочитаемое для пользователя имя устройства, с которой необходимо принимать данные. Например, "src.test.local".
    - **Хост** (обязательно) – IP-адрес или доменное имя устройства, с которого необходимо принимать данные.
    - **Журналы Windows** (обязательно) – 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.

      Преднастроенные журналы:
      - Application
      - ForwardedEvents
      - Security
      - System
      - HardwareEvents
    - **Секрет** – учетные данные для доступа к удаленному устройству Windows с правами на чтение журналов. Можно выбрать ресурс секрета в раскрывающемся списке или создать его с помощью кнопки +. Выбранный секрет можно изменить, нажав на кнопку .

      Если оставить это поле пустым, то будут использоваться учетные данные из секрета, выбранного в раскрывающемся списке **Учетные данные, используемые по умолчанию**.
- 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**.

Изменение параметров на удаленной машине

Чтобы с удаленной машины можно было получать события с помощью WMI:

- На удаленных машинах требуется создать учетные записи 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 требуется открыть следующие TCP-порты: 135, 445, 49152-65535.
- На удаленных машинах требуется запустить следующие службы:
  - Remote Procedure Call (RPC)
  - RPC Endpoint Mapper

- **wec**

Тип **wec** используется для получения данных с помощью Windows Event Collector.

Доступные параметры:

- Закладка **Основные параметры**:
  - **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**.
  - **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
- 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**.

- **snmp**

Тип **snmp** используется для получения данных с помощью Simple Network Management Protocol. Поддерживаемые версии протокола:

- snmpV1
- snmpV2
- snmpV3

Доступные параметры:

- Закладка **Основные параметры**:
  - **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.
- 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**.

При использовании типа коннектора **tcp** или **upd** на этапе нормализации в поле событий DeviceAddress, если она пустая, 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.

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. Можно добавить несколько нормализаторов и реализовать сложную логику обработки событий.

При создании нового нормализатора в мастере установки он будет сохранен в наборе ресурсов для коллектора и не сможет быть использован в других коллекторах. Если вы хотите использовать один и тот же нормализатор в разных сервисах, рекомендуется создать его в виде отдельного ресурса.

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 **ОК**.

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. Введите в поле **Название** уникальное имя для нормализатора. Название должно содержать от 1 до 128 символов Юникода.

3. 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.

   - **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 один из возможных разделителей значений:

  - `\n` (используется по умолчанию)
  - `\t`
  - `\0`

- **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. По умолчанию используется символ перевода строки, однако 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. По умолчанию используется символ "=", однако 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.

  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 **netflow** 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 **netflow** 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 **netflow** 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.

4. В раскрывающемся списке **Хранить исходное событие** укажите, надо ли сохранять исходное "сырое" событие во вновь созданном нормализованном событии. Доступные значения:

   - **Не хранить** – 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.

5. 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.

6. Скопируйте в поле **Примеры событий** пример данных, которые вы хотите обработать. Это необязательный, но рекомендуемый шаг.

   Пример событий можно также загрузить из файла формата tsv, csv или txt с помощью кнопки **Загрузить из файла**.

7. 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 применения к значению регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для удаления 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 с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования.
- **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.

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*, при необходимости 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.

8. 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).

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 нормализатор и в окне **Парсинг событий** перейдите на закладку **Обогащение**.
2. Нажмите на кнопку **Добавить обогащение**.

   Появится блок параметров правила обогащения. Блок параметров можно закрыть 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:

   - **constant**

     Этот тип обогащения используется, если в поле события необходимо добавить константу.

     При выборе этого типа необходимо указать в поле **Константа** 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.

   - **dictionary**

     Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря.

     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.

   - **event**

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события.

При выборе этого типа в раскрывающемся списке **Исходное поле** необходимо выбрать 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 применения к значению регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для удаления 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 с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования.
- **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.

- **template**

  Этот тип обогащения используется, если в поле события необходимо записать в поле события значение, полученное при обработке шаблонов Go.

  При выборе этого типа в поле **Шаблон** требуется поместить 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}}`.

4. В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

5. Нажмите **OK**.

В нормализатор добавлены правила обогащения и окно **Парсинг событий** закрыто.

Создание структуры нормализаторов

Внутри нормализатора можно создать несколько дополнительных нормализаторов. Это позволяет настроить сложную логику обработки событий.

Последовательность создания нормализаторов имеет значение: события обрабатываются последовательно и их путь отображается в виде стрелочек.

Чтобы создать дополнительный нормализатор:

- Создайте начальный нормализатор (см. выше).

  Созданный нормализатор отобразится в окне в виде темного кружка.

- Наведите указатель мыши на начальный нормализатор и нажмите на появившуюся кнопку со значком плюса.

- В открывшемся окне **Добавление дополнительного нормализатора** укажите условия, при которых данные будут попадать в дополнительный нормализатор:

  - Если вы хотите отправлять в дополнительный нормализатор только события с определенными полями, перечислите их в поле **Поля, которые следует передать в нормализатор**.

  - Если вы хотите отправлять в дополнительный нормализатор только события, в которых определенным полям присвоены определенные значения, задайте название поля события в поле **Нормализовать, если поле события имеет определенное значение**, а значение, которое должно ему соответствовать, – в поле **Значение условия**.

  Обрабатываемые этими условиями 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 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 применения к значению регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для удаления 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 с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования.
- **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.

- Нажмите **OK**.

  Откроется окно **Парсинг событий**, в котором можно настроить правила обработки событий, как в начальном нормализаторе (см. выше). Параметр **Хранить исходное событие** недоступен. В поле **Примеры событий** отображаются значения, указанные при создании начального нормализатора.

- Укажите параметры дополнительного нормализатора по аналогии с параметрами начального нормализатора
- Нажмите **OK**.

Дополнительный нормализатор отображается в виде темного блока, на котором указаны условия, при котором этот нормализатор будет задействован. Условия можно изменить, редактируя значения в нужных полях. Если навести указатель мыши на дополнительный нормализатор, отобразится кнопка со значком плюса, с помощью которой можно создать новый дополнительный нормализатор. С помощью кнопки со значком корзины нормализатор можно удалить.

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, включите переключатель **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию переключатель выключен.
3. Если вы включили переключатель **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.

       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.
- **inActiveList** – этот фильтр имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inCategory** – устройству в левом операнде назначается по крайней мере одна из категорий устройств 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).

- 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 **с учетом регистра** можно выбрать, требуется ли учитывать регистр значений, переданных в фильтр.
- 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 фильтра. 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, в течение которого 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 ресурсом правила агрегации. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

   Создание фильтра в ресурсах

1. В раскрывающемся меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, включите переключатель **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию переключатель выключен.

3. Если вы включили переключатель **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.

       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.
       - **inActiveList** – этот фильтр имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
       - **inCategory** – устройству в левом операнде назначается по крайней мере одна из категорий устройств 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).

С помощью флажка **с учетом регистра** в раскрывающемся списке **оператор** можно указать, требуется ли учитывать регистр значений, переданных в фильтр. По умолчанию флажок снят.

- 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 ×.

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 же 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 запросов KUMA с ответами LDAP:

   - В столбце **Поле KUMA** укажите поле события KUMA, данные из которого следует отправить в LDAP.

   - В столбце **LDAP-атрибут** укажите тип отправляемых в LDAP данных.

- В столбце **Поле для записи данных** укажите, в какое поле события KUMA следует поместить данные, полученные из LDAP.

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 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 правила реагирования.

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 правила реагирования.

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 ним параметры:

   - **константа**

     Этот тип обогащения используется, если в поле события необходимо добавить константу.

     При выборе этого типа необходимо указать в поле **Константа** 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.

   - **словарь**

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря.

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.

При выборе этого типа в раскрывающемся списке **Исходное поле** необходимо выбрать 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 применения к значению регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для удаления 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 с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования.
- **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.

- **шаблон**

Этот тип обогащения используется, если в поле события необходимо записать в поле события значение, полученное при обработке шаблонов Go.

При выборе этого типа в поле **Шаблон** требуется поместить 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}}`.

- 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 кэша** – время жизни значений, хранящихся в кеше. Значение по умолчанию: `60`.
  - **Кэш 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 **Поля 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.

4. В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

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

6. 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 меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, включите переключатель **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию переключатель выключен.

3. Если вы включили переключатель **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.

       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.
       - **inActiveList** – этот фильтр имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
       - **inCategory** – устройству в левом операнде назначается по крайней мере одна из категорий устройств 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).

С помощью флажка **с учетом регистра** в раскрывающемся списке **оператор** можно указать, требуется ли учитывать регистр значений, переданных в фильтр. По умолчанию флажок снят.

- 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 ×.

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** и **file** с помощью кнопки **URL** можно указать несколько адресов отправки, если в вашу лицензию KUMA включен модуль High Level Availability.

     Если в качестве типа точки назначения выбраны **storage** или **correlator**, поле **URL** можно заполнить автоматически с помощью раскрывающегося списка **Копировать URL сервиса**, в котором отображаются активные сервисы выбранного типа.

   - Для типов **nats** и **kafka** в поле **Топик** укажите, в какой в какой топик должны записываться данные. Топик должен содержать от 1 до 255 символов Юникода.

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 хранилища** – идентификатор хранилища 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.

     При использовании TLS вы не можете указывать 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**
     - **Сначала первый**
     - **По очереди**
   - **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**.
   - **Очистка 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 ресурсом правила агрегации. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах

1. В раскрывающемся меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, включите переключатель **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию переключатель выключен.

3. Если вы включили переключатель **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.

       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.
       - **inActiveList** – этот фильтр имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
       - **inCategory** – устройству в левом операнде назначается по крайней мере одна из категорий устройств 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).

С помощью флажка **с учетом регистра** в раскрывающемся списке **оператор** можно указать, требуется ли учитывать регистр значений, переданных в фильтр. По умолчанию флажок снят.

- 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 ×.

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

   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, как пользователь root.

2. Выполните следующую команду:

   ```
   /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: `/opt/kaspersky/kuma/kuma collector --core https://kuma.example.com:7210 --id XXXX --api.port YYYY --install`

   Команду, с помощью которой можно установить коллектор на сервере, 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. 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`.

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.

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 **Добавить 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 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 коррелятора рекомендуется убедиться в правильности его работы.

Запуск мастера установки коррелятора

Коррелятор состоит из двух частей: одна часть создается внутри веб-интерфейса KUMA, а другая устанавливается на сервере сетевой инфраструктуры, предназначенном для обработки событий. В мастере установки создается первая часть коррелятора.

Чтобы запустить мастер установки коррелятора:

- В веб-интерфейсе KUMA в разделе **Ресурсы** нажмите **Добавить коррелятор**.
- В веб-интерфейсе KUMA в разделе **Ресурсы** → **Коррелляторы** 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** → **Коррелляторы** 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 указывается 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 тенанта, 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. 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.

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.

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.

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 3. 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 ним параметры:

   - **константа**

     Этот тип обогащения используется, если в поле события необходимо добавить константу.

     При выборе этого типа необходимо указать в поле **Константа** 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.

   - **словарь**

     Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря.

     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.

При выборе этого типа в раскрывающемся списке **Исходное поле** необходимо выбрать 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 применения к значению регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для удаления 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 с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования.
- **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.

- **шаблон**

Этот тип обогащения используется, если в поле события необходимо записать в поле события значение, полученное при обработке шаблонов Go.

При выборе этого типа в поле **Шаблон** требуется поместить 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}}`.

- 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 кэша** – время жизни значений, хранящихся в кеше. Значение по умолчанию: `60`.
  - **Кэш 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 **Поля 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.

4. В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

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

6. 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 меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, включите переключатель **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию переключатель выключен.

3. Если вы включили переключатель **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.

       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.
       - **inActiveList** – этот фильтр имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
       - **inCategory** – устройству в левом операнде назначается по крайней мере одна из категорий устройств 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).

С помощью флажка **с учетом регистра** в раскрывающемся списке **оператор** можно указать, требуется ли учитывать регистр значений, переданных в фильтр. По умолчанию флажок снят.

- 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 ×.

В набор ресурсов для коррелятора добавлено новое правило обогащения.

Перейдите к следующему шагу мастера установки.

Шаг 4. Реагирование

Это необязательный шаг мастера установки. В закладке мастера установки **Реагирование** 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 ним параметры:

   - **ksctasks** – если настроена интеграция KUMA и Kaspersky Security Center, можно настроить правила реагирования на запуск задач Kaspersky Security Center, связанных с устройствами. Например, можно запустить антивирусную проверку или обновление базы данных. Такие задачи можно стартовать только для устройств, импортированных из Kaspersky Security Center.

     Параметры реагирования типа ksctasks

     - **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`".
     - **Поле события** (обязательно) – определяет поле события для устройства, 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.

   - **script** – используется для выполнения последовательности команд, записанных в файл. Файл скрипта хранится на сервере, где установлен сервис коррелятора, использующий ресурс реагирования: /opt/kaspersky/kuma/correlator/<Идентификатор коррелятора>/scripts. Пользователь `kuma` этого сервера должен иметь права на запуск скрипта.

     Параметры реагирования типа script

     - **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}}"`

4. При необходимости в поле **Рабочие процессы** укажите количество рабочих процессов, которые одновременно могут быть заняты задачами реагирования.

5. 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 меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, включите переключатель **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию переключатель выключен.

3. Если вы включили переключатель **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.

       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.
       - **inActiveList** – этот фильтр имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
       - **inCategory** – устройству в левом операнде назначается по крайней мере одна из категорий устройств 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).

С помощью флажка **с учетом регистра** в раскрывающемся списке **оператор** можно указать, требуется ли учитывать регистр значений, переданных в фильтр. По умолчанию флажок снят.

- 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 ×.

В набор ресурсов для коррелятора добавлено новое правило реагирования.

Перейдите к следующему шагу мастера установки.

Шаг 5. 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, если в вашу лицензию KUMA включен модуль High Level Availability.

     Если в качестве типа точки назначения выбраны **storage** или **correlator**, поле **URL** можно заполнить автоматически с помощью раскрывающегося списка **Копировать URL сервиса**, в котором отображаются активные сервисы выбранного типа.

   - Для типов **nats** и **kafka** в поле **Топик** укажите, в какой в какой топик должны записываться данные. Топик должен содержать от 1 до 255 символов Юникода.

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 хранилища** – идентификатор хранилища 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.

     При использовании TLS вы не можете указывать 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**
     - **Сначала первый**
     - **По очереди**
   - **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**.
   - **Очистка 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 ресурсом правила агрегации. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах

1. В раскрывающемся меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, включите переключатель **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию переключатель выключен.

3. Если вы включили переключатель **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.

       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.
       - **inActiveList** – этот фильтр имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
       - **inCategory** – устройству в левом операнде назначается по крайней мере одна из категорий устройств 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).

С помощью флажка **с учетом регистра** в раскрывающемся списке **оператор** можно указать, требуется ли учитывать регистр значений, переданных в фильтр. По умолчанию флажок снят.

- 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 ×.

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 6. 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** → **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

   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, как пользователь root.

2. Выполните следующую команду:

   `/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: `/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 событий корреляции.

Если события корреляции 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 перезапустить коррелятор.

> Когда вы закончите тестирование правил корреляции, необходимо удалить все тестовые и временные правила корреляции из KUMA и перезапустить коррелятор.

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 тенанта, 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** (для Linux-агента)

Тип **tcp** используется для связи по протоколу TCP.

Доступные параметры:

- Закладка **Основные параметры**:
  - **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. По умолчанию используется `\n`.
- 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.

    При использовании TLS вы не можете указывать 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**.

- udp (для Linux-агента)

Тип **udp** используется для связи по протоколу UDP.

Доступные параметры:

- Закладка **Основные параметры**:
  - **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. По умолчанию используется `\n`.
- 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**.

- **nats** (для Linux-агента)

Тип **nats** используется для коммуникации через NATS.

Доступные параметры:

- Закладка **Основные параметры**:
  - **URL** (обязательно) – URL, с которым необходимо установить связь.
  - **Топик** (обязательно) – тема сообщений NATS. Должно содержать от 1 до 255 символов Юникода.
  - **Разделитель** – используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.
- 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: `io.nats`.
  - **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 хранилища** – идентификатор хранилища NATS.
  - **Режим TLS** – использование шифрования TLS:
    - **Выключено** (по умолчанию) – не использовать шифрование TLS.
    - **Включено** – использовать шифрование, но без верификации.
    - **С верификацией** – использовать шифрование с верификацией.

    При использовании TLS вы не можете указывать 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**.

- **kafka** (для Linux-агента)

Тип **kafka** используется для коммуникации с помощью kafka.

Доступные параметры:

- Закладка **Основные параметры**:
  - **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port.
  - **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`.
- Закладка **Дополнительные параметры**:
  - **Идентификатор группы** – параметр GroupID для сообщений Kafka. Должен содержать от 1 до 255 следующих символов: a–z, A–Z, 0–9, "." , "_" , "-".
  - **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.

    При использовании TLS вы не можете указывать IP-адрес в качестве URL.
  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса. По умолчанию указывается значение **Выключено**.

- **http** (для Linux-агента)

Тип **http** используется для связи по протоколу HTTP.

Доступные параметры:

- Закладка **Основные параметры**:
  - **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. По умолчанию используется `\n`.
- 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.

    При использовании TLS вы не можете указывать 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**.

- **file** (для Linux-агента)

Тип **file** используется для получения данных из файла.

Доступные параметры:

- Закладка **Основные параметры**:
  - **URL** (обязательно) – полный путь до файла, с которым требуется выполнять взаимодействие. Например, `/var/*som?[1-9].log`.

    Шаблоны масок для файлов и директорий

    Маски:
    - '*' – соответствует любой последовательности символов;
    - '[' ['^'] { диапазон символов } ']' – класс символов (не должен быть пустым);
    - c – соответствует символу c (c != '*', '?', '\\', '[');
    - '\\' c – соответствует символу c.

    Диапазоны символов:
    - c – соответствует символу c (c != '\\', '-', ']');
    - '\\' c – соответствует символу c;
    - lo '-' hi – соответствует символу c для lo <= c <= hi.

    Примеры:
    - /var/*som?[1-9].log
    - /mnt/dns_logs/*/dns.log
    - /mnt/proxy/access*.log
- 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**.

- **ftp** (для Linux-агента)

Тип **ftp** используется для получения данных по протоколу File Transfer Protocol.

Доступные параметры:

- Закладка **Основные параметры**:
  - **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);
    - c – соответствует символу c (c != '*', '?', '\\', '[');
    - '\\' c – соответствует символу c.

    Диапазоны символов:
    - c – соответствует символу c (c != '\\', '-', ']');
    - '\\' c – соответствует символу c;
    - lo '-' hi – соответствует символу c для lo <= c <= hi.

    Примеры:
    - /var/*som?[1-9].log
    - /mnt/dns_logs/*/dns.log
    - /mnt/proxy/access*.log

    Если в URL не содержится порт ftp сервера, подставляется 21 порт.
- 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**.

- **nfs** (для Linux-агента)

Тип **nfs** используется для получения данных по протоколу Network File System.

Доступные параметры:

- Закладка **Основные параметры**:
  - **URL** (обязательно) – путь до удаленной директории в формате nfs://host/path.
  - **Запрос** (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.
- 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**.

- wmi (для Windows-агента)

Тип **wmi** используется для получения данных с помощью Windows Management Instrumentation.

Доступные параметры:

- Закладка **Основные параметры**:
  - **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**.
  - **Учетные данные, используемые по умолчанию** – раскрывающийся список для выбора ресурса секрета, в котором хранятся учетные данные для подключения к удаленным устройствам Windows. При необходимости секрет можно создать в окне создания коннектора с помощью кнопки +. Выбранный секрет можно изменить, нажав на кнопку .
  - В таблице **Удаленные хосты** перечисляются удаленные устройства Windows, к которым требуется установить подключение. Доступные столбцы:
    - **Сервер** – удобочитаемое для пользователя имя устройства, с которой необходимо принимать данные. Например, "src.test.local".
    - **Хост** (обязательно) – IP-адрес или доменное имя устройства, с которого необходимо принимать данные.
    - **Журналы Windows** (обязательно) – 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.

      Преднастроенные журналы:
      - Application
      - ForwardedEvents
      - Security
      - System
      - HardwareEvents
    - **Секрет** – учетные данные для доступа к удаленному устройству Windows с правами на чтение журналов. Можно выбрать ресурс секрета в раскрывающемся списке или создать его с помощью кнопки +. Выбранный секрет можно изменить, нажав на кнопку .

Если оставить это поле пустым, то будут использоваться учетные данные из секрета, выбранного в раскрывающемся списке **Учетные данные, используемые по умолчанию**.

- 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**.

Изменение параметров на удаленной машине

Чтобы с удаленной машины можно было получать события с помощью WMI:

- На удаленных машинах требуется создать учетные записи 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 требуется открыть следующие TCP-порты: 135, 445, 49152-65535.
- На удаленных машинах требуется запустить следующие службы:
  - Remote Procedure Call (RPC)
  - RPC Endpoint Mapper

- **wec** (для Windows-агента)

Тип **wec** используется для получения данных с помощью Windows Event Collector.

Доступные параметры:

- Закладка **Основные параметры**:
  - **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**.
  - **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
- 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**.

- **snmp** (для Linux-агента)

Тип **snmp** используется для получения данных с помощью Simple Network Management Protocol. Поддерживаемые версии протокола:

- snmpV1
- snmpV2
- snmpV3

Доступные параметры:

- Закладка **Основные параметры**:
  - **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.
- 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**.

Типом агента считается тип использованного в нем коннектора.

При использовании типа коннектора **tcp** или **upd** на этапе нормализации в поле событий DeviceAddress, если она пустая, 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. Агенты могут перенаправлять данные только в коллекторы.

   - Если хотите выбрать существующий ресурс, выберите его в раскрывающемся списке.
   - Если хотите создать новый ресурс, выберите в раскрывающемся списке **Создать** и укажите его параметры.

     Параметры точки назначения

1. Укажите параметры в закладке **Основные параметры**:

   - 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: **nats**, **tcp**, **http**, **kafka** или **file**.
   - Укажите **URL**, куда следует отправлять события.

     Для всех типов, кроме **nats** и **file** с помощью кнопки **URL** можно указать несколько адресов отправки, если в вашу лицензию KUMA включен модуль High Level Availability.
   - Для типов **nats** и **kafka** в поле **Топик** укажите, в какой в какой топик должны записываться данные. Топик должен содержать от 1 до 255 символов Юникода.
   - В поле **Описание** можно добавить описание ресурса: до 256 символов Юникода

2. 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 хранилища** – идентификатор хранилища 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.

     При использовании TLS вы не можете указывать 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**
     - **Сначала первый**

- По очереди

- **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**.

- **Очистка 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 ресурсом правила агрегации. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах

1. В раскрывающемся меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, включите переключатель **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию переключатель выключен.

3. Если вы включили переключатель **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.

       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.
- **inActiveList** – этот фильтр имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inCategory** – устройству в левом операнде назначается по крайней мере одна из категорий устройств 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).

С помощью флажка **с учетом регистра** в раскрывающемся списке **оператор** можно указать, требуется ли учитывать регистр значений, переданных в фильтр. По умолчанию флажок снят.

- 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 ×.

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.

В зависимости от типа агента, сервис устанавливается на устройствах Linux или Windows:

- Установка на Windows:
  - wmi

- wec

- Установка на Linux:
  - tcp
  - udp
  - nats
  - kafka
  - http
  - file
  - nfs
  - snmp

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 logon as a service.

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:\ProgramData\Kaspersky Lab\KUMA\agent\<Идентификатор Агента>`, в нее установлен сервис агента KUMA. Агент пересылает события Windows в KUMA: можно настроить коллектор для их приема.

Когда сервис агента установлен, он запускается автоматически. Сервис также настроен на перезапуск в случае сбоев. Агент можно перезапустить из веб-интерфейса KUMA, но только когда сервис активен. В противном случае сервис требуется перезапустить вручную на машине Windows.

Удаление агента KUMA с устройств Windows

Чтобы удалить агент KUMA с устройства Windows:

1. Запустите командную строку на компьютере Windows с правами администратора и найдите папку с файлом kuma.exe.
2. Выполните следующую команду:

   `kuma 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>`.

Установка агента KUMA на устройствах Linux

Чтобы установить агент KUMA на устройство Linux:

1. Войдите на сервер, на котором вы хотите установить сервис, как пользователь root.
2. Выполните следующую команду:

   `/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>`

   Пример: `/opt/kaspersky/kuma/kuma agent --core https://kuma.example.com:7210 --id XXXX`

   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`.

Агент KUMA установлен на устройство Linux. Агент пересылает данные в KUMA: можно настроить коллектор для их приема.

Автоматически созданные агенты

При создании коллектора с коннекторами типа wec и wmi автоматически создаются агенты для приема событий Windows. Такие агенты отображаются в разделе **Ресурсы** → **Агенты**, в конце их названия указаны слова `auto created`.

Автоматически созданные агенты имеют ряд ограничений:

- Они могут иметь только одно подключение, то есть они могут получать данные только от одного устройства.
- Их можно изменить только из коллектора, в котором они были созданы. В разделе **Ресурсы** → **Агенты** они доступны только для просмотра.

В интерфейсе KUMA автоматически созданные агенты появляются одновременно с созданием коллектора, однако их 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.

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.

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.

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 KUMA

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

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 тенанта, которому будет принадлежать хранилище.

4. В поле **Описание** можно добавить описание сервиса: до 256 символов Юникода.

5. В поле **Срок хранения по умолчанию, дней** укажите, в течение какого времени вы хотите хранить события в кластере.

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

7. При необходимости добавьте в хранилище пространства с помощью кнопки **Добавить пространство**. Пространств может быть несколько. Пространства можно удалить с помощью кнопки **Удалить пространство**. После создания сервиса пространства можно будет просматривать и удалять в окне **Разделы**.

   Доступные параметры:

   - В поле **Название** укажите название пространства: от 1 до 128 символов Юникода.
   - В поле **Срок хранения, дней** укажите количество дней, в течение которых события будут храниться в кластере.
   - 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 меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, включите переключатель **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию переключатель выключен.

3. Если вы включили переключатель **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.

       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.
       - **inActiveList** – этот фильтр имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
       - **inCategory** – устройству в левом операнде назначается по крайней мере одна из категорий устройств 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).

С помощью флажка **с учетом регистра** в раскрывающемся списке **оператор** можно указать, требуется ли учитывать регистр значений, переданных в фильтр. По умолчанию флажок снят.

- 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 ×.

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 агента хранилища, можно перейти к созданию сервиса агента 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, как пользователь root.

2. Выполните следующую команду:

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

> При развертывании нескольких сервисов KUMA на одном хосте в процессе установки необходимо указать уникальные порты для каждого компонента с помощью параметра `--api.port <порт>`. По умолчанию используется значение `--api.port 7221`.

3. Повторите шаги 1–2 для каждого узла хранилища.

Хранилище установлено.

Аналитика

KUMA предоставляет обширную аналитику по данным, доступным программе из следующих источников:

- События в хранилище
- Алерты
- Устройства
- 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.

Отображаемый формат даты и времени зависит от локали вашего компьютера.

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. 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.

Данные, отображаемые на панели мониторинга, зависят от доступных вам тенантов.

Создание макета панели мониторинга

Чтобы создать макет выполните следующие действия:

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.

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, 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**.

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.

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)
  - Alerts distribution (Распределение алертов)
  - Alerts by Assignee (Алерты по исполнителю)
  - Alerts by Status (Алерты по статусу)
  - Alerts count by rule (Количество алертов по правилу)
  - Alerts by Priority (Алерты по уровню важности)
  - Affected Assets (Затронутые устройства)
  - Affected Assets Categories (Затронутые категории устройств)
  - Affected Users (Затронутые пользователи)
  - Latest Alerts (Последние алерты)
  - Top Log Sources by Alerts count (Топ источников событий по количеству алертов)
  - Top Log Sources by convention rate (Топ источников событий по условному рейтингу)
  - Alerts by tenant (Алерты по тенантам)
- Макет Incidents Overview (Обзор инцидентов):
  - Active incidents (Активные инциденты)

- Unassigned Incidents (Неназначенные инциденты)
- Incidents distribution (Распределение инцидентов)
- Incidents by assignee (Инциденты по исполнителю)
- Incidents by Status (Инциденты по статусам)
- Incidents by Priority (Инциденты по уровню важности)
- Incidents by Tenant (Инциденты по тенантам)
- Affected Assets in Incidents (Устройства в инцидентах)
- Affected Assets Categories in Incidents (Категории устройств в инцидентах)
- Affected Users in Incidents (Пользователи в инцидентах)
- Latest Incidents (Последние инциденты)

- Макет Network Overview (Обзор сетевой активности):
  - Top internal IP by Netflow Traffic Volume (BytesIn) (Топ внутренних IP-адресов по полученному netflow-трафику)
  - Top external IP by Netflow Traffic Volume (BytesIn) (Топ внешних IP-адресов по полученному netflow-трафику)
  - Netflow top hosts for remote control (ports 3389, 22, 135) (Топ хостов, на которые были обращения на порты 3389, 22, 135 для удаленного управления)
  - Netflow total bytes by internal ports (Топ внутренних портов по приему netflow-трафика)
  - Top Log Sources by Events count (Топ источников событий)
  - Top Events categories (Топ категорий событий)
  - Assets count (Количество устройств)
  - Users count (Количество пользователей)

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**.

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:

- **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**.

- **Период** – период времени, за который извлекается аналитика отчета.

- **Расписание** – периодичность, с которой отчеты должны формироваться по созданным шаблонам. Если расписание отчета не настроено, отображается значение `выключено`.

- **Создан** – имя пользователя, создавшего шаблон отчета.

- **Время обновления** – 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 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.
   - **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 **Изменить логотип**.

   Если нажать кнопку **Изменить 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.

   b. В поле **Время** укажите время, когда должен быть сформирован отчет. Вы можете ввести значение вручную или с помощью значка часов.

4. В раскрывающемся списке **Отправить** можно выбрать пользователей, которым следует отправлять по электронной почте ссылки на сформированные отчеты.

   Чтобы сформированные отчеты можно было отправлять по электронной почте, следует настроить SMTP-соединение.

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 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 с помощью кнопки **Изменить логотип**.
- 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 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 с помощью кнопки **Изменить логотип**.
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 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:

- **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.

Вы можете нажать на название отчета, чтобы открыть раскрывающийся список с доступными командами:

- **Открыть отчет** – используйте эту команду, чтобы открыть окно данными отчета.
- **Сохранить как HTML** – используйте эту команду, чтобы сохранить отчет в виде HTML-файла.
- **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.
3. Отчет можно сохранить в html-файл с помощью кнопки **Сохранить как HTML**.

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 в формате HTML

Чтобы сохранить отчет в формате HTML:

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 HTML**.

Отчет сохраняется в виде HTML-файла используя настройки вашего браузера.

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 **ОК**.

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 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**. Данные обновляются ежеминутно, на одной странице отображается до 250 источников. Таблицу можно сортировать, нажимая на заголовок столбца нужного параметра. Источники событий можно искать с помощью поля **Поиск**. При нажатии на источник событий открывается график поступления данных.

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;
  - DeviceProcessName;
  - DeviceAddress и/или DeviceHostname.

  Вы можете изменить название источника событий.

  Если название источника превышает 128 символов, ему нельзя присвоить политику или удалить. Однако сведения о таком источнике можно выгрузить в CSV-файл (см. ниже).

- **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.
- **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.
- **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.

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 тенанта, 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 будет 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 с помощью кнопки **Адрес электронной почты** электронные адреса, на которые следует отправить уведомления о срабатывании политики мониторинга KUMA.

     Для рассылки уведомлений необходимо настроить подключение к SMTP-серверу.
2. Нажмите **Добавить**.

Политика мониторинга добавлена.

Чтобы удалить политику мониторинга,

Выберите нужную политику, 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.

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.
- Алерты – группа для аналитики об алертах. В эту группу входят следующие виджеты:
  - **Активные алерты** – количество незакрытых алертов.
  - **Неназначенные алерты** – количество алертов со статусом **Новый**.
  - **Алерты по исполнителю** – количество алертов, сгруппированных по исполнителю.
  - **Алерты по статусу** – количество алертов, сгруппированных по статусу.
  - **Алерты по уровню важности** – количество новых незакрытых алертов, сгруппированных по уровню важности.
  - **Количество алертов по правилу** – количество незакрытых алертов, сгруппированных по правилам корреляции.
  - **Последние алерты** – таблица, содержащая последние 10 незакрытых алертов.
  - **Распределение алертов** – распределение создания алертов по времени.
- Устройства – группа для аналитики об устройствах из обработанных событий. В эту группу входят следующие виджеты:
  - **Затронутые устройства** – таблица связанных с алертами устройств, в которой указан уровень важности устройства и количество незакрытых алертов, с которыми оно связано.
  - **Затронутые категории устройств** – группы, устройства которых связаны с алертами.
  - **Количество устройств** – количество устройств, добавленных в KUMA.
- Инциденты – группа для аналитики об инцидентах.
  - **Активные инциденты** – количество незакрытых инцидентов.
  - **Неназначенные инциденты** – количество инцидентов со статусом **Открыт**.
  - **Распределение инцидентов** – количество инцидентов со статусом **Открыт** за указанный период времени.
  - **Инциденты по исполнителю** – количество инцидентов со статусом **Открыт**, 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.
- **Инциденты по тенантам** – количество незакрытых инцидентов, сгруппированных по тенантам, доступным пользователю.
- **Устройства в инцидентах** – количество устройств в незакрытых инцидентах.
- **Категории устройств в инцидентах** – категории устройств, которые затронуты незакрытыми инцидентами. Доступные типы диаграмм: круговая, столбчатая.
- **Пользователи в инцидентах** – пользователи, затронутые в инцидентах. Доступные типы диаграмм: таблица, круговая, столбчатая.
- **Последние инциденты** – последние 10 незакрытых инцидентов.

- Источники событий – группа для аналитики об источниках событий.
  - **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
- Пользователи – группа для аналитики о пользователях из обработанных событий.
  - **Затронутые пользователи** – количество пользователей, указанных в алерте, сгруппированных по имени пользователя.
  - **Количество пользователей AD** – количество активных учетных записей KUMA из Active Directory.

Стандартные виджеты

В этом разделе описываются параметры всех виджетов, кроме виджета **События**.

Доступные параметры виджетов зависят от выбранного типа виджета. Тип виджета определяется по значку:

- – круговая диаграмма
- – счетчик
- – таблица
- и – столбчатая диаграмма

Параметры круговых диаграмм, счетчиков и таблиц

Параметры круговых диаграмм, счетчиков и таблиц располагаются в 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 512 символов Юникода, описывающих виджет.

- **Тенант** – раскрывающийся список для выбора тенанта, по данным которого будет отображаться аналитика. По умолчанию используется параметр **Как на панели мониторинга**.

- **Период времени** – раскрывающийся список для настройки периода времени, за который должна отображаться аналитика. Доступные варианты:

  - **Как на панели мониторинга** – когда выбран этот параметр, значение периода времени виджета отражает период, который был настроен для панели мониторинга. 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.

- **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.
- – 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 времени** – раскрывающийся список для настройки периода времени, за который должна отображаться аналитика. Доступные варианты:
    - **Как на панели мониторинга** – когда выбран этот параметр, значение периода времени виджета отражает период, который был настроен для панели мониторинга. 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.

- **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**.

Пользовательский виджет

Вы можете использовать этот виджет для поиска событий и извлечения аналитики из результатов. 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 тенанта, по данным которого будет отображаться аналитика. По умолчанию используется параметр **Как на панели мониторинга**.

- **Период времени** – раскрывающийся список для настройки периода времени, за который должна отображаться аналитика. Доступные варианты:

  - **Как на панели мониторинга** – когда выбран этот параметр, значение периода времени виджета отражает период, который был настроен для панели мониторинга. Этот вариант выбран по умолчанию.

  - **1 час** – получить аналитику за предыдущий час.

  - **1 день** – получить аналитику за предыдущий день.

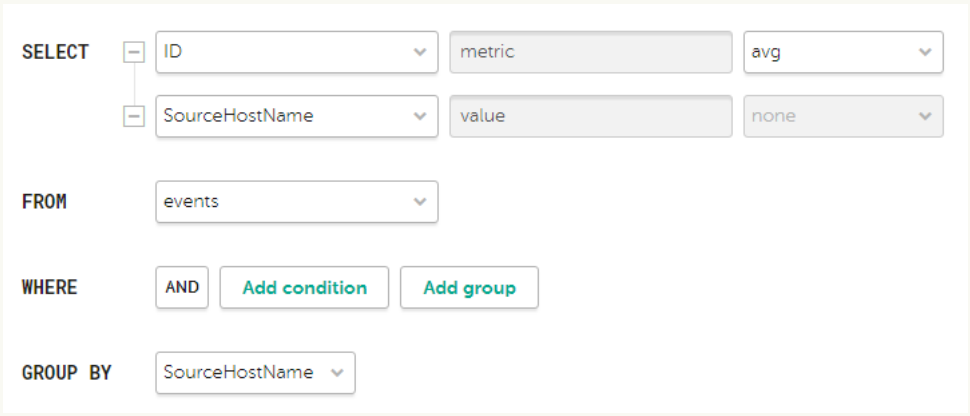
  - **7 дней** – получить аналитику за предыдущие 7 дней.

- **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** – хранилище, в котором должен выполняться поиск.
- Группа настроек поиска событий, состоящая из закладок **Конструктор запросов** и **SQL-запрос** – эта группа настроек используется для составления поисков для извлечения данных из событий и определения того, как извлеченные данные должны отображаться в виджете.

  - **Конструктор запросов** – на этой закладке отображаются параметры запроса поиска событий, аналогичные параметрам конструктора фильтра событий:

    Пример условий поиска

    Параметры условия поиска для виджета, показывающие среднее количество байтов, полученных с одного хоста

  - **ВЫБРАТЬ** – 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 вы можете выбрать, как должны обрабатываться значения поля события типа **metric** (метрики) для виджета:

    - **количество** – выберите этот вариант для подсчета событий. Эта опция доступна только для поля события ID.
    - **макс** – выберите этот параметр, чтобы отобразить максимальное значение поля события из выборки событий.
    - **мин** – выберите этот параметр, чтобы отображать минимальное значение поля события из выборки событий.

- **сред** – выберите эту опцию, чтобы отображать среднее значение поля события из выборки событий.

- **сумм** – выберите этот параметр, чтобы отобразить сумму значений полей событий из выборки событий.

- **ИСТОЧНИК** – этот раскрывающийся список используется для выбора типа источника данных. Для выбора доступна только опция **events** (события).

- **ГДЕ** – 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 нужного оператора. 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 **И**, однако если на него нажать, оператор можно поменять. Доступные значения: **И**, **ИЛИ**, **НЕ**. Группы условий удаляются с помощью кнопки **Удалить группу**.

- **ГРУП.** – этот раскрывающийся список используется для выбора полей событий, по которым осуществляется группировка событий. Этот параметр недоступен для типа графиков **Счетчик**.

- **СОРТ.** – 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: **ВОЗР** – для сортировки по возрастанию, **УБЫВ** – для сортировки по убыванию.

  Для графиков типа **Таблица** можно добавить условия сортировки с помощью кнопки **ДОБАВИТЬ СТОЛБЕЦ**.

- **ЛИМИТ** – это поле используется для установки максимального количества точек данных для виджета. Этот параметр недоступен для типов графиков **Календарная диаграмма** и **Счетчик**.

- **SQL-запрос** – на этой закладке находится поле для ввода поискового запроса, аналогичного фильтрации событий с использованием синтаксиса SQL.

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.

- 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.
- **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. Значение по умолчанию: **авто**.

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 тенанта:

1. В разделе веб-интерфейса KUMA **Параметры** → **Тенанты** нажмите **Добавить**.

   Откроется окно **Добавить тенанта**.
2. В поле **Название** укажите имя 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 тенанта:

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 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, устройств и других параметров KUMA, где можно выбрать тенанта.

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 тананту 2 (tenantID=2)

  Сценарий:

  1. Коллектор тенанта 2 получает и отправляет события в коррелятор тенанта 2.
  2. При срабатывании корреляционных правил в коррелляторе 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 тенанта 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.

Отображаемый формат даты и времени зависит от локали вашего компьютера. В английской версии первый день недели – воскресенье.

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:

   - **Длительность инцидента**.
   - **Название**.
   - **Создано**.
   - **Тенант**.
   - **Статус**.
   - **Количество алертов**.
   - **Уровень важности**.
   - **Категории затронутых устройств**.

3. При необходимости измените порядок отображения столбцов, перетащив заголовки столбцов.

4. Чтобы отсортировать инциденты по определенному параметру, нажмите на заголовок нужного столбцы 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.

   Чтобы снять фильтры, нажмите на заголовок нужного столбца и выберите **Очистить фильтр**.

Выбранные столбцы будут отображаться в таблице раздела **Инциденты** в указанном вами порядке.

Доступные столбцы таблицы инцидентов:

- **Длительность инцидента** – время, на протяжении которого происходил инцидент (время между первым и последним событием, относящимся к инциденту).
- **Создано** – 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**.
- **Устройства** – категории, к которым принадлежат связанные с инцидентом устройства.
- **Назначен** – имя сотрудника службы безопасности, которому инцидент передан для расследования или реагирования.
- **Изменен** – дата и время последнего изменения, сделанного в инциденте.
- **Появление первого события** и **Появление последнего события** – дата и время первого и последнего события в инциденте.
- **Категория** и **Тип** – 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.

При необходимости вы можете воспользоваться полем **Поиск хостов и пользователей**, чтобы найти инциденты по определенным пользователям и устройствам.

Сохранение и выбор конфигураций фильтра инцидентов

В KUMA можно сохранять изменения настроек 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 настройки 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 тенанта, 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 **ОК**.

   Конфигурация фильтра удалена для всех пользователей KUMA.

Просмотр подробных данных об инциденте

В окне инцидента вы можете ознакомиться с подробными данными об инциденте.

Чтобы просмотреть подробные сведения из инцидента,

в веб-интерфейсе KUMA откройте раздел **Инциденты** и выберите нужный инцидент.

Откроется окно инцидента, содержащее подробные данные об инциденте. Некоторые параметры инцидентов доступны для редактирования.

В верхней части окна инцидента расположена панель инструментов и указано имя пользователя, которому назначен инцидент. 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 необходимого тенанта 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 раскрывающемся списке и нажав **Сохранить**.
- **Категории затронутых устройств** – категории, к которым принадлежат связанные с инцидентом устройства.
- **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, устройствам 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 устройства** и **Связанные пользователи** содержат таблицы с данными о хостах и пользователях, относящихся к инциденту. Эта информация поступает из алертов, связанных с инцидентом.

Таблицы в разделах **Связанные алерты**, **Связанные устройства** 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.

Раздел **Журнал изменений** содержит записи об изменениях, которые вы и пользователи вносили в инцидент. Изменения регистрируются автоматически, при этом есть возможность вручную добавлять комментарии.

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 тенанта, 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 и устройствам 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 пользователи** 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 устройства** добавьте устройства, относящиеся к инциденту.

  Привязка устройств к инцидентам

Чтобы привязать устройство к инциденту:

1. В разделе **Связанные устройства** окна инцидента нажмите **Привязать**.

   Откроется окно со списком устройств.

2. Выберите нужные устройства.

   Устройства можно искать с помощью поля **Поиск**.

3. Нажмите **Привязать**.

Устройства связаны с инцидентом и отображаются в разделе **Связанные устройства**.

Чтобы отвязать устройства от инцидента:

1. Выберите нужные устройства в разделе **Связанные пользователи** и нажмите на кнопку **Отвязать**.
2. Нажмите **Сохранить**.

Устройства 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. При необходимости измените параметры инцидента.

4. 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.

5. 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 устройствам или пользователям. Если настройка включена, то при создании алерта программа выполняет поиск инцидентов за указанный период, к которым относятся устройства 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 устройствам** 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

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.

Экспорт инцидентов в НКЦКИ

Инциденты, созданные в KUMA можно экспортировать в НКЦКИ. Перед экспортом инцидентов требуется настроить интеграцию с НКЦКИ. Инцидент можно экспортировать только один раз.

Экспорт инцидентов в НКЦКИ доступен, только если лицензия программы включает модуль GosSOPKA.

Чтобы экспортировать инцидент в НКЦКИ:

1. В разделе **Инциденты** веб-интерфейса KUMA выберите инцидент, который вы хотите экспортировать, одним из указанных ниже способов:

   - Установите флажок рядом с нужным инцидентом.
   - Откройте нужный инцидент.

2. Нажмите **Экспортировать в НКЦКИ**.

   Откроется окно с параметрами экспорта.

3. 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.

     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

- **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 критичной 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.

  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

- **Местоположение** (обязательно) – выберите в раскрывающемся списке местоположение вашей организации.

- **Затронутая система имеет подключение к интернету** – установите этот флажок, если устройства, относящиеся к инциденту, имеют подключение к интернету. Кроме того, дополнительно после завершения экспорта в личном кабинете ГосСОПКА в карточке уведомления укажите технические сведения о компьютерном инциденте, компьютерной атаке или уязвимости. По умолчанию этот флажок снят.

- **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**.

4. 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 помощью 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.

5. Нажмите **Экспорт**.

6. Подтвердите экспорт.

Сведения об инциденте переданы в НКЦКИ, параметр инцидента **Экспорт в НКЦКИ** меняется на **Успешно экспортирован**. Если в экспортированный инцидент требуется внести изменения, это следует делать в вашем личном кабинете ГосСОПКА.

Работа с алертами

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.

Отображаемый формат даты и времени зависит от локали вашего компьютера. В английской версии первый день недели – воскресенье.

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.

Фильтрация алертов

В KUMA в разделе **Алерты** можно делать выборки алертов с помощью инструментов фильтрации и сортировки.

Настройки фильтра можно сохранить. Существующие настройки фильтров можно удалить.

Настройка таблицы алертов

В основной части раздела **Алерты** отображается таблица с информацией о зарегистрированных алертах. Нажав на заголовки столбцов можно открыть раскрывающиеся списки с инструментами для фильтрации алертов и настройки таблицы алертов:

- 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.
- **Тенант** – название тенанта, которому принадлежит алерт.

В поле **Поиск устройств и пользователей с помощью регулярного выражения PCRE** можно ввести регулярное выражение, чтобы найти алерты с определенными пользователями или устройствами.

Сохранение и выбор конфигураций фильтра алертов

В KUMA можно сохранять изменения настроек 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 настройки 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 тенанта, 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 **ОК**.

Конфигурация фильтра удалена для всех пользователей KUMA.

Окно алертов

В этом окне можно ознакомиться с выбранным алертом и всеми связанными с ним данными.

Чтобы увидеть подробные сведения об алерте:

В разделе **Алерты** веб-интерфейса KUMA нажмите на алерт, сведения о котором вы хотите просмотреть.

Откроется окно алерта с название алерта в верхнем левом углу.

В верхней части окна алерта расположена панель инструментов, а также указаны уровень важности алерта и имя пользователя, которому назначен этот алерт. Здесь можно обработать алерт: изменить его уровень важности, назначить его пользователю, закрыть, создать на его основе инцидент.

Раздел **Информация об алерте** окна алерта содержит следующие данные:

- **Уровень важности правила корреляции** – уровень важности правила корреляции, которое породило этот алерт.
- **Наивысшая важность категории устройств** – самый высокий уровень важности категории устройств из тех, которые принадлежат связанным с этим алертом устройствам. Если с алертом связано несколько активов, отображается наибольшее значение.
- **Привязан к инциденту** – если алерт привязан к инциденту, тут отображается его название и статус.
- **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, которое породило алерт. Название правила представлено в виде ссылки, по которой можно перейти к настройкам этого правила корреляции.

- **Переполнен** – этот тег означает, что размер алерта достиг или приближается к пределу и необходимо обработать алерт как можно скорее. Новые события не добавляются к переполненным алертам, но можно нажав на ссылку **Смотреть все возможные связанные события** можно отфильтровать все события, которые были бы связаны с алертом, если бы не было ограничения на его размер.

Раздел **Связанные события** окна алерта содержит таблицу событий, относящихся к алерту. Если нажать значок › рядом с правилом корреляции, отобразятся базовые события из этого правила корреляции. События можно сортировать по уровню важности и времени.

При выборе события в правой части окна веб-интерфейса открывается область деталей. Эта область содержит информацию о выбранном событии. Если выбрать корреляционное событие, в области деталей также будет отображаться кнопка **Подробные сведения**, при нажатии на которую откроется окно корреляционного события.

Ссылки **Найти в событиях** под корреляционными событиями и кнопка **Найти в событиях** справа от заголовка раздела используются для детализированного анализа.

Раздел **Связанные устройства** окна алерта содержит таблицу хостов, относящихся к алерту. Эта информация поступает из событий, связанных с алертом. С помощью поля **Поиск по IP или FQDN** можно искать нужные хосты. Устройства можно сортировать по столбцам **Количество** и **Устройство**.

Если с алертом связаны устройства, они отображаются в этом разделе. При нажатии на название устройства открывается окно **Информация об устройстве**.

Раздел **Связанные пользователи** окна алерта содержит таблицу пользователей, относящихся к алерту. Эта информация 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**.

Раздел **Журнал изменений** окна алерта 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**.

Чтобы добавить комментарий к алерту,

В окне алерта введите комментарий в поле **Комментарий** и нажмите **Добавить**.

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.

     Открывается 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 отображается 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 меняется на **Назначен**, а в раскрывающемся списке **Назначить** отображается имя выбранного пользователя.

4. 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 меняется на **Эскалирован**. Алерт можно отвязать от инцидента, выбрав его и нажав **Отвязать**.

5. 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 меняется на **Закрыт**. Алерты с таким статусом не обновляются новыми событиями корреляции 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 события корреляции. 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.

Вы можете вручную привязать событие к алертам. 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 таблице событий будут отображены все события, соответствующие критериям фильтра, независимо от того, привязаны ли они к алерту, выбранному для детализированного анализа.

Чтобы привязать базовое 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 кнопку **Найти в событиях**.

   Откроется таблица событий с включенными фильтрами даты и времени, соответствующим дате и времени регистрации привязанных к алерту событий, а 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. Измените фильтры, чтобы найти событие, которое требуется привязать к алерту.

5. Выберите нужное событие и нажмите 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 его окне в разделе **Журнал изменений** добавляется запись об этом действии. Вы можете перейти по ссылке в этой записи и в открывшейся области деталей события или отвязать его, или привязать к алерту с помощью кнопок **Привязать к алерту** и **Отвязать от алерта**.

Срок хранения алертов

По умолчанию алерты хранятся в KUMA в течение года, но этот срок можно изменить с помощью исполняемого файла /opt/kaspersky/kuma/kuma на сервере Ядра KUMA.

Чтобы изменить срок хранения алертов:

1. Войдите в ОС сервера, на котором установлено Ядро KUMA, как пользователь root.
2. Выполните следующую команду:
3. `kuma core --alerts.retention <количество дней, в течение которых требуется хранить алерты> --external :7220 --internal :7210 --mongo mongodb://localhost:27017`
4. Перезапустите KUMA, выполнив последовательно следующие команды:
   a. `sudo systemctl stop kuma-core`
   b. `sudo systemctl start kuma-core`

Срок хранения алертов изменен.

Правила сегментации алертов

В KUMA можно настроить *правила сегментации алертов*, то есть создание отдельных алертов по определенным условиям. Это может оказаться полезным, когда коррелятор группирует однотипные корреляционные события в один общий алерт, однако вы хотите, чтобы на основе некоторых из этих событий, отличающихся чем-то важным от других, создавались отдельные алерты.

Правила сегментации создаются отдельно для каждого тенанта. Они отображаются в разделе **Параметры** → **Алерты** веб-интерфейса KUMA в таблице со следующими столбцами:

- **Тенант** – название тенанта, которому принадлежат правила сегментации.
- **Обновлен** – дата и время последнего обновления правил сегментации.
- **Выключено** – в этом столбце отображается метка, если правила сегментации выключены.

Чтобы создать правило сегментации алерта:

1. Откройте раздел **Параметры** → **Алерты** веб-интерфейса KUMA.
2. Выберите тенант, для которого вы хотите создать правило сегментации:
   - У тенанта уже есть правила сегментации, выберите его в таблице.

- Если у тенанта нет правил сегментации, нажмите **Добавить** и в раскрывающемся списке **Тенант** выберите нужного тенанта.

3. В блоке параметров **Правила сегментации** нажмите **Добавить** и укажите параметры правила сегментации:

   - **Название** (обязательно) – в этом поле укажите название правила сегментации.

   - **Правило корреляции** (обязательно) – в этом раскрывающемся списке выберите правило корреляции, события которого вы хотите выделить в отдельный алерт.

   - **Селектор** (обязательно) – в этом блоке параметров требуется задать условие, при котором правило сегментации будет срабатывать. Условия формулируются аналогично фильтрам.

4. Нажмите **Сохранить**.

Правило сегментации алертов создано. События, подходящие под эти правила, будут объединены в отдельный алерт с названием правила сегментации.

Чтобы выключить правила сегментации:

1. Откройте раздел **Параметры** → **Алерты** веб-интерфейса KUMA и выберите тенант, правила сегментации которого вы хотите выключить

2. Установите флажок **Выключено**.

3. Нажмите **Сохранить**.

Правила сегментации алертов выбранного тенанта выключены.

Работа с событиями

В разделе **События** веб-интерфейса Ядра KUMA вы можете просматривать события, находящиеся в кластере хранилища, чтобы расследовать угрозы безопасности или создавать правила корреляции.

События можно фильтровать. Для отображения самых последних записей по выбранным событиям обновите веб-страницу или установите период обновления таблицы событий.

События можно анализировать ретроспективно.

Отображаемый формат даты и времени зависит от локали вашего компьютера. В английской версии первый день недели – воскресенье.

Фильтрация событий

В KUMA можно настраивать, какие события будут отображаться в таблице событий, с помощью конструктора запросов или запросов SQL. Оба метода взаимозаменяемы, условия фильтрации можно просматривать или создавать с помощью любого из них.

Вы также можете создавать или обновлять фильтры в таблице событий следующими способами:

- **Изменение настроек фильтра из окна статистики**

  *Чтобы изменить фильтр из окна **Статистика**:*

  1. Откройте область деталей **Статистика**:

     - 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 указатель мыши на требуемое значение.

     Рядом со значением отображаются значки плюса и минуса.

  3. Измените фильтр с помощью значков плюса или минуса:

     - Чтобы включить в выборку событий только события с выбранным значением, нажмите +.
     - Чтобы исключить из выборки событий все события с выбранным значением, нажмите –.

     В результате фильтр и таблица событий будут обновлены, а в верхней части экрана отображается измененный поисковый запрос.

- **Изменение фильтра из таблицы событий**

Чтобы изменить фильтр из таблицы событий:

В разделе **События** веб-интерфейса KUMA нажмите любое значение параметра события в таблице событий и выберите в открывшемся меню следующие опции:

- Чтобы включить в выборку событий только события с выбранным значением, нажмите **Искать события с этим значением**.
- Чтобы исключить из выборки событий все события с выбранным значением, нажмите **Искать события без этого значения**.

В результате фильтр и таблица событий будут обновлены, а в верхней части экрана отображается измененный поисковый запрос.

- **Изменение фильтра из области деталей события**

Чтобы изменить фильтр из 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 фильтр, используя значки плюса или минуса рядом с необходимыми параметрами:

   - Чтобы включить в выборку событий только события с выбранным значением, нажмите +.
   - Чтобы исключить из выборки событий все события с выбранным значением, нажмите −.

В результате фильтр и таблица событий будут обновлены, а в верхней части экрана отображается измененный поисковый запрос.

События можно также фильтровать по временному периоду. Настройки фильтра можно сохранить. Существующие настройки фильтров можно удалить.

Конструктор запросов и поисковые запросы SQL можно использовать для указания количества событий, загружаемых на одной странице. Если настроенный фильтр возвращает больше событий, чем настроено для отображения на одной странице, в конце страницы отображается кнопка **Показать больше событий**. Максимальное количество событий, отображаемых на странице, устанавливается в разделе **ЛИМИТ** конструктора фильтра или в параметре **ЛИМИТ** SQL-запроса. Эту функцию можно задействовать, только если события также фильтруются по временному периоду.

Функции фильтрации доступны пользователям всех ролей.

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** KUMA в верхней части окна откройте раскрывающийся список справа от раскрывающегося списка .

2. Если вы хотите фильтровать по стандартному периоду, выберите один из доступных вариантов:

   - **5 минут**
   - **15 минут**
   - **1 час**
   - **24 часа**

3. Период можно задать вручную:

   a. В раскрывающемся списке справа от раскрывающегося списка выберите **В течение периода**.

   Откроется окно с календарем.

   b. Установите дату начала и окончания периода с помощью календаря.

   Формат даты и времени зависит от настроек вашей операционной системы. При желании вы можете изменить значения даты вручную, следуя формату даты и времени вашей операционной системы.

   c. Нажмите **Применить фильтр**.

4. Нажмите кнопку .

Если установлен фильтр по периоду, будут отображаться только события, зарегистрированные в течение указанного интервала времени. Период будет отображаться в верхней части окна.

Вы также можете установить период с помощью гистограммы событий в верхней части раздела **События**, нажав на серое поле с нужным периодом времени или перетащив указатель мыши на требуемый период времени и нажав кнопку **Показать события**.

Фильтрация событий с помощью конструктора запросов

В KUMA вы можете задавать условия поиска событий с помощью конструктора запросов.

Чтобы создать фильтр с помощью конструктора:

1. В разделе **События** веб-интерфейса KUMA нажмите на поле и выберите закладку **Конструктор запросов**.

   Откроется окно конструктора запросов.

2. Сформулируйте поисковый запрос:

   - В раскрывающемся списке раздела **ВЫБРАТЬ** выберите параметр события, который должен отображаться в таблице событий. Вы можете выбрать несколько параметров с помощью кнопки **ДОБАВИТЬ СТОЛБЕЦ**. По умолчанию выбрано значение *, что означает, что должны отображаться все доступные параметры события.

     Можно оптимизировать процесс поиска, выбирая только ключевые параметры: другие данные событий при этом не будут загружаться для отображения.

   - В раскрывающемся списке раздела **ИСТОЧНИК** выберите **events**.

   - В разделе **ГДЕ** задайте условия поиска:

a. В раскрывающемся списке слева выберите параметр события, который вы хотите использовать в качестве фильтра.

b. В среднем выпадающем списке выберите нужный оператор. Доступные операторы различаются в зависимости от типа значения выбранного параметра.

c. Введите значение параметра.

В зависимости от выбранного типа параметра вам потребуется ввести значение вручную, выбрать его в раскрывающемся списке или выбрать в календаре.

Вы можете добавить условия фильтра с помощью кнопки **Добавить условие** или удалить их с помощью кнопки ✕.

Вы также можете добавить группы условий, используя кнопку **Добавить группу**. По умолчанию группы условий добавляются с оператором **И**, однако если на него нажать, оператор можно поменять. Доступные значения: **И**, **ИЛИ**, **НЕ**. Группы условий удаляются с помощью кнопки **Удалить группу**.

- В разделе **СОРТ.** установите порядок, в котором будут отображаться события:
  - В раскрывающемся списке слева выберите параметр, по которому необходимо сортировать события.
  - В раскрывающемся списке справа выберите порядок сортировки по возрастанию (**ВОЗР**) или убыванию (**УБЫВ**).

  Параметры событий для сортировки событий можно добавлять с помощью кнопки **ДОБАВИТЬ СТОЛБЕЦ** или удалить с помощью кнопки ✕.
- В поле **ЛИМИТ** введите количество событий, отображаемых на одной странице. По умолчанию используется значение `250`.

3. Нажмите **Поиск**.

В таблице событий отображаются только события, соответствующие созданному фильтру, а выражение фильтра отображается в поле **Поиск**.

Чтобы удалить фильтр:

1. В разделе **События** веб-интерфейса KUMA нажмите на поисковый запрос фильтра.

   Откроется окно конструктора запросов.

2. Нажмите на кнопку **Новый поиск**.

   Параметры фильтра будут сброшены.

3. Нажмите на кнопку **Поиск**.

Фильтр больше не будет применяться к отображаемым событиям.

Это действие также удалит временной фильтр.

Фильтрация событий с помощью SQL-запросов

В KUMA можно задавать условия поиска событий с помощью SQL-запросов.

Чтобы создать фильтр с использованием SQL-запросов:

1. В KUMA, в разделе **События**, выберите поле и выберите закладку **SQL-запрос**.

   Отображается поле для ввода SQL-запроса.

2. Сформулируйте поисковый запрос.

3. Нажмите **Поиск**.

   В таблице событий отображаются только события, соответствующие созданному фильтру, а выражение фильтра отображается в поле **Поиск**.

Чтобы удалить фильтр:

1. В разделе **События** веб-интерфейса KUMA нажмите на поисковый запрос фильтра.

2. Нажмите **Новый поиск**.

   Фильтр больше не будет применяться к отображаемым событиям.

> Это действие также удалит временной фильтр.

Сохранение и выбор конфигураций фильтра событий

В KUMA вы можете сохранять конфигурации фильтров для использования в будущем или другими пользователями. При сохранении фильтра вы сохраняете настройки сразу всех активных фильтров: фильтр по периоду, конструктору запросов и настройки таблицы событий. Поисковые запросы сохраняются на сервере Ядра KUMA и доступны всем пользователям KUMA выбранного тенанта.

Чтобы сохранить текущие настройки фильтра, поискового выражения и временного периода,

1. В разделе **События** веб-интерфейса KUMA нажмите раскрывающийся список 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 тенанта, которому будет принадлежать создаваемый фильтр.

4. Нажмите **Сохранить**.

   Конфигурация фильтра сохранена.

Чтобы выбрать ранее сохраненную конфигурацию фильтра:

В разделе **События** веб-интерфейса KUMA нажмите раскрывающийся список рядом с выражением фильтра и выберите нужный фильтр.

Выбранная конфигурация активна.

Если нажать на значок ☆ рядом с названием конфигурации фильтра, она станет использоваться в качестве конфигурации по умолчанию.

Список конфигураций фильтров также можно открыть с помощью кнопки **Сохранить условия поиска** в окне конструктора запросов.

Удаление конфигураций фильтра событий

Чтобы удалить ранее сохраненную конфигурацию фильтра:

1. В разделе **События** веб-интерфейса KUMA нажмите раскрывающийся список рядом с поисковым запросом фильтра и нажмите значок рядом с конфигурацией, которую требуется удалить.
2. Нажмите **ОК**.

Конфигурация фильтра удалена для всех пользователей KUMA.

Список конфигураций фильтров также можно открыть с помощью кнопки **Сохранить условия поиска** в окне конструктора запросов.

Просмотр информации о событии

В KUMA можно просмотреть параметры любого события вашей выборки, что может оказаться полезным при расследовании алертов или при работе с правилами корреляции.

Чтобы просмотреть параметры события,

В разделе **События** веб-интерфейса KUMA нажмите на нужное событие.

В правой части окна отображается область деталей **Информация о событии** со списком параметров события и их значений. В этой области деталей можно:

- Изменить выборку событий с помощью значков + и – рядом со значениями параметров.
- Открыть ответственный за регистрацию события сервис с помощью ссылки на значении параметра **Service**.
- Открыть окно со сведениями об устройстве, если оно упоминается в полях события и зарегистрировано в программе.
- Привязать событие к алерту, если программа находится в режиме детализированного анализа.
- Открыть окно **Информация о корреляционном событии**, если выбранное событие является корреляционным.

- Если настроена интеграция с Kaspersky CyberTrace и/или Kaspersky Threat Intelligence Portal, просмотреть и запросить из этих источников информацию об объектах в полях события.

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.

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 (или 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 настроек фильтра.

Статистику можно получить одним из указанных ниже 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**.

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, отобразится его пять наиболее частотных значений. С помощью поля **Поиск** можно искать нужные параметры.

В окне **Статистика** можно менять фильтр событий.

Настройка таблицы событий

Столбцы таблицы событий, отображаемые по умолчанию:

- **Timestamp**
- **Name**
- **DeviceProduct**
- **DeviceVendor**
- **DestinationAddress**
- **DestinationUserName**
- **Тенант**

В KUMA можно настроить отображаемый набор столбцов таблицы и их порядок отображения. Измененные настройки можно сохранить.

Чтобы настроить параметры отображения для таблицы событий:

1. В правом верхнем углу таблицы событий нажмите значок ⚙.

   Откроется окно для настройки таблицы событий.

2. Установите флажки напротив параметров, требуется отображать в таблице.

   Вы можете отобразить в таблице любой параметра из модели данных событий KUMA. С помощью поля **Поиск** можно искать нужные поля. Параметры **Время** и **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, нажав на его заголовок и в раскрывающемся списке выбрав **Скрыть столбец**.

3. Порядок отображения столбцов можно изменить, перетаскивая заголовки столбцов.

4. Чтобы отсортировать события по определенному столбцу, нажмите на его заголовок и в раскрывающемся списке выберите один из вариантов: **По возрастанию** или **По убыванию**.

Выбранные столбцы будут отображаться в таблице раздела **События** 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 теперь обновляется автоматически.

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 событий корреляции, 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 устройства** окна корреляционного события содержит таблицу узлов, относящихся к корреляционному событию. Эта информация поступает из базовых событий, связанных с корреляционным событием. При нажатии на название устройства открывается окно **Информация об устройстве**.

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.

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. Если вы хотите, чтобы при обработке 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 таблица, в которой отражаются события, обработанные в ходе ретроспективной проверки, а также агрегированные и корреляционные события, созданные во время обработки.

Управление устройствами

В разделе **Устройства** веб-интерфейса KUMA можно просматривать и изменять информацию об известных устройствах и их категории.

В левой части раздела **Устройства** отображается дерево категорий устройств. Вы можете просматривать дерево, а также развертывать и свертывать его узлы. Если выбрать узел, в правой части окна отображаются устройства, относящиеся к соответствующей категории.

Если выбрать устройство, в правой части окна открывается область **Информация об устройстве** со следующими параметрами устройства:

- **Название** – имя устройства. Устройства, импортированные из Kaspersky Security Center, сохраняют свои имена Kaspersky Security Center.
- **Название тенанта** – название тенанта, которому принадлежит устройство.
- **Создан** – дата и время добавления устройства в KUMA.
- **Изменен** – дата и время изменения информации об устройстве.
- **Владелец** – владелец устройства, если он указан.
- **IP-адрес** – IP-адрес устройства (если предоставлен).

  Если в KUMA есть несколько устройств с одинаковыми IP-адресами, устройство, добавленное позже, возвращается во всех случаях поиска устройств по IP-адресу. Если в сети вашей организации допустимо наличие устройств с одинаковыми IP-адресами, разработайте и используйте дополнительные атрибуты для идентификации устройств. Это может оказаться важным при корреляции.

- **Полное доменное имя** – полностью определенное имя домена устройства, если указано.
- **MAC-адрес** – MAC-адрес устройства (если предоставлен).
- **Операционная система** – операционная система устройства.
- **Связанные алерты** – алерты, с которыми связано устройство (если есть).

  Для просмотра списка алертов, с которыми связано устройство, можно перейти по ссылке **Найти в алертах**. Откроется закладка **Алерты** с поисковым выражением, позволяющим отфильтровать все устройства с соответствующим идентификатором.
- **Категории** – категории, к которым относится устройство (если есть).
- **Уязвимости** – уязвимости устройства, если есть. Эта информация доступна только для устройств, 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.
- **Информация о программном обеспечении** – если указаны параметры программного обеспечения устройства, они отображаются в этом разделе.

- **Информация об оборудовании** – если указаны параметры оборудования устройства, они отображаются в этом разделе.
- **Идентификатор Агента Windows** – идентификатор сетевого агента устройства, если указан.
- **Время последнего подключения к KSC** – если устройство было импортировано из Kaspersky Security Center, в этом разделе отображается время последнего подключения к Kaspersky Security Center.

Вы можете установить флажки рядом с устройствами, а затем назначить им категорию с помощью кнопки **Привязать к категории**.

Не назначайте устройствам категорию `Categorized assets`.

Категории устройств

В KUMA устройства распределены по категориям, имеющим древовидную структуру. Дерево категорий отображается в левой части раздела **Устройства** веб-интерфейса KUMA закладки **Все устройства**, которая открывается по умолчанию. Если выбрать узел дерева, в правой части окна отображаются устройства, относящиеся к соответствующей категории. Устройства из подкатегорий выбранной категории не отображаются, если вы не укажете, что хотите отображать устройства рекурсивно.

Категории устройствам можно присваивать вручную или автоматически. Автоматическая категоризация может быть реактивной, когда категории наполняются устройствами с помощью правил корреляции, или активной, когда категории присваиваются все устройства, 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 устройства** – просмотреть устройства выбранной категории в правой части окна.
- **Отображать устройства рекурсивно** – просмотреть устройства 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 устройств 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 устройств 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 устройств

Чтобы добавить категорию устройств:

1. Откройте раздел **Устройства** 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 устройств: 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 устройствами. В зависимости от выбора может потребоваться указать дополнительные параметры:
   - **Вручную** – устройства можно привязать к категории только вручную.
   - **Активно** – устройства будут с определенной периодичностью привязываться к категории, если удовлетворяют заданному фильтру.

     Активная категория устройств

1. В раскрывающемся списке **Регулярность категоризации** укажите периодичность, в которой устройства 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 условия для привязывания к категории.

   Условия можно добавлять с помощью кнопок **Добавить условия**. 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 **Устройства, найденные по заданным условиям** с перечнем устройств, удовлетворяющим условиям поиска.

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

5. Нажмите **Сохранить**.

Новая категория добавлена в дерево категорий устройств.

Настройка таблицы устройств

В KUMA можно настроить содержимое и порядок отображения столбцов в таблице устройств. Эти параметры хранятся локально на вашем компьютере.

Чтобы настроить параметры отображения таблицы устройств:

1. В правом верхнем углу таблицы устройств нажмите значок .

2. В раскрывшемся списке установите флажки напротив параметров, требуется отображать в таблице:

   - **Полное доменное имя**
   - **IP-адрес**
   - **Владелец**
   - **MAC-адрес**
   - **Создан**
   - **Изменен**
   - **Название тенанта**

   Когда вы устанавливаете флажок, таблица устройств 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 устройств настроены.

Импорт информации об устройствах из Kaspersky Security Center

В Kaspersky Security Center зарегистрированы все устройства, отслеживаемые этим приложением. К этим данным можно получить доступ с помощью API. Если установлено активное соединение между KUMA и Kaspersky Security Center, вы можете импортировать устройства из Kaspersky Security Center в KUMA.

Чтобы импортировать данные об устройствах из Kaspersky Security Center:

1. Откройте веб-интерфейс KUMA и выберите раздел **Устройства**.
2. Нажмите **Импортировать устройства из KSC**.

   Откроется окно **Импортировать устройства из KSC**.

3. В раскрывающемся списке выберите тенант для импорта данных из Kaspersky Security Center.
4. Нажмите на кнопку **OK**.

Информация об устройствах будет импортирована из Kaspersky Security Center в KUMA.

Поиск устройств

В KUMA есть функция полнотекстового поиска по параметрам устройств. Поиск выполняется по параметрам **Название**, **Полное доменное имя**, **IP-адрес**, **MAC-адрес** и **Владелец**.

Чтобы найти нужное устройство,

в разделе **Устройства** веб-интерфейса KUMA введите поисковый запрос в поле **Поиск** и нажмите **ENTER** или значок .

В таблице отобразятся все устройства, названия которых соответствуют критериям поиска.

Добавление устройств

В KUMA можно добавлять устройства вручную или импортировать их из Kaspersky Security Center.

Чтобы добавить устройство вручную:

1. В разделе **Устройства** веб-интерфейса KUMA нажмите на кнопку **Добавить устройство**.

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

2. Введите параметры устройства:

   - **Название устройства** (обязательно).
   - **Название тенанта** (обязательно).
   - **IP-адрес** и/или **Полное доменное имя** (обязательно).
   - **MAC-адрес**.
   - **Владелец**.

3. При необходимости присвойте устройству одну или несколько категорий:

   a. Нажмите кнопку .

   Откроется окно **Выбор категорий**.

   b. Установите флажки рядом с категориями, которые следует присвоить устройству. С помощью значков и подкатегории можно разворачивать и сворачивать.

   c. Нажмите **Сохранить**.

   Выбранные категории отобразятся в полях **Категории**.

4. При необходимости добавьте в раздел **Программное обеспечение** сведения об операционной системе устройства.

5. При необходимости добавьте в раздел **Информация об оборудовании** сведения об оборудовании устройства.

6. Нажмите на кнопку **Добавить**.

Устройство создано и отображается в таблице устройств в назначенной ему категории или в категории **Устройства без категории**.

Удаление устройств

В KUMA есть возможность удалять устройства.

Чтобы удалить устройство:

1. В разделе **Устройства** веб-интерфейса KUMA нажмите на устройство, которое вы хотите удалить.

   В правой части окна откроется область **Информация об устройстве**.

2. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения.

3. Нажмите **ОК**.

Устройство удалено.

Устройства, импортированные из Kaspersky Security Center, невозможно удалить вручную. Они удаляются автоматически, если информация о них не обновлялась в течение 30 дней.

Изменение параметров устройств

В KUMA можно изменять параметры устройств. У добавленных вручную устройств можно изменять все параметры. У устройств, импортированных из Kaspersky Security Center, можно изменить только название устройства и его категорию.

Чтобы изменить параметры устройства:

1. В разделе **Устройства** веб-интерфейса KUMA нажмите на устройство, которое вы хотите изменить.

   В правой части окна откроется область **Информация об устройстве**.

2. Нажмите на кнопку **Изменить**.

   Откроется окно **Изменить устройство**.

3. Внесите необходимые изменения в доступные поля:

   - **Название устройства** (обязательно. Это единственное поле, доступное для редактирования у устройств, импортированных из Kaspersky Security Center.)
   - **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 устройства:

Доступные поля для описания CPU устройства:

- **Название процессора**
- **Частота процессора**
- **Количество ядер процессора**

  Устройству можно добавить процессоры с помощью ссылки **Добавить процессор**.

Доступные поля для описания диска устройства:

- **Свободных байт на диске**
- **Объем диска**

  Устройству можно добавить диски с помощью ссылки **Добавить диск**.

Доступные поля для описания RAM устройства:

- **Частота оперативной памяти**
- **Общий объем ОЗУ**

Доступные поля для описания сетевой карты устройства:

- **Название сетевой карты**
- **Производитель сетевой карты**
- **Версия драйвера сетевой карты**

  Устройству можно добавить сетевые карты с помощью ссылки **Добавить сетевую карту**.

4. Назначьте или измените устройству категорию:

   a. Нажмите кнопку .

   Откроется окно **Выбор категорий**.

   b. Установите флажки рядом с категориями, которые следует присвоить устройству.

   c. Нажмите **Сохранить**.

Выбранные категории отобразятся в полях **Категории**.

Кроме того, можно выбрать устройство и перетащить его в нужную категорию. Эта категория будет добавлена в список категорий устройства.

Не назначайте устройствам категорию `Categorized assets`.

5. Если требуется, разделе **Программное обеспечение** добавьте сведения об операционной системе устройства.

6. Если требуется, в разделе **Информация об оборудовании** добавьте сведения об оборудовании устройства.

7. Нажмите на кнопку **Сохранить**.

Параметры устройства будут изменены.

Управление KUMA

В этом разделе описываются работа с пользователями в KUMA, роли пользователей, а также метрики.

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 имени и пароля для входа.

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.

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**.

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**.

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.
   - Установите флажок **Главный администратор**, если хотите присвоить пользователю роль главного администратора. Пользователи с ролью главного администратора могут изменять параметры других учетных записей пользователей. По умолчанию этот флажок снят.

3. 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.
   - Установите флажок **Главный администратор**, если хотите присвоить пользователю роль главного администратора. Пользователи с ролью главного администратора могут изменять параметры других учетных записей пользователей. По умолчанию этот флажок снят.

3. 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 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.

4. При необходимости сгенерируйте API-токен с помощью кнопки **Сгенерировать токен**. При нажатии на эту кнопку отображается окно с автоматически созданным токеном.

   При закрытии окна токен больше не отображается, и, если вы его не скопировали, потребуется сгенерировать новый токен.

5. 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.
   - **Получать уведомление по протоколу SMTP** – установите этот флажок, если хотите получать SMTP-уведомления от KUMA.

3. Если требуется изменить пароль, нажмите на кнопку **Изменить пароль** и в открывшемся окне заполните поля, описанные ниже. По завершении нажмите **ОК**.

   - **Действующий пароль** (обязательно) – введите действующий пароль своей учетной записи.
   - **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.

4. При необходимости сгенерируйте API-токен с помощью кнопки **Сгенерировать токен**. При нажатии на эту кнопку отображается окно с автоматически созданным токеном.

   При закрытии окна токен больше не отображается, и, если вы его не скопировали, потребуется сгенерировать новый токен.

5. Нажмите **Сохранить**.

Ваша учетная запись отредактирована.

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.

- *Оператор* – эта роль предназначена для пользователей, которые сталкиваются с непосредственными угрозами безопасности определенного тенанта.

Права пользователей

Раздел веб-интерфейса и действия	Главный администратор	Администратор	Аналитик	Оператор	Ком
Отчеты					
Просматривать и изменять шаблоны и отчеты	есть	есть	есть	нет	Аналитик может: • Просмотреть и отчеты, которые • Просмотреть от отправлены ана • Просмотреть пр шаблоны.
Формировать отчеты	есть	есть	есть	нет	Аналитик может ге которые создал са (из шаблона и из от Аналитик не может которые были отпр почту.
Выгружать сформированные отчеты	есть	есть	есть	нет	Аналитик может вы • Отчеты, которы • Предустановле • Отчеты, которы
Удалять шаблоны и сформированные отчеты	есть	есть	есть	нет	Аналитик может уд которые создал са Аналитик не может • Предустановле • Отчеты, которы • Предустановле может удалять т администратор

Изменять настройки формирования отчетов	есть	есть	есть	нет	Аналитик может из генерации отчетов и предустановленн
Дублировать шаблон отчета	есть	есть	есть	нет	Аналитик может ду отчетов, которые с предустановленны
Панель мониторинга					
Просматривать данные на панели мониторинга и менять макеты	есть	есть	есть	есть	
Добавлять макеты	есть	есть	есть	нет	В том числе добавл
Изменять и переименовывать макеты	есть	есть	есть	нет	В том числе добавл виджеты. Аналитик может из предустановленны созданные своей у
Удалять макеты	есть	есть	есть	нет	Администратор те макеты в доступны Аналитик может уд своей учетной запи Предустановленны только главный адм
Ресурсы → Сервисы и **Ресурсы → Сервисы → Активные сервисы**					
Просматривать список активных сервисов	есть	есть	есть	нет	Только главный адм просматривать и уд хранилища. Права доступа не з меню тенантов.
Просматривать содержимое активного листа	есть	есть	есть	нет	
Импортировать/ экспортировать/ очищать содержимое активного листа	есть	есть	есть	нет	
Создавать набор ресурсов для сервисов	есть	есть	есть	нет	Аналитик не может
Создавать сервис в разделе Ресурсы - Сервисы - Активные сервисы	есть	есть	нет	нет	
Удалять сервисы	есть	есть	нет	нет	
Перезапускать сервисы	есть	есть	нет	нет	

Обновлять параметры сервисов	есть	есть	есть	нет	
Сбрасывать сертификаты	есть	есть	нет	нет	Пользователь с ро может сбрасывать только в тенантах,
Ресурсы → Ресурсы					
Просматривать список ресурсов	есть	есть	есть	нет*	Аналитики не могу ресурсов секретов доступны им при с
Добавлять ресурсы	есть	есть	есть	нет	Аналитики не могу секретов.
Изменять ресурсы	есть	есть	есть	нет	Аналитики не могу секретов.
Создавать/ редактировать/ удалять ресурсы в общем тенанте	есть	нет	нет	нет	
Удалять ресурсы	есть	есть	есть	нет	Аналитики не могу секретов.
Импортировать ресурсы	есть	есть	есть	нет	Импортировать ре может только главн
Экспортировать ресурсы	есть	есть	есть	нет	В том числе ресурс
Просматривать/ редактировать черновики коллектора или коррелятора	есть	есть	есть	нет	Пользователю дос черновики вне зави тенанта, список че принадлежности к
Состояние источников → Список источников событий					
Просматривать источники событий	есть	есть	есть	есть	
Изменять источники событий	есть	есть	есть	нет	Редактировать наи назначать политику политику монитори
Удалять источники событий	есть	есть	есть	нет	
Состояние источников → Политики мониторинга					
Просматривать политики мониторинга	есть	есть	есть	есть	
Создавать политики мониторинга	есть	есть	есть	нет	

Изменять политики мониторинга	есть	есть	есть	нет	Только главный адм редактировать пре мониторинга.
Удалять политики мониторинга	есть	есть	есть	нет	Предустановленны для удаления.
Устройства					
Просматривать устройства и категорий устройств	есть	есть	есть	есть	Включая категории
Добавлять/ редактировать/ удалять категории устройств	есть	есть	есть	нет	В рамках доступно
Добавлять категорий категории устройств в общем тенанте	есть	нет	нет	нет	В том числе редакт категории общего
Привязывать устройства к категории устройств общего тенанта	есть	есть	есть	нет	
Добавлять устройства	есть	есть	есть	нет	
Изменять устройства	есть	есть	есть	нет	
Удалять устройства	есть	есть	есть	нет	
Импортировать устройства из Kaspersky Security Center	есть	есть	есть	нет	
Запускать задачи на устройстве в Kaspersky Security Center	есть	есть	есть	нет	
Алерты					
Просматривать список алертов	есть	есть	есть	есть	
Изменять уровень важности алертов	есть	есть	есть	есть	
Открывать детали алертов	есть	есть	есть	есть	
Назначать ответственных пользователей	есть	есть	есть	есть	
Закрывать алерты	есть	есть	есть	есть	
Добавлять комментарий к алертам	есть	есть	есть	есть	
Привязывать	есть	есть	есть	есть	

событие к алертам					
Отвязывать событие от алертов	есть	есть	есть	есть	
Изменять и удалять чужие фильтры	есть	есть	нет	нет	
Инциденты					
Просматривать список инцидентов	есть	есть	есть	есть	
Создавать пустые инциденты	есть	есть	есть	есть	
Создавать вручную инциденты из алертов	есть	есть	есть	есть	
Изменять уровень важности инцидентов	есть	есть	есть	есть	
Открывать детали инцидентов	есть	есть	есть	есть	В деталях инциден только тех тенанто пользователя есть
Назначать исполнителей	есть	есть	есть	есть	
Закрывать инциденты	есть	есть	есть	есть	
Добавлять комментарии к инцидентам	есть	есть	есть	есть	
Привязывать алерты к инцидентам	есть	есть	есть	есть	
Отвязывать алерты от инцидентов	есть	есть	есть	есть	
Изменять и удалять чужие фильтры	есть	есть	нет	нет	
Экспортировать инциденты в НКЦКИ	есть	есть	есть	есть	
События					
Просматривать список событий	есть	есть	есть	есть	
Выполнять поиск событий	есть	есть	есть	есть	
Открывать детали событий	есть	есть	есть	есть	
Открывать статистику	есть	есть	есть	есть	
Провозить ретроспективную проверку	есть	есть	есть	нет	
Выгружать события в	есть	есть	есть	есть	

TSV-файл					
Изменять и удалять чужие фильтры	есть	есть	нет	нет	
Запускать ktl-обогащение	есть	есть	есть	нет	
Параметры → Пользователи					Раздел доступен то администратору.
Увидеть список пользователей	есть	нет	нет	нет	
Добавить пользователя	есть	нет	нет	нет	
Изменить пользователя	есть	нет	нет	нет	
Увидеть данные своего профиля	есть	есть	есть	есть	
Изменить данные своего профиля	есть	есть	есть	есть	Роль пользователя изменения.
Параметры → LDAP					
Просматривать параметры подключения к LDAP	есть	есть	нет	нет	
Изменять параметры подключения к LDAP	есть	есть	нет	нет	
Параметры → Тенанты					Раздел доступен то администратору.
Просматривать список тенантов	есть	нет	нет	нет	
Добавлять тенантов	есть	нет	нет	нет	
Изменять тенантов	есть	нет	нет	нет	
Отключать тенантов	есть	нет	нет	нет	
Параметры → Active directory					Раздел доступен то администратору.
Просматривать параметры подключения к Active directory	есть	нет	нет	нет	
Изменять параметры подключения к Active directory	есть	нет	нет	нет	
Добавлять фильтры по ролям для тенантов	есть	нет	нет	нет	
Параметры → Уведомления					Раздел доступен то администратору.
Просматривать параметры	есть	нет	нет	нет	

подключения к SMTP					
Изменять параметры подключения к SMTP	есть	нет	нет	нет	
Параметры → Лицензия					Раздел доступен то администратору.
Просматривать список добавленных лицензий	есть	нет	нет	нет	
Добавлять лицензии	есть	нет	нет	нет	
Удалять лицензии	есть	нет	нет	нет	
Параметры → KSC					
Просматривать список Kaspersky Security Center-серверов, с которыми выполнена интеграция	есть	есть	нет	нет	
Добавлять подключения к Kaspersky Security Center	есть	есть	нет	нет	
Удалять подключения к Kaspersky Security Center	есть	есть	нет	нет	
Параметры → CyberTrace					Раздел доступен то администратору.
Просматривать параметры интеграции с CyberTrace	есть	нет	нет	нет	
Изменять параметры интеграции с CyberTrace	есть	нет	нет	нет	
Параметры → R-Vision					Раздел доступен то администратору.
Просматривать параметры интеграции с R-Vision IRP	есть	нет	нет	нет	
Изменять параметры интеграции с R-Vision IRP	есть	нет	нет	нет	
Параметры → KTL					Раздел доступен то администратору.
Просматривать параметры интеграции с Threat Lookup	есть	нет	нет	нет	

Изменять параметры интеграции с Threat Lookup	есть	нет	нет	нет	
Параметры → Алерты					
Просматривать параметры	есть	есть	есть	нет	
Изменять параметры	есть	есть	есть	нет	
Параметры → Инциденты → Автоматическая привязка алертов к инцидентам					
Увидеть настройки	есть	нет	нет	нет	
Изменить настройки	есть	нет	нет	нет	
Параметры → Инциденты → Типы инцидентов					
Просматривать справочник категорий	есть	есть	нет	нет	
Просматривать карточки категорий	есть	есть	нет	нет	
Добавлять категории	есть	есть	нет	нет	Доступно, если у п администратора хо
Изменять категории	есть	есть	нет	нет	Доступно, если у п администратора хо
Удалять категории	есть	есть	нет	нет	Доступно, если у п администратора хо
Параметры → НКЦКИ					
Просматривать параметры	есть	нет	нет	нет	
Изменять параметры	есть	нет	нет	нет	
Метрики					
Открывать метрики	есть	нет	нет	нет	
Диспетчер задач					
Просматривать список своих задач	есть	есть	есть	есть	Раздел и задачи не тенанту. Задачи до создавшему их пол
Завершать свои задачи	есть	есть	есть	есть	
Перезапускать свои задачи	есть	есть	есть	есть	
Просматривать список всех задач	есть	нет	нет	нет	

Завершать любые задачи	есть	нет	нет	нет	
Перезапускать любые задачи	есть	нет	нет	нет	
CyberTrace					Раздел не отображ если не настроена в разделе Парамет
Открывать раздел	есть	нет	нет	нет	
Доступ к данным тенантов					
Доступ к тенантам	есть	есть	есть	есть	Пользователь имее тенанту, если его н параметров ролей пользователя. Уров того, в какой из рол Права доступа к гл означают доступ к к данным этого тен
Главный тенант	есть	есть	есть	есть	Общий тенант испо общих ресурсов, ко доступны для всех Сервисы не могут тенанту, но в них мо принадлежащие об При этом такие сер своему тенанту. События, алерты и общими. Права доступа к об • чтение и запись администратор • чтение – осталь включая пользо доступа к главн
Общий тенант	есть	есть	есть	есть	Пользователь имее тенанту, если его н параметров ролей пользователя. Уров того, в какой из рол Права доступа к гл означают доступ к к данным этого тен

* Пользователь с ролью оператор посредством REST API видит ресурсы на общем тенанте.

Просмотр метрик KUMA

Полная информация о рабочих характеристиках Ядра, коллекторов, коррелляторов 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.

Логин и пароль Grafana по умолчанию: `admin` и `admin`.

Доступные показатели описаны ниже.

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 коррелляторов

- 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.

Просмотр задач KUMA

В разделе **Диспетчер задач** вы можете просматривать задачи, созданные текущим пользователем. Пользователь с ролью главного администратора может видеть задачи всех пользователей.

В окне **Диспетчер задач** отображается список созданных задач со следующими столбцами:

- **Статус** – статус задачи.
  - *Мигает зеленая точка* – задача активна.
  - Значок – 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. Виды задач:
  - *event-export* – задача экспорта событий.
  - *ktl* – задача по запроса данных с портала Kaspersky Threat Intelligence Portal.
  - *replay* – задание на воспроизведение событий.
- **Создан** – пользователь, создавший задачу. Этот столбец доступен только для ролей пользователей Главный администратор и Администратор.
- **Время создания** – время создания задачи.
- **Время обновления** – время обновлении задачи.

Вы можете отменить активную задачу, нажав тип задачи и выбрав в раскрывающемся списке **Отмена**.

Также можно повторить задачу, нажав тип задачи и выбрав в раскрывающемся списке **Перезапустить**.

Управление подключением к SMTP-серверу

В KUMA можно настроить отправку уведомлений по электронной почте с помощью SMTP-сервера. Для обработки уведомлений KUMA можно добавить только один SMTP-сервер. Управление подключением к SMTP-серверу осуществляется в разделе веб-интерфейса KUMA **Параметры → Уведомления**.

Чтобы настроить подключение к SMTP-серверу:

1. В разделе **Ресурсы** веб-интерфейса KUMA откройте закладку **Секреты**.

   Отобразится список доступных секретов.

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

   Откроется окно секрета.

3. Введите данные секрета:

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

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

   c. В полях **Пользователь** и **Пароль** введите учетные данные для вашего SMTP-сервера.

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

4. Нажмите **Сохранить**.

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

5. Откройте веб-интерфейс KUMA и выберите раздел **Параметры → Уведомления**.

6. 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** (обязательно) – адрес электронной почты отправителя сообщения. Например, `kuma@company.com`.

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

8. Выберите периодичность уведомлений в раскрывающемся списке **Регулярность уведомлений мониторинга**.

9. Включите переключатель **Выключить уведомления мониторинга**, если не хотите получать уведомления о состоянии источников событий. По умолчанию переключатель выключен.

10. Нажмите **Сохранить**.

    Соединение с SMTP-сервером настроено, пользователи могут получать сообщения электронной почты от 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,

Откройте 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 хранятся на машине, на которой установлен требуемый сервис или сервис, использующий требуемый ресурс. Журналы можно просмотреть с помощью команды `journalctl` в консоли Linux. Например, выполнение команды `journalctl -u kuma-collector * kuma-correlator * -f` вернет последние журналы из коллекторов и коррелляторов, установленных на машине, где была выполнена команда.

Сервисы, где доступно ведение журнала:

- Коррелляторы
- Коллекторы
- Агенты

Ресурсы, где доступно ведение журнала:

- Коннекторы
- Правила обогащения
- Точки назначения

Резервное копирование KUMA

KUMA позволяет выполнять резервное копирование базы данных Ядра KUMA и сертификатов. Резервное копирование осуществляется с помощью исполняемого файла /opt/kaspersky/kuma/kuma.

Восстановление данных из резервное копии доступно только при сохранении версии KUMA.

Чтобы выполнить резервное копирование:

1. Войдите в ОС сервера, на котором установлено Ядро KUMA, как пользователь root.

2. Выполните следующую команду:

   ```
   /opt/kaspersky/kuma/kuma tools backup --dst=<путь к директории для резервной копии> --certificates
   ```

   Флаг `--certificates` не является обязательным и используется для резервного копирования сертификатов.

Резервная копия создана.

Чтобы восстановить данные из резервной копии:

1. Войдите в ОС сервера, на котором установлено Ядро KUMA, как пользователь root.

2. Остановите Ядро KUMA, выполнив следующую команду:

   ```
   sudo systemctl stop kuma-core
   ```

3. Выполните следующую команду:

   ```
   /opt/kaspersky/kuma/kuma tools restore --dst=<путь к директории с резервной копией> --certificates
   ```

   Флаг `--certificates` не является обязательным и используется для восстановления сертификатов.

4. Запустите KUMA, выполнив следую команду:

   ```
   sudo systemctl start core
   ```

5. Пересоздайте сервисы, используя восстановленные наборы ресурсов для сервисов.

Данные восстановлены из резервной копии.

Резервное копирование коллекторов не требуется, за исключением коллекторов с SQL-подключением. При восстановлении таких коллекторов следует вернуть к исходному начальное значение идентификатора.

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".

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, однако его можно изменить с помощью команды `/opt/kaspersky/kuma/kuma core --rest <желаемый номер порта>`.

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

Авторизация REST API

Каждый запрос REST API должен включать авторизацию с помощью токена, который можно сгенерировать в профиле своей учетной записи или, если у вас достаточно прав, в учетных записях других пользователей. Вы всегда можете сгенерировать новый токен.

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 коррелляторе

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	Пример значения
correlatorID	string	Да	Идентификатор сервиса коррелятора	00000000-0000-0000-0000-000000000000
activeListID	string	Если не указан activeListName	Идентификатор активного листа	00000000-0000-0000-0000-000000000000
activeListName	string	Если не указан activeListID	Имя активного листа	Attackers
format	string	Да	Формат импортируемых записей	csv, tsv, internal
keyField	string	Только для форматов csv и tsv	Имя поля в заголовке csv или tsv файла, которое будет использовано в качестве ключевого поля записи	ip

			активного листа. Значения этого поля должны быть уникальными	
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 значения
page	number	Нет	Номер страницы. Начинается с 1. Размер страницы - 250 записей. Если не 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.	00000000-0000-0000-0000-000000000000
tenantID	string	Нет	Идентификатор тенанта алерта. Если параметр указан	00000000-0000-0000-0000-

			несколько раз, то формируется список и применяется логический оператор ИЛИ. Если пользователь не имеет необходимой роли в указанном тенанте, то данный тенант игнорируется.	000000000000
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, firstSeen
from	string	Нет	Нижняя границы периода в формате RFC3339. <timestampField> >= <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	Нет	Верхняя периода в формате RFC3339. <timestampField> <= <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)
status	string	Нет	Статус алерта. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	new, assigned, escalated, closed
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 ассетах 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 устройств

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 не параметр не указан, то используется значение по умолчанию - 1.	1

id	string	Нет	Идентификатор устройства. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	00000000-0000-0000-0000-000000000000
tenantID	string	Нет	Идентификатор тенанта устройства. 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 устройства. Регистронезависимое регулярное выражение (PCRE).	asset ^My asset$
ip	string	Нет	IP адрес устройства. Регистронезависимое регулярное выражение (PCRE).	10.10 ^192.168.1.2$
mac	string	Нет	MAC адрес устройства. 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 устройств

POST /api/v1/assets/import

Массовое создание или обновление устройств. Если указан FQDN устройства, то он играет роль уникального идентификатора устройства в рамках тенанта. Если FQDN не указан, то для идентификации устройства используется первый IP-адрес из указанного массива адресов. Если имя устройства не указано, то оно заполняется либо значением FQDN, либо значением первого IP-адреса. Устройства, импортированные из Kaspersky Security Center не могут быть обновлены, поэтому, в процессе импорта, могут возникать конфликты по FQDN, если в тенанте уже существует устройство Kaspersky Security Center с таким FQDN. Возникновение такого конфликта препятствует обработке конфликтующего устройства, но не препятствует обработке других устройств, указанных в теле запроса.

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 ассетов	

Обязательные поля Asset

Имя	Тип данных	Обязательный	Описание	Пример значения
fqdn	string	Если не	FQDN	my-asset-1.example.com

		указан ipAddresses	устройства. Рекомендуется указывать именно FQDN, а не просто имя хоста. Приоритетный признак для идентификации устройства.	my-asset-1
ipAddresses	[]string	Если не указан fqdn	Массив IP-адресов устройства. IPv4 или IPv6. Первый элемент массива используется как второстепенный признак для идентификации устройства.	["192.168.1.1", "192.168.2.2"] ["2001:0db8:85a3:0000:0000:8a2e:0370:7334"]

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 ассетов в shared тенант	import into shared tenant not allowed	
400	В теле запроса не указан ни один ассет	at least one asset required	
400	Не указано ни одно из	one of fields	asset[<index>]: fqdn, ipAddresses

	обязательных полей	required	
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[<index>]
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 устройств

POST /api/v1/assets/delete

Доступ: администратор, аналитик.

Тело запроса

Формат: JSON

Имя	Тип данных	Обязательный	Описание	Пример значения
tenantID	string	Да	Идентификатор тенанта	00000000-0000-0000-0000-000000000000
ids	[]string	Если не указаны ни fqdns, ни ipAddresses	Список идентификаторов устройств	["00000000-0000-0000-0000-000000000000"]
fqdns	[]string	Если не указаны ни ids, ни ipAddresses	Массив FQDN устройств	["my-asset-1.example.com", "my-asset-1"]
ipAddresses	[]string	Если не указаны ни ids, ни fqdns	Массив основных IP адресов устройств (первый элемент массива ipAddresses в запросе на импорт)	["192.168.1.1", "2001:0db8:85a3:0000:0000:8a2e:0370:7334"]

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 устройств из shared 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 Stroage 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 Main 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 не 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	Приме
page	number	Нет	Номер страницы.	1

			Начинается с 1. Размер страницы – 250 записей. Если не параметр не указан, то используется значение по умолчанию – 1.	
id	string	Нет	Идентификатор ресурса. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	00000000-0000-0000-0000-0000000000
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.	00000000-0000-0000-0000-0000000000
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, storage, activeList, aggre enrichmentRule, destination, filter, normalizer,

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.

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

POST /api/v1/resources/toc

Доступ: администратор, аналитик, оператор.

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.	00000000-0000-0000-0000-000000000000
password	string	Да	Пароль файла с ресурсами.	SomePassword!88
tenantID	string	Да	Идентификтор целевого тенанта	00000000-0000-0000-0000-000000000000
actions	map[string]uint8	Да	Маппинг идентификатора ресурса к действию, которое нужно предпринять в отношении него.	0 – не импортировать (используется при разрешении конфликтов) 1 – импортировать (изначально должно быть присвоено каждому ресурсу) 2 – заменить (используется при разрешении конфликтов) `{ "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.

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.

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 значения
page	number	Нет	Номер страницы. Начинается с 1. Размер страницы - 250 записей. Если не 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.	00000000-0000-0000-0000-000000000000
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	00000000-0000-0000-0000-000000000000

			указанном тенанте, то данный тенант игнорируется.	
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, storage, agent
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 не 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	Имя 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"`
}
```

Приложения

В этом разделе представлена 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.
`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 запуска установки сервиса коллектора

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.

Название поля	Тип поля	Описание
AggregationRuleName	внутренний	Название правила агрегации, которое обработало событие.
BaseEventIDs	внутренний	Идентификаторы базовых событий, на основе которых было создано корреляционное событие.
Code	внутренний	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.
CorrelationRuleName	внутренний	Заполняется только для корреляционного события. Название корреляционного правила, которое породило корреляционное событие.
ID	внутренний	Уникальный идентификатор события типа UID. Для базового события, генерируемого на коллекторе, идентификатор генерируется коллектором. Идентификатор корреляционного события генерируется коррелятором. Идентификатор никогда не меняет своего значения. Событие в Хранилище можно искать по этому идентификатору.
Raw	внутренний	Неизмененный текст исходного события.
Score	внутренний	Заполняется у событий, которые были обработаны сработавшим правилом корреляции. Это уровень важности выявленного алерта, который был задан в правиле корреляции.
ServiceAddress	внутренний	IP-адрес хоста, на котором развернут сервис.
ServiceID	внутренний	Идентификатор экземпляра сервиса — коррелятора, коллектора, хранилища.
ServiceKind	внутренний	Категория сервиса: коррелятор, коллектор, хранилище
ServiceName	внутренний	Название экземпляра сервиса, которое дает администратор KUMA при создании сервиса.
Tactic	внутренний	Название тактики из MITRE
Technique	внутренний	Название техники из MITRE
Timestamp	внутренний	Время создания базового события на коллекторе. Время создания корреляционного события на коллекторе.
Extra	внутренний	Поле для маппинга нераспарсенного значения при нормализации события.
TICategories	внутренний	Поле, в котором будут содержаться категории, которые были получены от внешнего TI по индикаторам из события.
DeviceVendor	CEF	Название производителя источника журнала. Значение берется из "сырого" события. DeviceVendor, DeviceProduct и DeviceVersion однозначно идентифицируют источник журнала.

DeviceProduct	CEF	Название продукта из источника журнала. Значение берется из "сырого" события. DeviceVendor, DeviceProduct и DeviceVersion однозначно идентифицируют источник журнала.
DeviceVersion	CEF	Версия продукта из источника журнала. Значение берется из "сырого" события. DeviceVendor, DeviceProduct и DeviceVersion однозначно идентифицируют источник журнала.
DeviceEventClassID	CEF	Уникальный идентификатор типа события из источника журнала. Некоторые источники журнала определяют категорию событий.
Name	CEF	Название события в "сыром" событии.
Severity	CEF	Уровень важности ошибки из "сырого" события. Это может быть поле Severity или поле Level и т.п., зависит от журнала.
DeviceAction	CEF	Действие, совершенное устройством. Действие, которое было предпринято производителем источника лога. Например, blocked, detected.
ApplicationProtocol	CEF	Протокол уровня приложений (HTTP, HTTPS, Telnet и т.д.)
DeviceCustomIPv6Address1	CEF	Поле для маппинга значения адреса IPv6, которое не может быть сопоставлено любому другому элементу модели данных. Может использоваться для обработки логов сетевых устройств, где необходимо отличать IP-адреса разных устройств (для брандмауэров и т.п.). Поле кастомизируется.
DeviceCustomIPv6Address1Label	CEF	Поле для описания назначения поля DeviceCustomIPv6Address1.
DeviceCustomIPv6Address2	CEF	Поле для маппинга значения адреса IPv6, которое не может быть сопоставлено любому другому элементу модели данных. Может использоваться для обработки логов сетевых устройств, где необходимо отличать IP-адреса разных устройств (для брандмауэров и т.п.). Поле кастомизируется.
DeviceCustomIPv6Address2Label	CEF	Поле для описания назначения поля DeviceCustomIPv6Address2.
DeviceCustomIPv6Address3	CEF	Поле для маппинга значения адреса IPv6, которое не может быть сопоставлено любому другому элементу модели данных. Может использоваться для обработки логов сетевых устройств, где необходимо отличать IP-адреса разных устройств (для брандмауэров и т.п.). Поле кастомизируется.
DeviceCustomIPv6Address3Label	CEF	Поле для описания назначения поля DeviceCustomIPv6Address3.
DeviceCustomIPv6Address4	CEF	Поле для маппинга значения адреса IPv6, которое не может быть сопоставлено любому другому элементу модели данных.

		Может использоваться для обработки логов сетевых устройств, где необходимо отличать IP-адреса разных устройств (для брандмауэров и т.п.). Поле кастомизируется.
DeviceCustomIPv6Address4Label	CEF	Поле для описания назначения поля DeviceCustomIPv6Address4.
DeviceEventCategory	CEF	Категория "сырого" события из схемы определения категорий событий производителя лога.
DeviceCustomFloatingPoint1	CEF	Поле для маппинга значения типа Float, которое не может быть сопоставлено любому другому элементу модели данных. Поле кастомизируется.
DeviceCustomFloatingPoint1Label	CEF	Поле для описания назначения поля DeviceCustomFloatingPoint1.
DeviceCustomFloatingPoint2	CEF	Поле для маппинга значения типа Float, которое не может быть сопоставлено любому другому элементу модели данных. Поле кастомизируется.
DeviceCustomFloatingPoint2Label	CEF	Поле для описания назначения поля DeviceCustomFloatingPoint2.
DeviceCustomFloatingPoint3	CEF	Поле для маппинга значения типа Float, которое не может быть сопоставлено любому другому элементу модели данных. Поле кастомизируется.
DeviceCustomFloatingPoint3Label	CEF	Поле для описания назначения поля DeviceCustomFloatingPoint3.
DeviceCustomFloatingPoint4	CEF	Поле для маппинга значения типа Float, которое не может быть сопоставлено любому другому элементу модели данных. Поле кастомизируется.
DeviceCustomFloatingPoint4Label	CEF	Поле для описания назначения поля DeviceCustomFloatingPoint4.
DeviceCustomNumber1	CEF	Поле для маппинга целочисленного значения, которое не может быть сопоставлено любому другому элементу модели данных. Поле кастомизируется.
DeviceCustomNumber1Label	CEF	Поле для описания назначения поля DeviceCustomNumber1.
DeviceCustomNumber2	CEF	Поле для маппинга целочисленного значения, которое не может быть сопоставлено любому другому элементу модели данных. Поле кастомизируется.
DeviceCustomNumber2Label	CEF	Поле для описания назначения поля DeviceCustomNumber2.
DeviceCustomNumber3	CEF	Поле для маппинга целочисленного значения, которое не может быть сопоставлено любому другому элементу модели данных.

		Поле кастомизируется.
DeviceCustomNumber3Label	CEF	Поле для описания назначения поля DeviceCustomNumber3.
BaseEventCount	CEF	Для корреляционного события — это количество базовых событий, которые были обработаны корреляционным правилом, которое создало корреляционное событие. Для "свернутого базового события" – это количество базовых событий, которые были обработаны правилом агрегации.
DeviceCustomString1	CEF	Поле для маппинга строкового значения, которое не может быть сопоставлено любому другому элементу модели данных. Поле кастомизируется.
DeviceCustomString1Label	CEF	Поле для описания назначения поля DeviceCustomString1.
DeviceCustomString2	CEF	Поле для маппинга строкового значения, которое не может быть сопоставлено любому другому элементу модели данных. Поле кастомизируется.
DeviceCustomString2Label	CEF	Поле для описания назначения поля DeviceCustomString2.
DeviceCustomString3	CEF	Поле для маппинга строкового значения, которое не может быть сопоставлено любому другому элементу модели данных. Поле кастомизируется.
DeviceCustomString3Label	CEF	Поле для описания назначения поля DeviceCustomString3.
DeviceCustomString4	CEF	Поле для маппинга строкового значения, которое не может быть сопоставлено любому другому элементу модели данных. Поле кастомизируется.
DeviceCustomString4Label	CEF	Поле для описания назначения поля DeviceCustomString4.
DeviceCustomString5	CEF	Поле для маппинга строкового значения, которое не может быть сопоставлено любому другому элементу модели данных. Поле кастомизируется.
DeviceCustomString5Label	CEF	Поле для описания назначения поля DeviceCustomString5.
DeviceCustomString6	CEF	Поле для маппинга строкового значения, которое не может быть сопоставлено любому другому элементу модели данных. Поле кастомизируется.
DeviceCustomString6Label	CEF	Поле для описания назначения поля DeviceCustomString6.
DestinationDnsDomain	CEF	DNS-часть полного доменного имени (FQDN) точки назначения, если "сырое" событие содержит сведения об отправителе и получателе данных.

		Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationServiceName	CEF	Название сервиса на стороне приемника трафика. Например, «sshd». Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationTranslatedAddress	CEF	IP-адрес устройства приемника трафика (после трансляции). Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationTranslatedPort	CEF	Номер порта на устройстве приемника трафика (после трансляции адреса приемника). Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
DeviceCustomDate1	CEF	Поле для маппинга значения типа Timestamp, которое не может быть сопоставлено любому другому элементу модели данных. Поле кастомизируется.
DeviceCustomDate1Label	CEF	Поле для описания назначения поля DeviceCustomDate1.
DeviceCustomDate2	CEF	Поле для маппинга значения типа Timestamp, которое не может быть сопоставлено любому другому элементу модели данных. Поле кастомизируется.
DeviceCustomDate2Label	CEF	Поле для описания назначения поля DeviceCustomDate2.
DeviceDirection	CEF	Поле для описания направления соединения из "сырого" события. 0 – входящее соединение 1 – исходящее соединение
DeviceDnsDomain	CEF	DNS-часть полного доменного имени (FQDN) IP-адреса устройства, с которого пришло "сырое" событие.
DeviceExternalID	CEF	Внешний уникальный идентификатор устройства (продукта), если такой передается в "сыром" событии.
DeviceFacility	CEF	Facility из "сырого" события, если есть. Например, в Syslog в поле Facility может передаваться название компоненты ОС, в которой произошла ошибка.
DeviceInboundInterface	CEF	Название интерфейса входящего соединения.
DeviceNtDomain	CEF	Доменное имя Windows устройства
DeviceOutboundInterface	CEF	Название интерфейса исходящего соединения.

DevicePayloadID	CEF	Уникальный идентификатор полезной нагрузки, который ассоциирован с "сырым" событием.
DeviceProcessName	CEF	Название процесса из "сырого" события
DeviceTranslatedAddress	CEF	Ретранслированный IP-адрес устройства, с которого пришло "сырое" событие.
DestinationHostName	CEF	Название хоста приемника трафика. Полное доменное имя приемника трафика, если доступно. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationMacAddress	CEF	MAC-address устройства приемника трафика. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationNtDomain	CEF	Доменное имя Windows устройства приемника трафика. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationProcessID	CEF	Идентификатор системного процесса, ассоциированного с приемником трафика в "сыром" событии. Например, если в событии указано Process ID 105, то DestinationProcessId=105 Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationUserPrivileges	CEF	Названия security ролей, которые идентифицируют пользовательские привилегии на стороне точки назначения. Например, «User», «Guest», «Administrator» и т.п. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationProcessName	CEF	Название системного процесса в точке назначения. Например, «sshd», «telnet» и т.п. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationPort	CEF	Номер порта на стороне точке назначения. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationAddress	CEF	IPv4-адрес точки назначения. Используется для обработки логов сетевого

		трафика, где необходимо отличать источник и точку назначения.
DeviceTimeZone	CEF	Часовой пояс устройства, на котором было сгенерировано событие
DestinationUserID	CEF	Идентификатор пользователя на стороне точки назначения. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationUserName	CEF	Имя пользователя на стороне точки назначения. Может содержать адрес электронной почты пользователя. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
DeviceAddress	CEF	IPv4-адрес устройства, с которого получено событие.
DeviceHostName	CEF	Название хоста устройства, с которого было получено событие. Полное доменное имя устройства, если доступно.
DeviceMacAddress	CEF	MAC-адрес устройства, с которого было получено событие. Полное доменное имя устройства, если доступно.
DeviceProcessID	CEF	Идентификатор системного процесса устройства, который сгенерировал событие.
EndTime	CEF	Время завершения события.
ExternalID	CEF	Идентификатор устройства, который сгенерировал событие.
FileCreateTime	CEF	Время создания файла из события.
FileHash	CEF	Хеш-код файла
FileID	CEF	Идентификатор файла, если есть
FileModificationTime	CEF	Время последней модификации файла
FilePath	CEF	Путь к файлу, включая имя файла
FilePermission	CEF	Список разрешений к файлу.
FileType	CEF	Тип файла. Например, application, pipe, socket и т.п.
FlexDate1	CEF	Поле для маппинга значения типа Timestamp, которое не может быть сопоставлено любому другому элементу модели данных. Поле кастомизируется.
FlexDate1Label	CEF	Поле для описания назначения поля flexDate1Label.
FlexString1	CEF	Поле для маппинга значения типа String, которое не может быть сопоставлено любому другому элементу модели данных. Поле кастомизируется.

FlexString1Label	CEF	Поле для описания назначения поля flexString1Label.
FlexString2	CEF	Поле для маппинга значения типа String, которое не может быть сопоставлено любому другому элементу модели данных. Поле кастомизируется.
FlexString2Label	CEF	Поле для описания назначения поля flexString2Label.
FlexNumber1	CEF	Поле для маппинга целочисленного типа, которое не может быть сопоставлено любому другому элементу модели данных. Поле кастомизируется.
FlexNumber1Label	CEF	Поле для описания назначения поля flexNumber1Label.
FlexNumber2	CEF	Поле для маппинга целочисленного типа, которое не может быть сопоставлено любому другому элементу модели данных. Поле кастомизируется.
FlexNumber2Label	CEF	Поле для описания назначения поля flexNumber2Label.
FileName	CEF	Имя файла, без указания пути к файлу.
FileSize	CEF	Размер файла
BytesIn	CEF	Количество полученных байтов, которые были получены источником и переданы получателю. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
Message	CEF	Краткое описание ошибки (проблемы) из события.
OldFileCreateTime	CEF	Время создания old-файла из события.
OldFileHash	CEF	Хеш-код old-файла
OldFileID	CEF	Идентификатор old-файла, если есть.
OldFileModificationTime	CEF	Время последней модификации old-файла
OldFileName	CEF	Имя old-файла (без пути)
OldFilePath	CEF	Путь к old-файлу, включая имя файла
OldFilePermission	CEF	Список разрешений к old-файлу.
OldFileSize	CEF	Размер old-файла
OldFileType	CEF	Тип файла. Например, application, pipe, socket и т.п.
BytesOut	CEF	Количество отправленных байтов. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
EventOutcome	CEF	Результат выполнения Action. Например, «success», «failure».
TransportProtocol	CEF	Название протокола 4-уровня OSI (TCP, UDP и т.п.)

Reason	CEF	Краткое описание причины аудита в сообщениях аудита.
RequestUrl	CEF	Запрошенный URL
RequestClientApplication	CEF	Агент, который обрабатывал Request
RequestContext	CEF	Описание контекста запроса
RequestCookies	CEF	Файлы cookie, связанные с запросом
RequestMethod	CEF	Метод, который использовался для доступа к веб-адресу (POST, GET и т.п.)
DeviceReceiptTime	CEF	Время получения события
SourceHostName	CEF	Название хоста источника трафика. Полное доменное имя источника трафика, если доступно. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceDnsDomain	CEF	Доменное имя Windows устройства источника трафика. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceServiceName	CEF	Название сервиса на стороне источника трафика. Например, «sshd». Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceTranslatedAddress	CEF	IPv4-адрес перехода источника. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceTranslatedPort	CEF	Номер порта перехода на стороне источника. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceMacAddress	CEF	MAC-адрес устройства источника трафика. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceNtDomain	CEF	Доменное имя Windows устройства источника трафика.Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceProcessID	CEF	Идентификатор системного процесса, ассоциированного с источником трафика в "сыром" событии. Например, если в событии указано Process ID 105, то SourceProcessId=105

		Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceUserPrivileges	CEF	Названия security ролей, которые идентифицируют пользовательские привилегии на стороне источника. Например, «User», «Guest», «Administrator» и т.п. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceProcessName	CEF	Название системного процесса на стороне источника. Например, «sshd», «telnet» и т.п. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
SourcePort	CEF	Номер порта на стороне источника. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceAddress	CEF	IPv4-адрес источника. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
StartTime	CEF	Время, когда началось связанное с событием действие.
SourceUserID	CEF	Идентификатор пользователя на стороне источника. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceUserName	CEF	Имя пользователя на стороне источника. Может содержать адрес электронной почты пользователя. Используется для обработки логов сетевого трафика, где необходимо отличать источник и точку назначения.
Type	CEF	Доступны следующие значения: • 1 – базовое событие. • 2 – агрегированное событие. • 3 – корреляционное событие. • 4 – событие аудита. • 5 – событие мониторинга.
CorrelationBucketHash	CEF	Ключ Correlation Bucket. При формировании ключа используются поля корреляционного события.

		Используется при формировании уведомлений пользователю.
GroupedBy	CEF	Список названия полей, по которым была группировка в корреляционном правиле. Заполняется только для корреляционного события.
tenantID	CEF	Название тенанта

Поля корреляционных событий

Корреляционные события создаются корреляторами KUMA при соблюдении определенных условий, заданных в правилах корреляции. Корреляционное событие соответствует модели данных нормализованного события.

Поля корреляционных событий

Поле	Описание
`ID`	Уникальный идентификатор
`Type`	Тип события. Корреляционному событию должно соответствовать значение `2`.
`Name`	Название корреляционного события. По умолчанию в качестве названия используется имя правила корреляции (то есть название ресурса Правило корреляции), которое породило это событие. Именования можно изменить в правилах корреляции в группе настроек **Обогащение**.
`Timestamp`	Время и дата создания корреляционного события.
`CorrelationRuleID`	Идентификатор правила корреляции, породившего это событие.
`CorrelationRuleName`	Название правила корреляции, породившего это событие.
`Priority`	Уровень важности корреляционного события
`ServiceID`	Идентификатор коррелятора, сервиса создавшего событие.
`DeviceProduct`	`KUMA`
`DeviceVendor`	`Kaspersky`
`BaseEventCount`	Количество базовых событий, связанных с корреляционным событием.
`BaseEventIDs`	Список идентификаторов базовых событий, на которых было основано корреляционное событие. Для DrillDown.
`AffectedAssets`	Список уникальных адресов, хостов, пользователей, идентификаторы устройств, которые были затронуты потенциальным инцидентом
<Поля, которые были указанные в поле **Группирующие поля** ресурса Правило корреляции>	Копируется из событий, обработанных правилом корреляции.

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.
Type	Тип события аудита. Событию аудита соответствует значение `4`.

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`

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	ID пользователя, который использовался для изменения данных.

DestinationUserName	Логин пользователя, данные которого были изменены.
DestinationUserID	ID 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.

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.

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 создания сервиса.
SourceUserID	Идентификатор пользователя, который использовался для создания сервиса.
DeviceExternalID	ID сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.

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 создания сервиса.
SourceUserID	Идентификатор пользователя, который использовался для создания сервиса.
DeviceExternalID	ID сервиса.
DeviceProcessName	Название сервиса.

DeviceFacility	Тип сервиса.

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.

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.

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`

Индекс 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 создания сервиса.
SourceUserID	Идентификатор пользователя, который использовался для создания сервиса.
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

Это событие может поступить со статусами `succeeded` или `failed`.

Поскольку запрос на очистку активного листа осуществляется через удаленное соединение, ошибка передачи данных может возникнуть как до удаления, так и после удаления.

Это означает, что активные лист может быть очищен успешно, но событие все равно будет иметь статус `failed`. Фактически, EventOutcome возвращает статус TCP/IP-соединения запроса, а статус проверки того, 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.

Элемент активного листа успешно удален или операция завершилась с ошибкой

Это событие может поступить со статусами `succeeded` или `failed`.

Поскольку запрос на удаление элемента активного листа осуществляется через удаленное соединение, ошибка передачи данных может возникнуть как до удаления, так и после удаления.

Это означает, что элемент активного листа может быть удален успешно, но событие все равно будет иметь статус `failed`. Фактически, EventOutcome возвращает статус TCP/IP-соединения запроса, а статус проверки того, 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, активные 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.

Активный лист успешно импортирован или операция завершилась с ошибкой

Частично импортировано через удаленное подключение.

Во время операции может произойти ошибка, что означает, что EventOutcome = `failed` также может означать ошибку подключения, при которой данные могут быть частично или полностью импортированы.

Однако в большинстве случаев ошибка означает, что данные не были импортированы или были импортированы лишь частично.

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.

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.

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

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`

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`

Устройство успешно создано

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 устройства.
SourceUserID	Идентификатор пользователя, который использовался для добавления устройства.
DeviceExternalID	Идентификатор устройства.
SourceHostName	Идентификатор устройства.
Name	Название устройства.
DeviceCustomString1	Разделенные запятыми IP-адреса устройства.
DeviceCustomString1Label	`addresses`

Устройство успешно удалено

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 устройства.
SourceUserID	Идентификатор пользователя, который использовался для добавления устройства.
DeviceExternalID	Идентификатор устройства.
SourceHostName	Идентификатор устройства.
Name	Название устройства.
DeviceCustomString1	Разделенные запятыми IP-адреса устройства.
DeviceCustomString1Label	`addresses`

Категория устройства 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.

Категория устройства 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.

Настройки 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 настроек.
SourceUserID	Идентификатор пользователя, который использовался для обновления настроек.

DeviceFacility	Тип настроек.

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.

Apache и Apache feather logo – товарные знаки Apache Software Foundation.

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.

Google, Chrome – товарные знаки Google, Inc.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Active Directory и Windows – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

CVE – зарегистрированный товарный знак MITRE Corporation.

Mozilla и Firefox – товарные знаки Mozilla Foundation.

CentOS – товарный знак компании Red Hat, Inc.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

ClickHouse – товарный знак компании YANDEX LLC.

Oracle – зарегистрированный товарный знак компании Oracle и/или аффилированных компаний.