Сбор событий AuditD с помощью Rsyslog

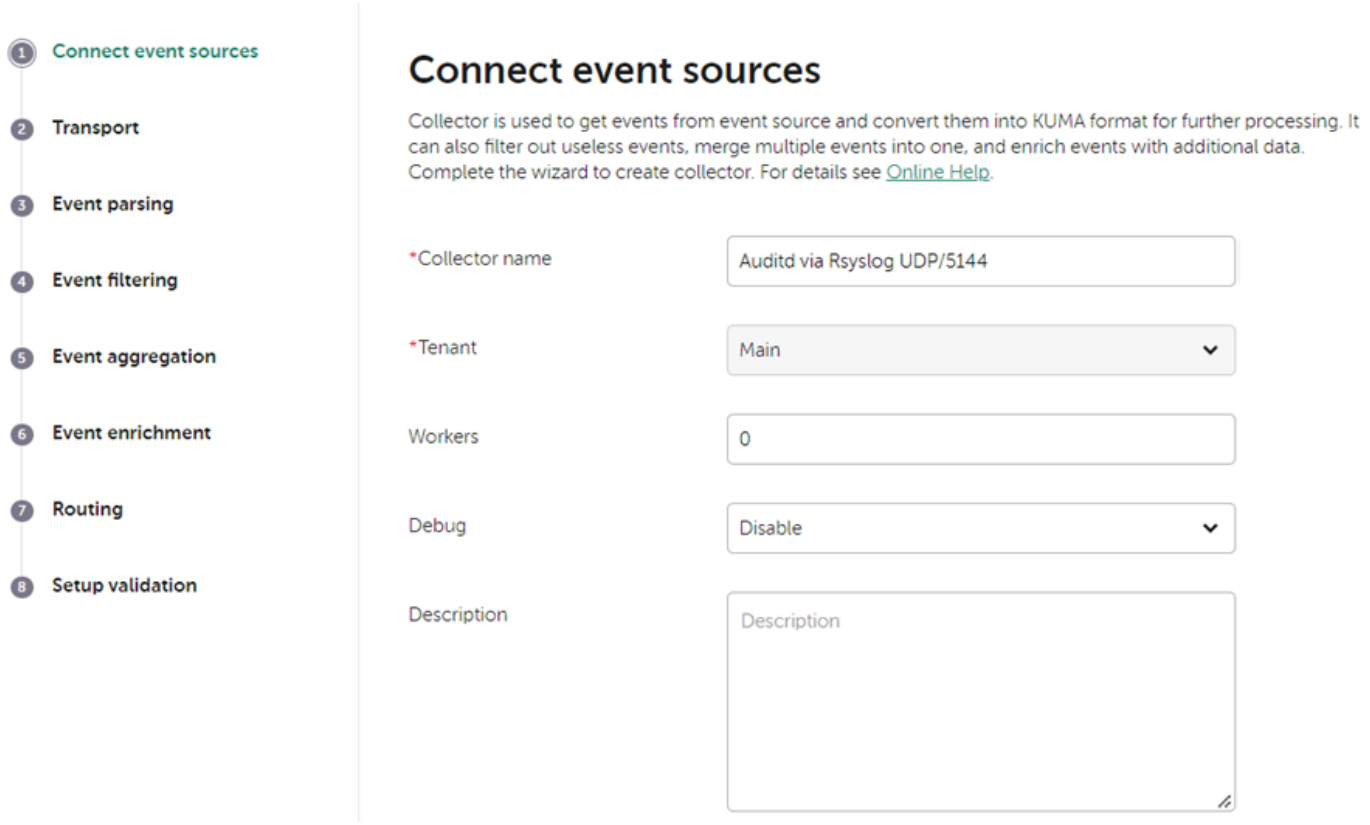
> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

> Официальная документация по данному разделу приведена в Онлайн-справке на продукт: https://support.kaspersky.com/KUMA/2.1/ru-RU/239760.htm

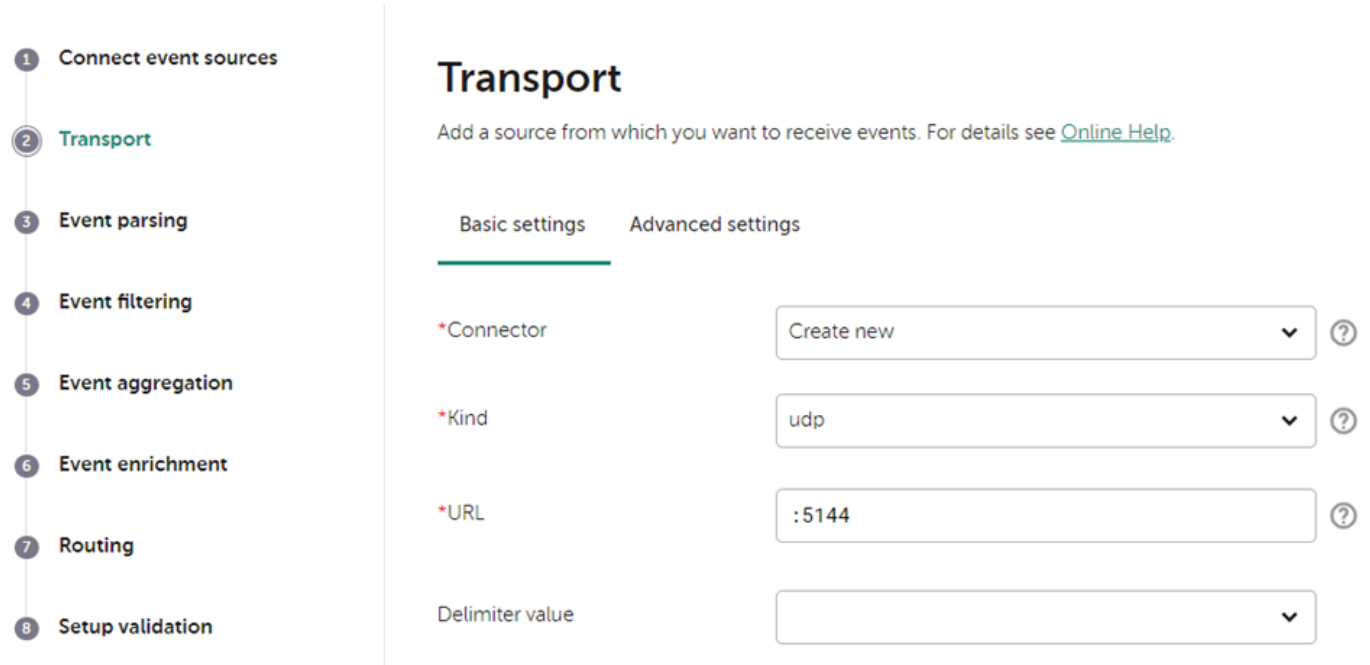
Создание коллектора KUMA

Для создания коллектора KUMA необходимо в веб-консоли KUMA перейти на вкладку **Ресурсы – Коллекторы** и нажать на кнопку **Добавить коллектор**. Также можно на вкладке **Ресурсы** выбрать пункт **Подключить источник**. В обоих случая откроется мастер подключения источников событий.

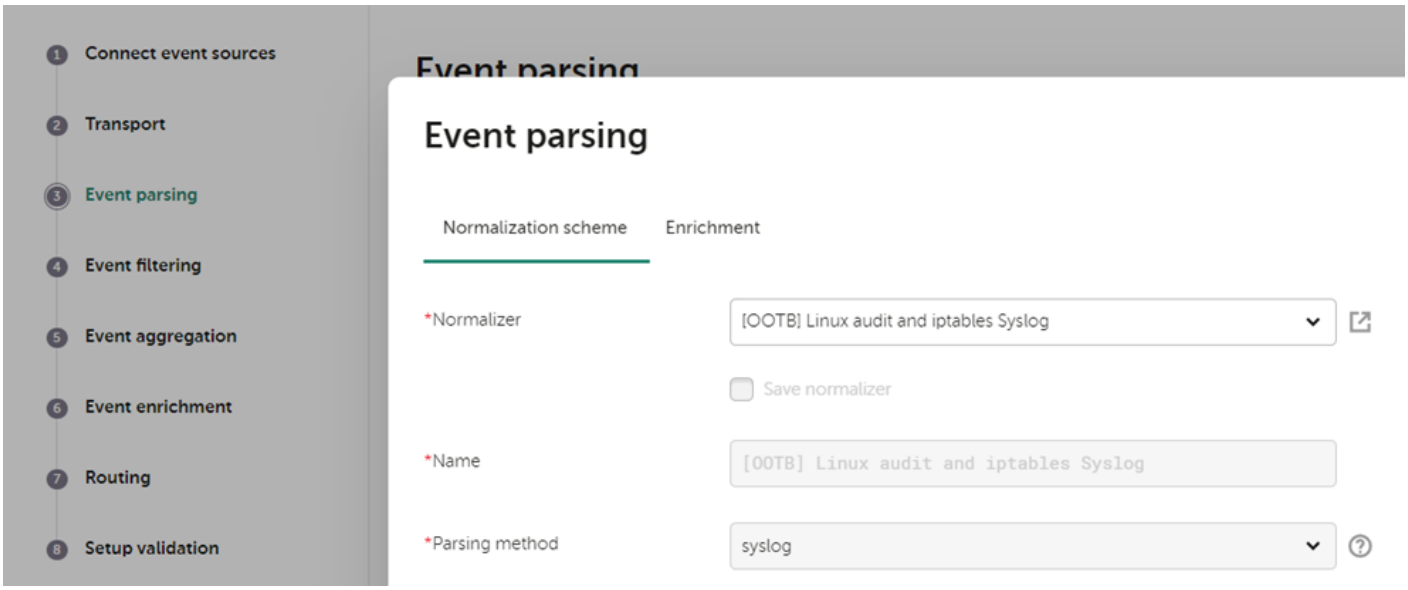
На первом шаге мастера необходимо выбрать **Тенант**, которому будет принадлежать коллектор и также задать **Имя** коллектора.



На втором шаге мастера необходимо выбрать тип подключения **udp** или **tcp** и указать **порт**, на котором коллектор будет ожидать входящие подключения. В данном примере выбран UDP/5144.

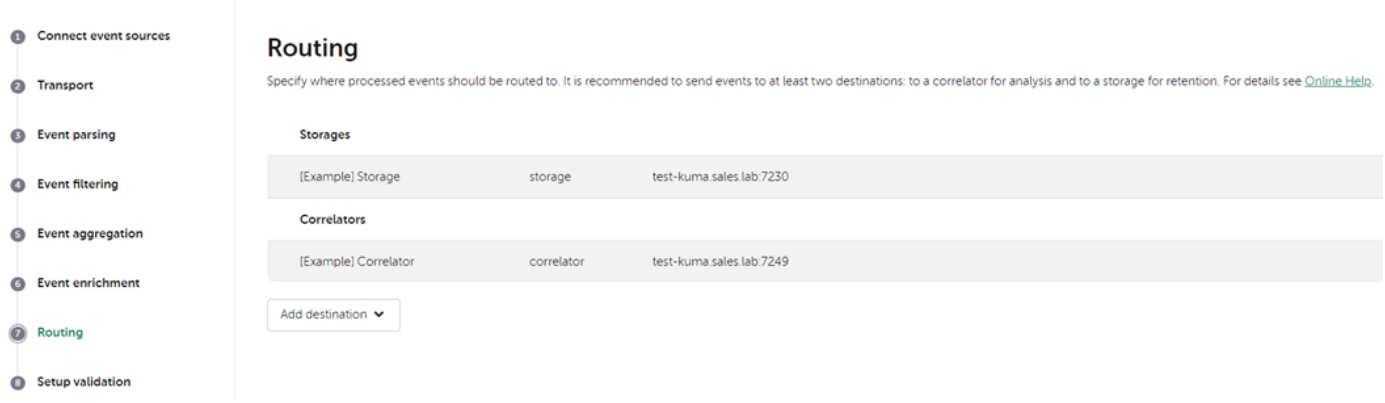


На третьем шаге мастера необходимо выбрать предустановленный нормализатор **[OOTB] Linux Audit and iptables Syslog (либо парсер AuditD из PreSales Pack)**. В случае отсутствия указанного нормализатора, обратитесь к своему менеджеру для его получения.

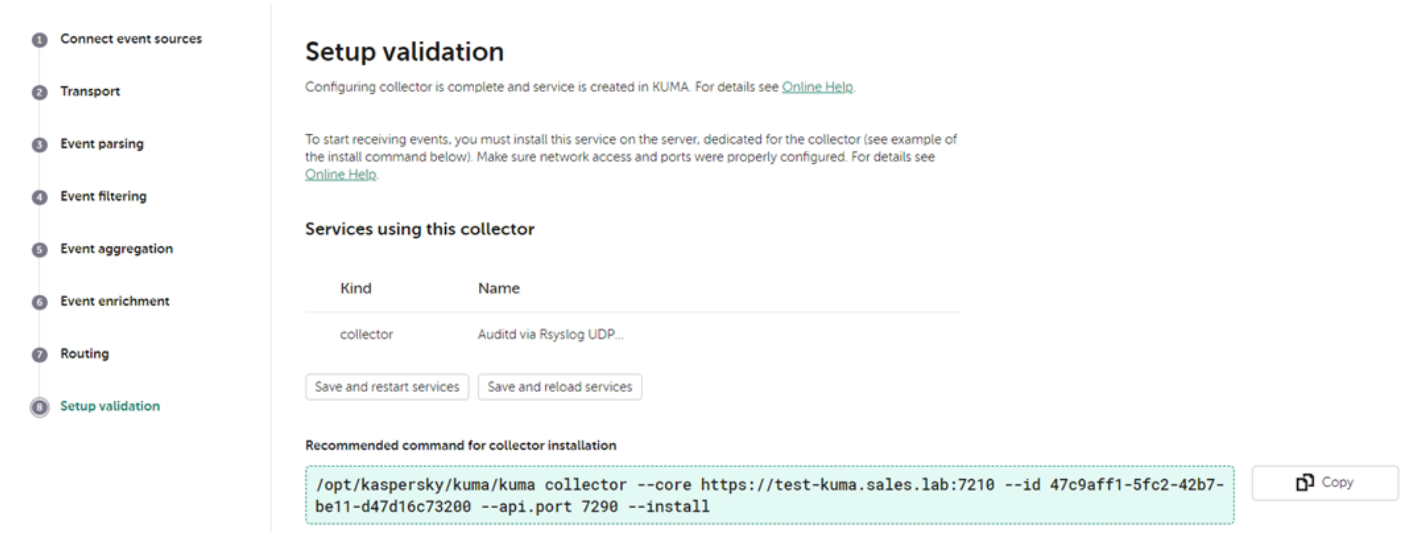


Шаги мастера с четвертого по шестой можно пропустить, либо заполнить позднее по своему усмотрению.

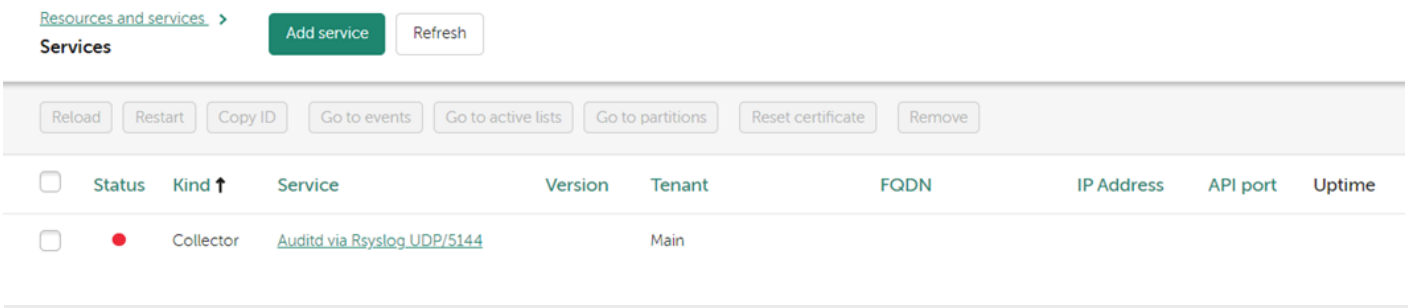
На седьмом шаге мастера необходимо указать точки назначения типа **Хранилище**, если требуется сохранение событий в БД и типа **Коррелятор**, если требуется корреляция событий.



На последнем шаге мастера необходимо нажать на кнопку **Сохранить и создать сервис**, после чего скопировать появившуюся команду для дальнейшей установки сервиса коллектора.



В результате на вкладке **Ресурсы – Активные сервисы** появится созданный сервис коллектора.



Установка коллектора KUMA

Для установки сервиса коллектора необходимо подключиться к консоли сервера коллектора KUMA.

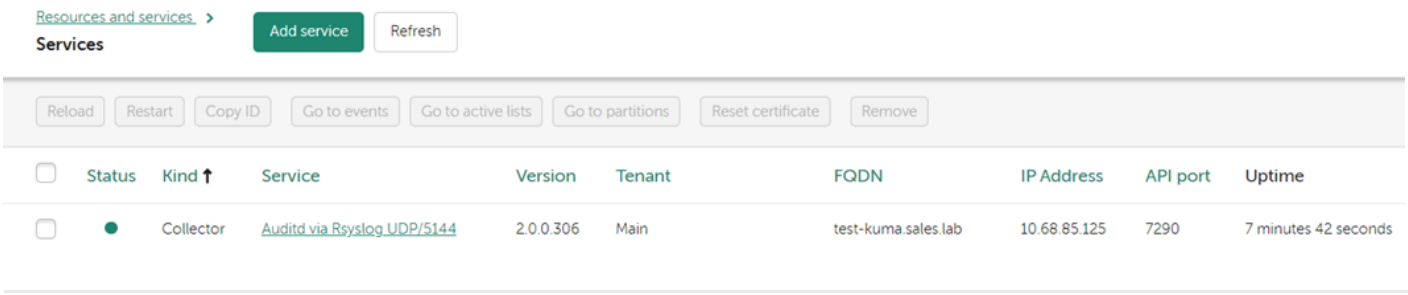
Для установки сервиса коллектора необходимо выполнить скопированную команду.

```
[root@test-kuma ~]# /opt/kaspersky/kuma/kuma collector --core https://test-kuma.sales.lab:7210 --id 4882d631-eae4-4c85-ba64-1efecf9ce744
--api.port 7286 --install
Created symlink /etc/systemd/system/multi-user.target.wants/kuma-collector-4882d631-eae4-4c85-ba64-1efecf9ce744.service → /usr/lib/system
d/system/kuma-collector-4882d631-eae4-4c85-ba64-1efecf9ce744.service.
[root@test-kuma ~]#
```

Также необходимо добавить порт коллектора в исключения фаервола и обновить параметры службы

```
firewall-cmd --add-port=5144/udp --permanent
firewall-cmd --reload
```

В результате статус коллектора в веб-интерфейсе KUMA изменится на **зеленый**.



Настройка сервера источника логов

> В случае наличия ошибок с доступом журналов, попробуйте отключить SELinux. Отключение SELinux вручную — SELINUX = Disabled в /etc/selinux/config и затем setenforce 0, команда getenforce для проверки.

На сервере источнике логов проверьте наличие сервиса **RSyslog** в системе:

```
systemctl status rsyslog.service
```

```
[root@test-kuma ~]# systemctl status rsyslog.service
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2022-09-12 16:16:24 MSK; 6 days ago
     Docs: man:rsyslogd(8)
           https://www.rsyslog.com/doc/
 Main PID: 3434786 (rsyslogd)
    Tasks: 3 (limit: 100357)
   Memory: 196.0M
   CGroup: /system.slice/rsyslog.service
           └─3434786 /usr/sbin/rsyslogd -n
```

В случае отсутствия сервиса его необходимо установить и запустить:

```
yum install rsyslog
systemctl enable rsyslog.service
systemctl start rsyslog.service
```

Далее в папке **/etc/rsyslog.d** необходимо создать файл **audit.conf** следующего содержания:

```
vi /etc/rsyslog.d/audit.conf
```

```
$ModLoad imfile
$InputFileName /var/log/audit/audit.log
$InputFileTag tag_audit_log:
```

```
$InputFileStateFile audit_log
$InputFileSeverity info
$InputFileFacility local6
$InputRunFileMonitor

local6.* @<ip адрес коллектора KUMA>:<порт коллектора KUMA>
```

Для отправки событий по протоколу TCP последнюю строчку следует заменить на:

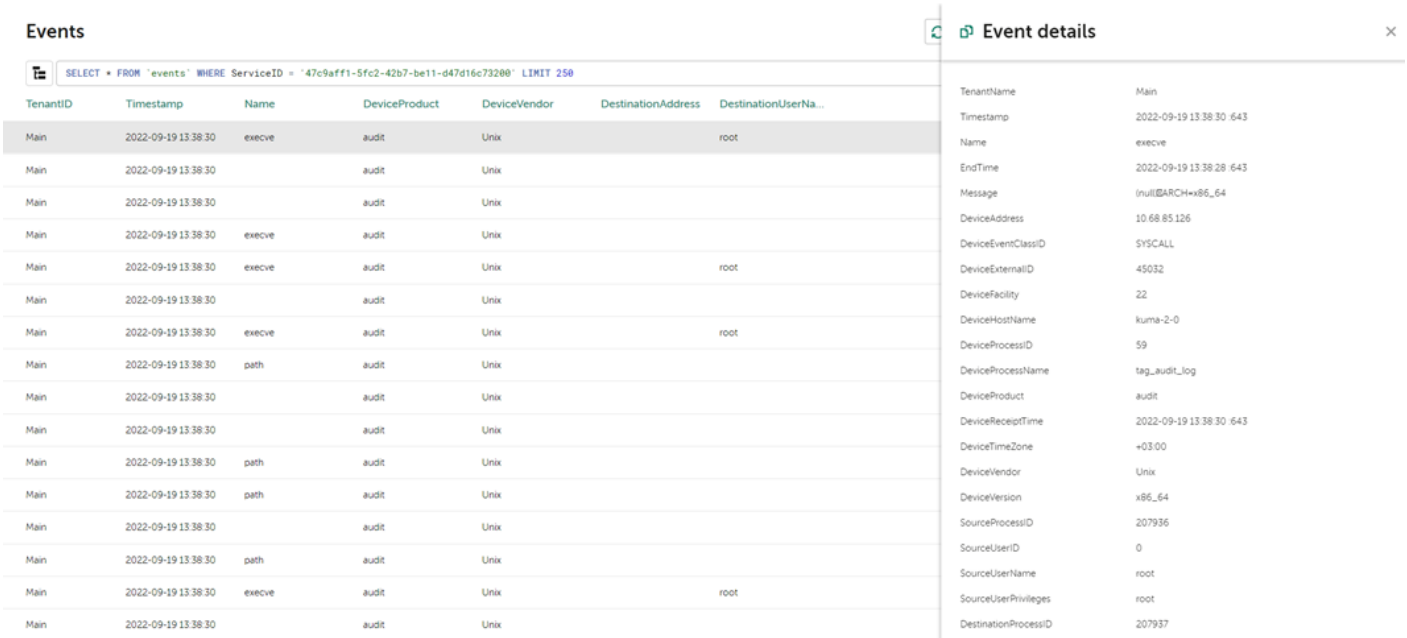
```
local6.* @@<ip адрес коллектора KUMA>:<порт коллектора KUMA>
```

После сохранения изменений в файле необходимо перезапустить сервис Rsyslog командой:

```
systemctl restart rsyslog.service
```

Проверка поступления событий

Для проверки поступления событий выберите соответствующий коллектор и нажмите на кнопку **Перейти к событиям**. В открывшемся окне события при нажатии на значок лупы должны появиться события **Auditd**.



Отправка лога без заголовка syslog

Иногда необходимо отпралять события без заголовка, в этом случае используются шаблоны, ниже пример использования в конфиге:

```
$template onlyMSG,"%msg%\n"
$ModLoad imfile
$InputFileName /var/log/audit/audit.log
$InputFileTag tag_audit_log:
$InputFileStateFile audit_log
$InputFileSeverity info
$InputFileFacility local6
$InputRunFileMonitor

local6.* @<ip адрес коллектора KUMA>:<порт коллектора KUMA>;onlyMSG
```

Revision #9
Created 14 August 2023 07:20:28 by Boris Rzr
Updated 24 January 2025 10:27:55 by Koala