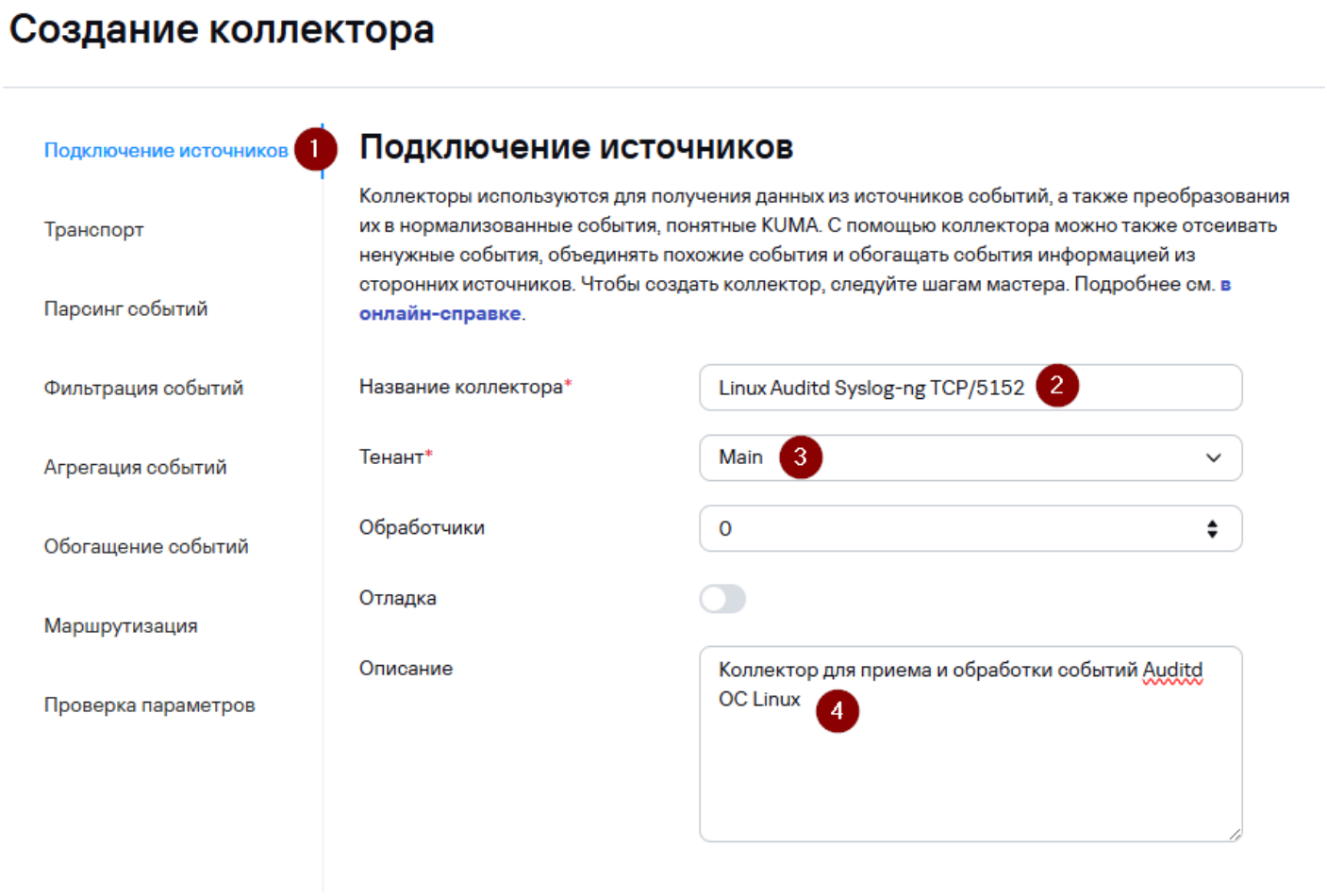
???? ??????? auditd ? ??????? Syslog-ng

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

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

Для создания коллектора в веб-интерфейсе KUMA:

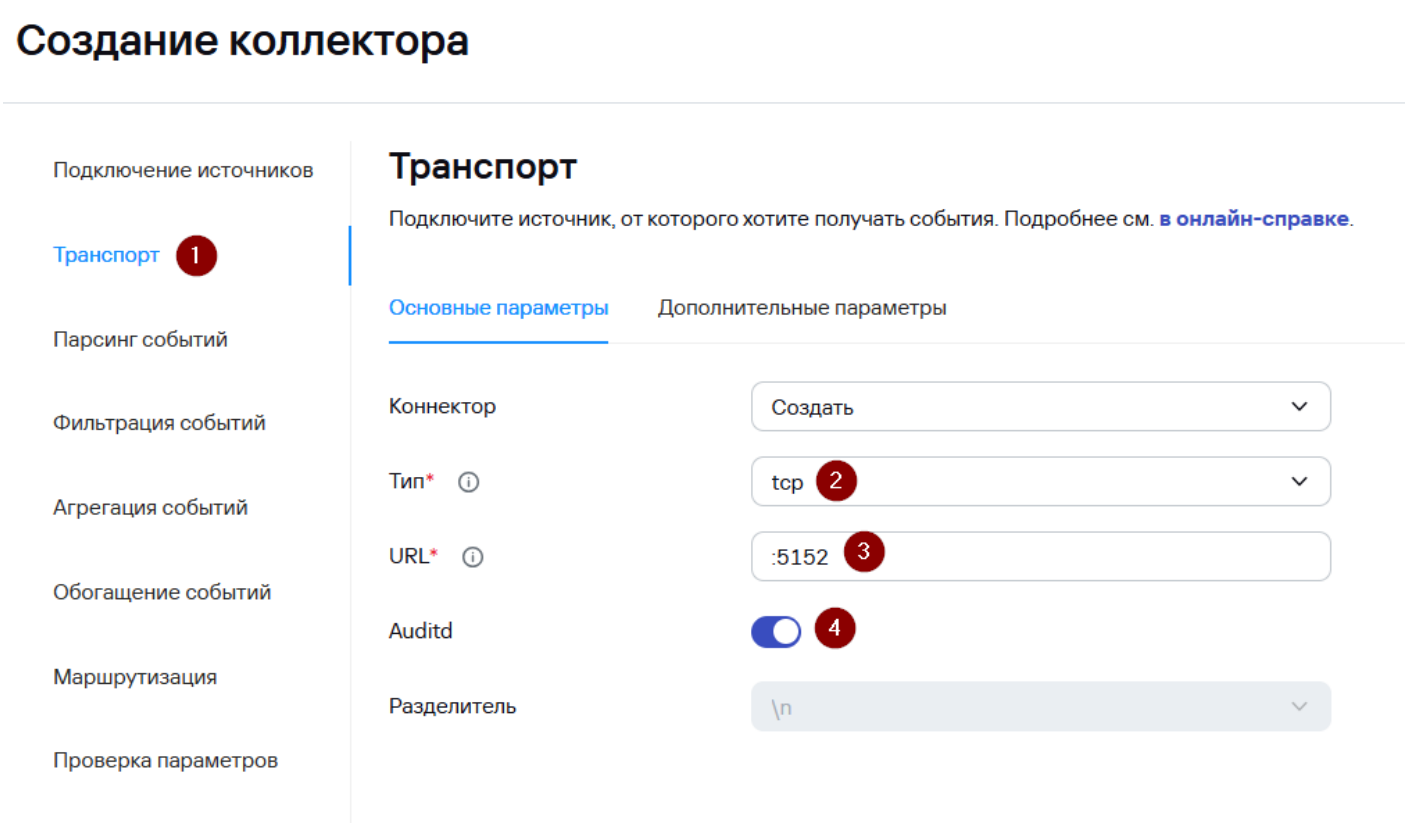
- Перейдите в раздел **Ресурсы** и нажмите на кнопку **Подключить источник**.
- В появившемся окне мастера настройки **Создание коллектора** на первом шаге (**Подключение источников**) выберите **Имя коллектора** и **Тенант**, к которому будет принадлежать создаваемый коллектор.



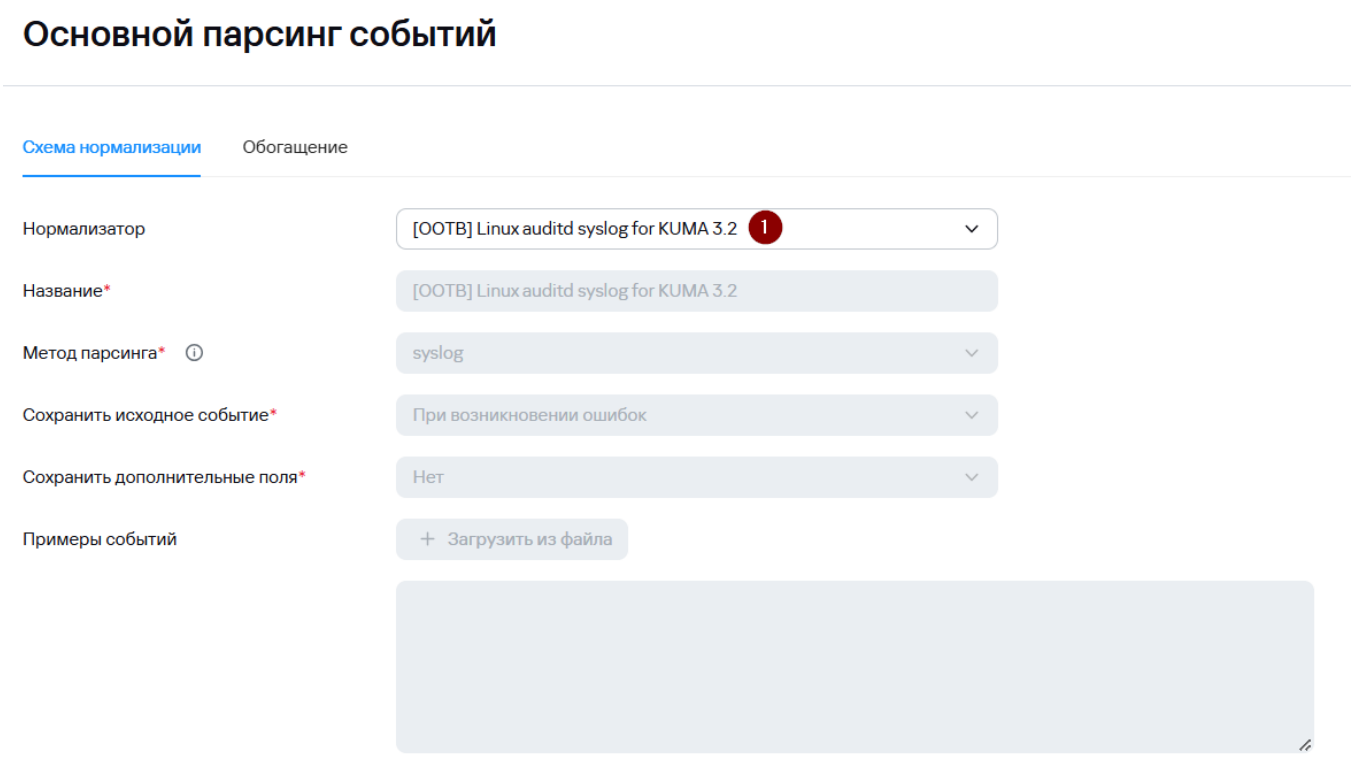
- На втором шаге мастера (**Транспорт**) укажите параметры коннектора для взаимодействия с подключаемым источником:
  - **Тип** – tcp/udp. В данном примере tcp.
  - **URL** – FQDN:порт (порт, на котором коллектор будет ожидать входящие подключения. Выбирается любой из незанятых, выше 1024). В данном примере 5152.
  - **Auditd** – включено

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

> Начиная с версии 3.2, в KUMA появился переключатель Auditd, который позволяет группировать полученные от коннектора строки событий auditd в одно событие auditd.

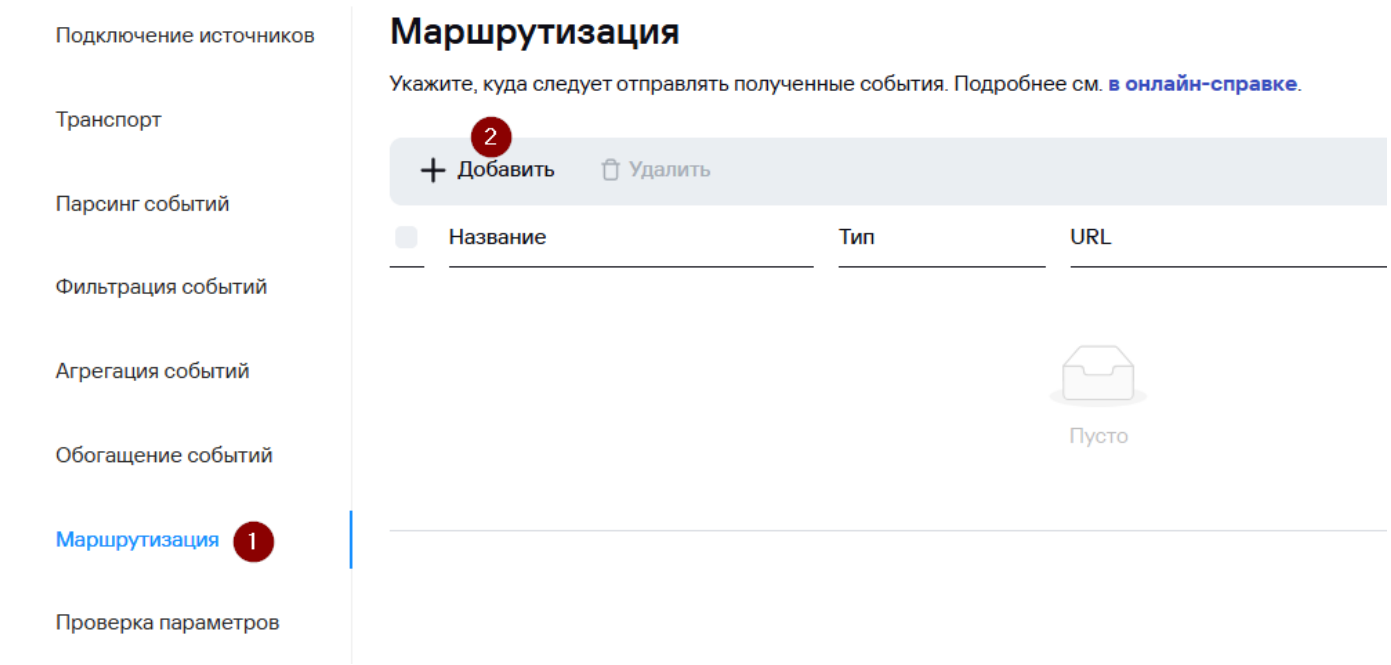


- На третьем шаге мастера укажите нормализатор. В данном случае рекомендуется использовать «коробочный» нормализатор для событий auditd Linux **[OOTB] Linux auditd syslog for KUMA 3.2**.

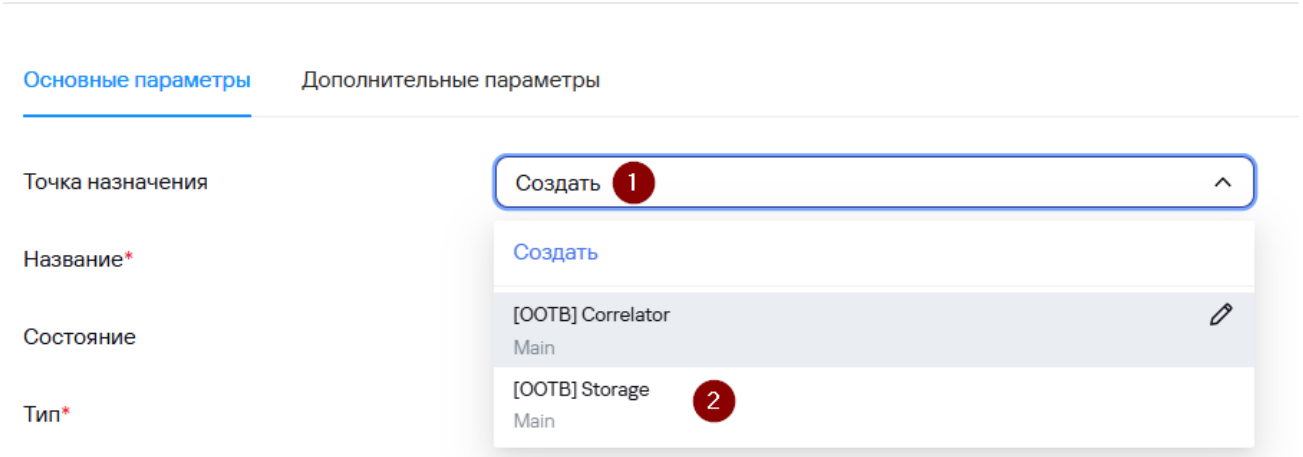


- Шаги мастера настройки с четвертого по шестой являются опциональными, их можно пропустить и вернуться к настройке позднее.
- На седьмом шаге мастера задайте точки назначения. Для хранения событий добавьте точку назначения типа **Хранилище**. В случае если предполагается также анализ потока событий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

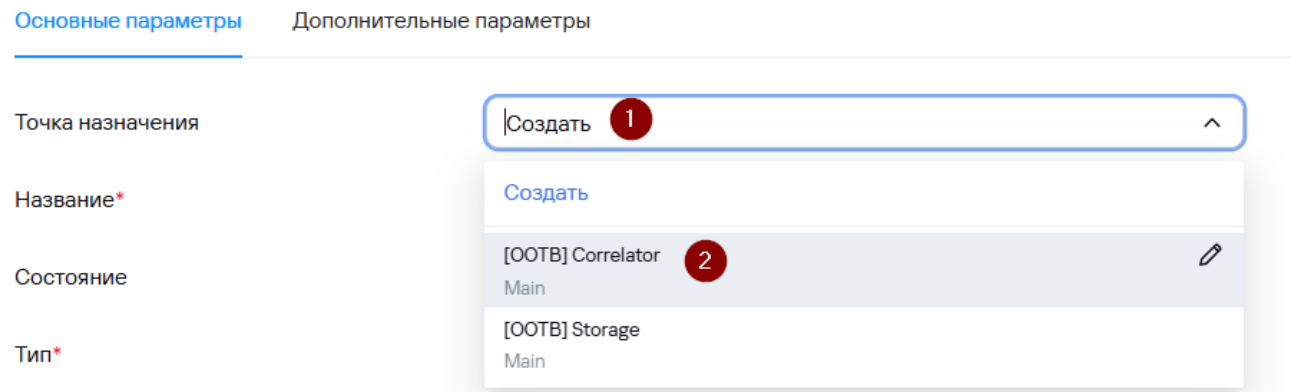
Создание коллектора



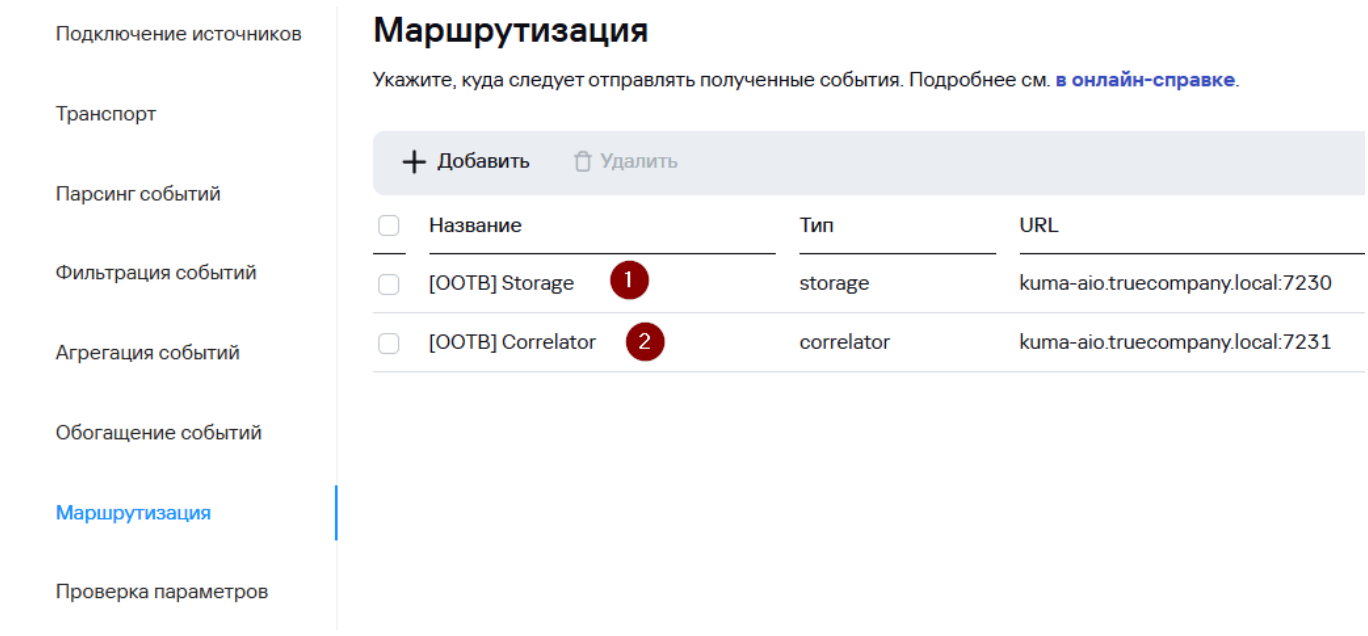
Создание точки назначения



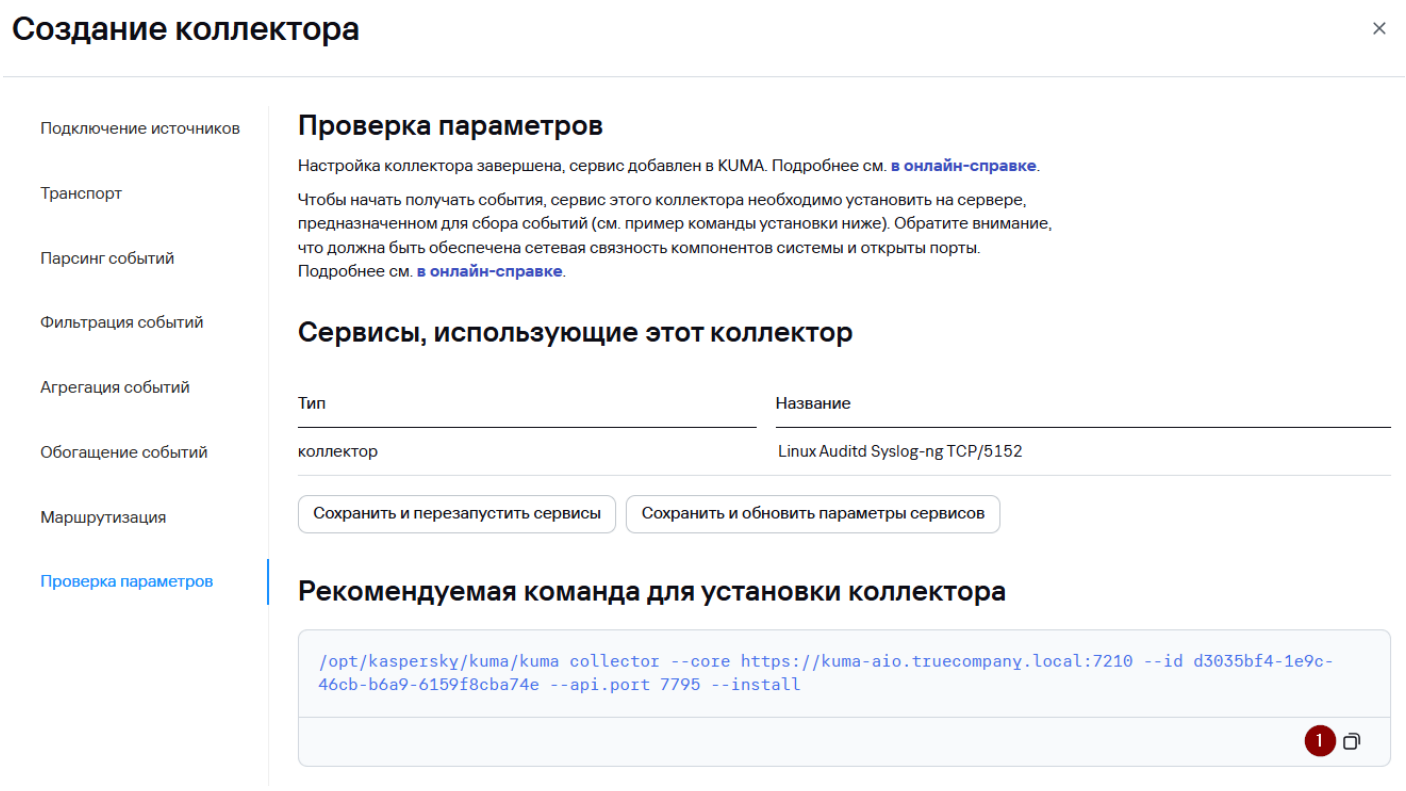
Создание точки назначения



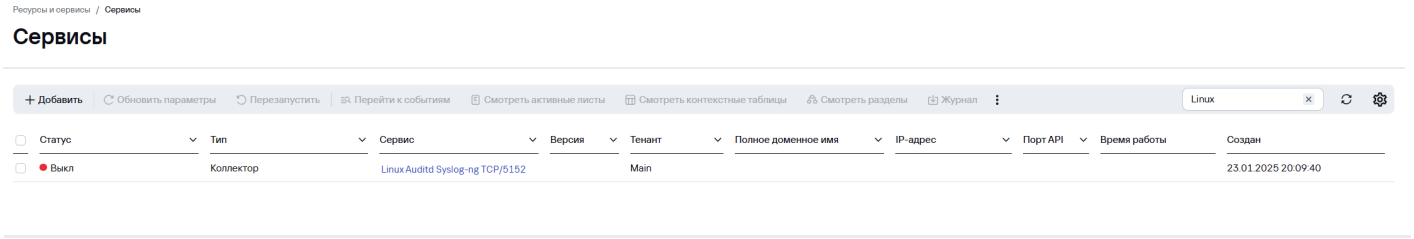
Создание коллектора



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



- Нажмите **Сохранить**.
- После выполнения вышеуказанных действий в разделе **Ресурсы → Активные сервисы** появится созданный сервис 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-aio:/home/kuma-adm# /opt/kaspersky/kuma/kuma collector --core https://kuma-aio.truecompany.local:7210 --id d3035bf4-1e9c-46cb-b6a9-6159f8cba74e --api.port 7795 --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
```

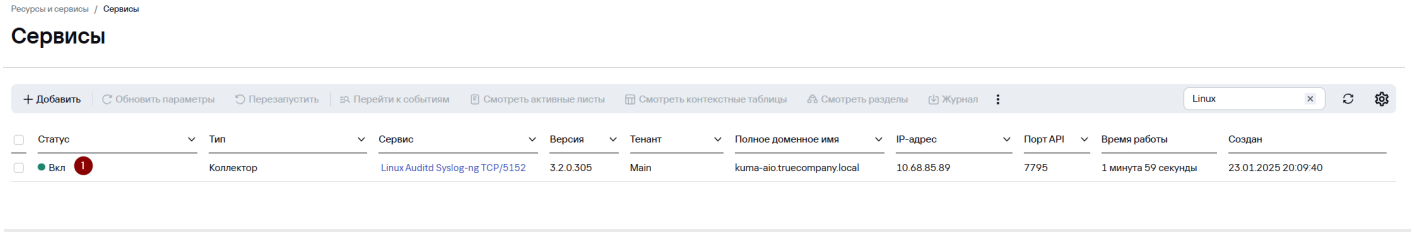
```
firewall-cmd –reload
```

  - 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.



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

Для передачи событий с рабочей станции/сервера в коллектор KUMA будет использоваться сервис syslog-ng.

> При разработке статьи использовалась версия 3.19 syslog-ng.

- На рабочей станции/сервере Linux убедитесь, что сервис syslog-ng уже установлен в ОС:

```
systemctl status syslog-ng.service
```

- Если сервис syslog-ng не установлен на сервере, установите его, выполнив следующие команды (пример для Astra Linux и Ubuntu):

```
apt install syslog-ng
```

```
systemctl enable syslog-ng.service
```

```
systemctl start syslog-ng.service
```

- Далее в папке **`/etc/syslog-ng/conf.d/`** создайте файл конфигурации (например, `30-kuma-tcp.conf` или `30-kuma-udp.conf`) со следующим содержанием в зависимости от используемого протокола:

Для отправки событий по протоколу TCP

```
# syslog-ng audit forwarding to KUMA (TCP)
# Version: 1
# Date: 26.01.2026
# Purpose: Forward auditd logs without parsing, loss-minimized

source s_audit {
```

```
    file("/var/log/audit/audit.log"
     flags(no-parse) # Читаем audit.log без парсинга (flags(no-parse)), чтобы "не ломать" формат auditd.
  follow-freq(1)
  tags("tag_audit_log")
  persist-name("kuma_audit_source")); # Необходим для сохранения состояния источника между рестартами syslog-ng.
};

template t_audit_format {
    template("<134>${ISODATE} ${HOST} auditd ${MSG}\n"); # <PRI> задан вручную, т.к. при flags(no-parse) ${PRI} не извлекается из события. Тег auditd задан руками, иначе будет дефолтное 0d.
    template_escape(no);
};

destination d_kuma {
    tcp("<IP-адрес/FQDN коллектора KUMA>" port(<Порт коллектора KUMA>)
     template(t_audit_format)
     disk-buffer(
      mem-buf-size(10000) # Размер буфера в RAM, в количестве сообщений. Пока есть место — ничего не пишется на диск. Можно увеличить при большом потоке событий.
   disk-buf-size(1G) # Максимальный размер буфера на диске. Когда RAM-буфер будет заполнен, запись продолжится на диск. Можно увеличить при большом потоке событий.
   reliable(yes) # Для гарантированной доставки. События не теряются при рестаре syslog-ng, проблем с сетью, перезапуске коллектора.
  )
 );
};

filter f_audit_kuma {
    tags("tag_audit_log");
};

log {
    source(s_audit);
    filter(f_audit_kuma);
    destination(d_kuma);
};
```

Для отправки событий по протоколу UDP

```
# syslog-ng audit forwarding to KUMA (UDP)
# Version: 1
# Date: 26.01.2026
# Purpose: Forward auditd logs without parsing, loss-minimized

source s_audit {
    file("/var/log/audit/audit.log"
     flags(no-parse) # Читаем audit.log без парсинга (flags(no-parse)), чтобы "не ломать" формат auditd.
  follow-freq(1)
  tags("tag_audit_log")
  persist-name("kuma_audit_source")); # Необходим для сохранения состояния источника между рестартами syslog-ng.
};

template t_audit_format {
    template("<134>${ISODATE} ${HOST} auditd ${MSG}\n"); # <PRI> задан вручную, т.к. при flags(no-parse) ${PRI} не извлекается из события. Тег auditd задан руками, иначе будет дефолтное 0d.
    template_escape(no);
};

destination d_kuma {
    udp("<IP-адрес/FQDN коллектора KUMA>" port(<Порт коллектора KUMA>)
     template(t_audit_format)
     disk-buffer(
      mem-buf-length(10000) # Размер буфера в RAM, в количестве сообщений. Пока есть место — ничего не пишется на диск. Можно увеличить при большом потоке событий.
   disk-buf-size(1G) # Максимальный размер буфера на диске. Когда RAM-буфер будет заполнен, запись продолжится на диск. Можно увеличить при большом потоке событий.
  )
 );
};

filter f_audit_kuma {
    tags("tag_audit_log");
};
```

```
log {
    source(s_audit);
    filter(f_audit_kuma);
    destination(d_kuma);
};
```

- Далее выполните проверку конфигурации syslog-ng:

```
syslog-ng -s
```

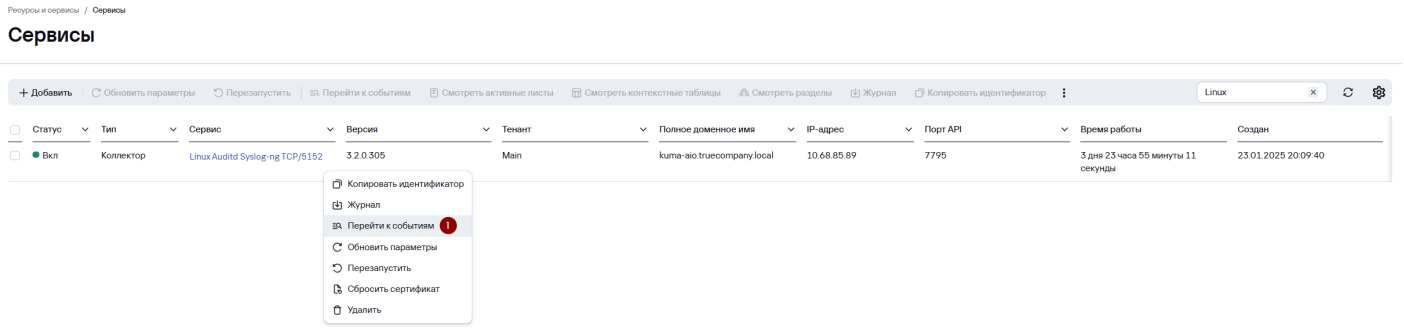
- Если ошибки при проверке конфигурации отсутствуют перезапустите сервис syslog-ng, выполнив следующую команду:

```
systemctl restart syslog-ng
```

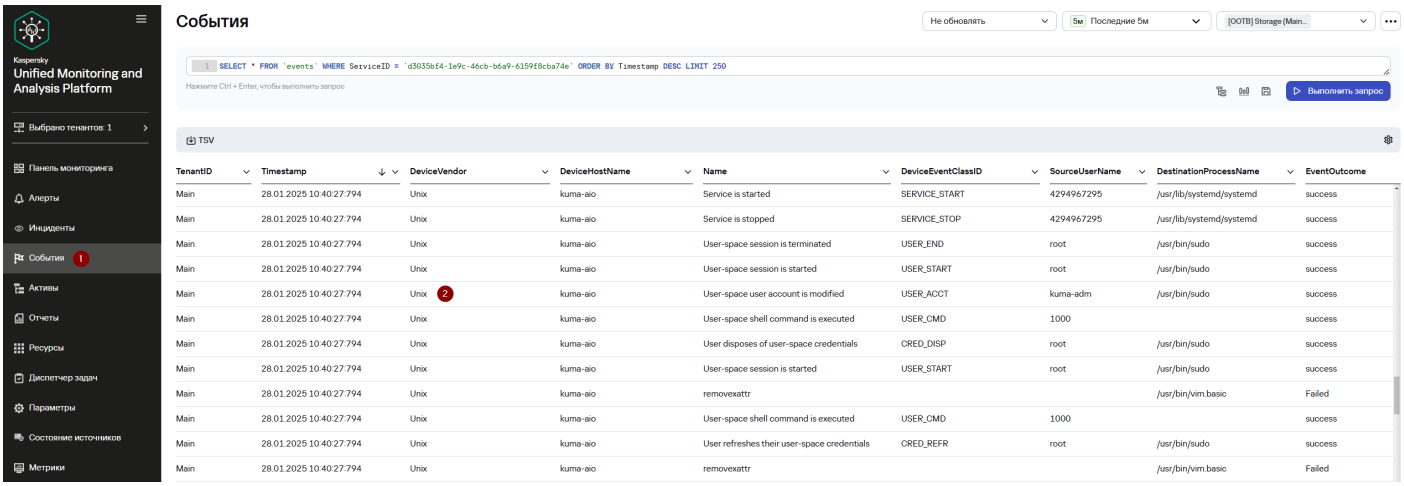
Рабочая станция/сервер Linux настроены. События передаются в коллектор KUMA.

???????? ???????????? ??????? Linux ? KUMA

- Для проверки, что сбор событий с устройств Linux успешно настроен перейдите в **Ресурсы → Активные сервисы →** выберите ранее созданный коллектор для Linux и нажмите **Перейти к событиям**.



- В открывшемся окне **События** убедитесь, что присутствуют события с устройств Linux.

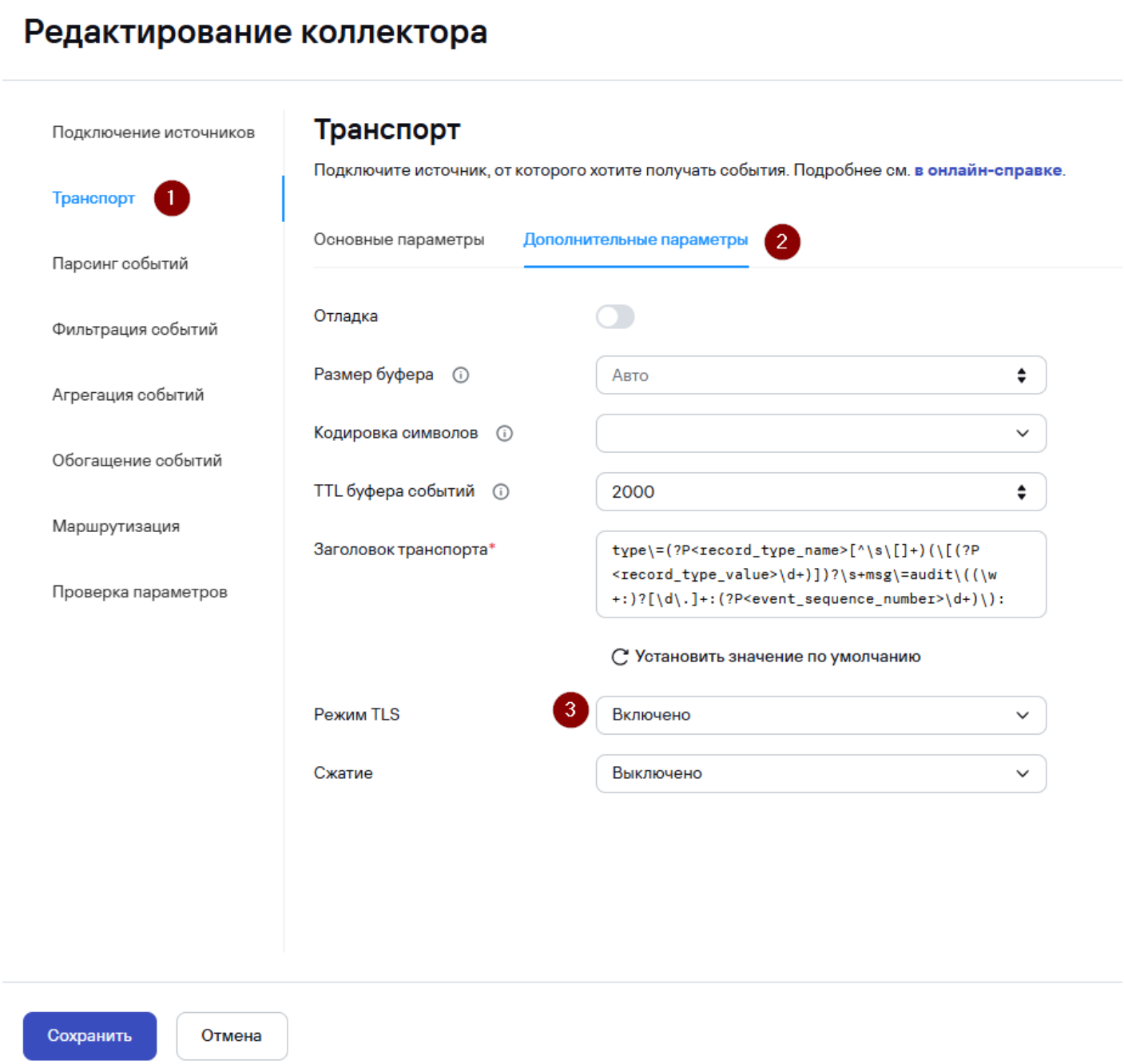


?????????? ?. ???????? ??????? ? ????????????? TLS (??? ????????? ?????????? ??????????)

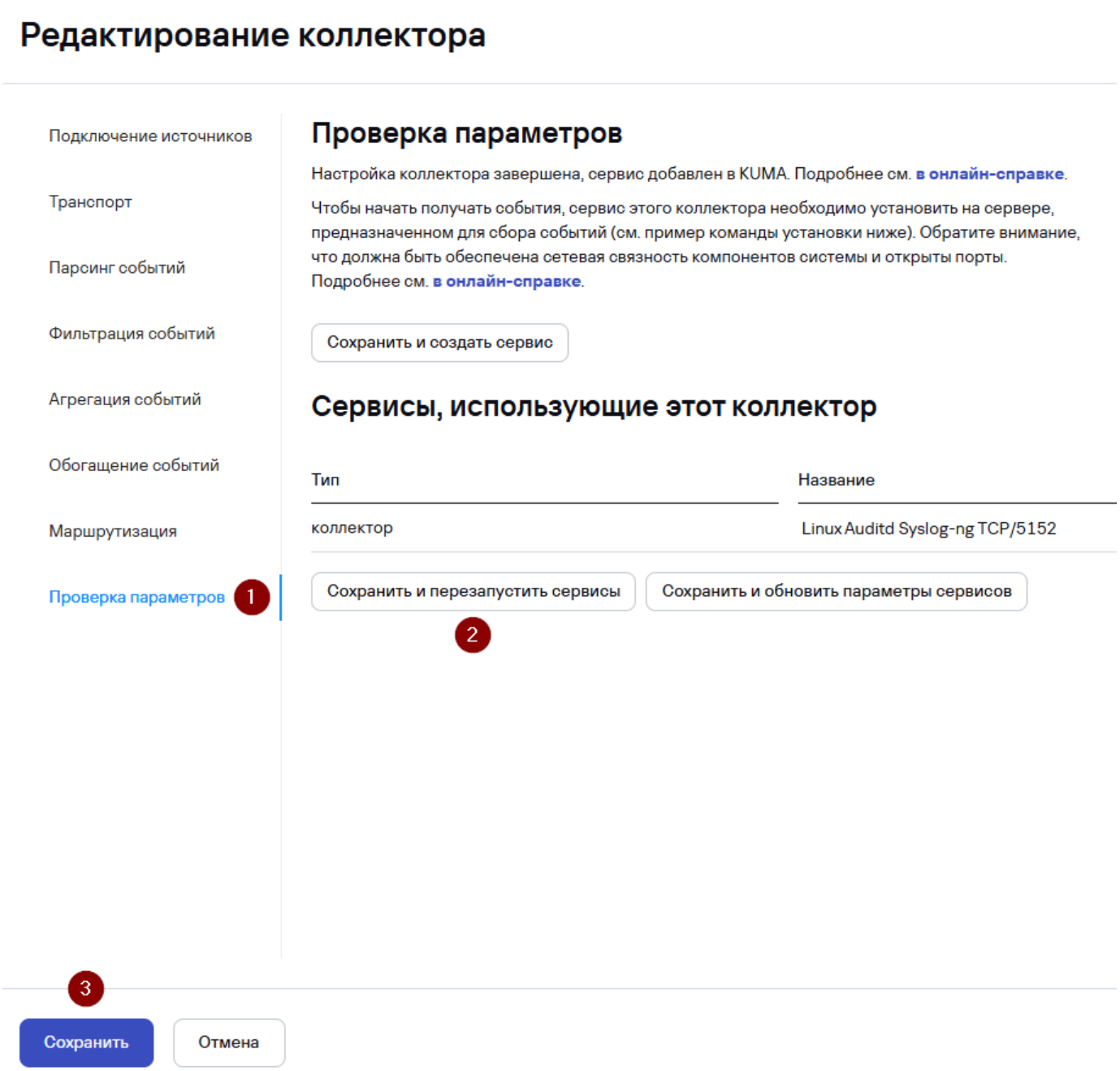
> Предварительно рекомендуется протестировать отправку событий auditd без использования шифрования - см. раздел **Настройка источника событий**.

Для передачи событий auditd с рабочей станции/сервера в коллектор KUMA с использованием TLS без валидации сертификата:

- В веб-интерфейсе KUMA:
  - Перейдите в раздел **Ресурсы → Активные сервисы** и выберите ранее созданный коллектор для приема и обработки событий auditd.
  - В появившемся окне **Редактирование коллектора** перейдите на вкладку **Дополнительные параметры** и в параметре **Режим TLS** выберите **Включено**.



- Перейдите на шаг Проверка параметров и нажмите **Сохранить и перезапустить сервисы**.
- Нажмите **Сохранить**.



- На рабочей станции/сервере Linux:
  - В папке `/etc/syslog-ng/conf.d/` создайте файл конфигурации (например, `30-kuma-tcp-tls-wo-cert-validation.conf`) со следующим содержанием:

```
# syslog-ng audit forwarding to KUMA (TCP with TLS without certificate validation)
# Version: 1
# Date: 26.01.2026
# Purpose: Forward auditd logs without parsing, loss-minimized

source s_audit {
    file("/var/log/audit/audit.log"
    flags(no-parse) # Читаем audit.log без парсинга (flags(no-parse)), чтобы "не ломать"
```

```
формат auditd.
  follow-freq(1)
  tags("tag_audit_log")
  persist-name("kuma_audit_source")); # Необходим для сохранения состояния источника между рестартами syslog-ng.
};

template t_audit_format {
    template("<134>${ISODATE} ${HOST} auditd ${MSG}\n"); # <PRI> задан вручную, т.к. при flags(no-parse) ${PRI} не извлекается из события. Тег auditd задан руками, иначе будет дефолтное 0d.
    template_escape(no);
};

destination d_kuma {
    tcp("<IP-адрес/FQDN коллектора KUMA>" port(<Порт коллектора KUMA>)
     template(t_audit_format)
     disk-buffer(
      mem-buf-size(10000) # Размер буфера в RAM, в количестве сообщений. Пока есть место — ничего не пишется на диск. Можно увеличить при большом потоке событий.
  disk-buf-size(1G) # Максимальный размер буфера на диске. Когда RAM-буфер будет заполнен, запись продолжится на диск. Можно увеличить при большом потоке событий.
  reliable(yes) # Для гарантированной доставки. События не теряются при рестаре syslog-ng, проблем с сетью, перезапуске коллектора.
  )
  tls(peer-verify(required-untrusted))
     );
};

filter f_audit_kuma {
    tags("tag_audit_log");
};

log {
    source(s_audit);
    filter(f_audit_kuma);
    destination(d_kuma);
};
```

- Удалите или переименуйте ранее созданный файл конфигурации для отправки событий по TCP, например, `30-kuma-tcp.conf.backup`
- Далее выполните проверку конфигурации syslog-ng:

```
syslog-ng -s
```

- Если ошибки при проверке конфигурации отсутствуют перезапустите сервис syslog-ng, выполнив следующую команду:

```
systemctl restart syslog-ng
```

Рабочая станция/сервер Linux настроены. События передаются в коллектор KUMA с использованием TLS.

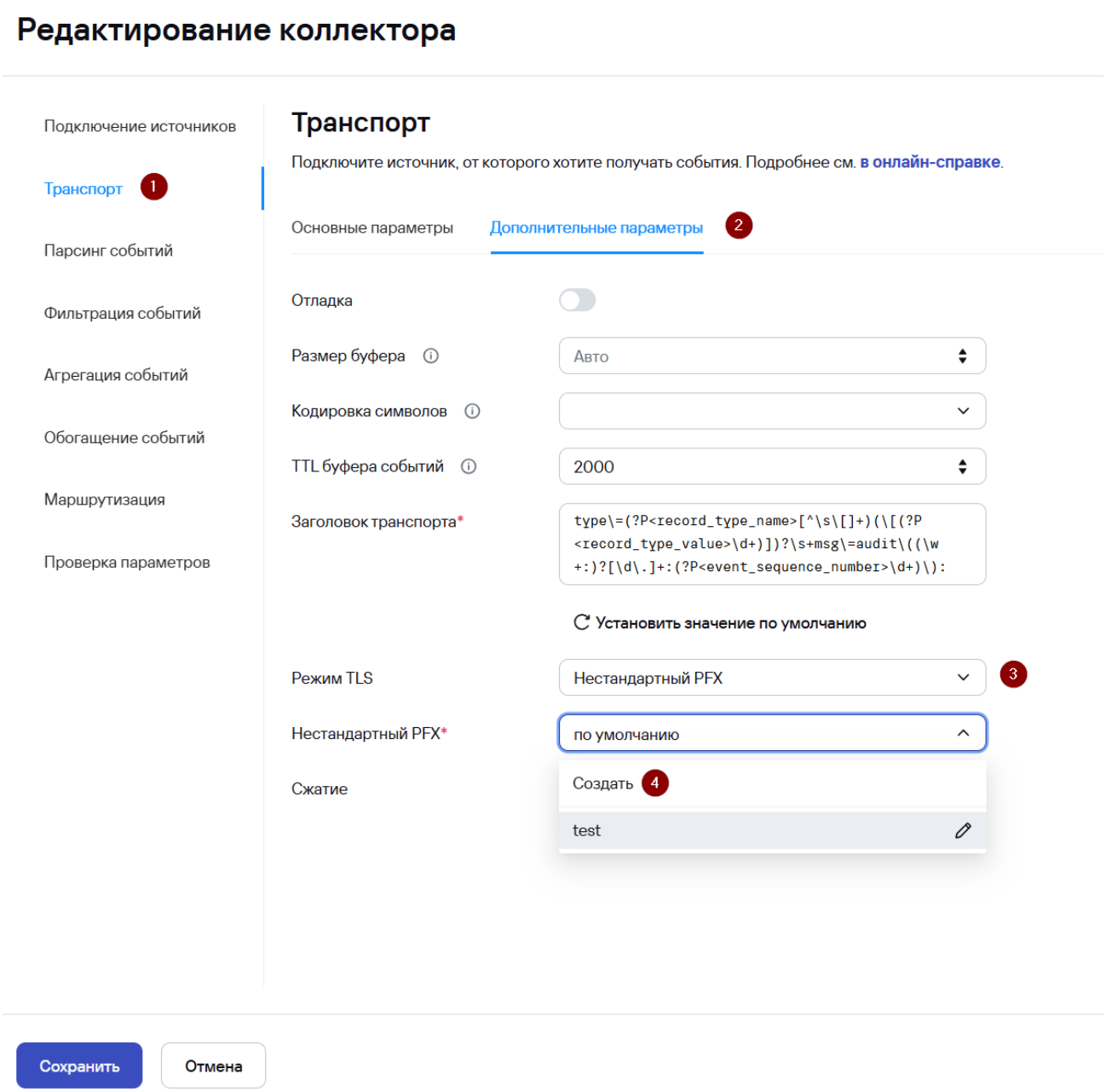
?????????? ?. ???????? ??????? ? ????????????? TLS (с ?????????? ?????????? ??????????)

> Предварительно рекомендуется протестировать отправку событий auditd без использования шифрования - см. раздел **Настройка источника событий**.

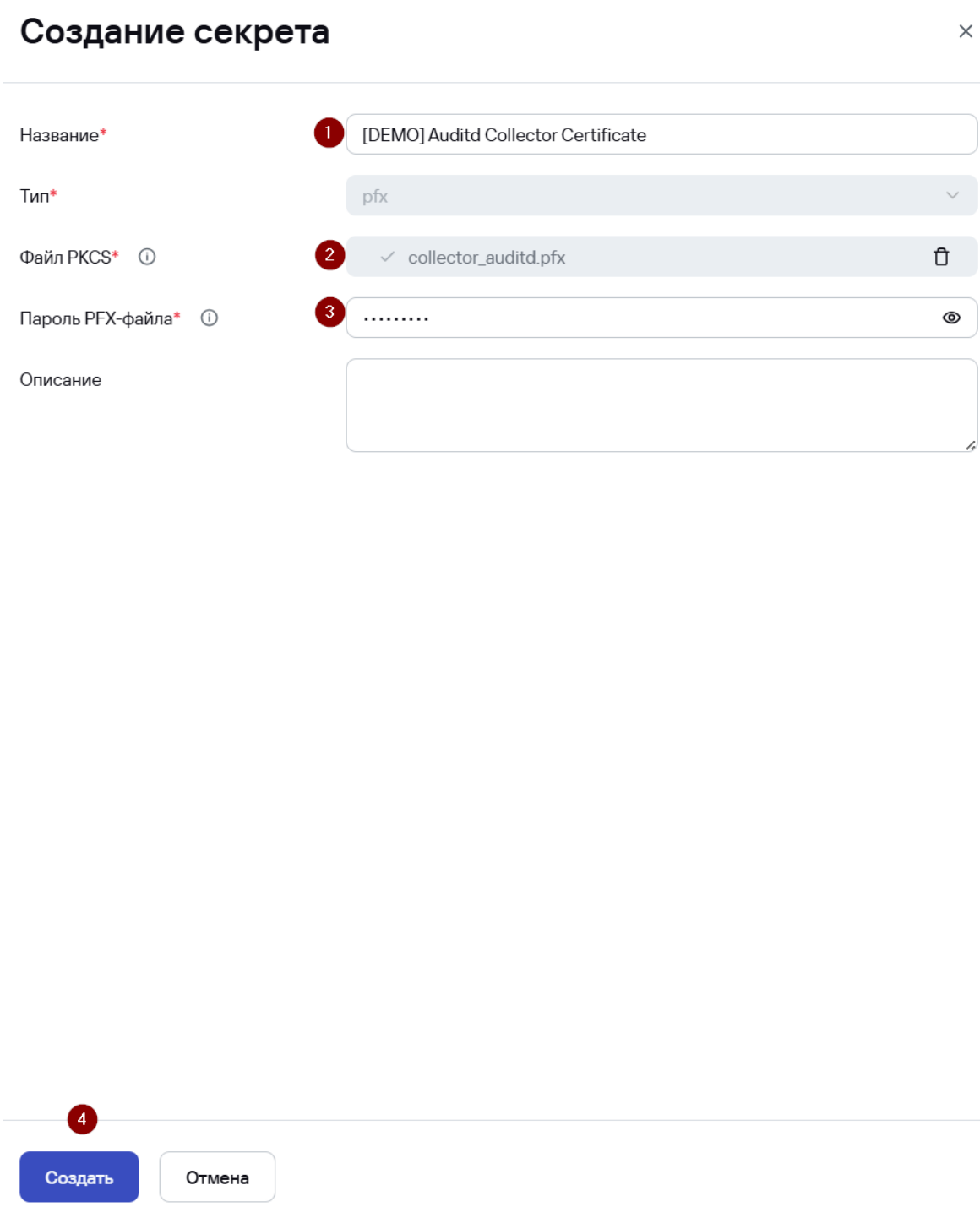
> Перед выполнением шагов по настройке создайте PFX-файл, содержащий закрытый ключ и сертификат, для использования в коллекторе auditd. **Важно**, чтобы в поле **CN** или **subject_alt_name** сертификата были указаны FQDN сервера коллектора или его IP-адрес.

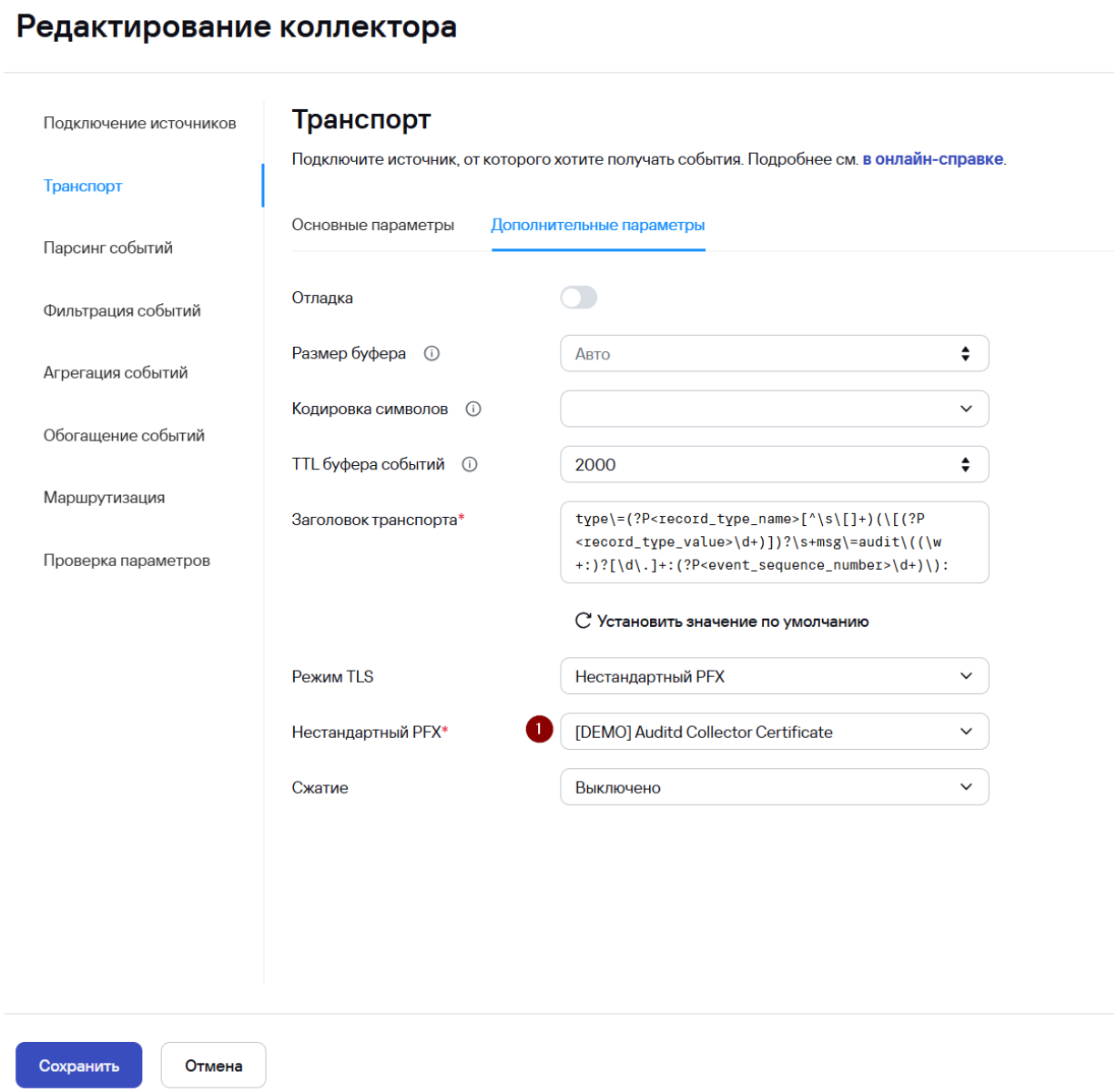
Для передачи событий auditd с рабочей станции/сервера в коллектор KUMA с использованием TLS с валидацией сертификата:

- В веб-интерфейсе KUMA:
  - Перейдите в раздел **Ресурсы → Активные сервисы** и выберите ранее созданный коллектор для приема и обработки событий auditd.
  - В появившемся окне **Редактирование коллектора** перейдите на вкладку **Дополнительные параметры**:
    - В параметре **Режим TLS** выберите **Нестандартный PFX**.
    - В параметре **Нестандартный PFX** нажмите **Создать**.

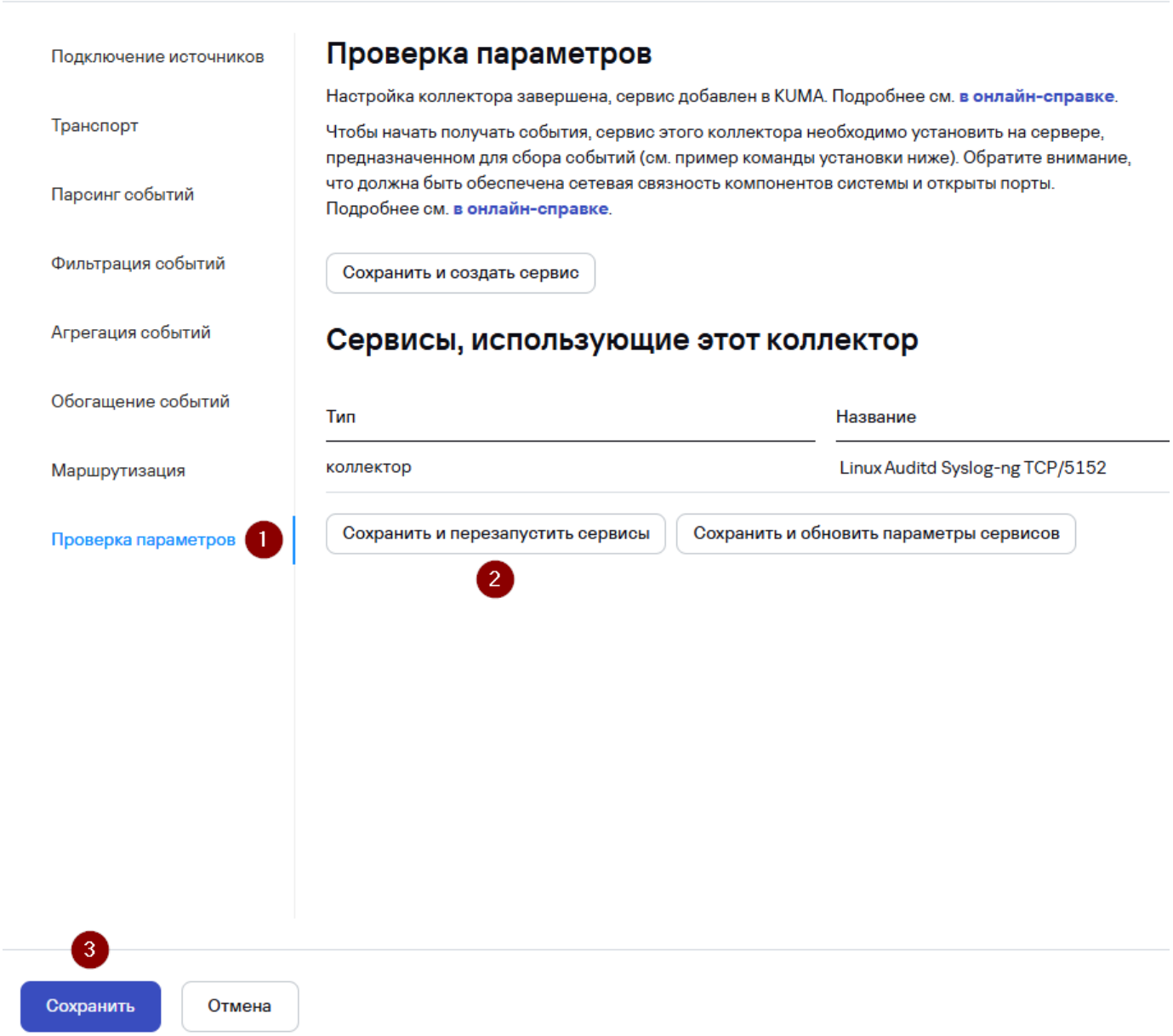


- В появившемся окне **Создание секрета** укажите:
  - **Название** секрета, например, [DEMO] Auditd Collector Certificate
  - **Файл PKCS** - выберите ранее созданный для коллектора auditd PFX-файл.
  - Введите **Пароль PFX-файла**
  - Нажмите **Создать**.


Создание секрета
Название*
1
[DEMO] Auditd Collector Certificate
Тип*
pfx
Файл PKCS*
2
collector_auditd.pfx
Пароль PFX-файла*
3
Описание
4
Создать
Отмена



- Перейдите на шаг **Проверка параметров** и нажмите **Сохранить и перезапустить сервисы**.
- Нажмите **Сохранить**.



- На рабочей станции/сервере Linux:
  - Загрузите в папку `/etc/syslog-ng/cert` сертификат удостоверяющего центра (CA), который выдал сертификат для коллектора auditd.
  - Перейдите в папку `/etc/syslog-ng/cert` и выполните команду:

```
openssl x509 -noout -hash -in <Имя CA-сертификата>.pem
```

  - Результатом выполнения команды будет хэш (например, e1442ae8) — последовательность символов, сгенерированная на основе Distinguished Name сертификата.
  - Выполните следующую команду, чтобы создать символическую ссылку на сертификат, используя хэш, полученный на предыдущем шаге, и добавьте суффикс `.0`:

```
ln -s <Имя CA-сертификата>.pem <Хэш>.0
```

- В результате папка `/etc/syslog-ng/cert` должна содержать CA-сертификат и символическую ссылку:

- Далее в папке `/etc/syslog-ng/conf.d/` создайте файл конфигурации (например, `30-kuma-tls-validation.conf`) со следующим содержанием:

```
# syslog-ng audit forwarding to KUMA (TCP with TLS and certificate validation)
# Version: 1
# Date: 10.02.2026
# Purpose: Forward auditd logs without parsing, loss-minimized

source s_audit {
    file("/var/log/audit/audit.log"
            flags(no-parse) # Читаем audit.log без парсинга (flags(no-parse)), чтобы "не ломать" формат auditd.
                follow-freq(1)
                tags("tag_audit_log")
                persist-name("kuma_audit_source")); # Необходим для сохранения состояния источника между рестартами syslog-ng.
};

template t_audit_format {
    template("<134>${ISODATE} ${HOST} auditd ${MSG}\n"); # <PRI> задан вручную, т.к. при flags(no-parse) ${PRI} не извлекается из события. Тег auditd задан руками, иначе будет дефолтное 0d.
    template_escape(no);
};

destination d_kuma {
    network("<IP-адрес/FQDN коллектора KUMA>" port(<Порт коллектора KUMA>)
            template(t_audit_format)
            disk-buffer(
                    mem-buf-size(10000) # Размер буфера в RAM, в количестве сообщений. Пока
```

```
есть место — ничего не пишется на диск. Можно увеличить при большом потоке событий.
                        disk-buf-size(1G) # Максимальный размер буфера на диске. Когда RAM-буфер будет заполнен, запись продолжится на диск. Можно увеличить при большом потоке событий.
                        reliable(yes) # Для гарантированной доставки. События не теряются при рестарте syslog-ng, проблем с сетью, перезапуске коллектора.
            )
                transport("tls")
                tls(
                    ca_dir("/etc/syslog-ng/cert/")
                    peer-verify(required-trusted)
                )
    );
};

filter f_audit_kuma {
    tags("tag_audit_log");
};

log {
    source(s_audit);
    filter(f_audit_kuma);
    destination(d_kuma);
};
```

- Удалите или переименуйте ранее созданный файл конфигурации для отправки событий по TCP, например, `30-kuma-tcp.conf.backup`
- Далее выполните проверку конфигурации syslog-ng:

```
syslog-ng -s
```

- Если ошибки при проверке конфигурации отсутствуют перезапустите сервис syslog-ng, выполнив следующую команду:

```
systemctl restart syslog-ng
```

Рабочая станция/сервер Linux настроены. События передаются в коллектор KUMA с использованием TLS и валидацией сертификата.

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

https://syslog-ng.github.io/admin-guide/README

https://syslog-ng.github.io/admin-guide/100_TLS-encrypted_message_transfer/001_Encrypting_log_messages_with_TLS/000_Configuring_TLS_client

---

Revision #16
Created 2023-10-04 07:15:23 UTC by Boris Rzr
Updated 2026-02-10 09:47:08 UTC by Dmitry Borisov