

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 случаях откроется мастер подключения источников событий.

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

1 Connect event sources

2 Transport

3 Event parsing

4 Event filtering

5 Event aggregation

6 Event enrichment

7 Routing

8 Setup validation

Connect event sources

Collector is used to get events from event source and convert them into KUMA format for further processing. It can also filter out useless events, merge multiple events into one, and enrich events with additional data. Complete the wizard to create collector. For details see [Online Help](#).

*Collector name

Auditd via Rsyslog UDP/5144

*Tenant

Main

Workers

0

Debug

Disable

Description

Description

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.

1 Connect event sources

2 Transport

3 Event parsing

4 Event filtering

5 Event aggregation

6 Event enrichment

7 Routing

8 Setup validation

Transport

Add a source from which you want to receive events. For details see [Online Help](#).

Basic settings

Advanced settings

*Connector

Create new

*Kind

udp

*URL

:5144

Delimiter value

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.

1 Connect event sources

2 Transport

3 Event parsing

4 Event filtering

5 Event aggregation

6 Event enrichment

7 Routing

8 Setup validation

Event parsing

Normalization scheme Enrichment

*Normalizer

[OOTB] Linux audit and iptables Syslog

Save normalizer

*Name

[OOTB] Linux audit and iptables Syslog

*Parsing method

syslog

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.

1 Connect event sources

2 Transport

3 Event parsing

4 Event filtering

5 Event aggregation

6 Event enrichment

7 Routing

8 Setup validation

Routing

Specify where processed events should be routed to. It is recommended to send events to at least two destinations: to a correlator for analysis and to a storage for retention. For details see [Online Help](#).

Storages

[Example] Storage	storage	test-kuma.sales.lab:7230
-------------------	---------	--------------------------

Correlators

[Example] Correlator	correlator	test-kuma.sales.lab:7249
----------------------	------------	--------------------------

Add destination

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

1 Connect event sources

2 Transport

3 Event parsing

4 Event filtering

5 Event aggregation

6 Event enrichment

7 Routing

8 Setup validation

Setup validation

Configuring collector is complete and service is created in KUMA. For details see [Online Help](#).

To start receiving events, you must install this service on the server, dedicated for the collector (see example of the install command below). Make sure network access and ports were properly configured. For details see [Online Help](#).

Services using this collector

Kind	Name
collector	Auditd via Rsyslog UDP...

Save and restart services

Save and reload services

Recommended command for collector installation

```
/opt/kaspersky/kuma/kuma collector --core https://test-kuma.sales.lab:7210 --id 47c9aff1-5fc2-42b7-be11-d47d16c73200 --api.port 7290 --install
```

Copy

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

[Resources and services](#) >

Add service

Refresh

Reload

Restart

Copy ID

Go to events

Go to active lists

Go to partitions

Reset certificate

Remove

<input type="checkbox"/>	Status	Kind ↑	Service	Version	Tenant	FQDN	IP Address	API port	Uptime
<input type="checkbox"/>	<div></div>	Collector	Auditd via Rsyslog UDP/5144		Main				

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/systemd/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**.

Resources and services >
Services

Add service Refresh

Reload Restart Copy ID Go to events Go to active lists Go to partitions Reset certificate Remove

<input type="checkbox"/>	Status	Kind ↑	Service	Version	Tenant	FQDN	IP Address	API port	Uptime
<input type="checkbox"/>	●	Collector	Auditd via Rsyslog UDP/5144	2.0.0.306	Main	test-kuma.sales.lab	10.68.85.125	7290	7 minutes 42 seconds

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**.

Events							Event details	
SELECT * FROM 'events' WHERE ServiceID = '47c9aff1-5fc2-42b7-be11-d47d16c73200' LIMIT 250								
TenantID	Timestamp	Name	DeviceProduct	DeviceVendor	DestinationAddress	DestinationUserNa...	TenantName	Main
Main	2022-09-19 13:38:30	execve	audit	Unix		root	Timestamp	2022-09-19 13:38:30 :643
Main	2022-09-19 13:38:30		audit	Unix			Name	execve
Main	2022-09-19 13:38:30		audit	Unix			EndTime	2022-09-19 13:38:28 :643
Main	2022-09-19 13:38:30	execve	audit	Unix			Message	(null)BARCH=x86_64
Main	2022-09-19 13:38:30	execve	audit	Unix			DeviceAddress	10.68.85.126
Main	2022-09-19 13:38:30	execve	audit	Unix	root		DeviceEventClassID	SYSCALL
Main	2022-09-19 13:38:30		audit	Unix			DeviceExternalID	45032
Main	2022-09-19 13:38:30		audit	Unix			DeviceFacility	22
Main	2022-09-19 13:38:30	execve	audit	Unix	root		DeviceHostName	kuma-2-0
Main	2022-09-19 13:38:30	path	audit	Unix			DeviceProcessID	59
Main	2022-09-19 13:38:30		audit	Unix			DeviceProcessName	tag_audit_log
Main	2022-09-19 13:38:30		audit	Unix			DeviceProduct	audit
Main	2022-09-19 13:38:30		audit	Unix			DeviceReceiptTime	2022-09-19 13:38:30 :643
Main	2022-09-19 13:38:30	path	audit	Unix			DeviceTimeZone	+03:00
Main	2022-09-19 13:38:30	path	audit	Unix			DeviceVendor	Unix
Main	2022-09-19 13:38:30		audit	Unix			DeviceVersion	x86_64
Main	2022-09-19 13:38:30		audit	Unix			SourceProcessID	207936
Main	2022-09-19 13:38:30	path	audit	Unix			SourceUserID	0
Main	2022-09-19 13:38:30	execve	audit	Unix	root		SourceUserName	root
Main	2022-09-19 13:38:30		audit	Unix			SourceUserPrivileges	root
Main	2022-09-19 13:38:30		audit	Unix			DestinationProcessID	207937

Отправка лога без заголовка syslog

Иногда необходимо отправлять 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