Сбор событий auditd с помощью Rsyslog

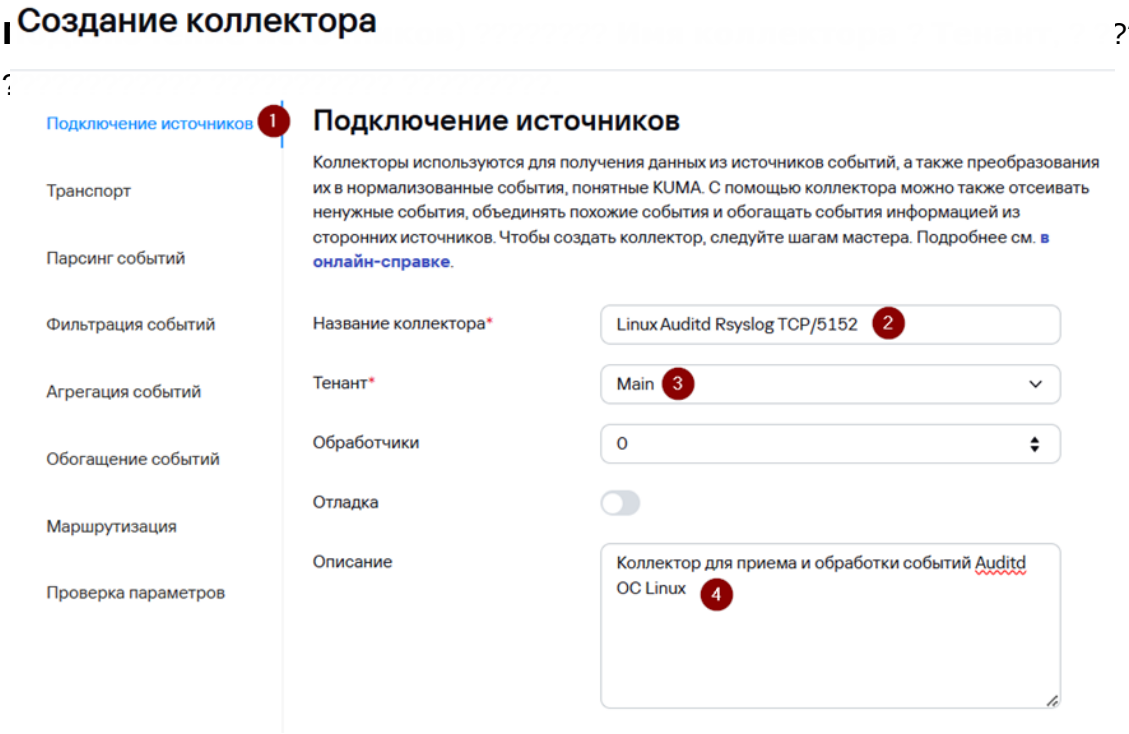
?????????, ??????????? ?? ?????? ????????, ???????? ??????????? ??????? pre-sales ?/??? community KUMA ? **НЕ** ???????? ??????????? ????????????? ???????.

??????????? ???????????? ?? ??????? ??????? ????????? ? ??????-??????? ?? ???????: https://support.kaspersky.ru/kuma/4.0/239760?page=help

Создание коллектора KUMA

1. ????????? ? ?????? **Ресурсы** ? ??????? ?? ?????? **Подключить источник**.

2. ? ??????????? ???? ??????? ????????? **Создание коллектора** ?? ?????? ???? (??????? ????? ?



3. ?? ?????? ???? ??????? (**Транспорт**) ??????? ????????? ?????????? ??? ????????????? ? ???????????? ??????????:

- **Тип** – tcp/udp. ? ?????? ??????? tcp

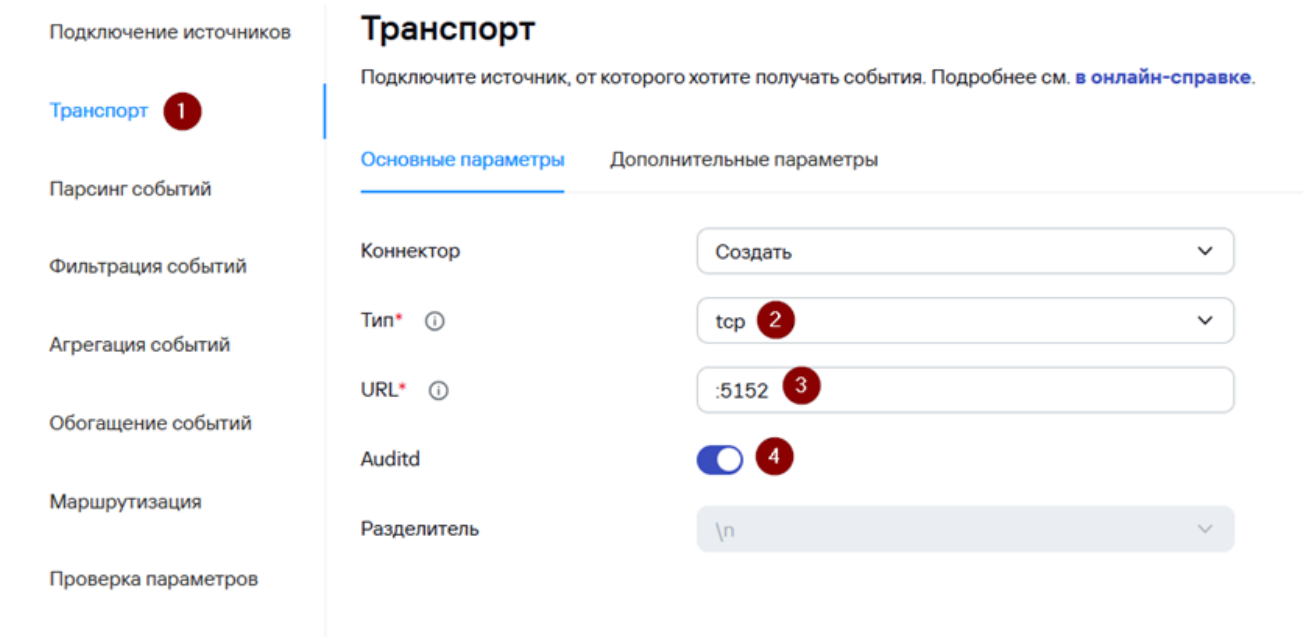
- **URL** – FQDN:???? (????, ?? ??????? ????????? ????? ??????? ???????? ???????????. ?????????? ????? ?? ?????????, ???? 1024). ? ?????? ??????? 5152.

- **Auditd –** ????????

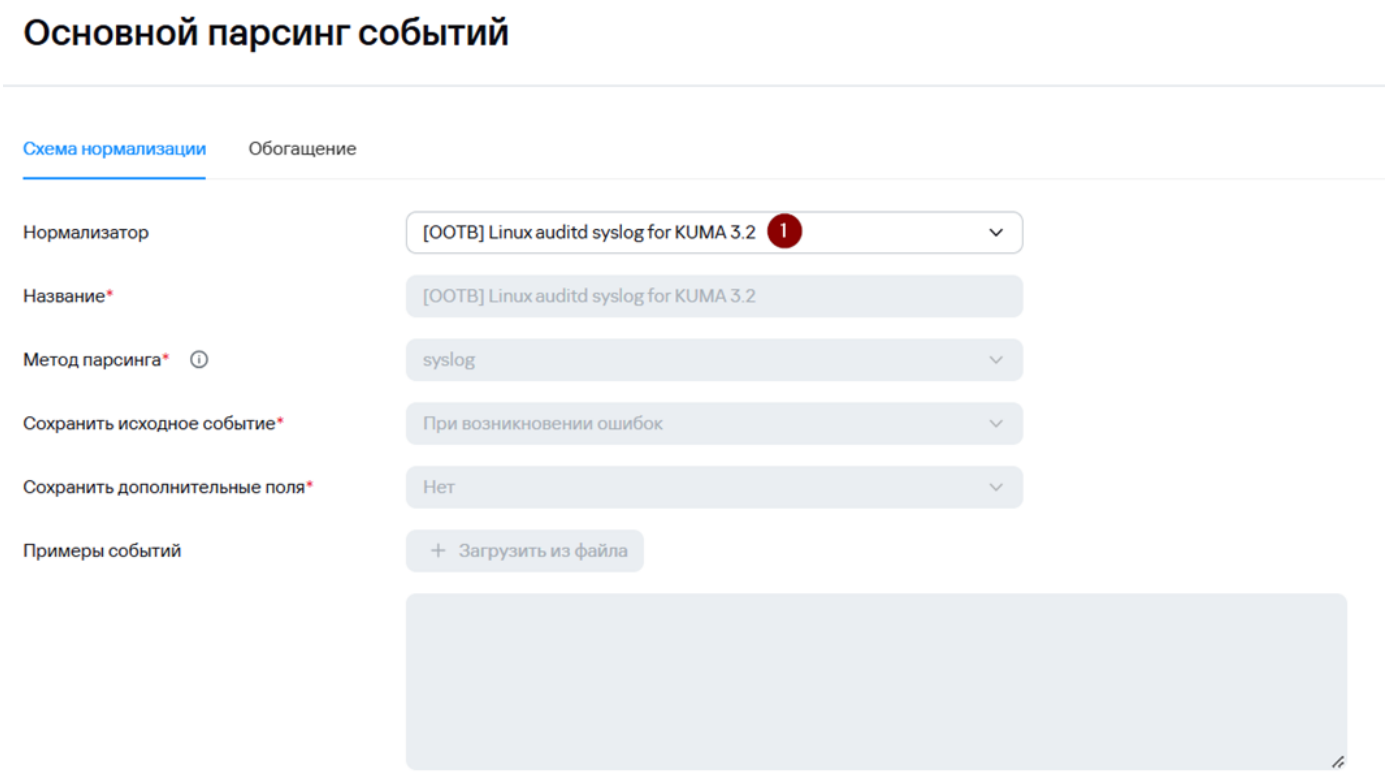
? ???? URL ????? ??????? ?????? ???? ??? ??????????? All-in-one

? ?????? KUMA 3.2 ???????? ????????????? Auditd, ??????? ????????? ???????????? ?????????? ?? ?????????? ?????? ??????? auditd ? ???? ??????? auditd.

Создание коллектора



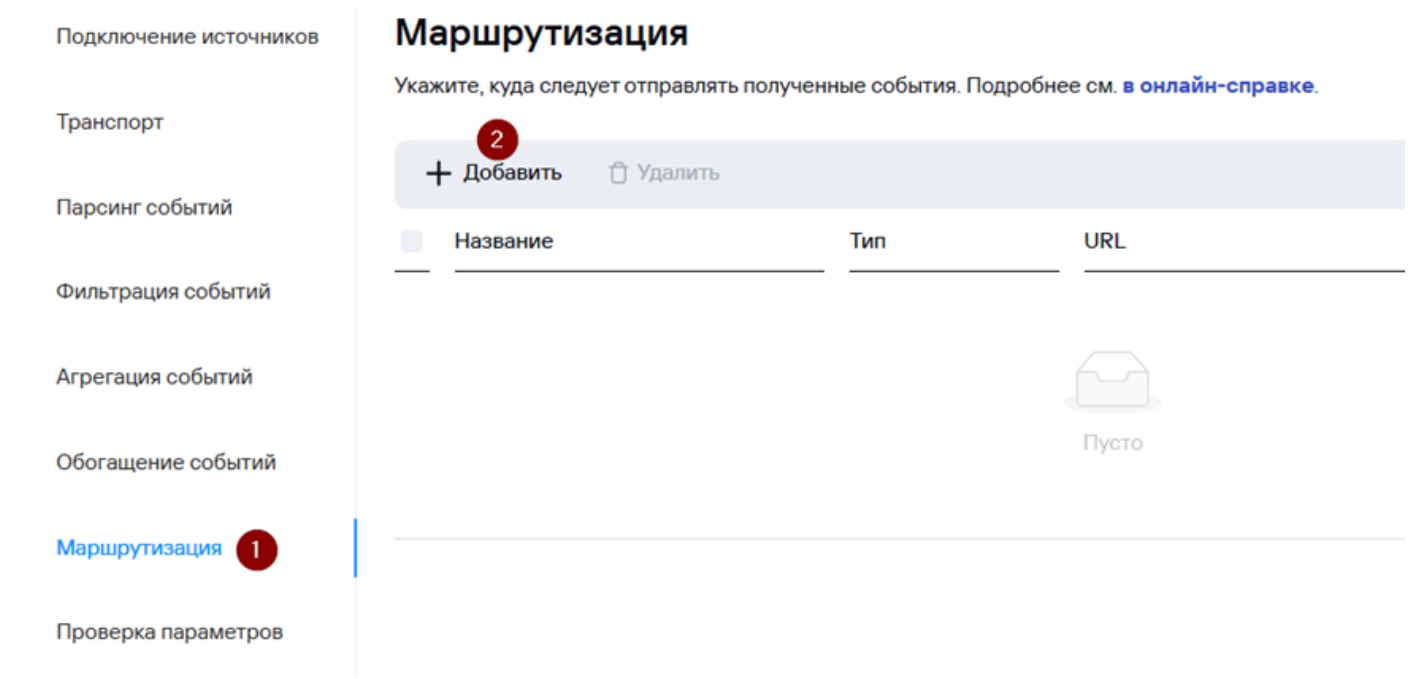
4. ?? ??????? ???? ??????? ??????? ????????????. ? ?????? ?????? ????????????? ????????????? «??????????» ????????????? ??? ??????? auditd Linux **[OOTB] Linux auditd syslog for KUMA 3.2**.



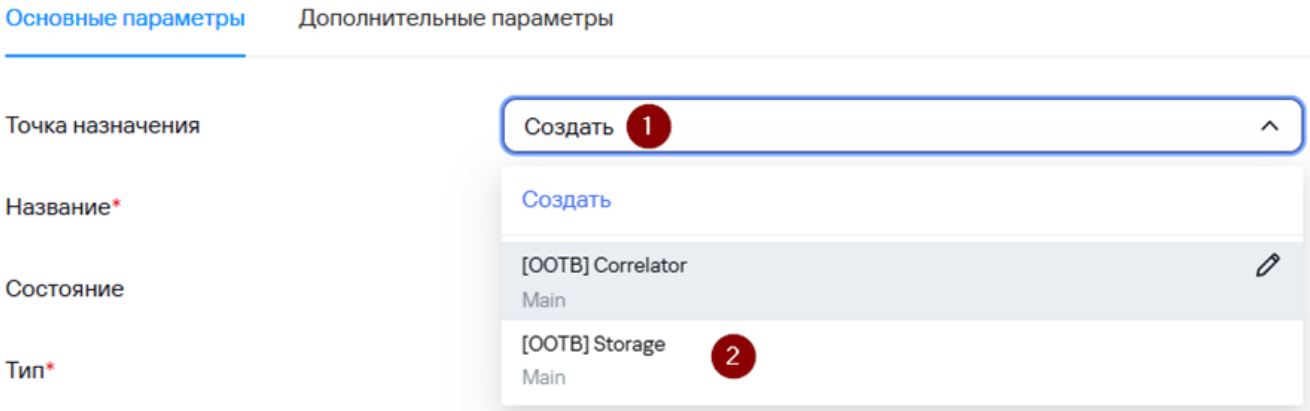
5. ???? ??????? ????????? ? ?????????? ?? ?????? ???????? ????????????, ?? ????? ?????????? ? ????????? ? ????????? ???????.

6. ?? ??????? ???? ??????? ??????? ????? ??????????. ??? ???????? ??????? ???????? ????? ?????????? ???? **Хранилище**. ? ?????? ???? ????????????? ????? ?????? ?????? ??????? ????????? ?????????? ???????? ????? ?????????? ???? **Коррелятор**.

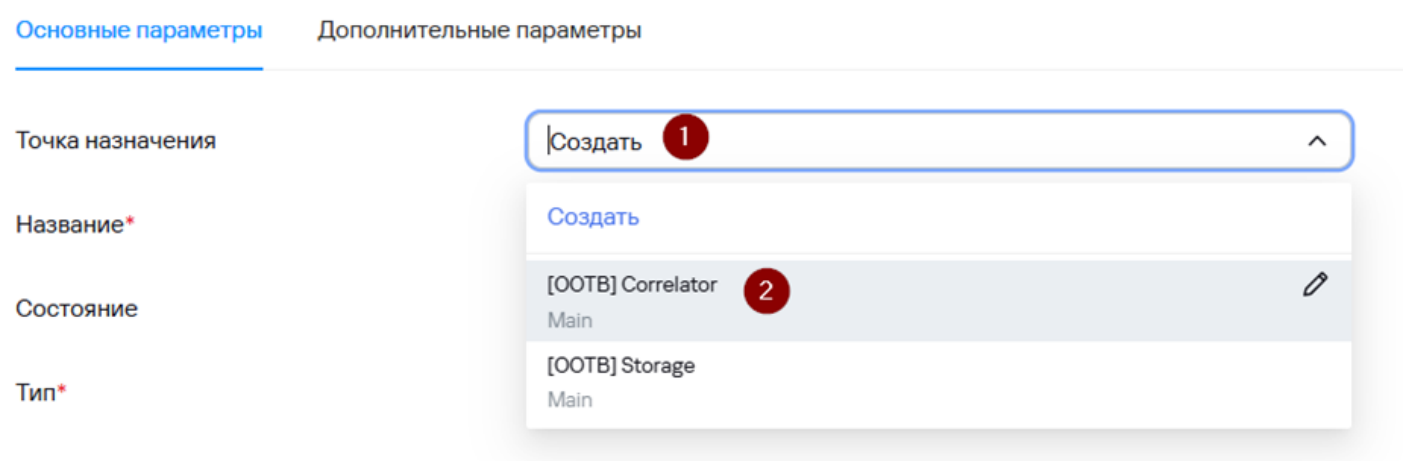
Создание коллектора



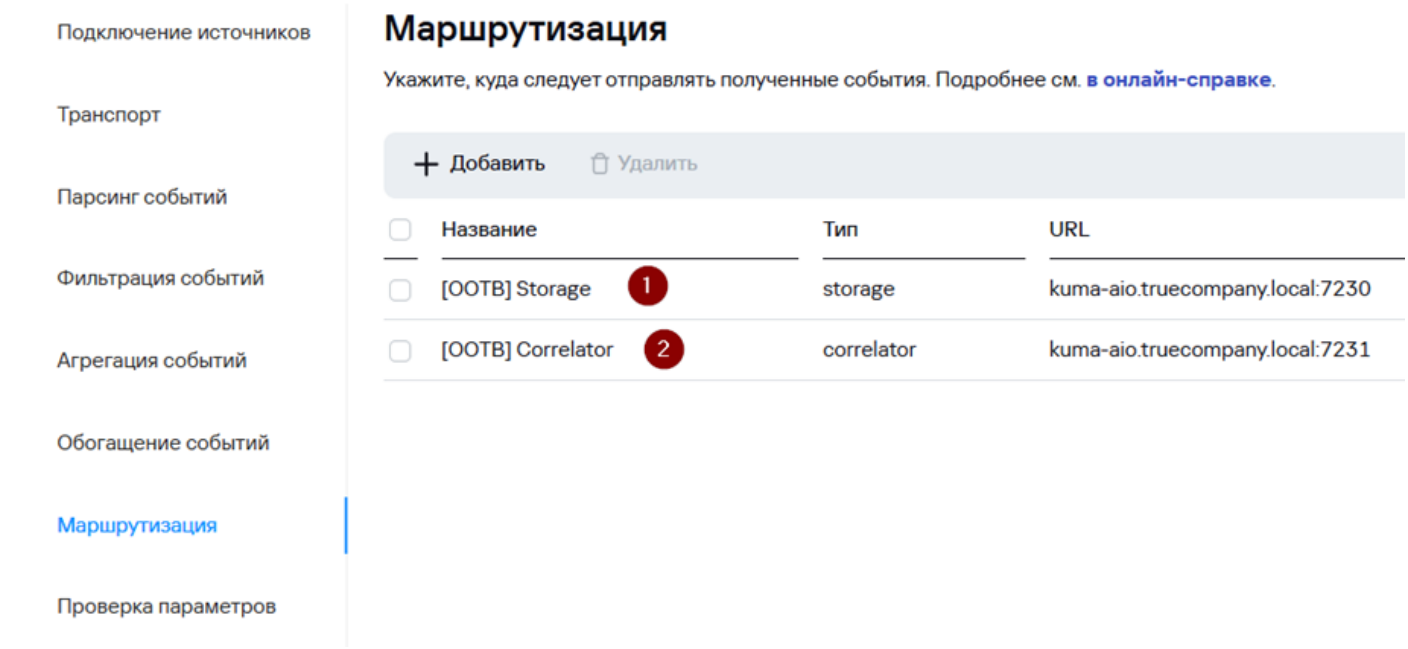
Создание точки назначения



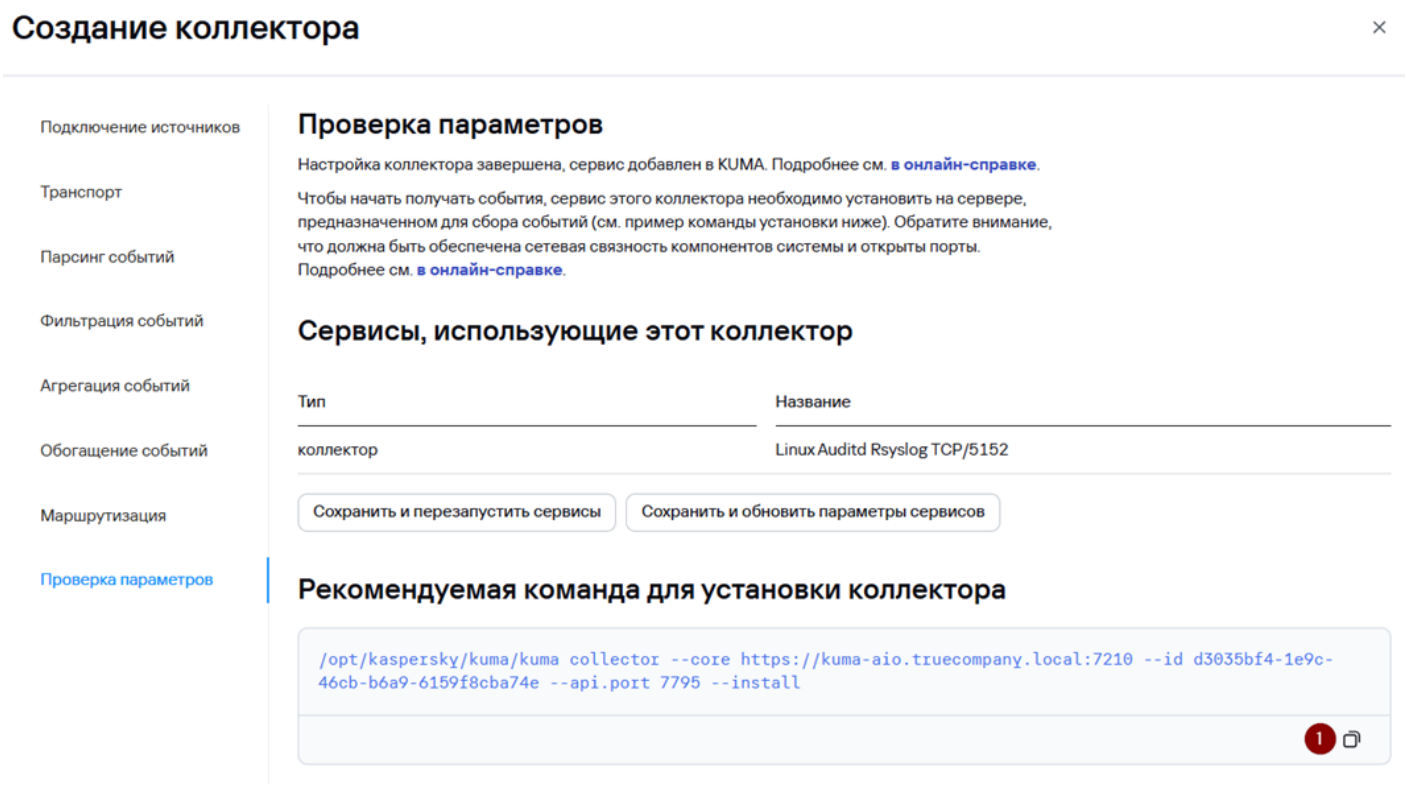
Создание точки назначения



Создание коллектора

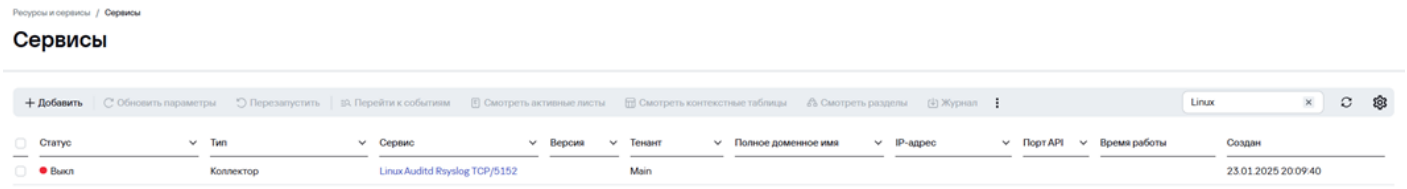


7. ?? ??????????? ???? ??????? ??????? ?? ?????? **Создать и сохранить сервис**. ????? ???? ???????? ?????? ????????? ???????, ??????? ?????????? ??????????? ??? ?????????? ?????????.



8. ??????? **Сохранить**.

9. ????? ?????????? ????????????? ???????? ? ??????? **Ресурсы → Активные сервисы** ???????? ????????? ?????? ??????????.



Установка коллектора KUMA

????? ?????????? ????????? KUMA:

1. ????????? ??????????? ? CLI ???????, ?? ??????? ??????????? ????????????? ?????????? KUMA.

2. ??? ????????? ??????? ?????????? ? ????????? ?????? ????????? ??????? ??? ??????? ??????? root, ????????????? ?? ??????? ????.

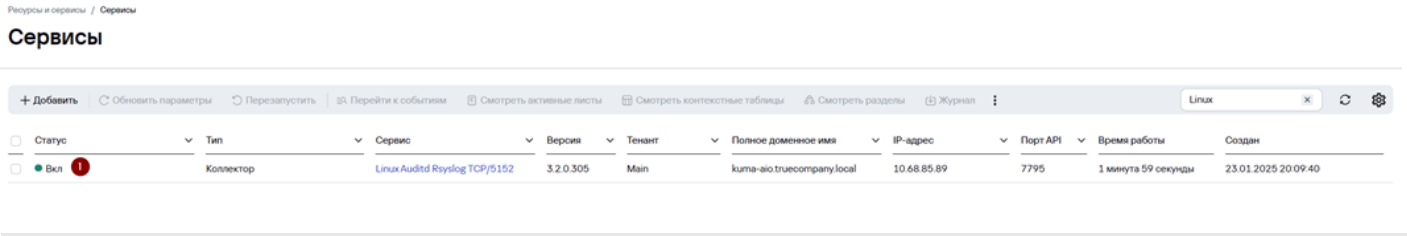
```
[root@test-kuma ~]# /opt/kaspersky/kuma/kuma collector --core https://test-kuma.sales.lab:7210 --id 4882d631-eae4-4c85-ba64-1efecf9ce744
--api.port 7286 --install
Created symlink /etc/systemd/system/multi-user.target.wants/kuma-collector-4882d631-eae4-4c85-ba64-1efecf9ce744.service → /usr/lib/system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

3. ??? ????????????? ???????? ??????????? ???? ??????? ?????????? ? ?????????? ?? ?? ? ???????? ????????? ??????.

```
# ?????? ??? firewalld
firewall-cmd --add-port=<????, ????????? ??? ??????????>/tcp|udp –permanent
firewall-cmd –reload

# ?????? ??? ufw
ufw allow <????, ????????? ??? ??????????>/tcp|udp
ufw reload
```

4. ????? ???????? ????????? ??????? ??? ?????? ? ???-??????? KUMA ????????? ?? ??? ? **зеленой индикацией**.



Настройка сервера источника логов

?? GitHub'? ???????? community-?????? ??? ????????????? ????????? ???????? ??????? ? Linux-??????: https://github.com/KUMA-Community/kuma_auditd

? ?????? ??????? ?????? ? ???????? ????????, ?????????? ????????? SELinux. ?????????? SELinux ??????? — SELINUX = Disabled ? /etc/selinux/config ? ????? setenforce 0, ??????? getenforce ??? ????????.

1. ?? ??????? ????????? ????? ????????? ??????? ??????? **RSyslog** ? ???????:

```
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
```

2. ? ?????? ?????????? ??????? ??? ?????????? ?????????? ? ?????????:

```
# ??? ?? Oracle Linux
yum install rsyslog
systemctl enable rsyslog.service
systemctl start rsyslog.service

# ??? Astra Linux ? Ubuntu
apt install rsyslog
systemctl enable rsyslog.service
systemctl start rsyslog.service

# ??? ??
dnf install rsyslog
systemctl enable rsyslog.service
systemctl start rsyslog.service
```

3. ????????????? ???? ???????? ??????? audit.service /etc/audit/auditd.conf ? ???????? ???????? ????????? name_format, ???????? ????? ????????? ???????? NONE:

```
name_format=NONE
```

4. ????? ????????? ???????? ????????????? ?????? auditd ? ??????? ???????:

```
sudo systemctl restart auditd.service
```

5. ????? ? ????? **/etc/rsyslog.d** ?????????? ??????? ???? **audit.conf** ?????????? ??????????:

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

- ??? ???????? ??????? ?? ????????? TCP (??? ? ????? ???????)

```
$ModLoad imfile
$InputFileName /var/log/audit/audit.log
$InputFileTag tag_audit_log:
$InputFileStateFile audit_log
$InputFileSeverity info
$InputFileFacility local6
$InputRunFileMonitor
*.* @@<ip ????? ?????????? KUMA>:<???? ?????????? KUMA>
```

????????:
. @@10.68.85.89:5152

- ??? ???????? ??????? ?? ????????? UDP

```
$ModLoad imfile
$InputFileName /var/log/audit/audit.log
$InputFileTag tag_audit_log:
$InputFileStateFile audit_log
$InputFileSeverity info
$InputFileFacility local6
$InputRunFileMonitor
template(name="AuditFormat" type="string" string="<%PRI%>%TIMESTAMP:::date-rfc3339% %HOSTNAME% %syslogtag%
%msg%\n")
```

```
*.* @<ip ????? ?????????? KUMA>:<???? ?????????? KUMA>;AuditFormat
```

????????:

. @10.68.85.89:5152;AuditFormat

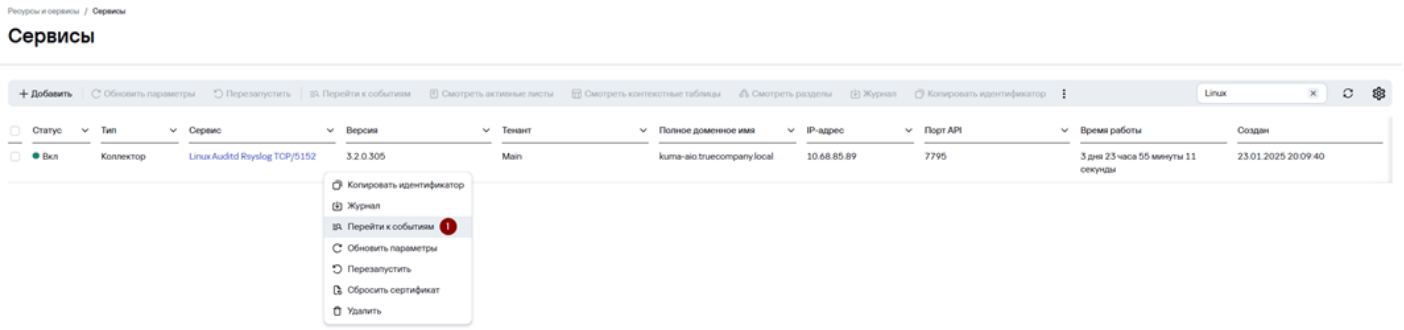
6. ????? ?????????? ????????? ? ????? ?????????? ????????????? ?????? Rsyslog ????????:

```
systemctl restart rsyslog.service
```

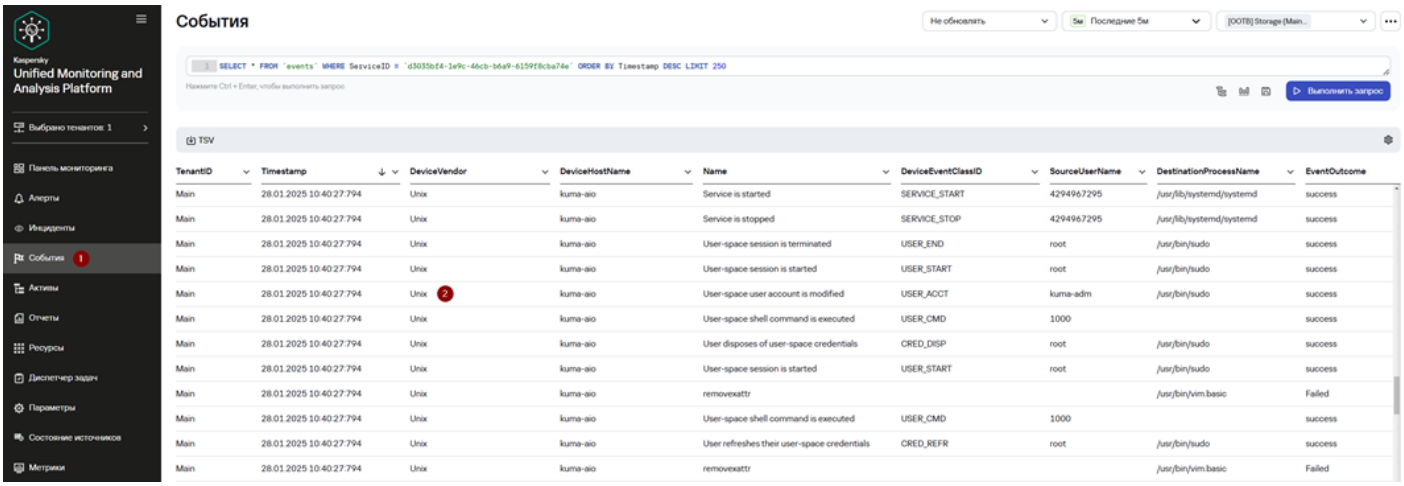
??????? ???????/?????? Linux ????????. ??????? ?????????? ? ????????? KUMA.

Проверка поступления событий

1. ??? ????????, ??? ???? ??????? ? ????????? Linux ??????? ???????? ????????? ? **Ресурсы** ? **Активные сервисы** ? ???????? ????? ????????? **коллектор** ??? Linux ? ??????? **Перейти к событиям.**



2. ? ??????????? ???? **События** ?????????, ??? ???????????? ??????? ? ????????? Linux.



Отправка с TLS

????????????? ????? ?????????? ????????????? ????? ??? ???????????? TLS:

```
apt install rsyslog-gnutls
```

????? ?????? ??????:

```
nano /etc/rsyslog.d/50-auditd-tls.conf
```

?? ????????? ?????????? (??? ?????????? ?????????? ???????):

```
# Load necessary modules
$ModLoad imfile
$ModLoad omfwd
$ModLoad gtls

# TLS settings
$DefaultNetstreamDriver gtls
$ActionSendStreamDriverMode 1       # TLS-only
$ActionSendStreamDriverAuthMode anon  # No server certificate validation
# No CA or client certs needed for anon mode

# Configure file monitoring for auditd log
$InputFileName /var/log/audit/audit.log
$InputFileTag tag_audit_log:
$InputFileStateFile audit_log
$InputFileSeverity info
$InputFileFacility local6
$InputRunFileMonitor

# Forward log lines matching the audit log tag
if $programname == 'tag_audit_log' then @@<ip ????? ?????????? KUMA>:<???? ?????????? KUMA>
```

Конфиг TLS с верификацией сервера

```
$ActionSendStreamDriverAuthMode x509/name
$ActionSendStreamDriverPermittedPeer rsyslog-server
$DefaultNetstreamDriverCAFile /etc/rsyslog/ca.crt
```

????? ????????? ? ????? ?????????? ????????????? ?????? Rsyslog ????????:

```
systemctl restart rsyslog.service
```

Отправка лога без заголовка syslog

?????? ?????????? ????????? ??????? ??? ?????????, ? ???? ?????? ???????????? ???????, ???? ?????? ????????????? ? ???????:

```
$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 ????? ?????????? KUMA>:<???? ?????????? KUMA>;onlyMSG
```

Полезные ссылки:

- ????????????? ???????? ?????? ?????? auditd: https://kb.kuma-community.ru/books/podkliucenie-istocnikov/page/nastroika-auditd-na-unix-sistemax
- ?????? ??????-??????? «????????? ????????? ??????? Auditd»: https://support.kaspersky.ru/kuma/3.2/239760
- ?????? KUMA Community «???? ??????? AuditD ? ??????? Rsyslog»: https://kb.kuma-community.ru/books/podkliucenie-istocnikov/page/sbor-sobytii-auditd-s-pomoshhiu-rsyslog

---

Revision #18
Created 2023-08-14 07:20:28 UTC by Boris Rzr
Updated 2026-08-04 11:26:15 UTC by Boris Rzr