Check Point NGFW (CEF)

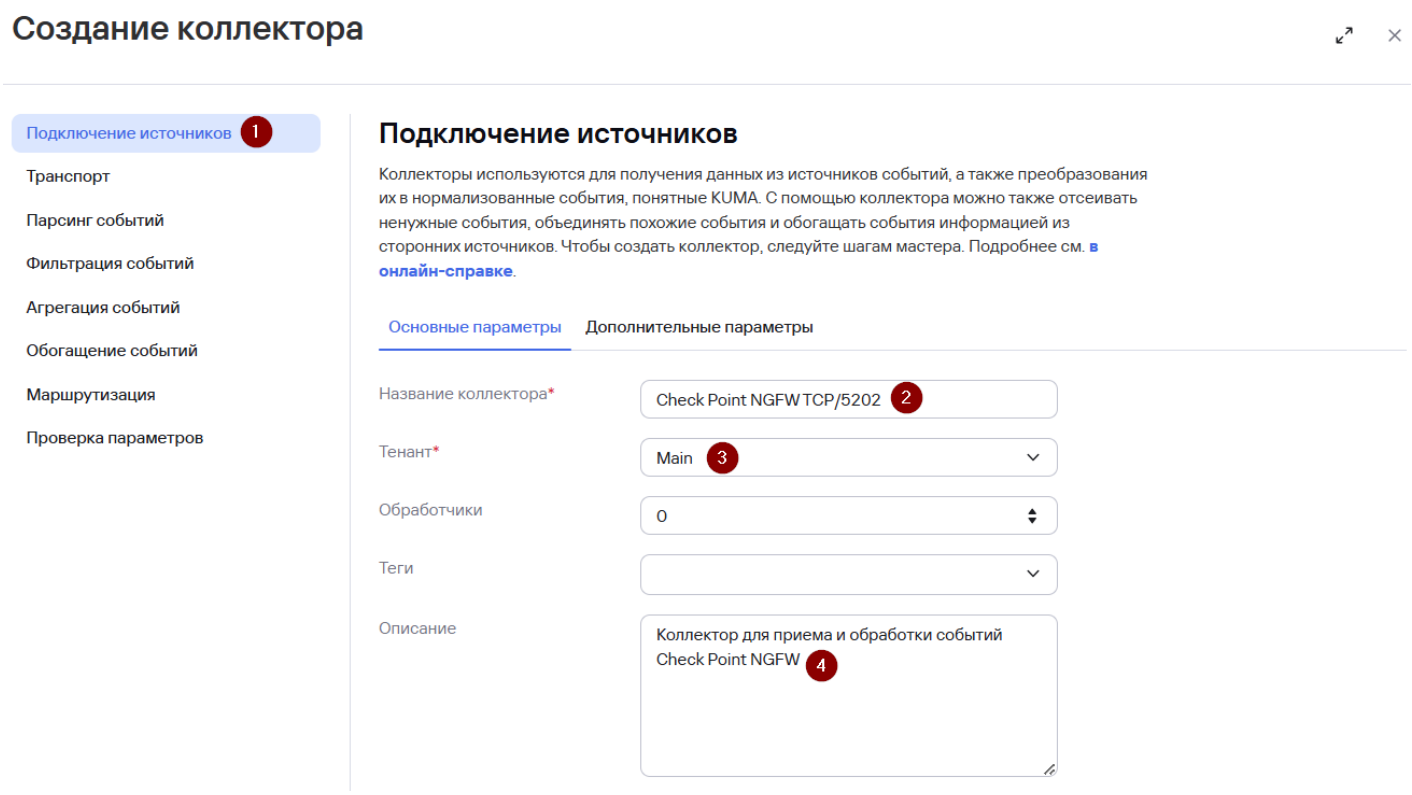
> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

????????? ????????? KUMA

???????? ????????? KUMA

Для приема и обработки событий Check Point NGFW необходимо создать сервис коллектора в KUMA. Для этого в веб-интерфейсе перейдите в раздел **Ресурсы** и нажмите на кнопку **Подключить источник.** В появившемся окне **Создание коллектора:**

- На шаге **Подключение источников** укажите **Название коллектора** и **Тенант**, которому будет принадлежать создаваемый коллектор

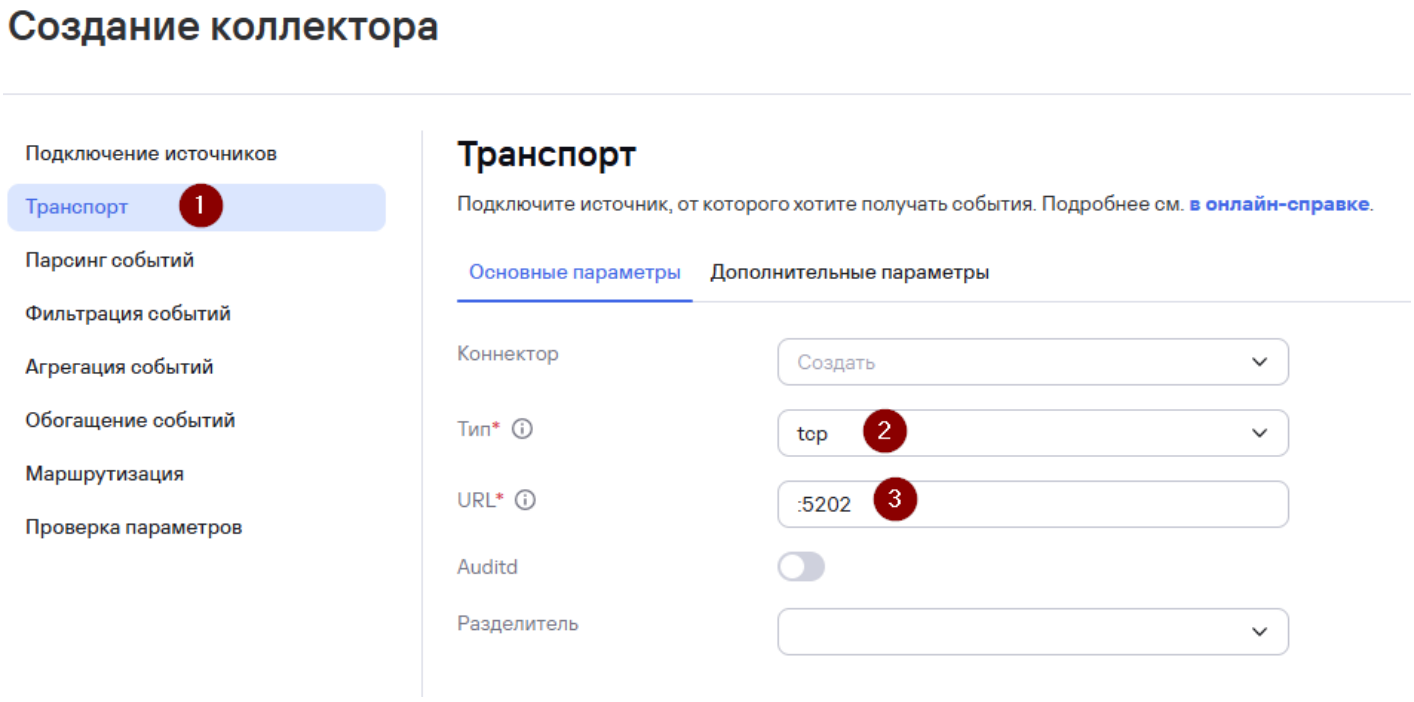


- На шаге **Транспорт** укажите **Тип коннектора** и **URL** (порт, выделенный сервису)

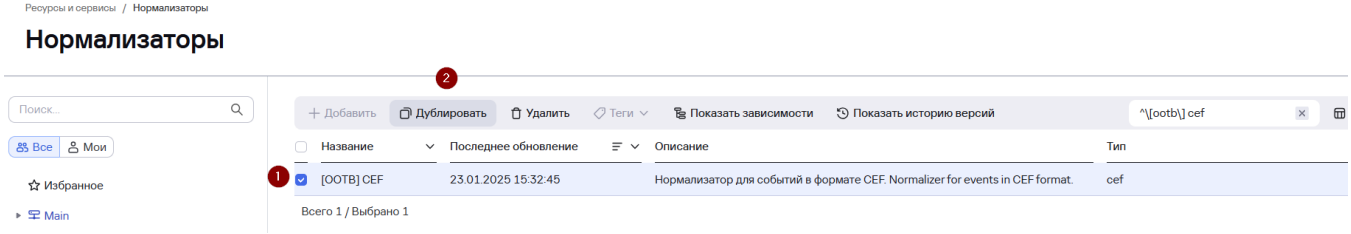
> Для распределенной инсталяции укажите hostname:port сервера коллектора в поле **URL**

>

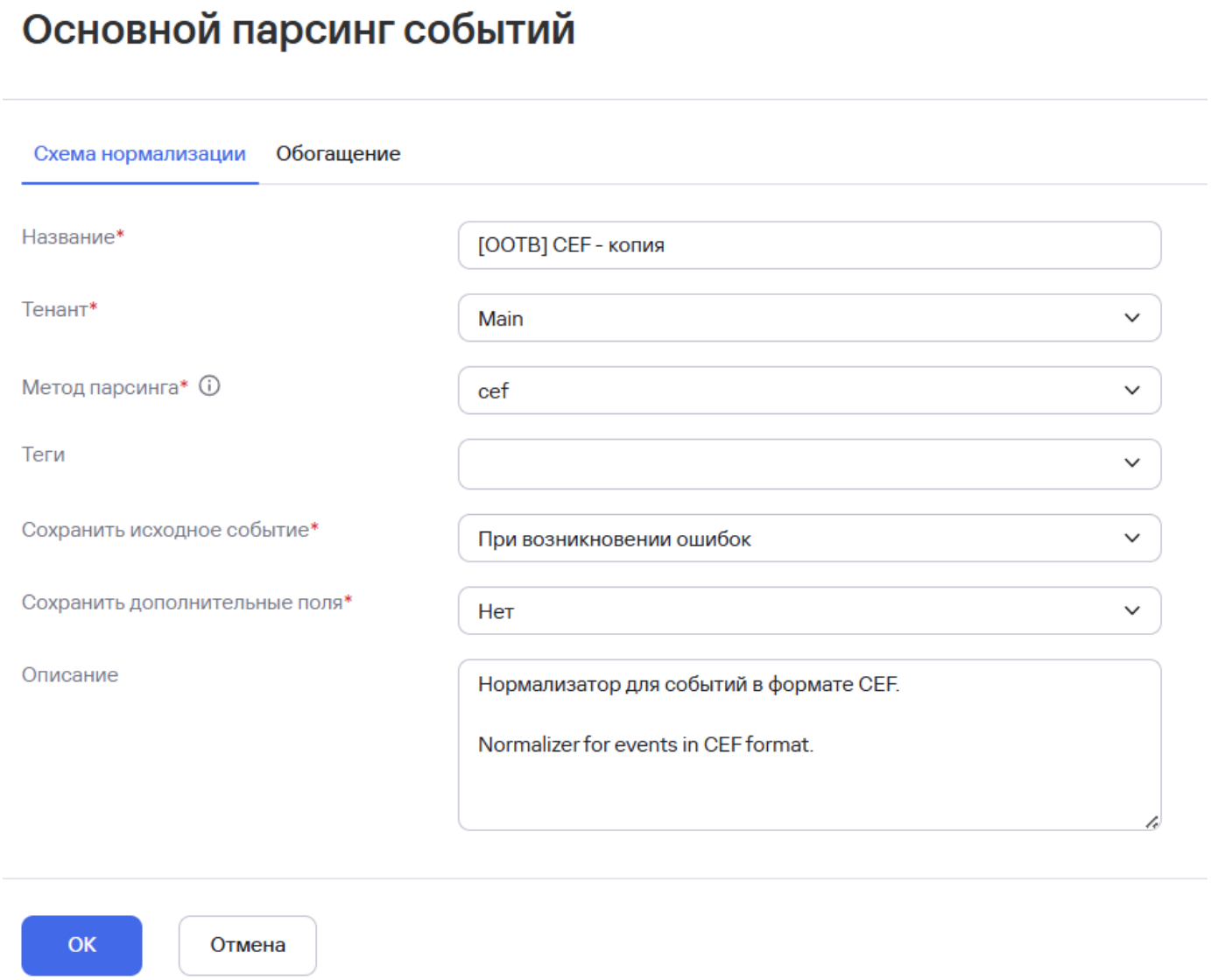
> Указанные параметры должны соответствовать настройкам на стороне Check Point

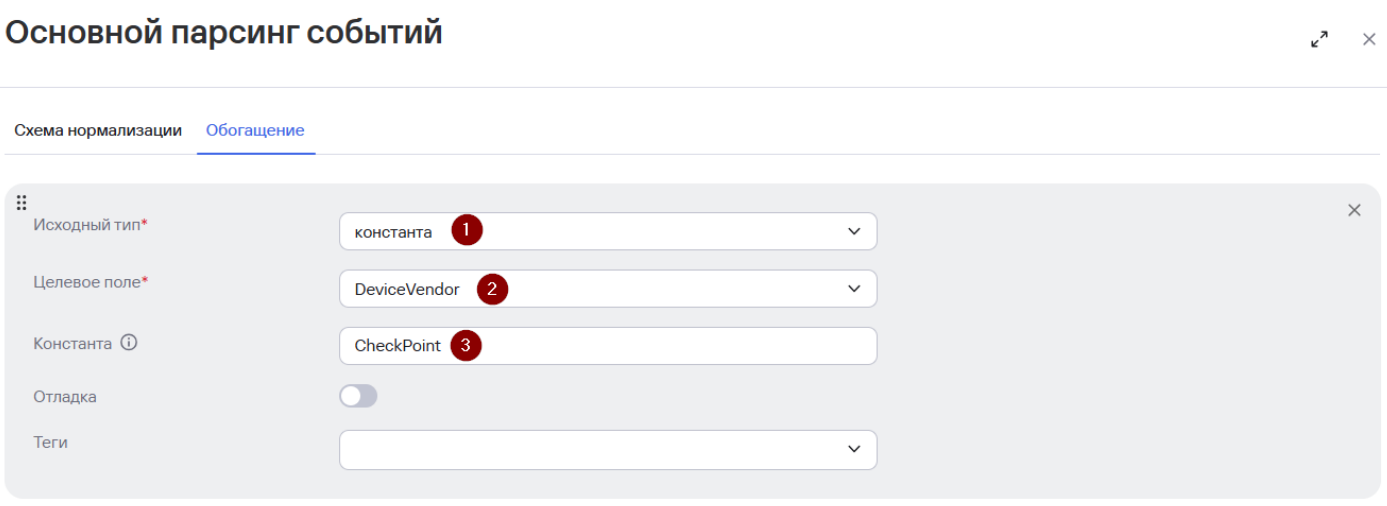


- На шаге **Парсинг событий** нажмите **Добавить парсинг событий** и укажите нормализатор.
  Рекомендуется создать и использовать в качестве нормализатора для событий Check Point дубликат предустановленного нормализатора **[OOTB] CEF.**



В параметрах нормализатора перейдите в окно **Основной парсинг событий** и выберите вкладку **Обогащение.** На вкладке **Обогащение** нажмите **Добавить обогащение** и настройте параметры обогащения согласно скриншоту ниже для корректной работы SOC и Community корреляционных правил.



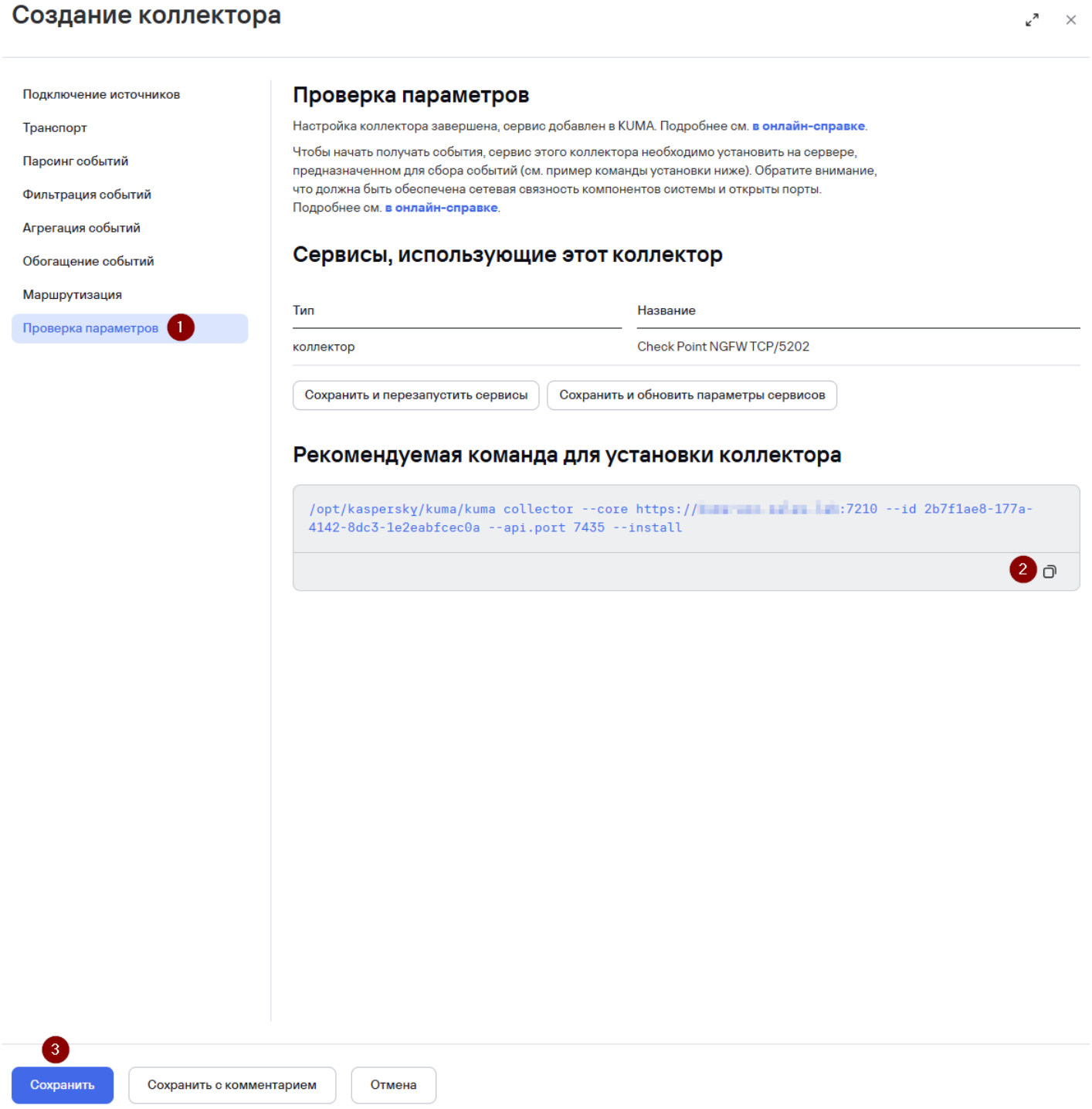


- Шаги мастера настройки с четвертого по шестой (**Фильтрация событий**, **Агрегация событий** и **Обогащение событий**) можно пропустить и вернуться к их настройке позднее.
- На седьмом шаге **Маршрутизация** задайте точки назначения. Для хранения событий добавьте точку назначения типа **Хранилище (Storage)**.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

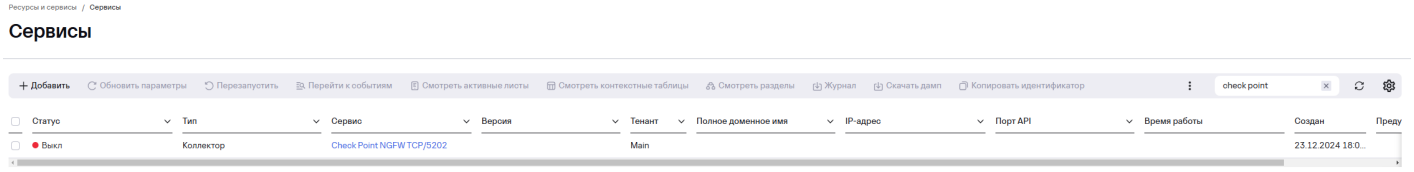
предполагается также анализ потока событий правилами корреляции добавьте точку назначения типа **Коррелятор (Correlator)**.

Создание коллектора

- На завершающем шаге **Проверка параметров** нажмите на кнопку **Сохранить и создать сервис**. После чего появится команда установки сервиса, которую необходимо скопировать для дальнейшей установки.



Также после выполнения вышеуказанных действий в разделе **Ресурсы > Активные сервисы** появится созданный сервис коллектора.



????????? ?????????? KUMA

Выполните подключение к CLI сервера KUMA (установка сервиса коллектора выполняется с правами root).

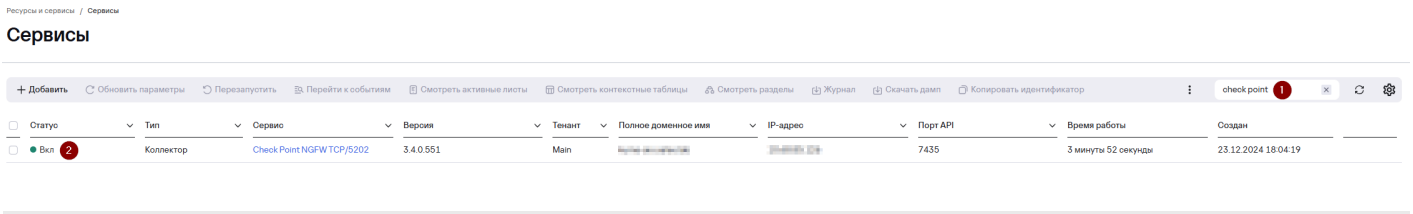
Для установки сервиса коллектора выполните команду, скопированную на прошлом шаге.

```
[root@ ]# /opt/kaspersky/kuma/kuma collector --core https://:7210 --id 2b7f1ae8-177a-4142-8dc3-1e2eabfcec0a --api.port 7435 --install
Created symlink /etc/systemd/system/multi-user.target.wants/kuma-collector-2b7f1ae8-177a-4142-8dc3-1e2eabfcec0a.service → /usr/lib/systemd/system/kuma-collector-2b7f1ae8-177a-4142-8dc3-1e2eabfcec0a.service.
```

При необходимости добавьте порт коллектора в исключения фаервола и обновите параметры службы.

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

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



????????? Check Point NGFW

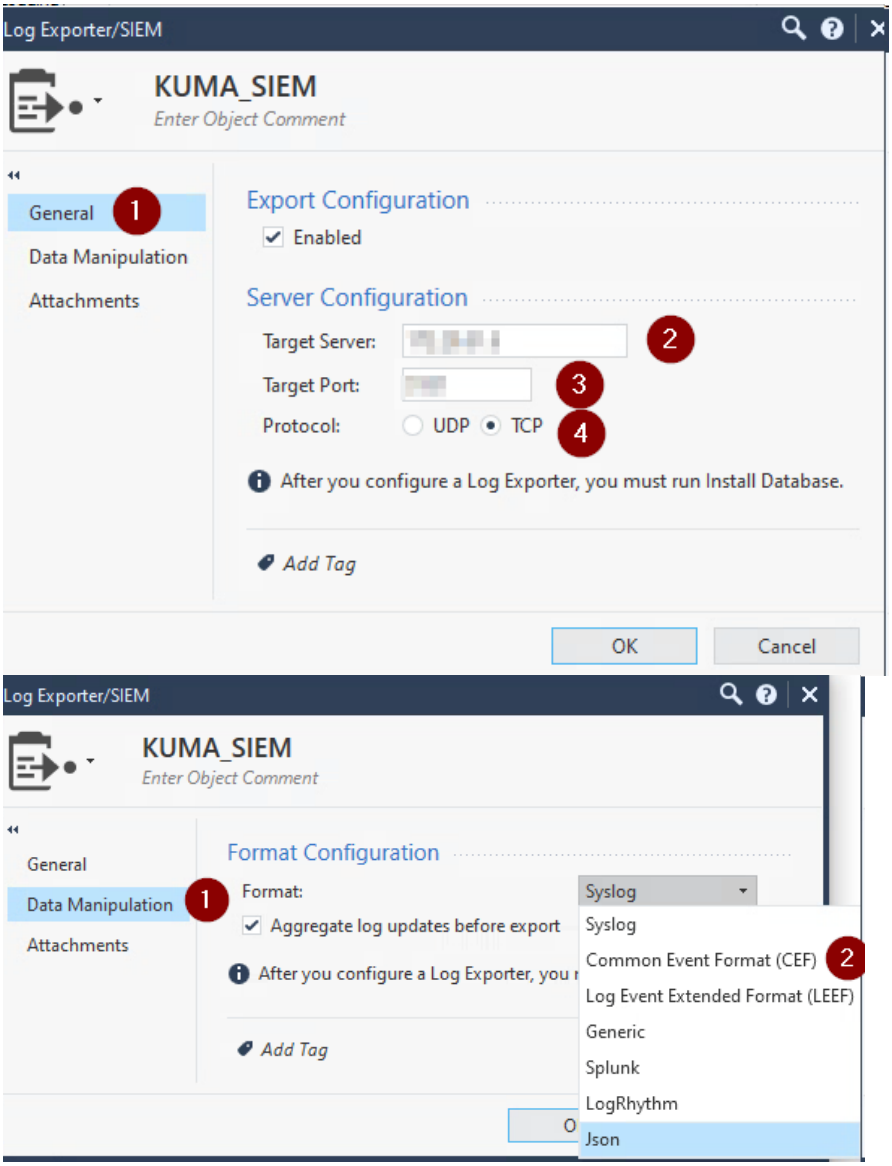
Отправка событий Check Point NGFW осуществляется средствами Log Exporter с Management Server/Log Server. Настройку конфигурации Log Exporter можно выполнить двумя способами:

- С помощью SmartConsole (начиная с версии R81)
- В CLI

SmartConsole

- Создайте новый объект Log Exporter/SIEM:
  - Выберите **Objects** > **More object types** > **Server** > **Log Exporter/SIEM**
  - В поле **Object Name** введите имя для создаваемого объекта **Log Exporter**
  - Перейдите во вкладку **General**:
    - В секции **Export Configuration** активируйте флаг **Enabled**
    - В секции **Server Configuration**:
      - В поле **Target Server** укажите IP-адрес или FQDN сервера коллектора KUMA (FQDN поддерживается, начиная с R81 SmartConsole Build 569)
      - В поле **Target Port** укажите порт, указанный на шаге **Транспорт** при создании сервиса коллектора
      - В поле **Protocol** выберите протокол (TCP или UDP), указанный на шаге **Транспорт** при создании сервиса коллектора

- Перейдите во вкладку **Data Manipulation:**
  - В поле **Format** выберите **Common Event Format (CEF)**
  - **(Опционально)** активируйте флаг **Aggregate log updates before export** для экспорта событий, содержащих полные данные, а не только изменения, произошедшие с момента последнего лога для одного и того же события.
- **(Опционально)** Перейдите во вкладку **Attachments:**
  - Активируйте флаги
    - **Add link to Log Details in SmartView**
    - **Add link to Log Attachment in SmartView**
    - **Add Log Attachment ID**
- Нажмите **OK**



- Выполните настройку параметров объекта **Management Server** или **Dedicated Log Server / SmartEvent Server:**
  - В навигационной панели слева выберите **Gateways & Servers**
  - Откройте объект **Management Server or Dedicated Log Server / SmartEvent Server**

    - Слева выберите **Logs** > **Export**
    - Нажмите **[+]** и выберите объект **Log Exporter / SIEM,** созданный ранее
    - Нажмите **OK**
- Нажмите **Menu** > **Install database**
- Выберите все объекты
- Нажмите **Install**

CLI

- Подключитесь к **Management Server / Log Server**
- Перейдите в режим **Expert**
- Настройте параметры **Log Exporter**

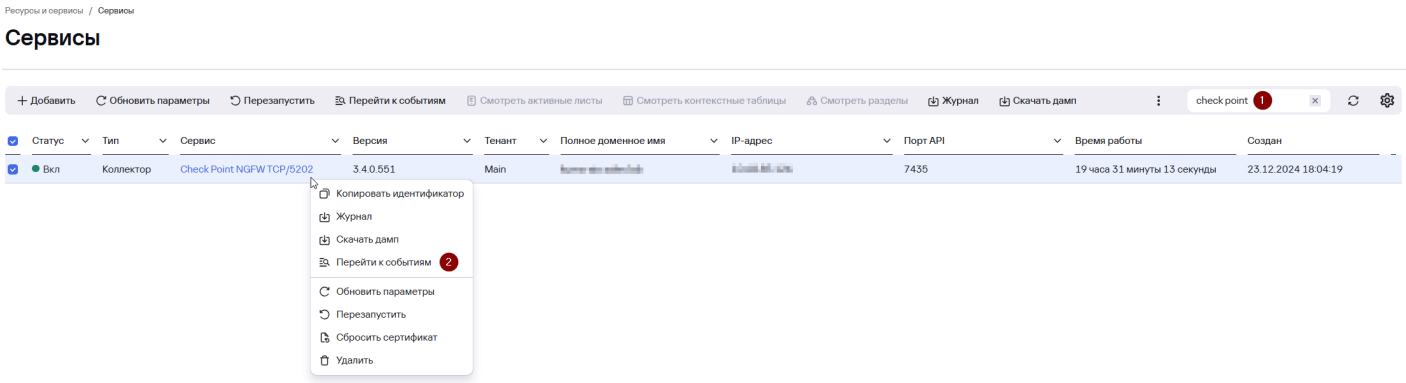
```
cp_log_export add name <Наименование конфигурации Log Exporter> target-server <IP-адрес или FQDN сервера коллектора KUMA> target-port <Порт, указанный на шаге Транспорт при создании сервиса коллектора> protocol {tcp | udp} format cef
```

- Запустите новый инстанс **Log Exporter**

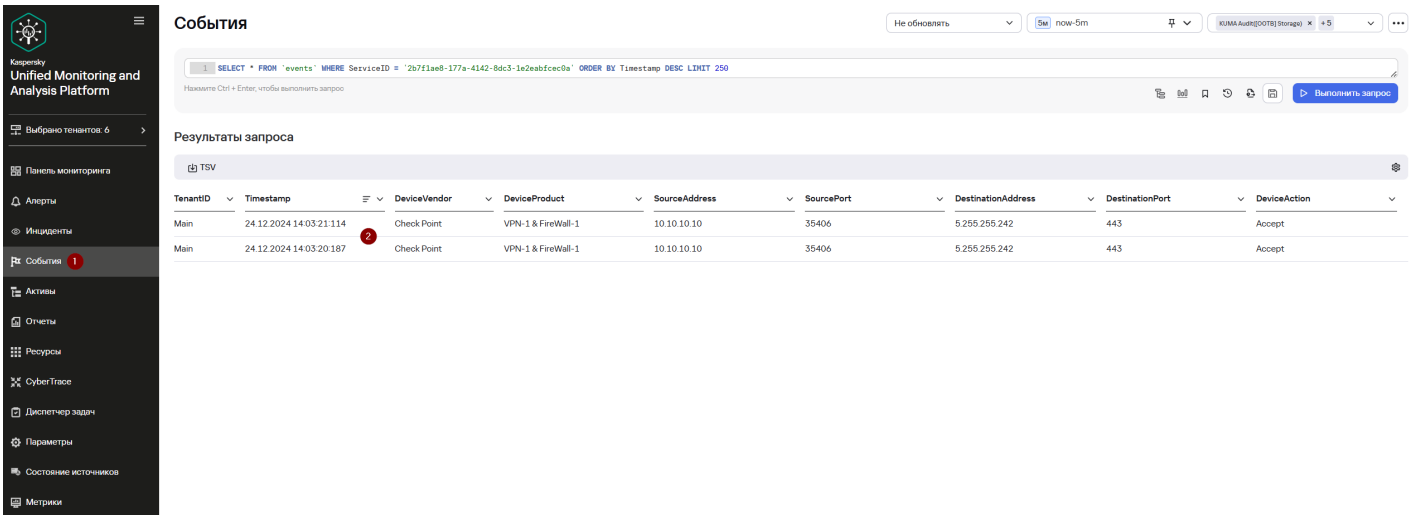
```
cp_log_export restart name <Наименование конфигурации>
```

???????? ???????????? ??????? Check Point NGFW ? KUMA

Для проверки, что сбор событий с Check Point NGFW успешно настроен перейдите в **Ресурсы** > **Активные сервисы** > выберите ранее созданный коллектор Check Point NGFW > ПКМ > **Перейти к событиям.**



В открывшемся окне **События** убедитесь, что присутствуют события Check Point NGFW.



???????? ??????

Настройка отправки событий Check Point с помощью Log Exporter - https://support.checkpoint.com/results/sk/sk122323

Описание полей событий Check Point - https://support.checkpoint.com/results/sk/sk144192

Revision #12
Created 2024-12-23 14:28:15 UTC by Dmitry Borisov
Updated 2025-03-27 14:38:17 UTC by Dmitry Borisov