

Создание коллектора KUMA

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Создание коллектора KUMA

Для создания коллектора в веб-интерфейсе KUMA:

- Перейдите в раздел **Ресурсы** и нажмите на кнопку **Подключить источник**.
- В появившемся окне мастера настройки **Создание коллектора** на первом шаге **Подключение источников** укажите **Имя коллектора** и выберите **Тенант**, к которому будет принадлежать создаваемый коллектор.
- Опционально заполните **Описание**.

Создание коллектора



Подключение источников 1

- Транспорт
- Парсинг событий
- Фильтрация событий
- Агрегация событий
- Обогащение событий
- Маршрутизация
- Проверка параметров

Подключение источников

Коллекторы используются для получения данных из источников событий, а также преобразования их в нормализованные события, понятные KUMA. С помощью коллектора можно также отсеивать ненужные события, объединять похожие события и обогащать события информацией из сторонних источников. Чтобы создать коллектор, следуйте шагам мастера. Подробнее см. [в онлайн-справке](#).

Основные параметры Дополнительные параметры

Название коллектора*	KATA TCP/5155 2
Тенант*	Main 3
Обработчики	0
Время загрузки геоданных ⓘ	
Теги	
Описание	Коллектор для приема и обработки событий KATA. 4

- На втором шаге мастера **Транспорт** укажите параметры коннектора для взаимодействия с подключаемым источником:
 - В раскрывающемся списке **Тип** выберите тип коннектора. Например, TCP или UDP.
 - **URL** для подключения – **DNS-имя/IP-адрес** сервера коллектора KUMA: **Порт**, на котором коллектор будет ожидать входящие подключения. Можно выбрать любой свободный порт выше 1024.

В поле **URL** можно указать только порт при инсталляции All-in-one.

Создание коллектора



Подключение источников

Транспорт **1**

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

Транспорт

Подключите источник, от которого хотите получать события. Подробнее см. [в онлайн-справке](#).

Основные параметры

Дополнительные параметры

Коннектор	Создать
Тип* ⓘ	tcp 2
URL* ⓘ	:5155 3
Auditd	☐
Разделитель	

Для настройки защищенной передачи событий между источником и коллектором KUMA на вкладке **Дополнительные параметры** выберите один из режимов TLS. На стороне источника также необходимо настроить параметры TLS.

- На третьем шаге мастера **Парсинг событий** выберите нормализатор.

Нормализатор [ОТВ] КАТА 1

Название* [ОТВ] КАТА

Метод парсинга* ⓘ cef

Сохранить исходное событие* При возникновении ошибок

Сохранить дополнительные поля* Да

Примеры событий + Загрузить из файла

- Шаги мастера настройки с четвертого по шестой (**Фильтрация событий**, **Агрегация событий** и **Обогащение событий**) являются опциональными, их можно пропустить и вернуться к настройке позднее.
- На седьмом шаге мастера **Маршрутизация** задайте точки назначения. Для хранения событий добавьте точку назначения типа **Хранилище**. В случае если предполагается также анализ потока событий правилами корреляции добавьте точку назначения типа **Коррелятор**.

Создание коллектора

- Подключение источников
- Транспорт
- Парсинг событий
- Фильтрация событий
- Агрегация событий
- Обогащение событий
- Маршрутизация 1
- Проверка параметров

Маршрутизация

Укажите, куда следует отправлять полученные события. Подробнее см. [в онлайн-справке](#).

2 + Добавить Удалить

Название	Тип	URL
Пусто		

Создание точки назначения

Основные параметры Дополнительные параметры

Точка назначения

Название*

Состояние

Тип*

Создать 1

Создать

[OOTB] Correlator
Main

[OOTB] Storage 2
Main

Создание точки назначения

Основные параметры Дополнительные параметры

Точка назначения

Название*

Состояние

Тип*

Создать 1

Создать

[OOTB] Correlator 2
Main

[OOTB] Storage
Main

Создание коллектора



Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация 1

Проверка параметров

Маршрутизация

Укажите, куда следует отправлять полученные события. Подробнее см. [в онлайн-справке](#).

+ Добавить Удалить			
☐	Название	Тип	URL
☐	[OOTB] Correlator	correlator	lab:7231 2
☐	[OOTB] Storage	storage	lab:7230 3

- На завершающем шаге мастера нажмите на кнопку **Создать и сохранить сервис**. После чего появится строка установки сервиса, которую необходимо скопировать для дальнейшей установки.

- Подключение источников
- Транспорт
- Парсинг событий
- Фильтрация событий
- Агрегация событий
- Обогащение событий
- Маршрутизация

Проверка параметров 1

Проверка параметров

Настройка коллектора завершена, сервис добавлен в KUMA. Подробнее см. [в онлайн-справке](#).

Чтобы начать получать события, сервис этого коллектора необходимо установить на сервере, предназначенном для сбора событий (см. пример команды установки ниже). Обратите внимание, что должна быть обеспечена сетевая связность компонентов системы и открыты порты. Подробнее см. [в онлайн-справке](#).

Сервисы, использующие этот коллектор

Тип	Название
коллектор	KATA TCP/5155
Сохранить и перезапустить сервисы Сохранить и обновить параметры сервисов	

Рекомендуемая команда для установки коллектора

```
/opt/kaspersky/kuma/kuma collector --core https://[redacted].lab:7210 --id 6ad2ec85-b77d-4a7f-930d-585935815fee --api.port 7656 --install
```

2

- Нажмите **Сохранить**.
- После выполнения вышеуказанных действий в разделе **Ресурсы → Активные сервисы** появится созданный сервис коллектора.

Сервисы

+

Добавить

↻

Обновить параметры

↺

Перезапустить

🔍

Перейти к событиям

📄

Смотреть активные листы

📊

Смотреть контекстные таблицы

📁

Смотреть разделы

🔔

Активные запросы

5155

✕

🔄

⚙️

☐ Статус	Тип	Сервис	Версия	Тенант	Полное доменное имя	IP-адрес	Порт API	Время работы	Создан
☒ ● Выкл	Коллектор	KATA TCP/5155		Main					31.03.2026 18:40:20

Установка коллектора KUMA

Чтобы установить коллектор KUMA:

- Выполните подключение к CLI сервера, на котором планируется развертывание коллектора KUMA.
- Для установки сервиса коллектора в командной строке выполните команду под учетной записью root, скопированную на прошлом шаге.

```
[root@kuma-ai events_examples]# /opt/kaspersky/kuma/kuma collector --core https://[redacted].lab:7210 --id 6ad2ec85-b77d-4a7f-930d-585935815fee --api.port 7656 --install
```

- При необходимости добавьте используемый порт сервиса коллектора в исключения МЭ ОС и обновите параметры службы.
 - **Пример для firewalld**

```
firewall-cmd --add-port=<порт, выбранный для коллектора>/tcp|udp --permanent
```

```
firewall-cmd --reload
```

◦ Пример для ufw

```
ufw allow <порт, выбранный для коллектора>/tcp|udp
```

```
ufw reload
```

- После успешной установки сервиса его статус в веб-консоли KUMA изменится на **ВКЛ** с зеленой индикацией.

Ресурсы и сервисы / Сервисы

Сервисы

+ Добавить ▾									
Обновить параметры									
Перезапустить									
Перейти к событиям									
Смотреть активные листы									
Смотреть контекстные таблицы									
5155									
Статус	Тип	Сервис	Версия	Тенант	Полное доменное имя	IP-адрес	Порт API	Время работы	Создан
☐ Вкл 1	Коллектор	KATA TCP/5155	42.0.259	Main	kompose.kataclouds.io	192.168.1.10	7656	1 минута 28 секунды	31.03.2026 18:40:20

Справочные материалы

Статья онлайн-справки [Создание коллектора](#).

Revision #2

Created 2026-03-31 15:17:18 UTC by Dmitry Borisov

Updated 2026-03-31 15:49:08 UTC by Dmitry Borisov