kaspersky

Kaspersky Unified Monitoring and Analysis Platform

Руководство администратора

kaspersky

Уважаемый пользователь!

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

Дата редакции документа: 25.09.2020

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

О "Лаборатории Касперского" https://www.kaspersky.ru/about/company

kaspersky

Содержание

kaspersky

О программе Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Unified Monitoring and Analysis Platform (далее KUMA или «программа») – решение класса SIEM (Security information and event management), предназначенное для централизованного сбора, анализа и корреляции событий информационной безопасности с различных источников данных. Решение обеспечивает единую консоль мониторинга, анализа и реагирования на угрозы ИБ, объединяя как продукты «Лаборатории Касперского», так и сторонних производителей. Kaspersky Unified Monitoring and Analysis Platform сочетает в себе следующие функциональные возможности:

- получение, обработка и хранение событий информационной безопасности;
- анализ и корреляция;
- поиск полученных событий;
- создание уведомлений о выявленных инцидентах.

Программа построена на микросервисной архитектуре. Это означает, что вы можете создавать и настраивать только необходимые микросервисы, 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.

В этом разделе

Комплект поставки

В комплект поставки входят следующие файлы:

- kuma-0.3.26-<номер сборки>.el8.x86_64 для установки на серверах Коллектора, Коррелятора и Хранилища KUMA;
- kuma-storage-0.3.0-<номер сборки>.el8.x86_64 для установки на серверах Хранилища KUMA;
- пакет kuma-core-0.3.0-<номер сборки>.el8.x86_64;
- пакет kuma-console-0.3.28-<номер сборки>.el8.x86_64;
- kuma.exe для установки Агента KUMA для Windows®;
- kuma-installer для установки компонентов KUMA;
- файлы с текстом Лицензионного соглашения на английском и русском языках;
- файлы с информацией о версии (примечания к выпуску) на английском языке.

kaspersky

В комплект поставки также входит бинарный файл для установки MongoDB, Elasticsearch OSS 7.5.1, Prometheus 2.12.0 и Grafana 6.3.5 вместе с лицензиями.

Аппаратные и программные требования

KUMA может работать на физическом оборудолвании и в виртуальных средах.

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 настроек.

- Серверы для установки Коллекторов:
  - ЦП: 8 vCPU
  - ОЗУ: 4 ГБ
  - Диск: 100 ГБ доступного места на диске, смонтированного в разделе /opt
- Серверы для установки Корреляторов:
  - ЦП: 8 vCPU
  - ОЗУ: 16 ГБ
  - Диск: 100 ГБ доступного места на диске, смонтированного в разделе /opt
- Серверы для установки Ядра:
  - ЦП: 4 vCPU
  - ОЗУ: 8 ГБ
  - Диск: 100 ГБ доступного места на диске, смонтированного в разделе /opt
- Серверы для установки Хранилища:
  - ЦП: 24 vCPU
  - 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 развертывайте все кластерные узлы на одном JBOD-массиве или одном физическом сервере (если используются виртуальные серверы).

  Для повышения эффективности рекомендуется развернуть все серверы в одном центре обработки данных.

kaspersky

Требования к программному обеспечению

На каждом сервере, который используется для установки микросервисов KUMA, необходимо установить операционную систему CentOS 8.x.

Требования к сети

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

Дополнительные требования

На компьютерах, используемых для веб-консоли KUMA, необходимо установить бразуер Google Chrome™ 78 или более поздней версии либо Mozilla™ Firefox™ 70 или более поздней версии.

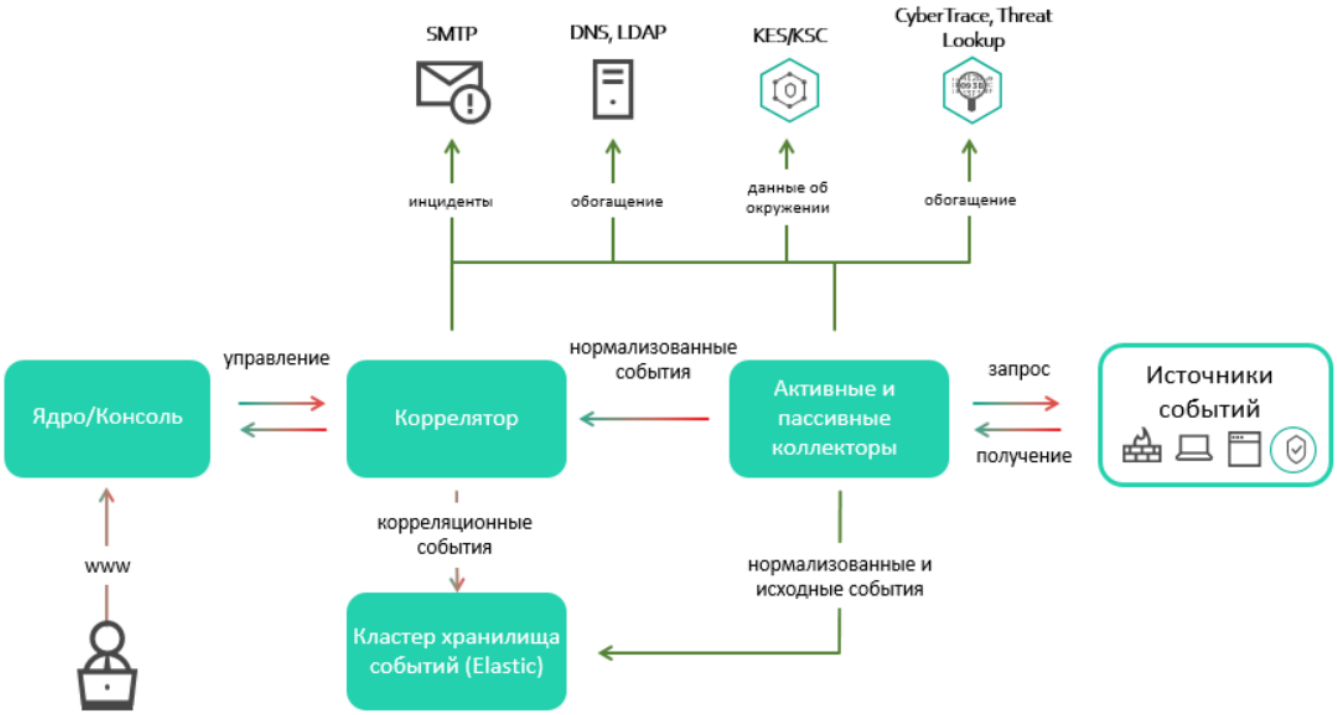
kaspersky

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 инциденты в соответствии с правилами корреляции;
- Ядро, поставляемое с графическим интерфейсом для мониторинга и управления настройками компонентов системы;
- Хранилище, в котором содержатся нормализованные события и зарегистрированные инциденты.

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



В этом разделе

kaspersky

Ядро

Ядро – это центральный компонент KUMA, через который производится управление всеми микросервисами. Предоставляемый ядром графический пользовательский интерфейс веб-консоли предназначен как для повседневного использования операторами и аналитиками, так и для настройки системы в целом.

Ядро позволяет решать следующие задачи:

- создание и настройка микросервисов (или компонентов) программы;
- централизованное управление микросервисами и учетными записями пользователей программы;
- визуальное представление статистических данных о работе программы;
- расследование угроз 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 каждого Коллектора нужно настроить как минимум 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 микросервисы, необходимо добавить точки назначения. В стандартном развертывании обычно используются две точки назначения: Хранилище и Коррелятор.

Алгоритм работы Коллектора включает следующие этапы:

a. **Получение сообщений из источников событий**

   Для получения сообщений требуется настроить активный или пассивный коннектор. Пассивный коннектор может только получать сообщения из источника события, а активный – инициировать подключение к источнику события, например, к системе управления базами данных.

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

   В программе доступны следующие типы коннекторов:

   - internal
   - tcp
   - udp
   - netflow
   - nats
   - kafka
   - http
   - file
   - sql

b. **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 корневой нормализатор типа CEF.

В программе доступны следующие нормализаторы:

- JSON
- CEF
- CSV/TSV
- Key-value
- Regexp
- Syslog (в соответствии с RFC3164 и RFC5424)
- XML
- NetFlow v9
- SQL

c. **Фильтрация нормализованных событий**

Вы можете настроить фильтры, которые позволяют отбирать для дальнейшей обработки только события, удовлетворяющие заданным условиям Событие, не удовлетворяющее условиям фильтрации, дальше не обрабатывается.

d. **Обогащение и преобразование нормализованных событий**

Правила обогащения позволяют дополнить содержимое события информацией 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

e. **Агрегация нормализованных событий**

Вы можете настроить правила агрегации, чтобы уменьшить количество схожих сообщений, передаваемых в Хранилище и/или Коррелятор. Например, вы можете 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 микросервисы, отвечающие за дальнейшую обработку событий, и сэкономить место для хранения.

f. **Передача нормализованных событий**

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

Коррелятор

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

Полученные в ходе анализа данные применяются для решения следующих задач:

- выявление инцидентов;
- уведомление о выявленных инцидентах;
- управление содержимым активных списков;
- отправка корреляционных событий в настроенные точки назначения.

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 может стать базовым для других правил корреляции. Результаты одного корреляционного правила могут использоваться другими корреляционными правилами.

Вы можете вручную распределять корреляционные правила и используемые ими активные листы между Корреляторами, регулируя распределение нагрузки между микросервисами. В этом случае Коллекторы будут отправлять одни и те же нормализованные события во все доступные Корреляторы.

Алгоритм работы Коррелятора включает следующие этапы:

a. **Получение события**

Коррелятор получает нормализованное событие из Коллектора или другого микросервиса.

b. **Применение правил корреляции**

Вы можете настроить правила корреляции на срабатывание на основе одного события или последовательности событий. Если по правилам корреляции не был выявлен инцидент, обработка события завершается.

c. **Реагирование на инцидент**

Вы можете задать действия, которые программа должна выполнить при выявлении инцидента.

В программе доступны следующие действия:

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

d. **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

Нормализованные события помещаются в кластер Elasticsearch (или Хранилище). Технология Elasticsearch позволяет выполнять поиск и агрегацию событий в Хранилище.

При выборе кластера конфигурации Elasticsearch учитывайте следующее:

- политики хранения события для вашей организации;
- лучшие практики по проектированию кластера Elasticsearch.

kaspersky

Установка KUMA

Вы можете развернуть компоненты KUMA на одном сервере с помощью приложения `kuma-installer`.

Имя сервера, на котором запускается установщик, должно отличаться от `localhost` или `localhost.<домен>`. Установщик через `kuma-installer` можно запустить из любой папки, но RPM-пакеты должны находится в одной папке с файлом `kuma-installer`.

После первоначальной установки вы можете использовать установщик повторно. При этом установщик повторит свои действия, не удаляя пользовательские данные. Это можно использовать при восстановлении системных файлов KUMA или примеров ресурсов и микросервисов, которые были изменены или удалены по ошибке.

Для установки продукта требуются root-привилегии.

► *Для запуска kuma-installer выполните следующую команду:*

```
kuma-installer [--with-example-services]
```

Действия, выполняемые установщиком

Установщик выполняет следующие действия:

1. Запрос на подтверждение установки программы.
2. Отключение SELinux.
3. Установка RPM-пакетов kuma, kuma-core и kuma-console.
4. Установка и запуск микросервиса kuma-core systemd.

   На этом шаге необходимо указать, принимаете ли вы условия Лицензионного соглашения. Если вы не принимаете условия Лицензионного соглашения, установка программы не выполняется.
5. Импорт примеров ресурсов.
6. Открытие портов для отправки сообщений между микросервисами KUMA.
7. Предоставление пользователю веб-адреса веб-консоли KUMA.
8. Предоставление имени и пароля пользователя для доступа к веб-консоли.

Действия, выполняемые установщиком при использовании флага `--with-example-services`

Помимо описанного ранее установщик также выполняет следующие действия:

1. Установка RPM-пакета kuma-storage.
2. Изменение конфигурации Elasticsearch и перезапуск микросервиса elasticsearch systemd.
3. Установка примеров Коллекторов, Коррелятора и Хранилища, а также запуск их микросервисов в systemd.
4. Открытие портов, через которые Коллекторы должны получать события из источников событий.

kaspersky

Подготовка к установке программы

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`.

Перед развертыванием программы убедитесь, что серверы, предназначенные для установки ее компонентов, соответствуют аппаратным и программным требованиям.

► *Для подготовки программы к установке сделайте следующее:*

1. При установке операционной системы выберите минимальный набор пакетов.
2. Задайте следующую разметку дискового пространства сервера:
   - корневой раздел /: Standard Partition, XFS, 16 Гб, разрешено шифрование;
   - раздел /opt: LVM, XFS, все доступное дисковое пространство, разрешено шифрование.
3. После установки операционной системы и перезагрузки сервера отключите SELinux.
   a. Если параметр `SELINUX` имеет значение `enforcing`, отключите запуск SELinux при загрузке системы. Для этого в файле /etc/selinux/config укажите `SELINUX=disabled` вместо `SELINUX=enforcing`.
   b. Если для параметра `SELinux status` значение включено, отключите SELinux, выполнив следующую команду:

      ```
      setenforce 0
      ```

О лицензионном соглашении

Лицензионное соглашение – это юридически обязывающий договор между вами и "Лабораторией Касперского", где определены условия, на которых вы можете использовать программу.

Перед началом использования программы внимательно прочитайте лицензионное соглашение.

Ознакомиться с условиями лицензионного соглашения можно следующими способами:

- в ходе установки KUMA;
- прочитав файл EULA_<идентификатор языка>, входящий в пакет поставки программы;
- выполнив следующую команду:

  ```
  kuma license
  ```

При установке программы вы принимаете условия лицензионного соглашения, подтверждая свое согласие с ними. Если вы не согласны с условиями лицензионного соглашения, отмените установку и не используйте программу.

kaspersky

Работа с инцидентами

В разделе **Alerts** веб-интерфейса KUMA можно просматривать и обрабатывать инциденты, зарегистрированные программой.

В верхней части раздела **Alerts** показана панель инструментов для фильтрации и поиска инцидентов.

В основной части раздела **Alerts** представлена таблица, в столбцах которой содержится информация о зарегистрированных инцидентах:

- Priority () **–** степень значимости потенциальной угрозы безопасности: критическая  , высокая  , умеренная  , низкая .
- **Status** – текущее состояние инцидента:
  - **new** – новый, еще не обработанный инцидент;
  - **assigned** – инцидент обработан и передан сотруднику службы безопасности для расследования или реагирования;
  - **closed** – инцидент закрыт. Инцидент был ложный или угроза безопасности устранена.
- **Assigned to** – имя сотрудника службы безопасности, которому инцидент передан для расследования или реагирования.
- **First seen** – дата и время создания первого корреляционного события в последовательности событий, приведшего к созданию инцидента.
- **Last seen** – дата и время создания последнего корреляционного события в последовательности событий, приведшего к созданию инцидента.

События и инциденты можно сортировать и фильтровать по значениям в столбцах.

При создании инцидента открывается окно со сведениями о нем.

Работа с событиями

В разделе **Events** веб-консоли Ядра KUMA вы можете просматривать события, хранящиеся в кластере Elasticsearch, чтобы расследовать угрозы безопасности или создавать правила корреляции.

События можно фильтровать. Для отображения самых последних записей по выбранным событиям обновите веб-страницу или установите флажок автоматического обновления **Auto refresh**.

События загружаются в браузер пакетами. Чтобы загрузить очередной пакет событий, прокрутите таблицу событий до конца и нажмите кнопку **Load next 250 events**.

Управление устройствами

В разделе **Assets** веб-консоли KUMA можно просматривать и изменять информацию об известных устройствах и их категории.

В левой части раздела **Assets** 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 щелкнуть по устройству, в правой части окна открывается область **Asset details** со следующими параметрами устройства:

- **Name** – имя устройства.
- **ID** – идентификатор устройства.
- **Created** – дата и время добавления устройства в KUMA.
- **Updated** – дата и время изменения информации об устройстве.
- **IP address** – IP-адрес устройства (если предоставлен).
- **DNS name** – доменное имя устройства (если предоставлено).
- **IP address** – IP-адрес устройства (если предоставлен).
- **Related alerts** – инциденты, с которыми связано устройство (если есть).

  Для просмотра списка инцидентов, с которыми связано устройство, можно щелкнуть по ссылке **Find in Alerts**. Откроется вкладка **Alerts** с поисковым выражением, позволяющим отфильтровать все устройства с соответствующим идентификатором.
- **Categories** – категории, к которым относится устройство (если есть).

Вход в веб-консоль программы

► *Для входа в веб-консоль программы сделайте следующее:*

1. В браузере введите следующий адрес:

   `https://<IP-адрес или FQDN сервера Ядра KUMA>:7220`

   Откроется страница авторизации веб-консоли с запросом на ввод имени и пароля для входа.
2. В поле **User name** введите имя учетной записи.
3. В поле **Password** введите пароль указанной учетной записи.
4. Нажмите на кнопку **Login**.

Откроется главное окно веб-консоли программы.

► *Для выхода из веб-консоли программы сделайте следующее:*

Откройте веб-консоль KUMA, в левом нижнем углу окна щелкните по имени учетной записи пользователя и в открывшемся меню учетной записи нажмите на кнопку **Logout**.

kaspersky

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".

kaspersky

Примеры настройки KUMA

В этом разделе приводятся примеры настройки KUMA.

Это только пример. При настройке KUMA в своей сети используйте собственную конфигурацию.

В этом разделе

Создание правил корреляции

В этом разделе приведены примеры создания правил корреляции:

- Правило корреляции на основе бакетов
- Правило корреляции на основе активного списка

Также описано, как добавить правила корреляции и активный список в существующий Коррелятор и как проверить их работу.

В этом разделе

Корреляция событий с использованием бакета

В этом примере показано создание правила корреляции, использующего бакеты для обнаружения корреляций.

Задача – выявить события создания учетной записи, которая затем была удалена в течение часа. Необходимо обнаружить событие создания (Windows EventID 4720) и событие удаления (Windows EventID 4726), промежуток времени между которыми менее одного часа.

kaspersky

Корреляция выполняется одним правилом корреляции, в котором используется два фильтра для поиска соответствующих событий. При получении события, удовлетворяющего условиям фильтра, правило корреляции ожидает другого события в течение 3600 секунд. Если оба события произошли в течение часа, создается событие корреляции.

Настройка корреляции выполняется поэтапно:

- Создание фильтров, используемых для поиска соответствующих событий. В данном примере это фильтры событий создания учетной записи и удаления учетной записи.
- Создание ресурса Правило корреляции.
- Связь Правила корреляции с существующим микросервисом Коррелятор.
- Проверка правильности работы правила корреляции.

В этом примере используются ресурсы, добавленные в KUMA как часть демонстрационного развертывания. Инструкции, приведенные в этом разделе, можно использовать для создания аналогичных ресурсов для ваших целей.

В этом разделе

Создание фильтра для поиска событий создания учетной записи

► *Чтобы создать ресурс Фильтр для поиска событий создания учетной записи, выполните следующие действия:*

1. Откройте веб-консоль KUMA и выберите закладку **Filters** в разделе **Resources**.
2. Нажмите на кнопку **Add**.

   Откроется окно для настройки параметров ресурса Фильтр.
3. В поле **Name** введите название фильтра, которое позволит идентифицировать созданный ресурс: `[Пример][AD] Созданная учетная запись`.
4. Перейдите по ссылке **Add condition**, чтобы добавить первое условие фильтра.

   Откроется окно **Condition**.
5. Задайте параметры для первого условия фильтра, как описано ниже:
   - В раскрывающемся списке **Operation** выберите **=**.
   - В группе параметров **Left operand** задайте параметры, как описано ниже:
     - В раскрывающемся списке **Kind** выберите **event**.
     - В раскрывающемся списке **Field** выберите **DeviceEventClassID**.
   - В группе параметров **Right operand** задайте параметры, как описано ниже:
     - В раскрывающемся списке **Kind** выберите **constant**.
     - В поле **Value** введите `4720`.

6. Нажмите на кнопку **Сохранить**.

   Окно **Condition** закроется, и отобразится созданное условие.

7. Перейдите по ссылке **Add condition**, чтобы добавить второе условие фильтра.

   Откроется окно **Condition**.

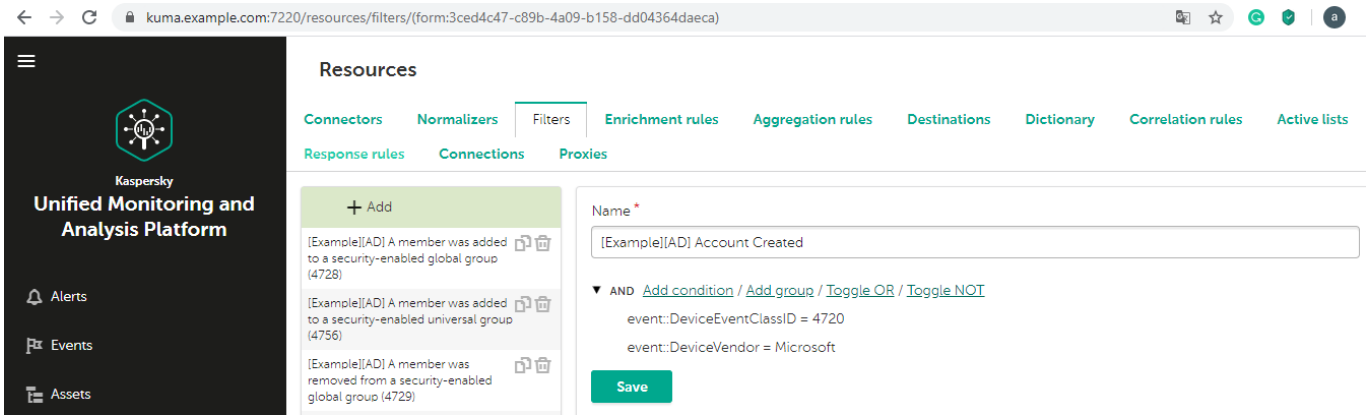
8. Задайте параметры для второго условия фильтра, как описано ниже:
   - В раскрывающемся списке **Operation** выберите **=**.
   - В группе параметров **Left operand** задайте параметры, как описано ниже:
     - В раскрывающемся списке **Kind** выберите **event**.
     - В раскрывающемся списке **Field** выберите **DeviceVendor**.
   - В группе параметров **Right operand** задайте параметры, как описано ниже:
     - В раскрывающемся списке **Kind** выберите **constant**.
     - В поле **Value** введите `Microsoft`.

9. Нажмите на кнопку **Сохранить**.

   Окно **Condition** закроется, и отобразится созданное условие.

10. Нажмите на кнопку **Сохранить**.

Фильтр будет создан и отобразится на закладке **Filters**.



Создание фильтра для поиска событий удаления учетной записи

► *Чтобы создать ресурс Фильтр для поиска событий создания учетной записи, выполните следующие действия:*

1. Откройте веб-консоль KUMA и выберите закладку **Filters** в разделе **Resources**.
2. Нажмите на кнопку **Add**.

   Откроется окно для настройки параметров ресурса Фильтр.

3. В поле **Name** введите название фильтра, которое позволит идентифицировать созданный ресурс: `[Пример][AD] Удаленная учетная запись`.
4. Перейдите по ссылке **Add condition**, чтобы добавить первое условие фильтра.

   Откроется окно **Condition**.

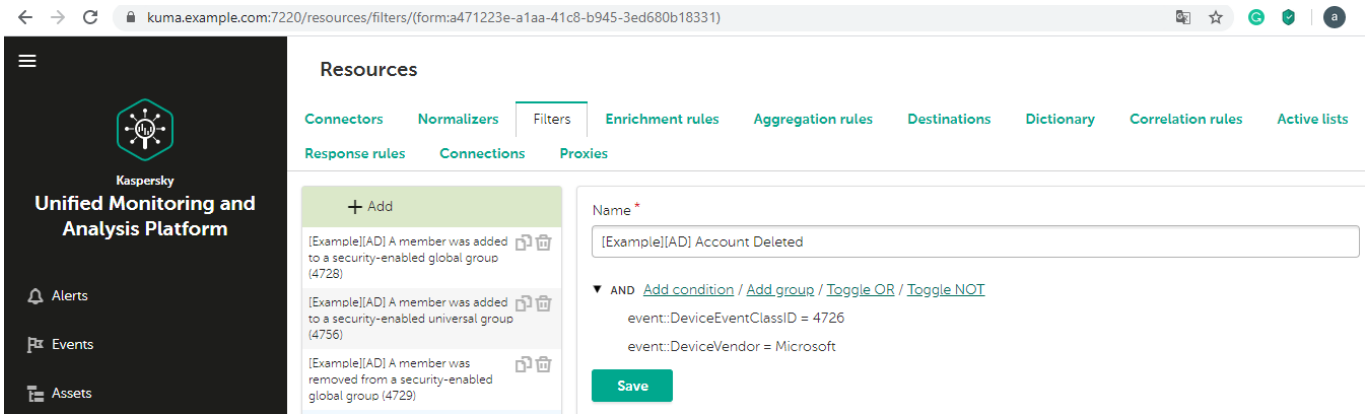
5. Задайте параметры для первого условия фильтра, как описано ниже:
   - В раскрывающемся списке **Operation** выберите **=**.
   - В группе параметров **Left operand** задайте параметры, как описано ниже:
     - В раскрывающемся списке **Kind** выберите **event**.
     - В раскрывающемся списке **Field** выберите **DeviceEventClassID**.
   - В группе параметров **Right operand** задайте параметры, как описано ниже:
     - В раскрывающемся списке **Kind** выберите **constant**.
     - В поле **Value** введите `4726`.
6. Нажмите на кнопку **Сохранить**.

   Окно **Condition** закроется, и отобразится созданное условие.
7. Перейдите по ссылке **Add condition**, чтобы добавить второе условие фильтра.

   Откроется окно **Condition**.
8. Задайте параметры для второго условия фильтра, как описано ниже:
   - В раскрывающемся списке **Operation** выберите **=**.
   - В группе параметров **Left operand** задайте параметры, как описано ниже:
     - В раскрывающемся списке **Kind** выберите **event**.
     - В раскрывающемся списке **Field** выберите **DeviceVendor**.
   - В группе параметров **Right operand** задайте параметры, как описано ниже:
     - В раскрывающемся списке **Kind** выберите **constant**.
     - В поле **Value** введите `Microsoft`.
9. Нажмите на кнопку **Сохранить**.

   Окно **Condition** закроется, и отобразится созданное условие.
10. Нажмите на кнопку **Сохранить**.

Фильтр будет создан и отобразится на закладке **Filters**.



kaspersky

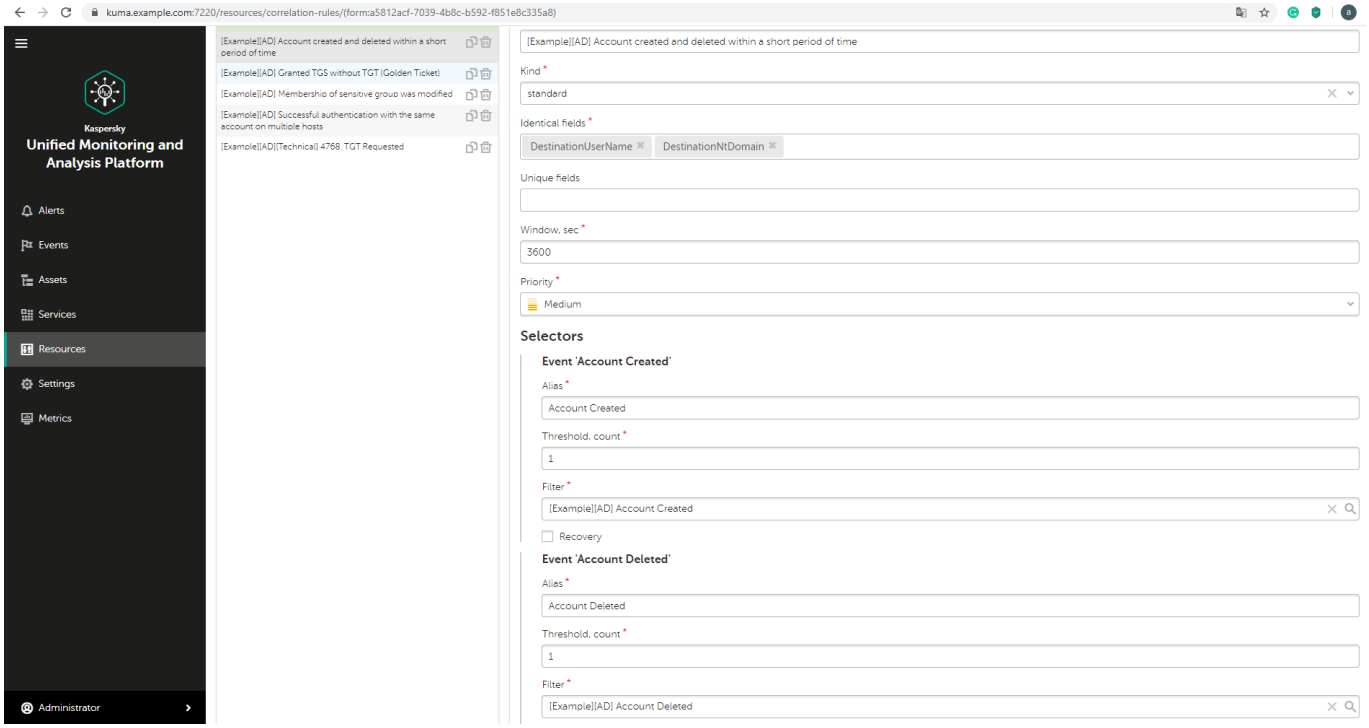
Создание правила корреляции для выявления создания и удаления учетных записей

► *Чтобы создать ресурс корреляции, выполните следующие действия:*

1. Откройте веб-консоль KUMA и выберите закладку **Correlation rules** в разделе **Resources**.
2. Нажмите на кнопку **Add**.

   Откроется окно для настройки параметров ресурса Правило корреляции.
3. В поле **Name** введите название фильтра, которое позволит идентифицировать созданный ресурс: `[Пример][AD] Учетная запись создана и удалена за короткий период времени`.
4. В раскрывающемся списке **Kind** выберите **standard**. Корреляция на основе бакетов доступна только для правил корреляции стандартного типа.
5. В раскрывающемся списке **Identical fields** выберите **DestinationUserName** и **DestinationNtDomain**.
6. В поле **Window, sec** укажите, сколько времени должен существовать бакет. Введите значение `3600`.
7. В раскрывающемся списке **Priority** выберите приоритет созданного правила корреляции. Выберите **Medium**.
8. В группе параметров **Selectors** добавьте фильтры, которые будут отбирать события для передачи в это правило корреляции:
   - Добавьте первый фильтр:
     - В поле **Alias** введите название фильтра: `Создана учетная запись`.
     - В поле **Threshold, count** введите количество событий, которое должно получить правило корреляции для срабатывания. Введите значение `1`.
     - В раскрывающемся списке **Filter** выберите созданный ранее фильтр `[Пример][AD] Создана учетная запись`.
   - Добавьте второй фильтр:
     - В поле **Alias** введите название фильтра: `Удалена учетная запись`.
     - В поле **Threshold, count** введите количество событий, которое должно получить правило корреляции для срабатывания. Введите значение `1`.

- В раскрывающемся списке **Filter** выберите созданный ранее фильтр `[Пример][AD] Удалена учетная запись`.



Оба фильтра добавлены к ресурсу Правило корреляции, но помимо этого необходимо убедиться, что правило срабатывает, только если событие создания учетной записи предшествует событию удаления учетной записи. Это условие можно задать в разделе **Join filter**.

9. В разделе **Join filter** перейдите по ссылке **Setup inline**.

   Откроется окно **Filter**, в котором можно настроить условия фильтрации. Добавьте условие фильтрации, как описано ниже:

   a. Перейдите по ссылке **Add condition**.

      Откроется окно **Condition**.

   b. В раскрывающемся списке **Operation** выберите **<**.

   c. В группе параметров **Left operand** задайте параметры, как описано ниже:

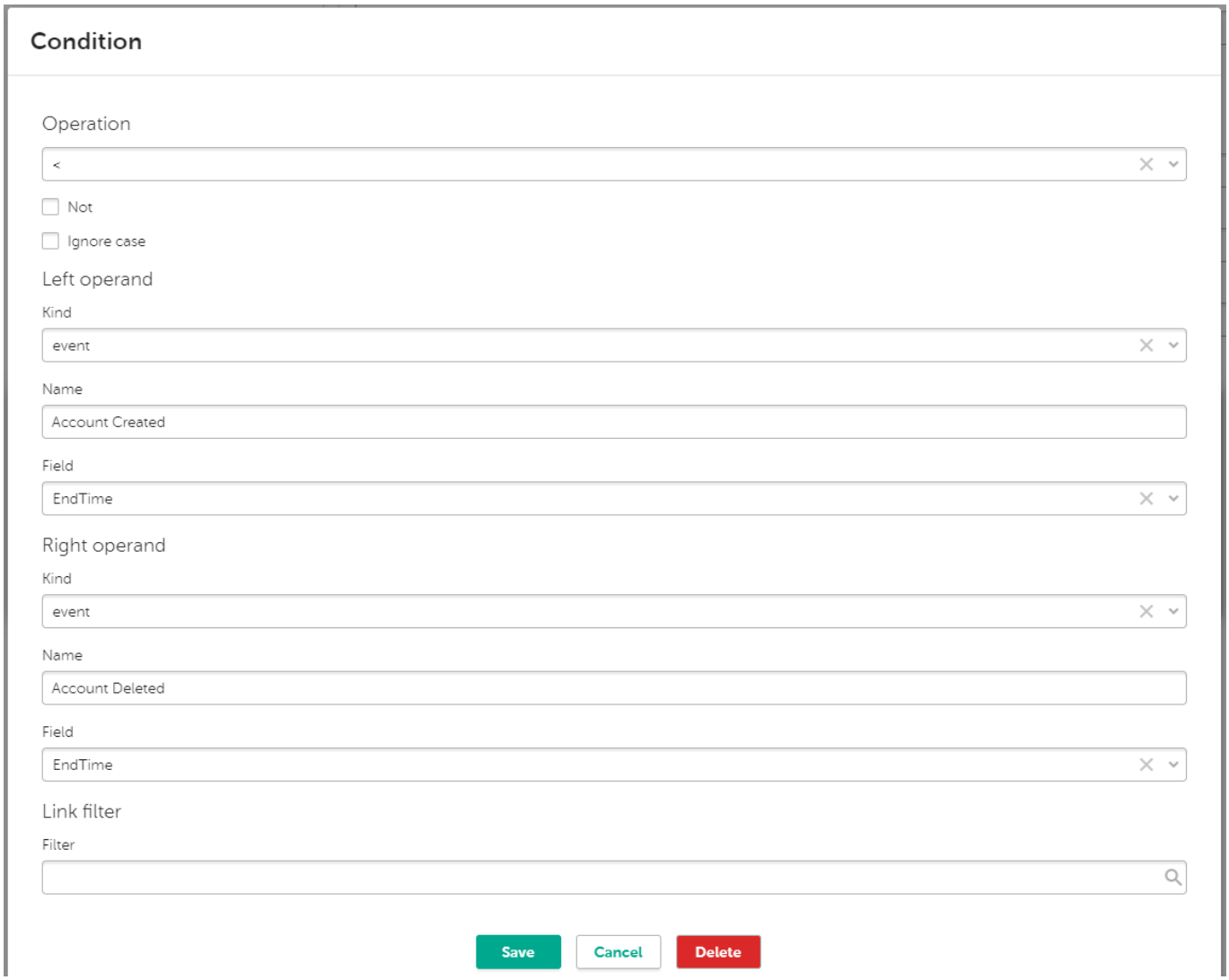
      - В раскрывающемся списке **Kind** выберите **event**.
      - В поле **Name** введите название одного из фильтров из раздела **Selector**. Введите `Создана учетная запись`.
      - В раскрывающемся списке **Field** выберите **EndTime**.

   d. В группе параметров **Right operand** задайте параметры, как описано ниже:

      - В раскрывающемся списке **Kind** выберите **event**.
      - В поле **Name** введите название одного из фильтров из раздела **Selector**. Введите `Удалена учетная запись`.
      - В раскрывающемся списке **Field** выберите **EndTime**.

   e. Нажмите на кнопку **Сохранить**.

Будет создано условие для объединенного фильтра, что обеспечит срабатывание правила корреляции, только если события от разных фильтров получены в определенном порядке.



10. Нажмите на кнопку **Ok**, чтобы завершить настройку объединенного фильтра.

    Когда все фильтры будут настроены, необходимо выбрать действия, которые будут выполняться при срабатывании правила.

11. В группе параметров **Actions** в разделе **onEveryThreshold** установите флажок **Output**.

    Это означает, что при каждом срабатывании правила корреляции будет создаваться событие корреляции и отправляться дальше микросервису Коррелятор.

12. Нажмите на кнопку **Сохранить**.

Правило корреляции будет создано и отобразится на закладке **Correlation rules**.

kaspersky

Корреляция событий с использованием активных списков

В этом примере показано создание правила корреляции, использующего активные списки для обнаружения корреляций.

Задача состоит в том, чтобы идентифицировать события запроса службы предоставления билетов (Ticket Granting Service – TGS) без предшествующего события билета на получение билетов (Ticket Granting Ticket – TGT). При получении TGT контроллер домена формирует событие с идентификатором 4768. При получении запроса TGS контроллер домена формирует событие с идентификатором 4769. Следовательно, потенциальный инцидент можно определить как получение события запроса TGS без предварительного получения события TGT.

Поскольку контроллеры домена получают большое количество событий с идентификаторами 4768 и 4769, а TGT действителен в течение 10 часов, использование правил корреляции на основе бакетов неэффективно. В этом случае следует использовать корреляцию на основе активного списка.

Корреляция будет осуществляться по двум правилам корреляции:

1. Первое правило срабатывает, когда пользователь получает TGT. Это событие записывается в активный список, где информация о нем хранится в течение 10 часов.
2. Второе правило срабатывает при получении события запроса TGS. Правило корреляции проверяет, содержит ли активный список информацию о событии TGT и созданном событии корреляции, если ничего не найдено.

Настройка правила корреляции выполняется поэтапно:

- Создание активного списка для хранения информации о событиях TGT.
- Создание правила корреляции для фильтрации событий TGT и их записи в активный список.
- Создание правила корреляции для фильтрации событий TGS и поиска соответствующих событий TGT в активном списке.
- Связь Правила корреляции с существующим микросервисом Коррелятор.
- Проверка правильности работы правила корреляции.

В этом примере используются ресурсы, добавленные в KUMA как часть демонстрационного развертывания. Инструкции, приведенные в этом разделе, можно использовать для создания аналогичных ресурсов для ваших целей.

В этом разделе

Создание активного списка для хранения TGT

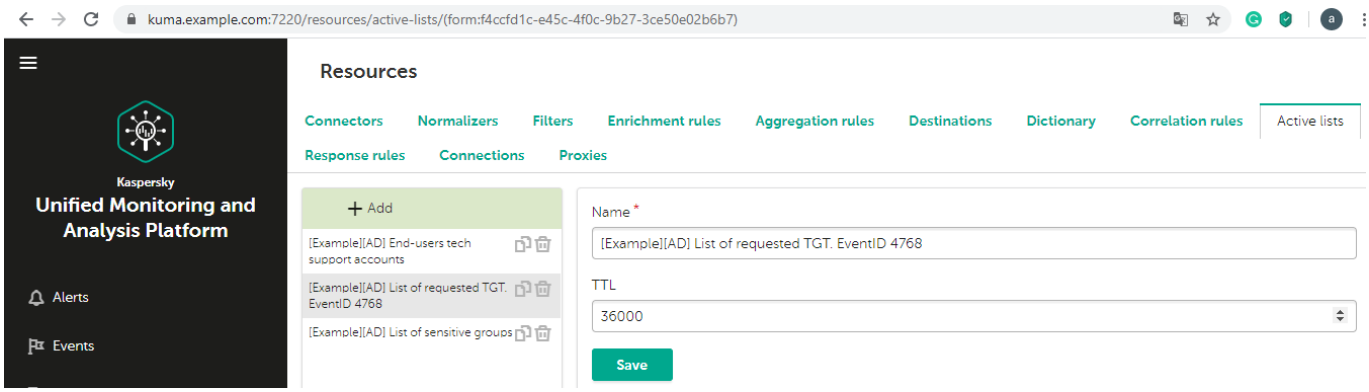
► *Чтобы создать активный список для хранения информации о событиях TGT, выполните следующие действия:*

1. Откройте веб-консоль KUMA и выберите закладку **Active lists** в разделе **Resources**.
2. Нажмите на кнопку **Add** и задайте параметры, как описано ниже.

- В поле **Name** введите название активного списка, которое позволит идентифицировать созданный ресурс: `[Пример][AD] Список запрашиваемых TGT. EventID 4768`.
- В поле **TTL** укажите, сколько секунд запись будет храниться в активном списке. Необходимо, чтобы запись в активном списке была доступна в течение периода времени, пока действует TGT, то есть в течение 10 часов. Введите значение `36000`.

3. Нажмите на кнопку **Save**.

Активный список будет создан и отобразится на закладке **Active lists**.



Создание правила корреляции для записи в активный список

► *Чтобы создать правило корреляции для записи информации о TGT в активный список, выполните следующие действия:*

1. Откройте веб-консоль KUMA и выберите закладку **Correlation rules** в разделе **Resources**.
2. Нажмите на кнопку **Add**.

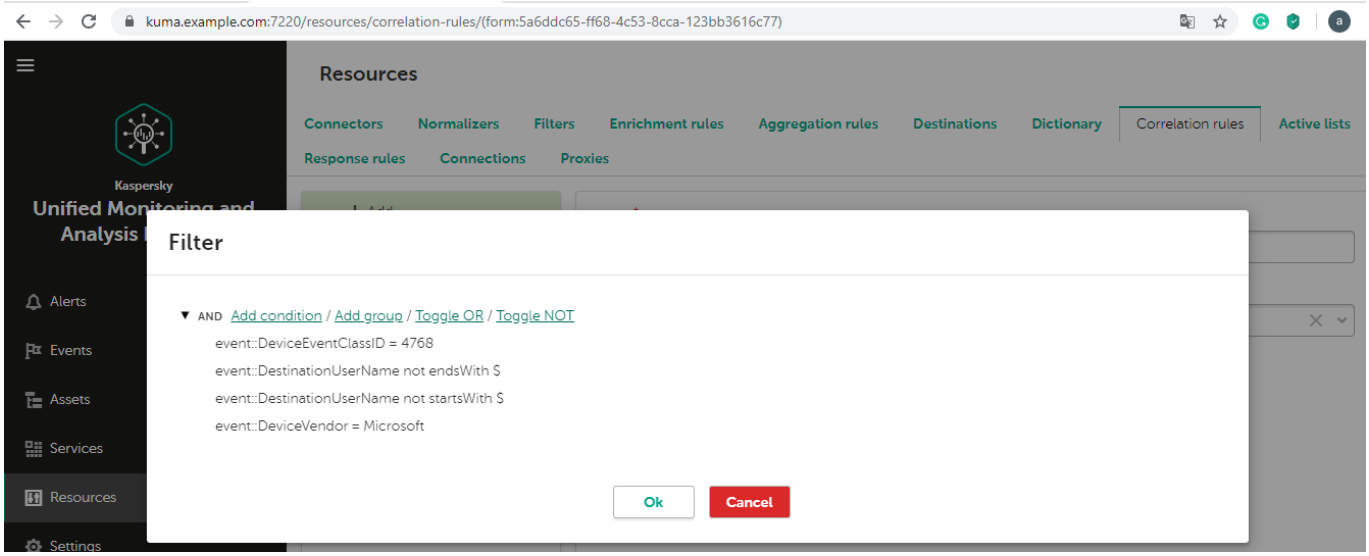
   Откроется окно для настройки параметров ресурса Правило корреляции.
3. В поле **Name** введите название фильтра, которое позволит идентифицировать созданный ресурс: `[Пример][AD][Технический] 4768. Запрашиваемый TGT`.
4. В раскрывающемся списке **Kind** выберите **operational**.
5. В разделе **Selectors** перейдите по ссылке **Setup inline**, чтобы добавить фильтр, который будет отбирать события для передачи в это правило корреляции.

   Откроется окно **Filter**, в котором можно настроить условия фильтрации. Добавьте условия фильтра с помощью кнопки **Add condition**, как описано ниже:

   - Первое условие:
     - В раскрывающемся списке **Operation** выберите =.
     - В группе параметров **Left operand** задайте параметры, как описано ниже:
       - В раскрывающемся списке **Kind** выберите **event**.
       - В раскрывающемся списке **Field** выберите **DeviceEventClassID**.
     - В группе параметров **Right operand** задайте параметры, как описано ниже:
       - В раскрывающемся списке **Kind** выберите **constant**.
       - В поле **Value** введите `4768`.

- Второе условие:
  - В раскрывающемся списке **Operation** выберите **endsWith**.
  - Установите флажок **Not**, чтобы создать фильтр, НЕ содержащий записей, соответствующих условию.
  - В группе параметров **Left operand** задайте параметры, как описано ниже:
    - В раскрывающемся списке **Kind** выберите **event**.
    - В раскрывающемся списке **Field** выберите **DestinationUserName**.
  - В группе параметров **Right operand** задайте параметры, как описано ниже:
    - В раскрывающемся списке **Kind** выберите **constant**.
    - В поле **Value** введите `S`.
- Третье условие:
  - В раскрывающемся списке **Operation** выберите **startsWith**.
  - Установите флажок **Not**, чтобы создать фильтр, НЕ содержащий записей, соответствующих условию.
  - В группе параметров **Left operand** задайте параметры, как описано ниже:
    - В раскрывающемся списке **Kind** выберите **event**.
    - В раскрывающемся списке **Field** выберите **DestinationUserName**.
  - В группе параметров **Right operand** задайте параметры, как описано ниже:
    - В раскрывающемся списке **Kind** выберите **constant**.
    - В поле **Value** введите `S`.
- Четвертое условие:
  - В раскрывающемся списке **Operation** выберите =.
  - В группе параметров **Left operand** задайте параметры, как описано ниже:
    - В раскрывающемся списке **Kind** выберите **event**.
    - В раскрывающемся списке **Field** выберите **DeviceVendor**.
  - В группе параметров **Right operand** задайте параметры, как описано ниже:
    - В раскрывающемся списке **Kind** выберите **constant**.
    - В поле **Value** введите `Microsoft`.

Условия фильтра будут созданы.



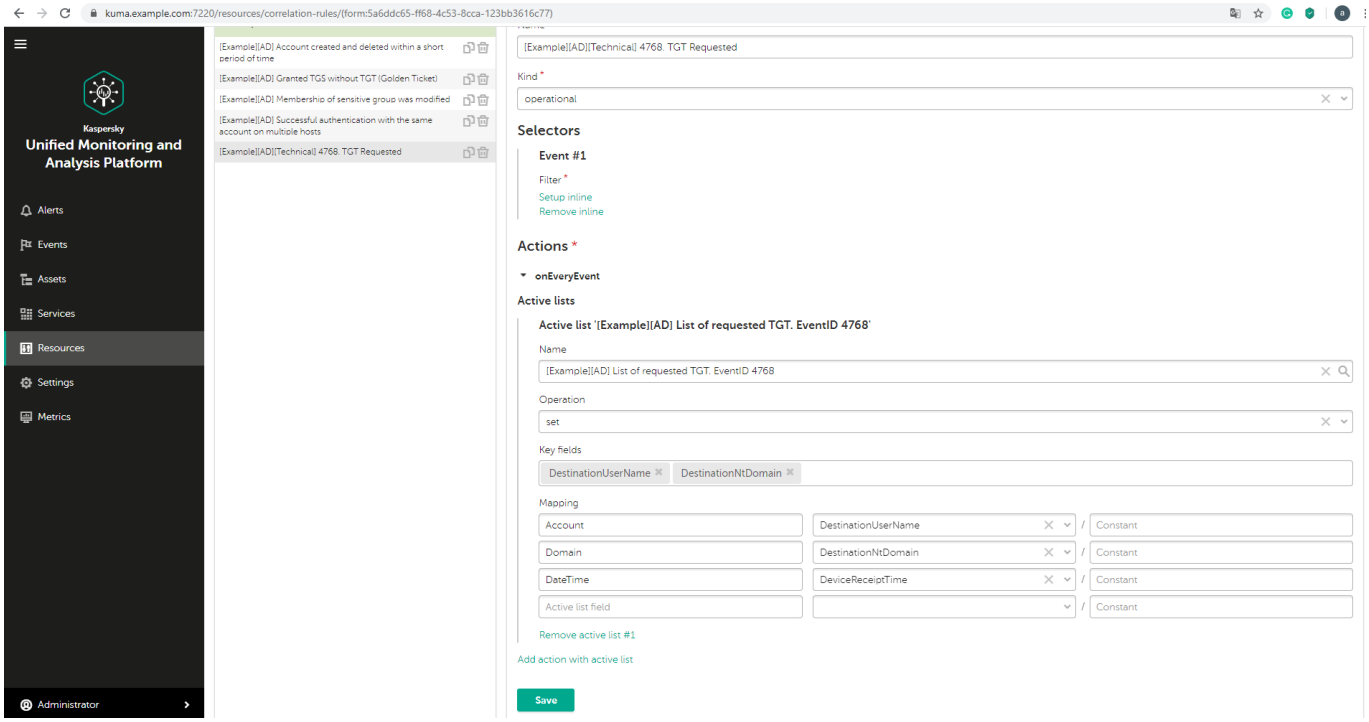
6. Нажмите на кнопку **Ok**, чтобы сохранить фильтр в правиле корреляции.

   Когда фильтр будет настроен, необходимо выбрать действия, которые будут выполняться при срабатывании правила.

7. В разделе **onEveryEvent** в группе параметров **Actions** перейдите по ссылке **Add action with active list** и задайте значения параметров, как описано ниже:

   - В поле **Name** введите название создаваемого триггера: `[Пример][AD] Список запрашиваемых TGT. EventID 4768`.
   - В раскрывающемся списке **Operation** выберите тип операции, которую требуется выполнить с активным списком. Выберите **set**.
   - В раскрывающемся списке **Key fields** выберите имена полей события, которые будут использоваться в идентификаторе записи активного списка. Выберите **DestinationUserName** и **DestinationNtDomain**.
   - В разделе **Mapping** задайте правила записи значений полей события в поля активного списка:
     - В поле **Active list field** введите `Account` и в раскрывающемся списке справа от этого поля выберите значение **DestinationUserName**.
     - В поле **Active list field** введите `Domain` и в раскрывающемся списке справа от этого поля выберите значение **DestinationNtDomain**.

- В поле **Active list field** введите `DateTime` и в раскрывающемся списке справа от этого поля выберите значение **DeviceReceiptTime**.



8. Нажмите на кнопку **Save**.

Событие корреляции будет создано и отобразится на закладке **Correlation rules**.

Создание правила корреляции для проверки, предшествует ли событие TGT запросу TGS

► *Чтобы создать правило корреляции для чтения информации о TGT из активного списка при получении событий запроса TGS, выполните следующие действия:*

1. Откройте веб-консоль KUMA и выберите закладку **Correlation rules** в разделе **Resources**.
2. Нажмите на кнопку **Add**.

   Откроется окно для настройки параметров ресурса Правило корреляции.
3. В поле **Name** введите название фильтра, которое позволит идентифицировать созданный ресурс: `[Пример][AD] Предоставленный TGS без TGT (Golden Ticket)`.
4. В раскрывающемся списке **Kind** выберите **simple**.
5. В раскрывающемся списке Identical fields выберите **DestinationUserName**, **SourceUserName** и **SourceAddress**.
6. В раскрывающемся списке **Priority** выберите приоритет созданного правила корреляции. Выберите **Medium**.
7. В разделе **Selectors** перейдите по ссылке **Setup inline**, чтобы добавить фильтр, который будет отбирать события для передачи в это правило корреляции.

   Откроется окно **Filter**, в котором можно настроить условия фильтрации. Добавьте условия фильтра с помощью кнопки **Add condition**, как описано ниже:

   - Первое условие:

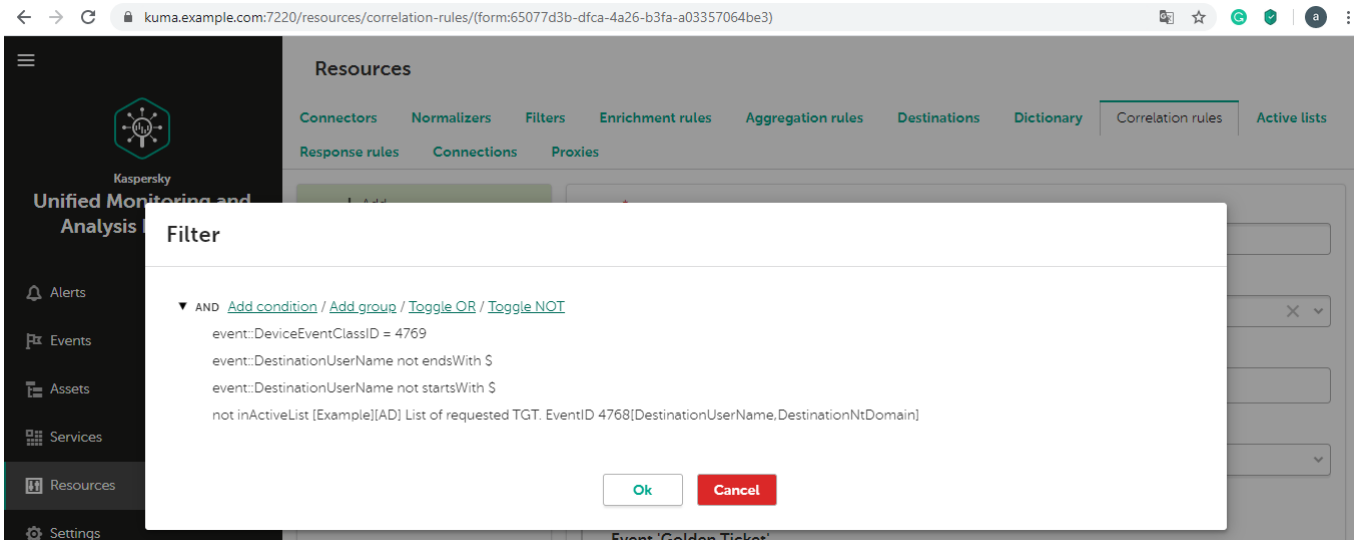
- В раскрывающемся списке **Operation** выберите =.
- В группе параметров **Left operand** задайте параметры, как описано ниже:
  - В раскрывающемся списке **Kind** выберите **event**.
  - В раскрывающемся списке **Field** выберите **DeviceEventClassID**.
- В группе параметров **Right operand** задайте параметры, как описано ниже:
  - В раскрывающемся списке **Kind** выберите **constant**.
  - В поле **Value** введите `4769`.

- Второе условие:
  - В раскрывающемся списке **Operation** выберите **endsWith**.
  - Установите флажок **Not**, чтобы создать фильтр, НЕ содержащий записей, соответствующих условию.
  - В группе параметров **Left operand** задайте параметры, как описано ниже:
    - В раскрывающемся списке **Kind** выберите **event**.
    - В раскрывающемся списке **Field** выберите **DestinationUserName**.
  - В группе параметров **Right operand** задайте параметры, как описано ниже:
    - В раскрывающемся списке **Kind** выберите **constant**.
    - В поле **Value** введите `S`.
- Третье условие:
  - В раскрывающемся списке **Operation** выберите **startsWith**.
  - Установите флажок **Not**, чтобы создать фильтр, НЕ содержащий записей, соответствующих условию.
  - В группе параметров **Left operand** задайте параметры, как описано ниже:
    - В раскрывающемся списке **Kind** выберите **event**.
    - В раскрывающемся списке **Field** выберите **DestinationUserName**.
  - В группе параметров **Right operand** задайте параметры, как описано ниже:
    - В раскрывающемся списке **Kind** выберите **constant**.
    - В поле **Value** введите `S`.
- Четвертое условие:
  - В раскрывающемся списке **Operation** выберите **inActiveList**.
  - Установите флажок **Not**, чтобы создать фильтр, НЕ содержащий записей, соответствующих условию.
  - В раскрывающемся списке Name выберите имя активного списка, из которого должна считываться информация о TGT: `[Пример][AD] Список запрашиваемых TGT. EventID 4768`.
  - В раскрывающемся списке **Key fields** выберите поля, которые будут использоваться в качестве ключа записи активного списка. Они должны совпадать с ключевыми полями,

используемыми при создании записи активного списка. Выберите **DestinationUserName** и **DestinationNtDomain**.

Условия фильтра будут созданы.

По этим условиям фильтра выполняется поиск всех событий с eventID 4769, у которых поля DestinationUserName и DestinationNtDomain НЕ находятся в активном списке, в котором хранится информация обо всех действительных TGT.



8. Нажмите на кнопку **Ok**, чтобы сохранить фильтр в правиле корреляции.

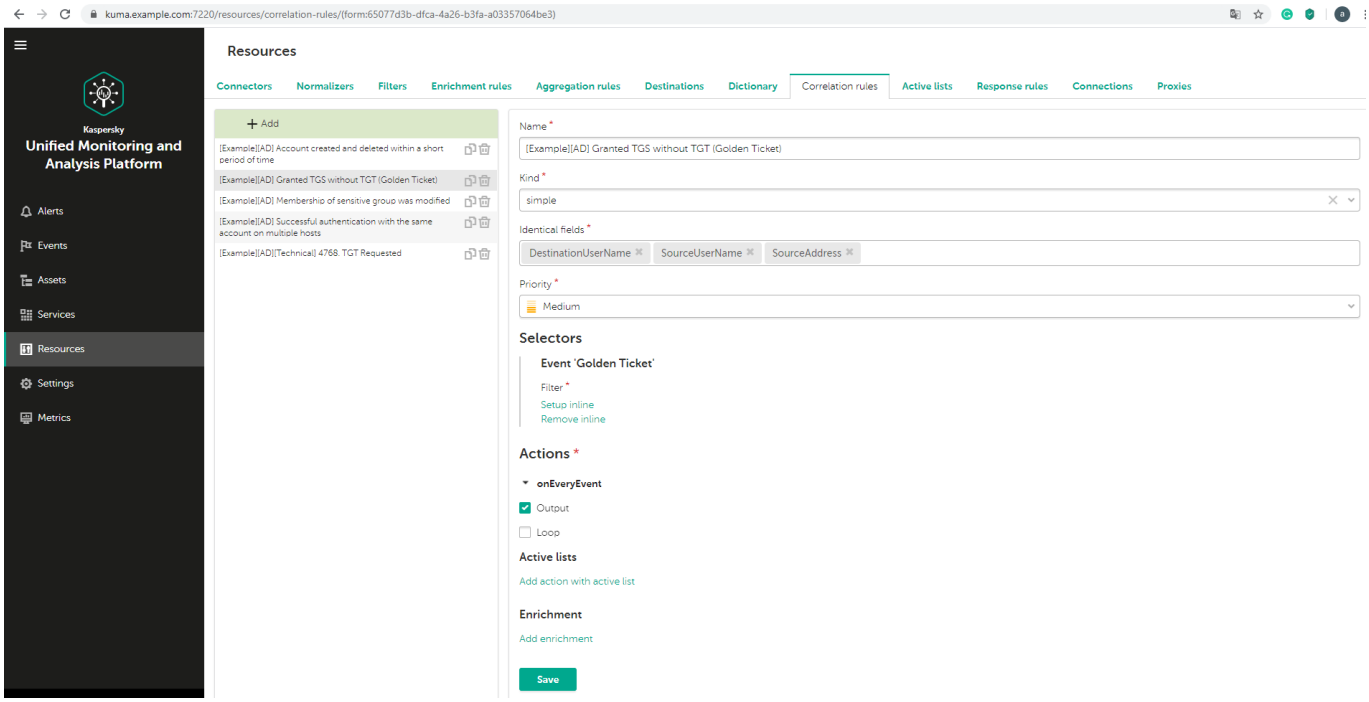
   Когда фильтр будет настроен, необходимо выбрать действия, которые будут выполняться при срабатывании правила.

9. В разделе **onEveryEvent** в группе параметров **Actions** установите флажок **Output**.

   Это означает, что при каждом срабатывании правила корреляции будет создаваться событие корреляции и отправляться дальше микросервису Коррелятор.

10. Нажмите на кнопку **Сохранить**.

Правило корреляции будет создано и отобразится на закладке **Correlation rules**.

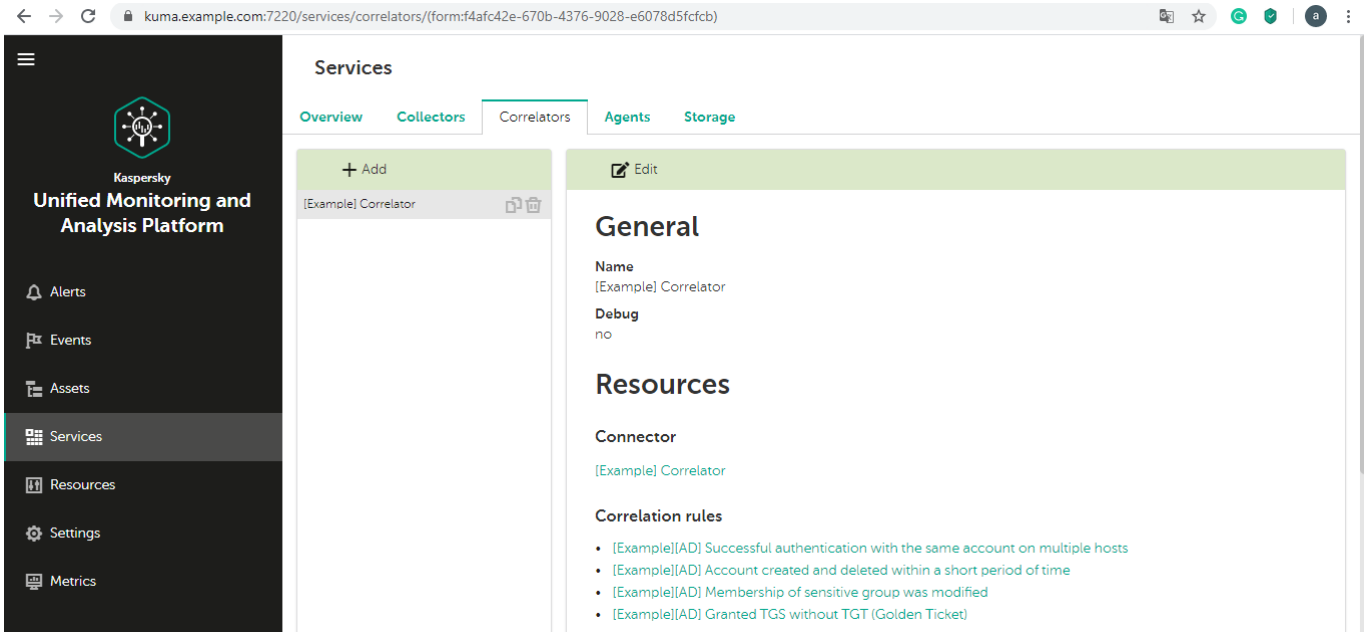


Связь правил корреляции с Коррелятором

При создании правила корреляции и активного списка, их необходимо связать с микросервисом Коррелятор, чтобы затем использовать при обработке событий.

► *Чтобы связать правило корреляции и активный список с существующим микросервисом Коррелятор, выполните следующие действия:*

1. Откройте веб-консоль KUMA и выберите закладку **Correlator** в разделе **Services**.



2. Выберите требуемый Коррелятор и нажмите на кнопку **Edit**.

   Откроется окно настройки микросервиса Коррелятор. Закладки настройки Коррелятора отображаются в верхней части окна: вы можете выбрать нужную закладку, щелкнув по ней, или переключаться между закладками с помощью кнопок **Next** и **Previous**.

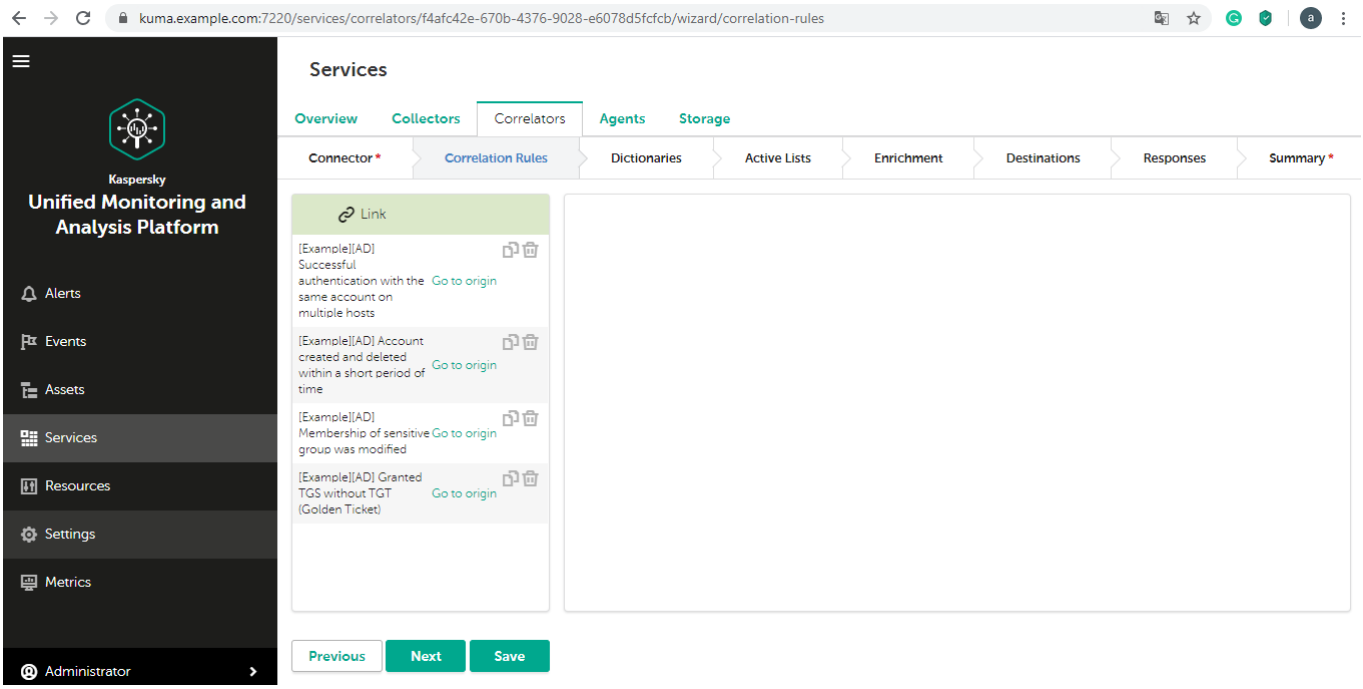
3. Откройте закладку **Correlation Rules** и добавьте правила корреляции:

   a. Нажмите на кнопку **Link** и в раскрывающемся списке **Choose resources** выберите правило корреляции, которое требуется добавить в Коррелятор.

   b. Нажмите на кнопку **Apply**.

      Правило корреляции будет добавлено в Коррелятор и отобразится на закладке **Correlation Rules**.

   Повторите этот шаг для каждого правила корреляции, которое требуется добавить в Коррелятор.



4. Если вы хотите добавить активные списки в Коррелятор, откройте закладку **Active Lists**:

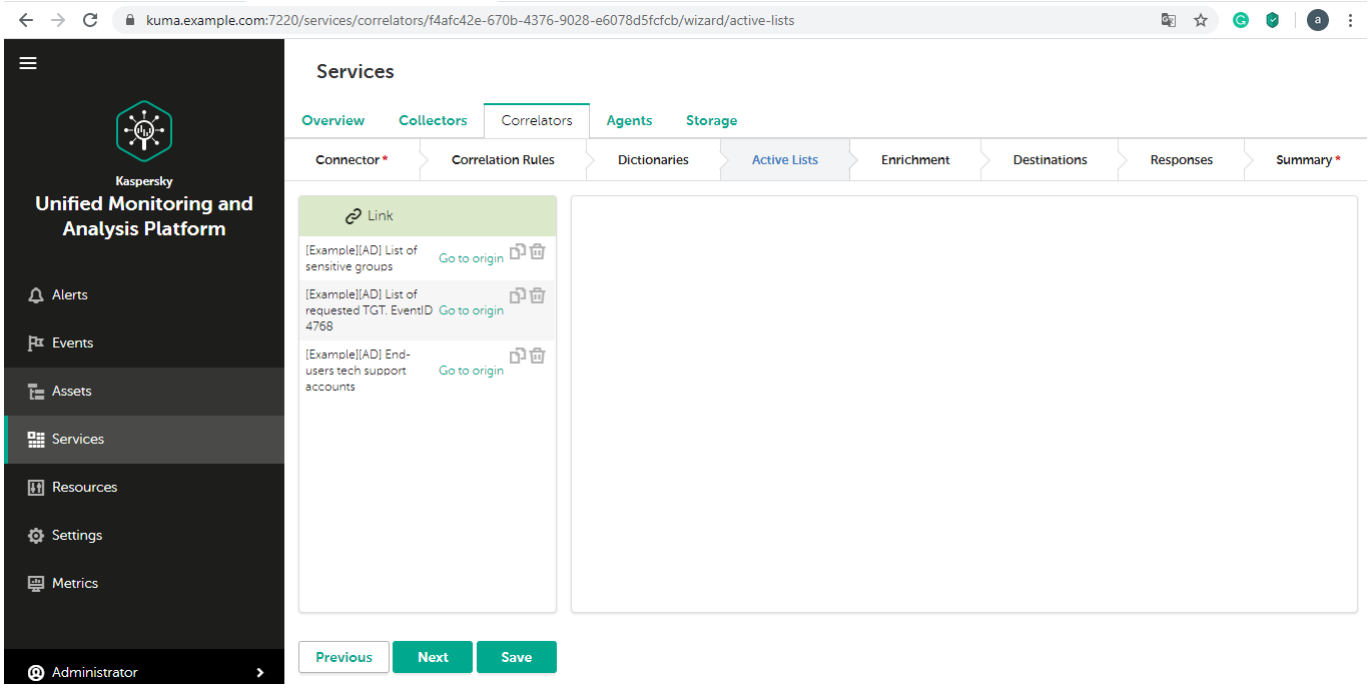
   > Если правила корреляции, которые вы добавили в Коррелятор, используют активные списки, убедитесь, что они также добавлены в Коррелятор.

   a. Нажмите на кнопку **Link** и в раскрывающемся списке **Choose resources** выберите активный список, который требуется добавить в Коррелятор.

   b. Нажмите на кнопку **Apply**.

      Активный список будет добавлен в Коррелятор и отобразится на закладке **Active Lists**.

Повторите этот шаг для каждого активного списка, который требуется добавить в Коррелятор.



5. Откройте закладку **Summary**.
6. Нажмите на кнопку **Сохранить**.

> Если после нажатия на кнопку **Save** появится сообщение о том, что требуется указать название, убедитесь, что поле **Name** не пусто на обеих закладках: **Connector** и **Summary**.

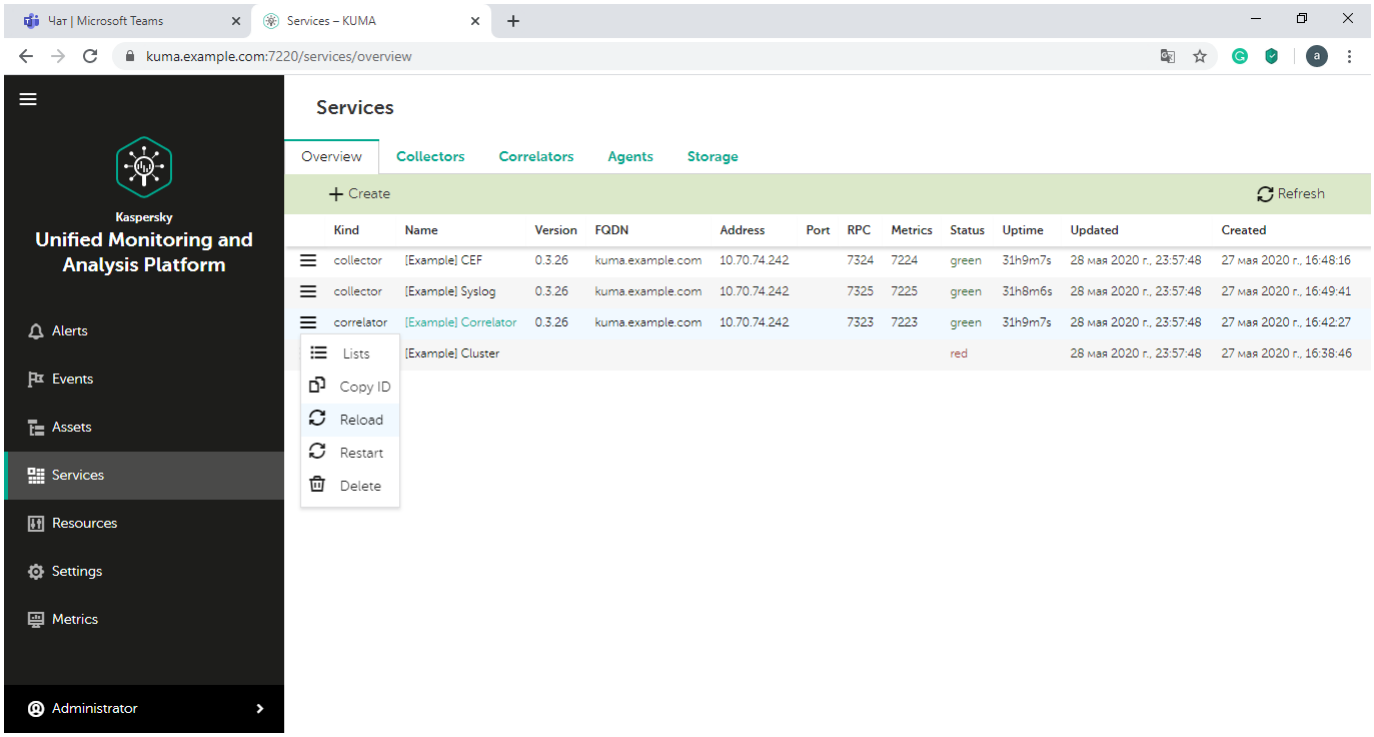
В конфигурацию Коррелятора будут добавлены новые ресурсы.

Необходимо перезагрузить микросервис Коррелятор, чтобы он начал использовать новую конфигурацию.

► *Чтобы перезагрузить микросервис Коррелятор, выполните следующие действия:*

1. Откройте веб-консоль KUMA и выберите вкладку **Overview** в разделе **Services**.
2. Щелкните мышью по значку ☰ рядом с микросервисом Коррелятор, который требуется перезагрузить, и выберите **Reload**.

Микросервис Коррелятор перезагрузится и будет обрабатывать события с использованием обновленной конфигурации.

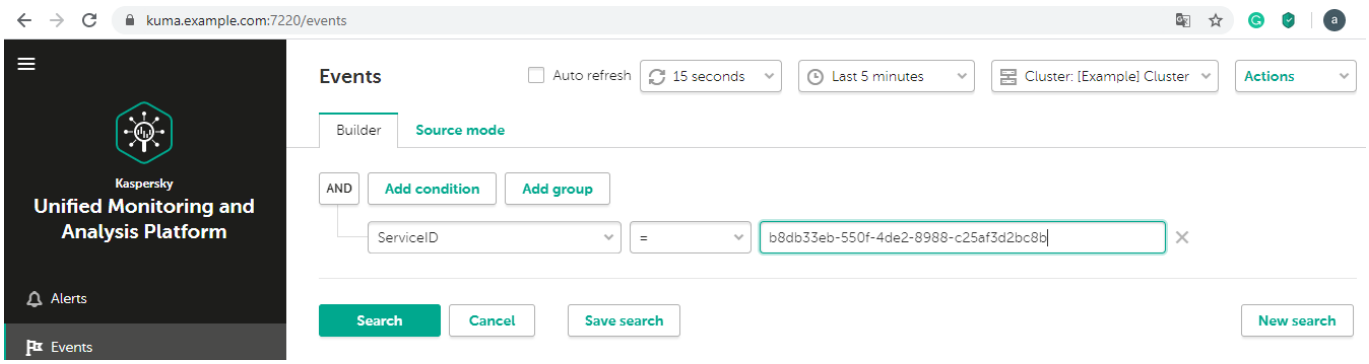


Проверка правильности работы правила корреляции

Например, можно проверить, правильно ли выполняется анализ событий правилами корреляции, выполнив поиск связанных правил корреляции в Хранилище KUMA с помощью раздела **Events** веб-консоли KUMA. Для поиска событий корреляции определенного Коррелятора требуется его параметр **ServiceID**.

Чтобы выполнить поиск событий корреляции из Коррелятора, выполните следующие действия:

1. Откройте веб-консоль KUMA и выберите раздел **Events**.
2. Щелкните мышью в поле **Search**, перейдите на закладку **Builder** и настройте фильтр поиска событий:
   - В раскрывающемся списке слева выберите значение **ServiceID**.
   - В раскрывающемся списке посередине выберите оператор **=**.
   - В раскрывающемся списке справа введите значение ServiceID для Коррелятора, правила корреляции которого требуется найти.



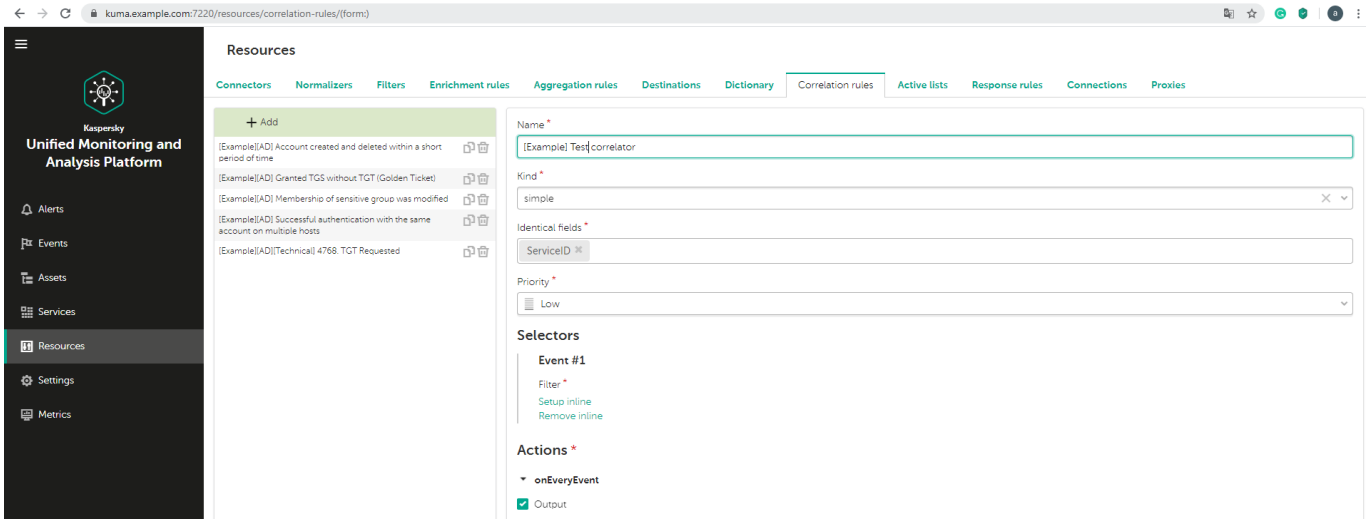
3. Нажмите на кнопку **Search**.

На закладке событий будут отображаться отфильтрованные события.

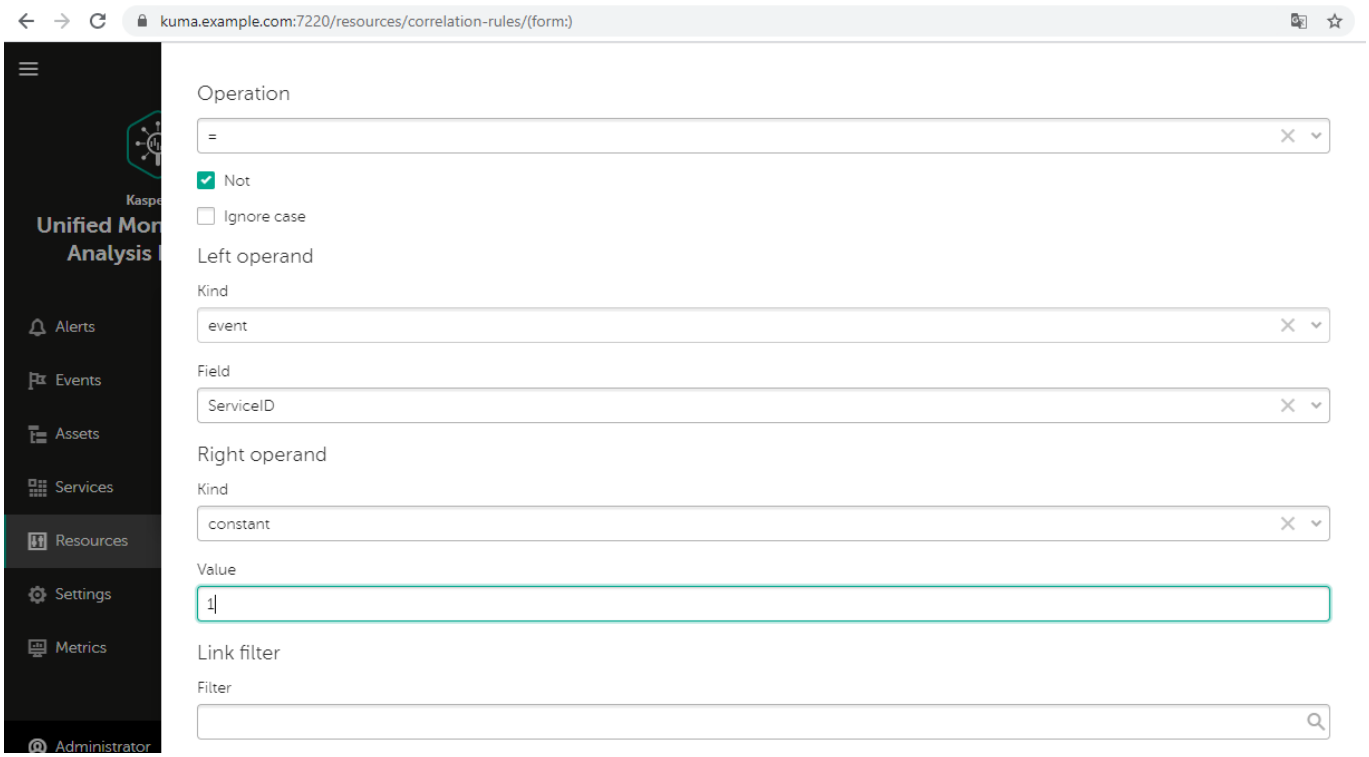
Если в Коррелятор поступают события, удовлетворяющие условиям фильтра правил корреляции, на закладке событий будут отображаться события с параметрами `DeviceVendor=Kaspersky` и `DeviceProduct=KUMA`. Название сработавшего правила корреляции будет отображаться как название этих событий корреляции.

Если события корреляции не найдены

Можно создать более простую версию правила корреляции, чтобы найти возможные ошибки. Используйте правило корреляции типа **simple** и одно действие **Output**.



Рекомендуется создать фильтр для поиска событий, которые KUMA получает регулярно. Если KUMA находится в начале процесса развертывания и количество полученных событий очень мало (несколько событий в секунду), вы можете использовать параметры фильтра, приведенные ниже, чтобы правило корреляции обрабатывало каждое событие, передаваемое в Коррелятор.



При обновлении, добавлении или удалении правила корреляции, микросервис Коррелятор должен быть перезагружен.

Когда вы закончите тестирование правил корреляции, необходимо удалить все тестовые и временные правила корреляции из KUMA и перезагрузить Коррелятор.

kaspersky

Добавление источника события с использованием стандартного нормализатора

В этом примере показано, как настроить KUMA для получения событий от Kaspersky Anti Targeted Attack (далее KATA). Сервер KATA (источник событий) настроен на отправку событий в формате CEF через порт TCP:5146. В KUMA события должны направляться в Хранилище KUMA и Коррелятор KUMA. В этом разделе описаны действия для выполнения этой задачи.

В примере предполагается, что микросервисы Хранилище и Коррелятор уже установлены и для них настроены точки назначения.

В этом разделе

Подготовка ресурсов к инициализации Коллектора KUMA для KATA

В этом разделе описано создание ресурсов, необходимых Коллектору KUMA для KATA.

Для микросервиса Коллектор требуются только ресурсы Соединение и Нормализатор.

В этом разделе

Создание Соединения для KATA

В веб-консоли KUMA нам нужно создать ресурс Соединение, который позволит ресурсу Коннектор использовать порт TCP:5146:

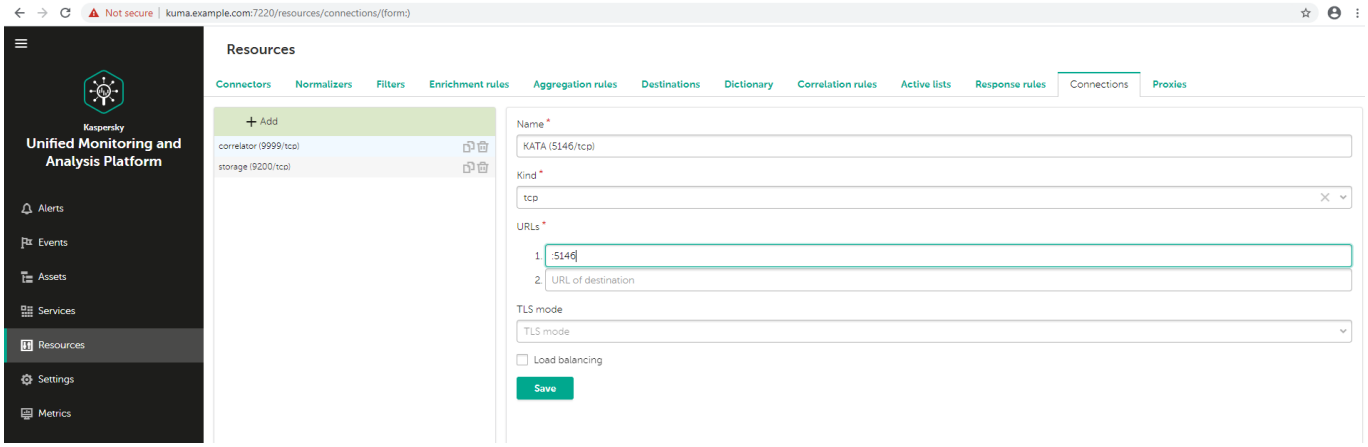
► *Для создания ресурса Соединение сделайте следующее:*

1. Откройте веб-консоль KUMA и выберите вкладку **Connections** в разделе **Resources**.
2. Нажмите на кнопку **Add** и задайте параметры, как описано ниже.
   - В поле **Name** введите имя ресурса Соединение для его идентификации. Введите `KATA (5146/tcp)`.
   - В раскрывающемся списке **Kind** выберите **tcp**, чтобы получать события по протоколу TCP.

- В поле **URLs** введите адрес, по которому Коннектор должен получать события. Значение может иметь формат <FQDN>:<порт>, <IP-адрес>:<порт> или :<порт>. Введите `:5146`.

3. Нажмите на кнопку **Save**.

На вкладке **Connections** появится новое соединение `KATA (5146/tcp)`.



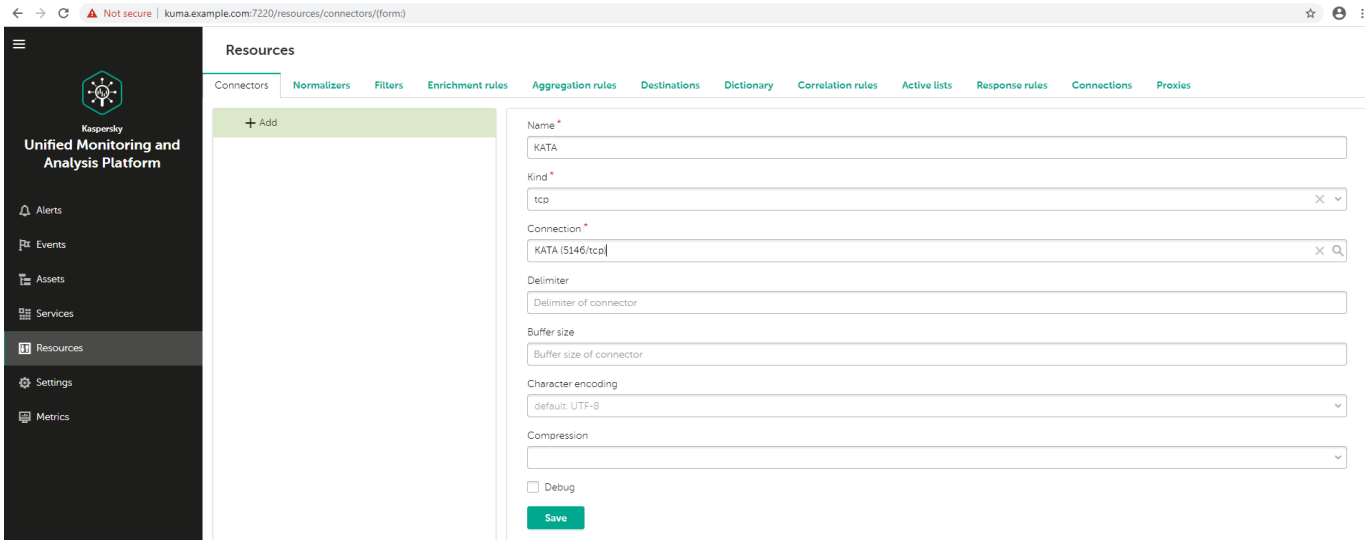
Создание Коннектора для KATA

В веб-консоли KUMA нам нужно создать ресурс Коннектор.

► *Для создания ресурса Коннектор сделайте следующее:*

1. Откройте веб-консоль KUMA и выберите вкладку **Connectors** в разделе **Resources**.
2. Нажмите на кнопку **Add** и задайте параметры, как описано ниже.
   - В поле **Name** введите имя ресурса Коннектор для его идентификации. Введите `KATA`.
   - В раскрывающемся списке **Kind** выберите **tcp**, поскольку нам нужно получать события по протоколу TCP.
   - В раскрывающемся списке **Connection** выберите ресурс Соединение, созданный на предыдущем этапе. Выберите `KATA (5146/tcp)`.
3. Нажмите на кнопку **Save**.

На вкладке **Connectors** появится новый коннектор `KATA`.



Создание Нормализатора для KATA

При отправке событий KATA используется формат CEF. Чтобы система KUMA могла найти корреляции в этих событиях, события KATA необходимо преобразовать в модель данных событий KUMA (или нормализовать) с помощью стандартного нормализатора CEF.

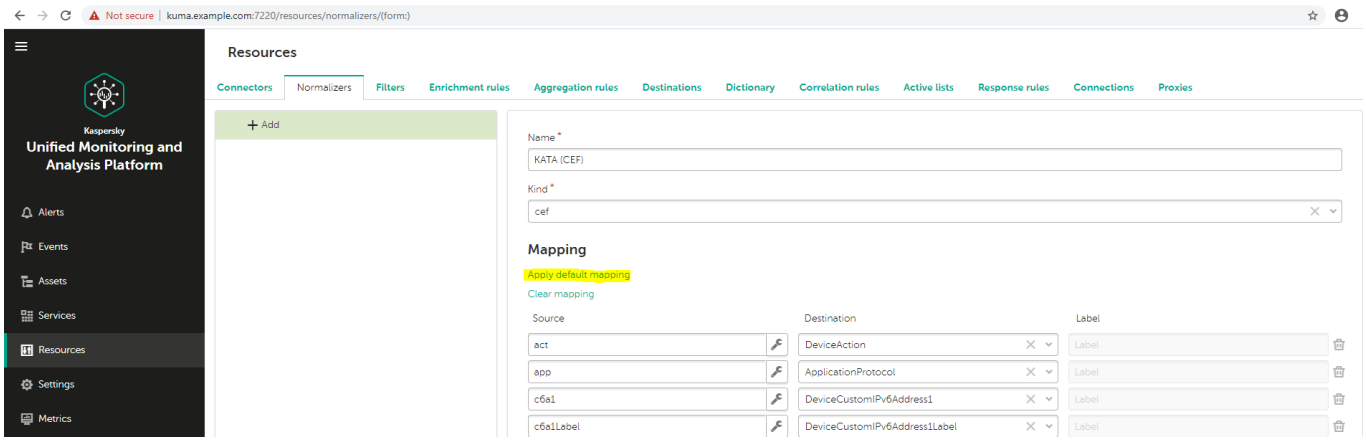
► *Для создания ресурса Нормализатор сделайте следующее:*

1. Откройте веб-консоль KUMA и выберите вкладку **Normalizer** в разделе **Resources**.
2. Нажмите на кнопку **Add** и задайте параметры, как описано ниже.
   - В поле **Name** введите имя ресурса Нормализатор для его идентификации. Введите `KATA (CEF)`.
   - В списке **Kind** выберите тип нормализатора. Выберите **CEF**.
   - Настройте сопоставление полей полученного события с полями события KUMA. В этом примере мы получаем события в формате CEF со стандартными полями. Щелкните по ссылке **Apply default mapping**.

     Правила сопоставления автоматически добавятся в таблицу сопоставлений.

   Остальные параметры ресурса Нормализатор необязательны.
3. Нажмите на кнопку **Save**.

На вкладке **Normalizer** появится новый нормализатор `KATA (CEF)`.



Инициализация Коллектора для KATA

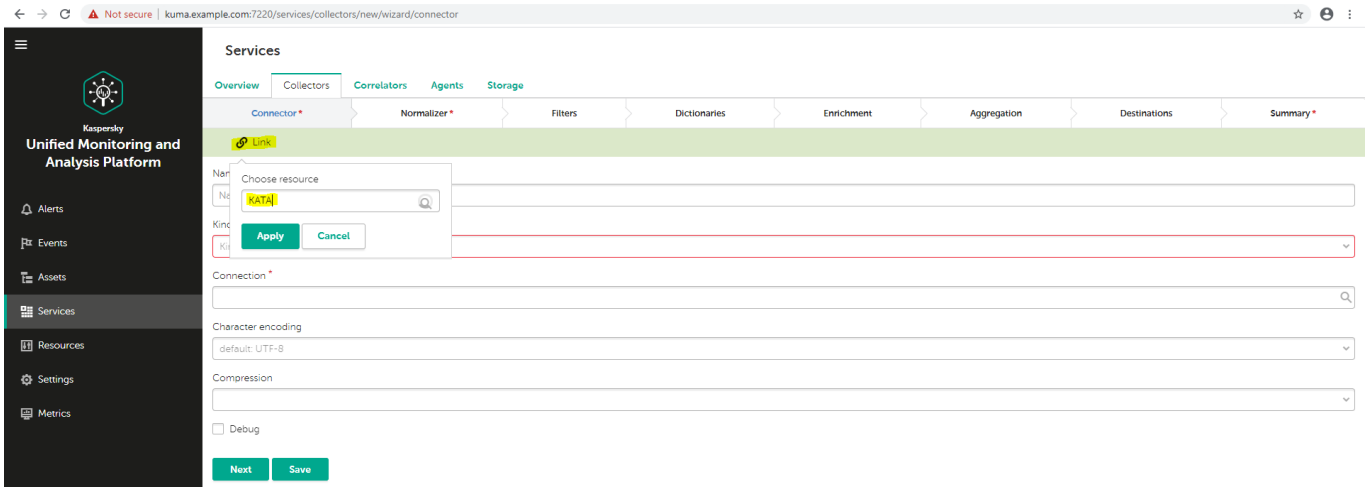
На этом этапе все необходимые ресурсы уже готовы, и их можно использовать для создания (или инициализации) Коллектора.

► *Для инициализации Коллектора сделайте следующее:*

1. Откройте веб-консоль KUMA и выберите вкладку **Collector** в разделе **Services**.
2. Нажмите на кнопку **Add**.

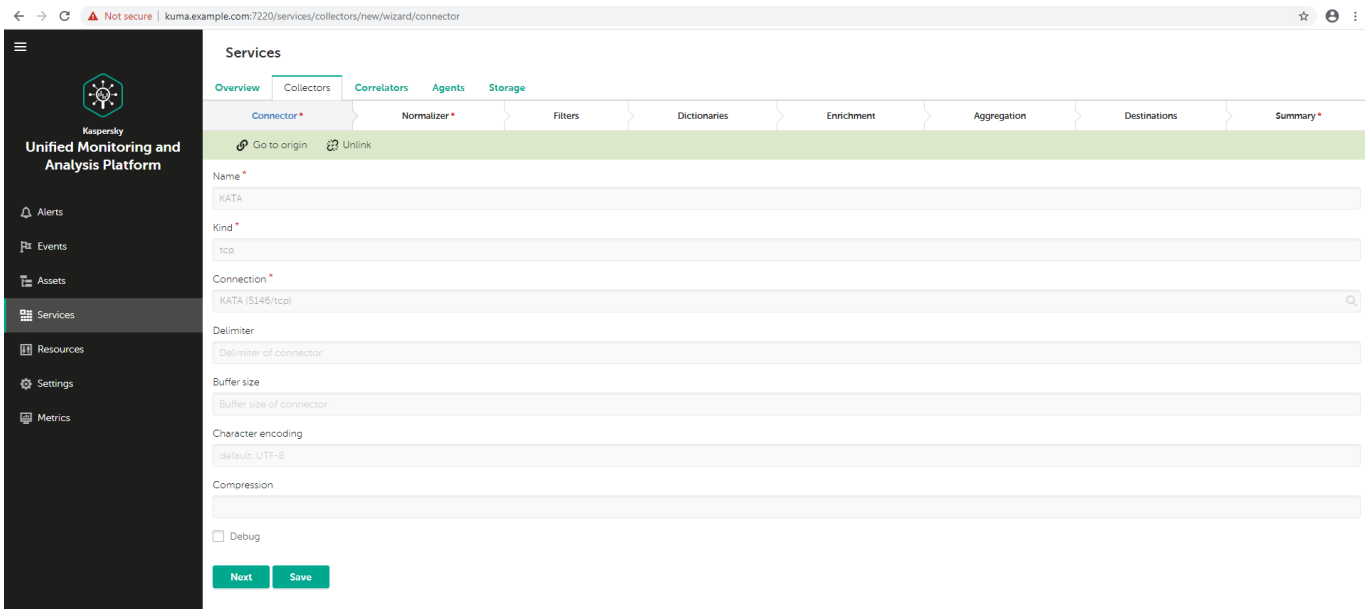
   Откроется окно для настройки микросервиса Коллектор. В верхней части окна отображаются вкладки для настройки Коллектора. Чтобы выбрать нужную вкладку, щелкните по ней или используйте для перехода между вкладками кнопки **Next** и **Previous**.

   Обязательными являются только вкладки **Connector**, **Normalizer** и **Summary**.
3. Откройте вкладку **Connector**.
4. Нажмите на кнопку **Link** и в раскрывающемся списке **Choose resource** выберите ресурс Коннектор, созданный на предыдущем этапе. Выберите `KATA`.



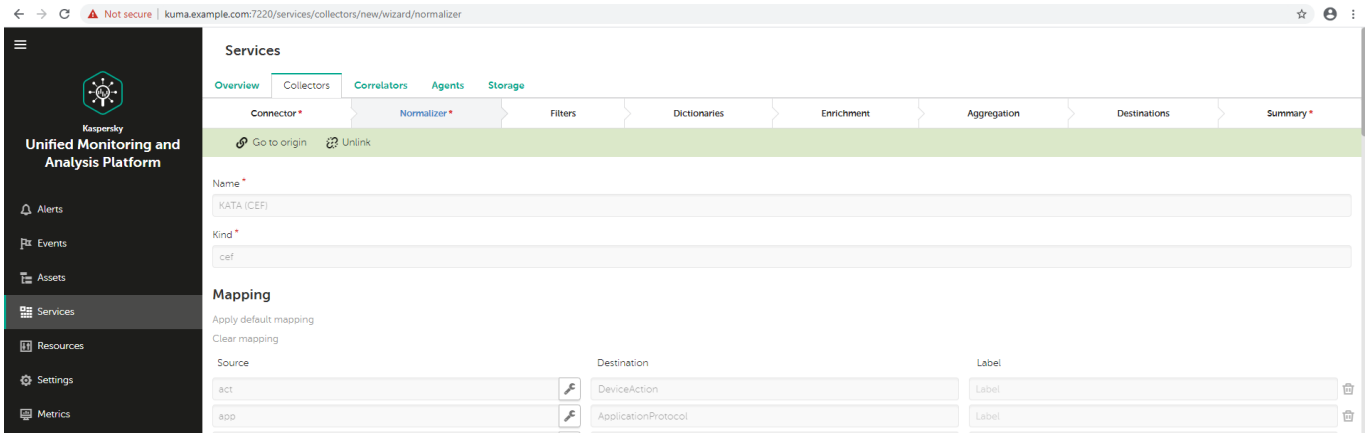
5. Нажмите на кнопку **Apply**.

На вкладке появится конфигурация выбранного ресурса.



6. Откройте вкладку **Normalizer**.
7. Нажмите на кнопку **Link** и в раскрывающемся списке **Choose resource** выберите ресурс Нормализатор, созданный на предыдущем этапе. Выберите `KATA CEF`.
8. Нажмите на кнопку **Apply**.

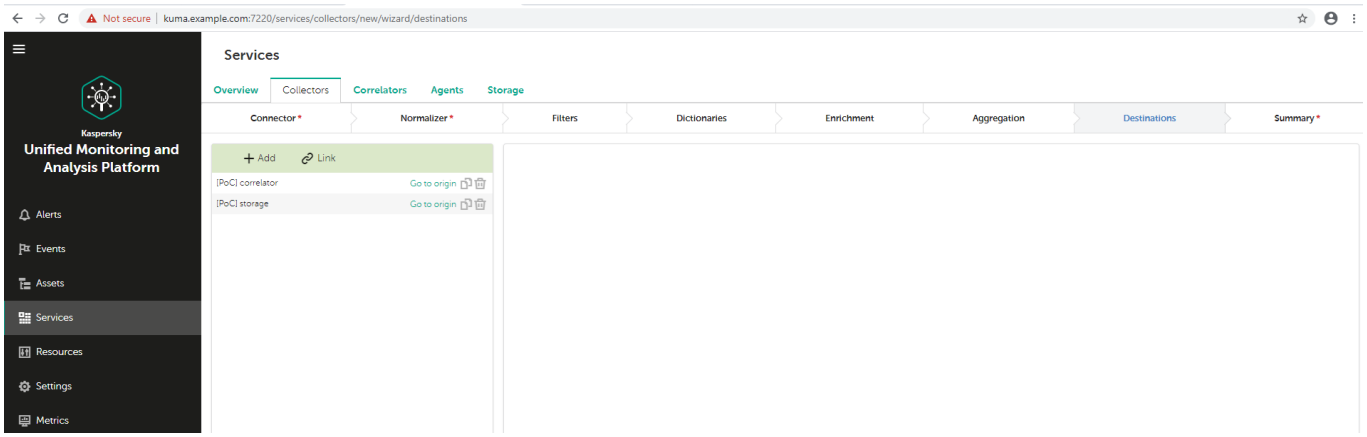
   На вкладке появится конфигурация выбранного ресурса.



9. Откройте вкладку **Destinations**.
10. Нажмите на кнопку **Link** и в раскрывающемся списке **Choose resource** выберите ресурс Точка назначения, созданный ранее.
11. Нажмите на кнопку **Apply**.

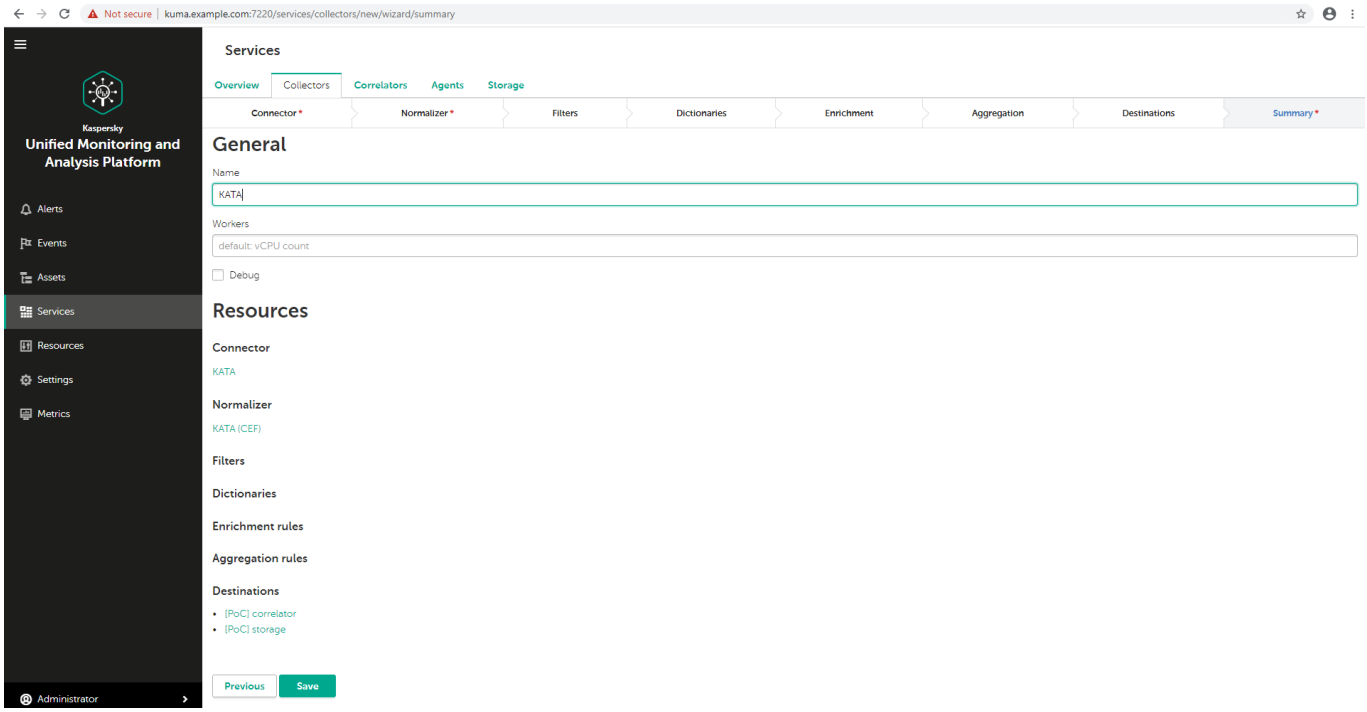
    На вкладке появится имя выбранного ресурса.

12. Повторите действия 10–11 для каждой точки назначения, которую нужно привязать к Коллектору.



13. Откройте вкладку **Summary**.

14. В поле **Name** введите имя Коллектора. Введите `KATA`.



15. Нажмите на кнопку **Save**.

> Если после нажатия на кнопку **Save** появляется сообщение о том, что требуется имя, убедитесь в том, что поле **Name** не пустое на всех обязательных вкладках: **Connector**, **Normalizer** и **Summary**.

Коллектор инициализируется и появится на вкладке **Collector**.

kaspersky

Создание Коллектора для KATA

После инициализации коллектора можно создать микросервис Коллектор.

► *Для создания микросервиса Коллектор сделайте следующее:*

1. Откройте веб-консоль KUMA и выберите вкладку **Overview** в разделе **Services**.
2. Нажмите на кнопку **Create** и в раскрывающемся списке выберите ранее созданный Коллектор. Выберите `collector/KATA`.
3. Нажмите на кнопку **Create**.

В списке микросервисов появится новый Коллектор с именем `KATA`.

Установка Коллектора для KATA на сервере

Чтобы Коллектор мог получать и обрабатывать события, необходимо установить соответствующий микросервис на сервере Коллектора KUMA. Установку Коллектора на сервере выполняют администраторы сети.

В ходе установки этого микросервиса требуются следующие параметры: **RPC** и **Metrics**. Эти параметры находятся на вкладке **Overview** в разделе **Services** веб-консоли KUMA.

► *Для установки Коллектора на сервере KUMA сделайте следующее:*

1. Откройте SSH-консоль сервера Коллектора KUMA с правами администратора сети.
2. Выполните следующие команды:

   ```
   rpm -Uhv kuma-0.3.26-<номер сборки>.el8.x86_64.rpm
   ```

   ```
   /opt/kuma/kuma collector --core <адрес сервера, с которого микросервис Коллектора получает параметры конфигурации> --id <идентификатор микросервиса, скопированный из веб-консоли KUMA> --metrics <порт, используемый для метрик установленных микросервисов> --rpc <порт, используемый для RPC установленных микросервисов> --install
   ```

   При развертывании нескольких микросервисов KUMA на одном хосте в процессе установки необходимо указать уникальные порты для каждого компонента с помощью параметров `--metrics <порт> --rpc <порт>`. По умолчанию используются значения `--metrics 7221 -rpc 7331`.

3. Укажите, принимаете ли вы условия Лицензионного соглашения.

   Если вы не принимаете условия Лицензионного соглашения, установка программы не выполняется.

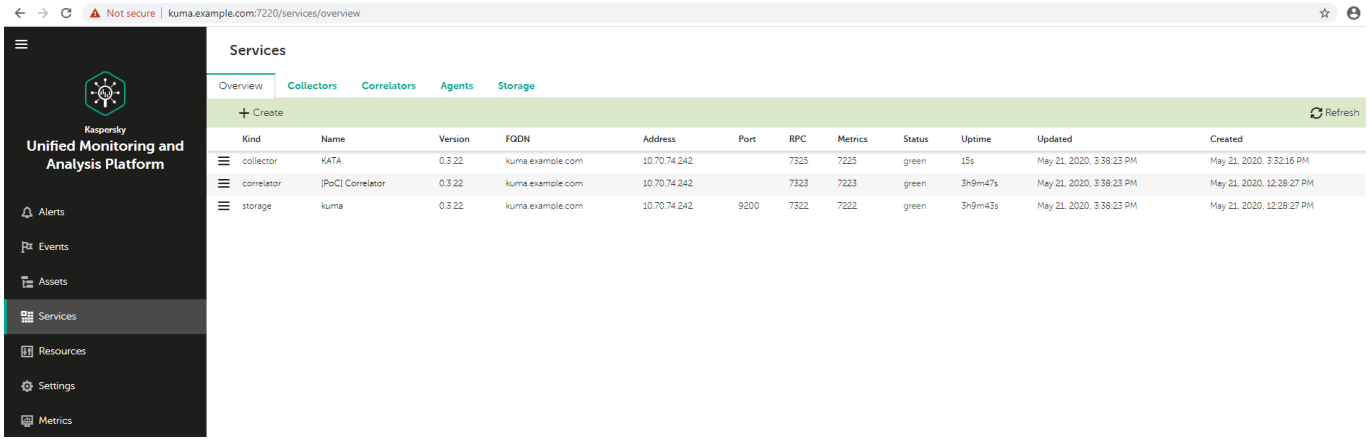
Микросервис Коллектора устанавливается. Он готов получать и передавать на обработку сообщения из источника события.

Проверка состояния Коллектора для KATA

После установки Коллектора на соответствующем сервере KUMA убедитесь в том, что этот микросервис работает.

► *Проверить готовность Коллектора к получению событий можно следующим образом:*

1. Откройте веб-консоль KUMA и выберите вкладку **Overview** в разделе **Services**.
2. Убедитесь, что для Коллектора, установленного на сервере `kuma.example.com`, отображается значение `green` в столбце **Status**.



Если все микросервисы установлены на одном сервере, как в данном примере, порты для параметров RPC и Metrics должны быть разными.

kaspersky

Добавление источника события с использованием настраиваемого нормализатора regexp

В этом примере показано, как настроить KUMA для получения файла журнала access.log с сервера Cisco™ WSA и его обработки. На сервере Коллектора файл журнала access.log монтируется в папку /mnt/cisco_wsa. События в KUMA отправляются в Хранилище KUMA и Коррелятор KUMA. В этом разделе описаны действия для выполнения этой задачи.

В примере предполагается, что микросервисы Хранилище и Коррелятор уже установлены и для них настроены точки назначения.

В этом разделе

Подготовка ресурсов к инициализации Коллектора KUMA для Cisco WSA

В этом разделе описано создание ресурсов, которые будут использоваться при инициализации Коллектора KUMA для Cisco WSA.

Для микросервиса Коллектор требуются только ресурсы Соединение и Нормализатор.

В этом разделе

Создание Соединения для Cisco WSA

В веб-консоли KUMA нам нужно создать ресурс Соединение для чтения файла журнала в каталоге /mnt/cisco_wsa/access.log.

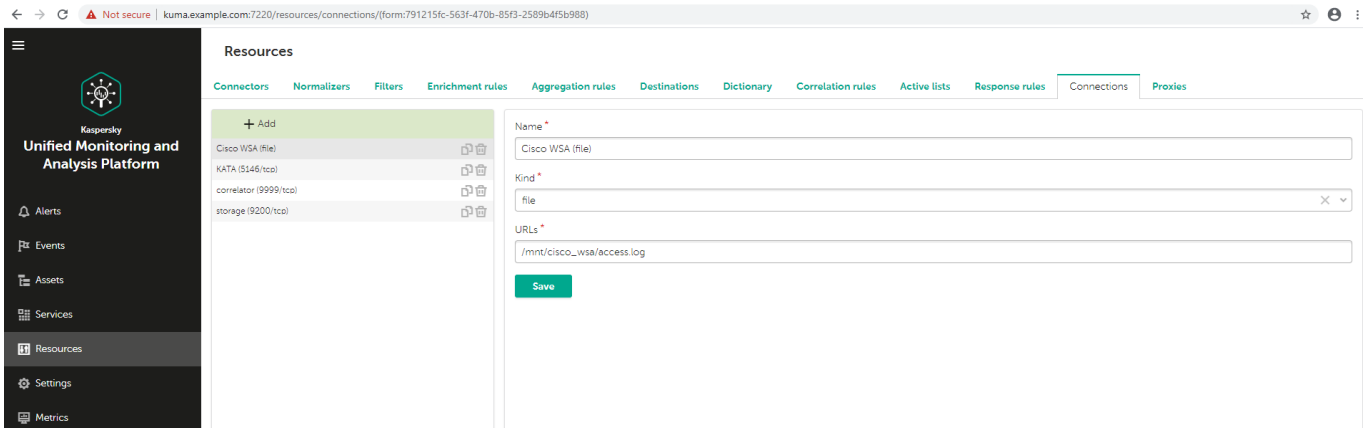
► *Для создания ресурса Соединение сделайте следующее:*

1. Откройте веб-консоль KUMA и выберите вкладку **Connections** в разделе **Resources**.
2. Нажмите на кнопку **Add** и задайте параметры, как описано ниже.
   - В поле **Name** введите имя ресурса Соединение для его идентификации. Введите `Cisco WSA (file)`.
   - В раскрывающемся списке **Kind** выберите **file**, поскольку нам нужно получать события из файла.

- В поле **URLs** введите путь к файлу. Введите `/mnt/cisco_wsa/access.log`.

3. Нажмите на кнопку **Save**.

На вкладке **Connections** появится новое соединение `Cisco WSA (file)`.



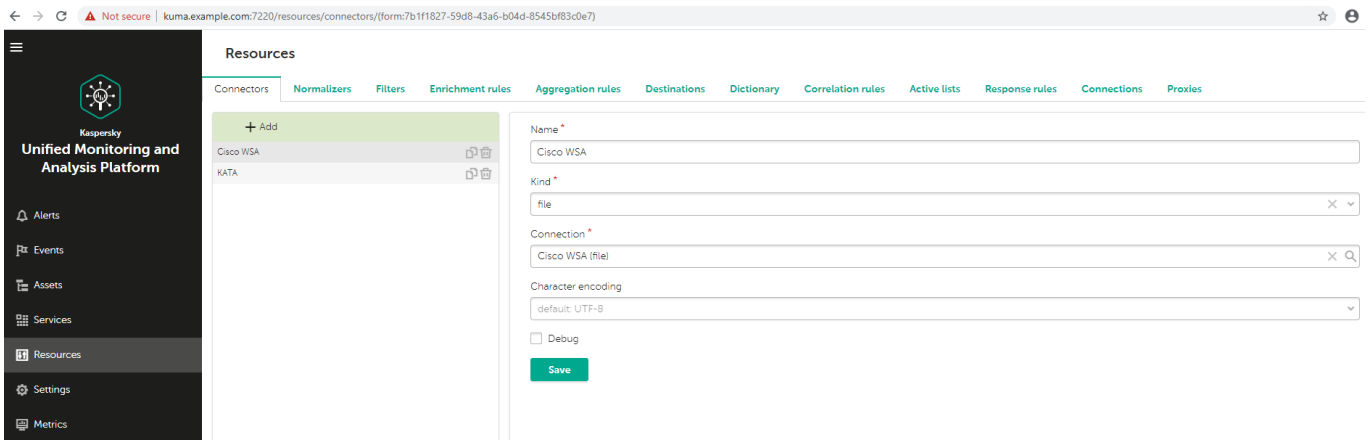
Создание Коннектора для Cisco WSA

В веб-консоли KUMA нам нужно создать ресурс Коннектор.

► *Для создания ресурса Коннектор сделайте следующее:*

1. Откройте веб-консоль KUMA и выберите вкладку **Connectors** в разделе **Resources**.
2. Нажмите на кнопку **Add** и задайте параметры, как описано ниже.
   - В поле **Name** введите имя ресурса Коннектор для его идентификации. Введите `Cisco WSA`.
   - В раскрывающемся списке **Kind** выберите **file**.
   - В раскрывающемся списке **Connection** выберите ресурс Соединение, созданный на предыдущем этапе. Выберите `Cisco WSA (file)`.
3. Нажмите на кнопку **Save**.

На закладке **Connectors** появится новый Коннектор `Cisco WSA`.



kaspersky

Создание Нормализатора для Cisco WSA

Для того чтобы решение KUMA смогло найти корреляции в событиях Cisco WSA, их необходимо нормализовать, используя синтаксический анализатор на основе регулярных выражений.

> В KUMA используются регулярные выражения типа RE2.

► *Для создания ресурса Нормализатор сделайте следующее:*

1. Откройте веб-консоль KUMA и выберите вкладку **Normalizer** в разделе **Resources**.
2. Нажмите на кнопку **Add** и задайте параметры, как описано ниже.
   - В поле **Name** введите имя ресурса Нормализатор для его идентификации. Введите `Cisco WSA access log`.
   - В списке **Kind** выберите тип нормализатора. Выберите **regexp**.
   - В полях **Expressions** введите одно или несколько регулярных выражений. Все переменные в выражении должны быть именами, чтобы их можно было использовать для установления соответствия.

     Пример содержимого файла WSA – access.log:

     ```
     1579866468.772 104 8.8.8.8 TCP_MISS/200 3642 CONNECT
     tunnel://ipmcloud.example.com:443/ "DOMAIN\username"
     DIRECT/ipmcloud.example.com application/octet-stream ALLOW_WBRS_12-
     DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup-NONE
     <"IW_csec",9.2,1,"-",-,-,-,1,"-",-,-,-,"-",1,-,"-","-",-,-
     ,"IW_csec",-,"-","Computer Security","-","Unknown","Unknown","-","-
     ",280.15,0,-,"-","-",1,"-",-,-,"-","-",-,1,"-",-> -
     ```

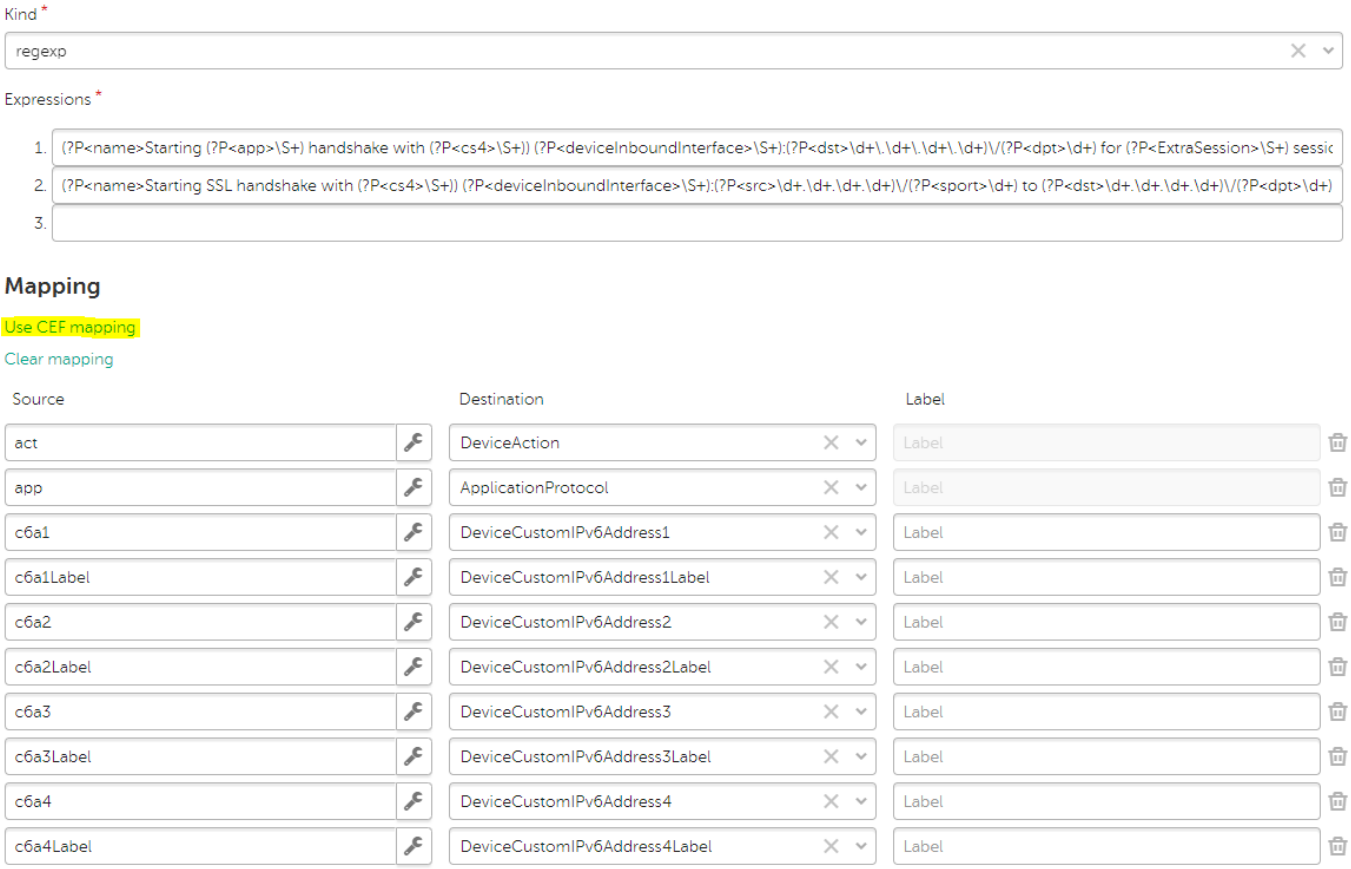
     Для синтаксического анализа строк, аналогичных приведенной выше, можно использовать следующее регулярное выражение:

     ```
     ^(?P<timestamp>\S+)\s+(?P<xElapsedTime>\d+)\s+(?P<cIp>\d{1,3}\.\d{1,3
     }\.\d{1,3}\.\d{1,3})\s+(?P<srcResultCode>[^\/].*?)\/(?P<scResultCodeD
     enial>\d+)\s+(?P<scBytes>\d+)\s+(?P<xReqFirstLine>[A-
     Z]+\s\S+)\s+(?P<csUsername>\S+)\s+(?P<sHierarchy>[^\/].*?)\/(?P<sHost
     name>\S+)\s+(?P<csMimeType>\S+)\s+(?P<xAcltag>\S+)\s+(?P<xResultCode>
     .*?\>)\s+(?P<xSuspectUserAgent>\S+)
     ```

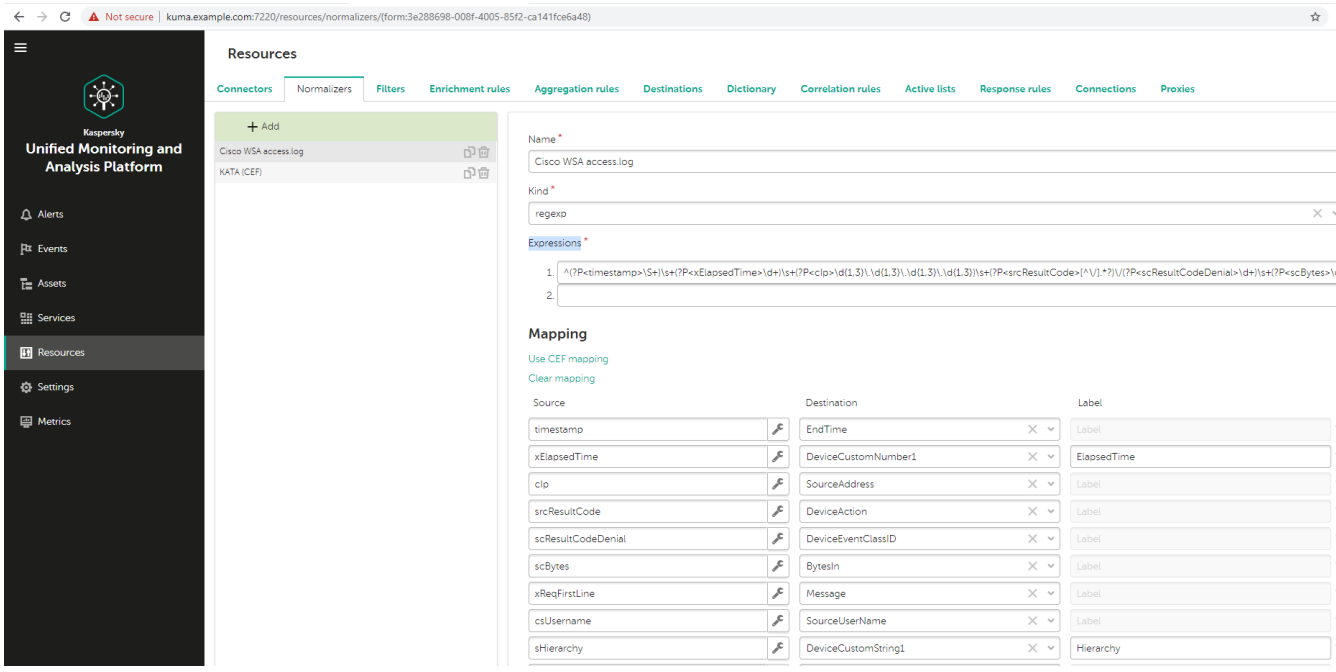
     Переменные названы в соответствии с форматом файла журнала W3C. Разобранные посредством анализа строки можно использовать для установления соответствия.

     Альтернативное именование переменных

Допускается альтернативный подход к именованию переменных. Например, можно использовать имена CEF. Это позволит автоматически применять соответствие CEF с помощью команды **Use CEF mapping** и избежать добавления правил соответствия вручную.



- В группе параметров **Mapping** добавьте правила установления соответствия, как показано на рисунке ниже:



- В группе параметров Enrichment можно добавить правила обогащения, например, для обновления значений полей `DeviceVendor`, `DeviceProduct` и `DeviceHostName`:

  a. Перейдите по ссылке **Add enrichment**.

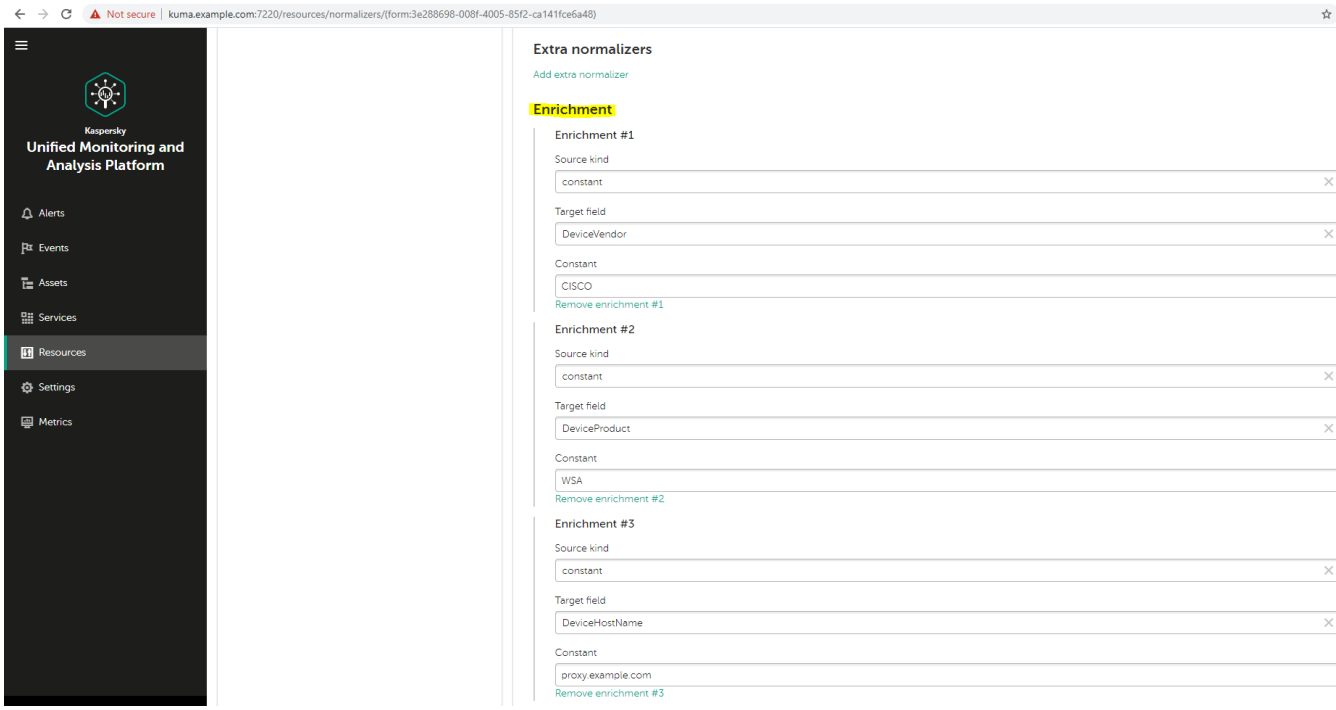
  Откроется группа параметров Enrichment rule:

  b. В раскрывающемся списке **Source kind** выберите **constant**.

  c. В раскрывающемся списке **Target field** выберите **DeviceVendor**.

  d. В поле **Constant** введите `CISCO`.

  Повторите эти шаги для каждого правила обогащения. См. рисунок ниже для справки.



1. Нажмите на кнопку **Save**.

На закладке **Normalizer** появится новый Нормализатор **Cisco WSA access log**.

Инициализация Коллектора для Cisco WSA

На этом этапе все необходимые ресурсы уже готовы, и их можно использовать для создания (или инициализации) Коллектора.

► *Для инициализации Коллектора сделайте следующее:*

1. Откройте веб-консоль KUMA и выберите вкладку **Collector** в разделе **Services**.
2. Нажмите на кнопку **Add**.

   Откроется окно для настройки микросервиса Коллектор. В верхней части окна отображаются вкладки для настройки Коллектора. Чтобы выбрать нужную вкладку, щелкните по ней или используйте для перехода между вкладками кнопки **Next** и **Previous**.

   Обязательными являются только вкладки **Connector**, **Normalizer** и **Summary**.
3. Откройте вкладку **Connector**.

4. Нажмите на кнопку **Link** и в раскрывающемся списке **Choose resource** выберите ресурс Коннектор, созданный на предыдущем этапе. Выберите `Cisco WSA (file)`.
5. Нажмите на кнопку **Apply**.

   На вкладке появится конфигурация выбранного ресурса.
6. Откройте вкладку **Normalizer**.
7. Нажмите на кнопку **Link** и в раскрывающемся списке **Choose resource** выберите ресурс Нормализатор, созданный на предыдущем этапе. Выберите `Cisco WSA log file`.
8. Нажмите на кнопку **Apply**.

   На вкладке появится конфигурация выбранного ресурса.
9. Откройте вкладку **Destinations**.
10. Нажмите на кнопку **Link** и в раскрывающемся списке **Choose resource** выберите ресурс Точка назначения, созданный ранее.
11. Нажмите на кнопку **Apply**.

    На вкладке появится имя выбранного ресурса.
12. Повторите действия 10–11 для каждой точки назначения, которую нужно привязать к Коллектору.
13. Откройте вкладку **Summary**.
14. В поле **Name** введите имя Коллектора. Введите `Cisco WSA`.
15. Нажмите на кнопку **Save**.

    Если после нажатия на кнопку **Save** появляется сообщение о том, что требуется имя, убедитесь в том, что поле **Name** не пустое на всех обязательных вкладках: **Connector**, **Normalizer** и **Summary**.

Коллектор инициализируется и появится на вкладке **Collector**.

Создание Коллектора для Cisco WSA

После инициализации коллектора можно создать микросервис Коллектор.

► *Для создания микросервиса Коллектор сделайте следующее:*

1. Откройте веб-консоль KUMA и выберите вкладку **Overview** в разделе **Services**.
2. Нажмите на кнопку **Create** и в раскрывающемся списке выберите ранее созданный Коллектор. Выберите `collector/Cisco WSA`.
3. Нажмите на кнопку **Create**.

В списке микросервисов появится новый микросервис Коллектор – `Cisco WSA` .

kaspersky

Установка Коллектора для Cisco WSA на сервере

Чтобы Коллектор мог получать и обрабатывать события, необходимо установить соответствующий микросервис на сервере Коллектора KUMA. Установку Коллектора на сервере выполняют администраторы сети.

В ходе установки этого микросервиса требуются следующие параметры: **RPC** и **Metrics**. Эти параметры находятся на вкладке **Overview** в разделе **Services** веб-консоли KUMA.

► *Чтобы установить Коллектор на сервере Коллекторов KUMA, выполните следующие действия:*

1. Откройте SSH-консоль сервера Коллектора KUMA с правами администратора сети.
2. Выполните следующие команды:

   ```
   rpm -Uhv kuma-0.3.26-<номер сборки>.el8.x86_64.rpm
   ```

   ```
   /opt/kuma/kuma collector --core <адрес сервера, с которого микросервис Коллектора получает параметры конфигурации> --id <идентификатор микросервиса, скопированный из веб-консоли KUMA> --metrics <порт, используемый для метрик установленных микросервисов> --rpc <порт, используемый для RPC установленных микросервисов> --install
   ```

   При развертывании нескольких микросервисов KUMA на одном хосте в процессе установки необходимо указать уникальные порты для каждого компонента с помощью параметров `--metrics <порт> --rpc <порт>`. По умолчанию используются значения `--metrics 7221 -rpc 7331`.

3. Укажите, принимаете ли вы условия Лицензионного соглашения.

   Если вы не принимаете условия Лицензионного соглашения, установка программы не выполняется.

Микросервис Коллектора устанавливается. Он готов получать и передавать на обработку сообщения из источника события.

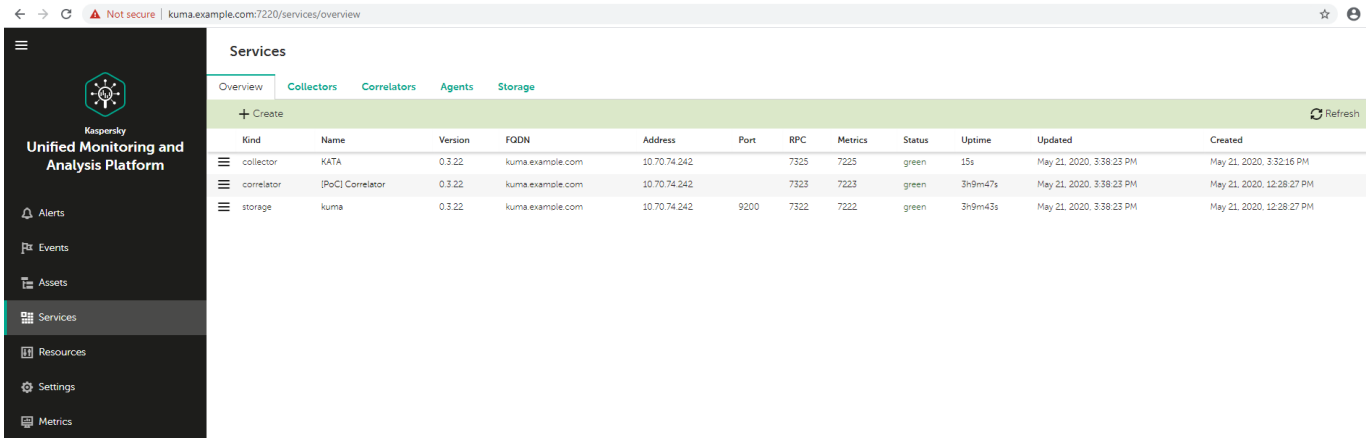
Проверка состояния Коллектора Cisco WSA

После установки Коллектора на соответствующем сервере KUMA убедитесь в том, что этот микросервис работает.

► *Проверить готовность Коллектора к получению событий можно следующим образом:*

1. Откройте веб-консоль KUMA и выберите вкладку **Overview** в разделе **Services**.

2. Убедитесь, что для Коллектора, установленного на сервере `kuma.example.com`, отображается значение `green` в столбце **Status**.



Если все микросервисы установлены на одном сервере, как в данном примере, порты для параметров RPC и Metrics должны быть разными.

При создании настраиваемого ресурса Нормализатор для микросервиса Коллектор также рекомендуется проверить, успешно ли выполняется процесс нормализации.

► *Чтобы проверить наличие ошибок нормализации с помощью раздела Events веб-консоли KUMA, выполните следующие действия:*

1. Убедитесь, что запущен микросервис Коллектор.
2. Убедитесь, что источник событий передает события в KUMA.
3. Убедитесь, что в разделе **Resources** веб-консоли KUMA в раскрывающемся списке **Finalization** ресурса **Normalizer** выбрано значение **error**.
4. В разделе **Events** в KUMA выполните поиск событий со следующими параметрами:
   - `ServiceID = <идентификатор микросервиса Коллектор, использующего ресурс Нормализатор, 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, выполните следующие действия:*

1. Убедитесь, что запущен микросервис Коллектор.
2. Убедитесь, что источник событий передает события в KUMA.
3. Откройте панель мониторинга Grafana и перейдите по ссылке KUMA Collectors.
4. Проверьте, отображаются ли ошибки в разделе Errors виджета Normalization.

Если в результате обнаружены ошибки нормализации, их необходимо исследовать.

kaspersky

Команды для запуска и установки компонентов вручную

В этом разделе описаны параметры исполняемого файла 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.

Таблица 1. Параметры команд

Параметр	Описание
tool certificates	Запуск инструмента для создания сертификатов, используемых для аутентификации компонентов KUMA и шифрования трафика между ними.
collector	Запуск или установка Коллектора.
core	Запуск или установка Ядра.
correlator	Запуск или установка Коррелятора.
help	Получение информации о доступных 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 файле или команде. 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 <параметр version установленного микросервиса> --metrics <параметр metrics установленного микросервиса> --rpc <параметр RPC установленного микросервиса>` – запуск установки микросервиса Коллектор.

Информация о стороннем коде

Информация о стороннем коде содержится в файле LEGAL_NOTICES, расположенном в каталоге /opt/kuma/LEGAL_NOTICES.

kaspersky

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Cisco – зарегистрированный в Соединенных Штатах Америки и в других странах товарный знак Cisco Systems, Inc. и / или ее аффилированных компаний.

Google Chrome – товарный знак Google, Inc.

Microsoft и Windows – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Mozilla и Firefox – товарные знаки Mozilla Foundation.

CentOS – товарный знак компании Red Hat, Inc.