

# ????? ?????????? 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.

### Создание коллектора

Подключение источников

1

#### Подключение источников

Коллекторы используются для получения данных из источников событий, а также преобразования их в нормализованные события, понятные KUMA. С помощью коллектора можно также отсеивать ненужные события, объединять похожие события и обогащать события информацией из сторонних источников. Чтобы создать коллектор, следуйте шагам мастера. Подробнее см. [в онлайн-справке](#).

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

Название коллектора\*

Linux Auditd Syslog-ng TCP/5152

2

Тенант\*

Main

3

Обработчики

0

Отладка



Описание

Коллектор для приема и обработки событий Auditd ОС Linux

4

- 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.

## Создание коллектора

Подключение источников

Транспорт **1**

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

### Транспорт

Подключите источник, от которого хотите получать события. Подробнее см. [в онлайн-справке](#).

Основные параметры

Дополнительные параметры

Коннектор

Создать

Тип\* ⓘ

tcp **2**

URL\* ⓘ

:5152 **3**

Auditd

**4**

Разделитель

\n

- 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**.

# Основной парсинг событий

Схема нормализации

Обогащение

Нормализатор	[OOTB] Linux auditd syslog for KUMA 3.2 <span>1</span>
Название*	[OOTB] Linux auditd syslog for KUMA 3.2
Метод парсинга* ⓘ	syslog
Сохранить исходное событие*	При возникновении ошибок
Сохранить дополнительные поля*	Нет
Примеры событий	+ Загрузить из файла

- 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

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация 1

Проверка параметров

### Маршрутизация

Укажите, куда следует отправлять полученные события. Подробнее см. [в онлайн-справке](#).

2 + Добавить Удалить

Название	Тип	URL
----------	-----	-----



Пусто

# Создание точки назначения

Основные параметры

Дополнительные параметры

Точка назначения

Создать

1



Название\*

Создать

Состояние

[OOTB] Correlator  
Main



Тип\*

[OOTB] Storage  
Main

2

# Создание точки назначения

Основные параметры

Дополнительные параметры

Точка назначения

Создать

1



Название\*

Создать

Состояние

[OOTB] Correlator  
Main

2



Тип\*

[OOTB] Storage  
Main

## Создание коллектора

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

### Маршрутизация

Укажите, куда следует отправлять полученные события. Подробнее см. [в онлайн-справке](#).

+ Добавить    Удалить

<input type="checkbox"/>	Название	Тип	URL
<input type="checkbox"/>	[OOTB] Storage <span>1</span>	storage	kuma-aio.truecompany.local:7230
<input type="checkbox"/>	[OOTB] Correlator <span>2</span>	correlator	kuma-aio.truecompany.local:7231

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

## Создание коллектора

×

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

### Проверка параметров

Настройка коллектора завершена, сервис добавлен в KUMA. Подробнее см. [в онлайн-справке](#).

Чтобы начать получать события, сервис этого коллектора необходимо установить на сервере, предназначенном для сбора событий (см. пример команды установки ниже). Обратите внимание, что должна быть обеспечена сетевая связность компонентов системы и открыты порты. Подробнее см. [в онлайн-справке](#).

### Сервисы, использующие этот коллектор

Тип	Название
коллектор	Linux Auditd Syslog-ng TCP/5152

Сохранить и перезапустить сервисы

Сохранить и обновить параметры сервисов

### Рекомендуемая команда для установки коллектора

```
/opt/kaspersky/kuma/kuma collector --core https://kuma-aio.truecompany.local:7210 --id d3035bf4-1e9c-46cb-b6a9-6159f8cba74e --api.port 7795 --install
```

1

- Нажмите **Сохранить**.
- После выполнения вышеуказанных действий в разделе **Ресурсы** → **Активные сервисы** появится созданный сервис коллектора.

## Сервисы

Статус	Тип	Сервис	Версия	Тенант	Полное доменное имя	IP-адрес	Порт API	Время работы	Создан
Выкл	Коллектор	Linux Auditd Syslog-ng TCP/5152		Main					23.01.2025 20:09:40

# ?????????? ?????????????? 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-admin /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.

## Сервисы

Статус	Тип	Сервис	Версия	Тенант	Полное доменное имя	IP-адрес	Порт API	Время работы	Создан
Вкл	Коллектор	Linux Auditd Syslog-ng TCP/5152	3.2.0.305	Main	kuma-aio.truecompany.local	10.68.85.89	7795	1 минута 59 секунды	23.01.2025 20:09:40

# ?????????? ?????????????? ????????????

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
```

```
root@kuma:~/home/user# systemctl status syslog-ng
● syslog-ng.service - System Logger Daemon
   Loaded: loaded (/lib/systemd/system/syslog-ng.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2026-01-30 00:00:25 MSK; 18h ago
     Docs: man:syslog-ng(8)
  Main PID: 4817 (syslog-ng)
    Tasks: 12 (limit: 4915)
   Memory: 24.1M
      CPU: 27.440s
   CGroup: /system.slice/syslog-ng.service
           └─4817 /usr/sbin/syslog-ng -F --no-caps
```

- 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**.

Ресурсы и сервисы / Сервисы

## Сервисы

Статус	Тип	Сервис	Версия	Тенант	Полное доменное имя	IP-адрес	Порт API	Время работы	Создан
<input checked="" type="checkbox"/>	Коллектор	LinuxAuditd Syslog-ng TCP/5152	3.2.0.305	Main	kuma-ai0.truecompany.local	10.68.85.89	7795	3 дня 23 часа 55 минуты 11 секунды	23.01.2025 20:09:40

- Копировать идентификатор
- Журнал
- Перейти к событиям **1**
- Обновить параметры
- Перезапустить
- Сбросить сертификат
- Удалить

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

События

SELECT \* FROM 'events' WHERE ServiceID = 'd5035b14-1e9c-46cb-b6a9-6159f8c8a74e' ORDER BY Timestamp DESC LIMIT 250

Нажмите Ctrl + Enter, чтобы выполнить запрос

Выполнить запрос

TenantID	Timestamp	Device/Vendor	Device/HostName	Name	DeviceEventClassID	SourceUserName	DestinationProcessName	EventOutcome
Main	28.01.2025 10:40:27.794	Unix	kuma-ai0	Service is started	SERVICE_START	4294967295	/usr/lib/systemd/systemd	success
Main	28.01.2025 10:40:27.794	Unix	kuma-ai0	Service is stopped	SERVICE_STOP	4294967295	/usr/lib/systemd/systemd	success
Main	28.01.2025 10:40:27.794	Unix	kuma-ai0	User-space session is terminated	USER_END	root	/usr/bin/sudo	success
Main	28.01.2025 10:40:27.794	Unix	kuma-ai0	User-space session is started	USER_START	root	/usr/bin/sudo	success
Main	28.01.2025 10:40:27.794	Unix	kuma-ai0	User-space user account is modified	USER_ACCT	kuma-adm	/usr/bin/sudo	success
Main	28.01.2025 10:40:27.794	Unix	kuma-ai0	User-space shell command is executed	USER_CMD	1000		success
Main	28.01.2025 10:40:27.794	Unix	kuma-ai0	User disposes of user-space credentials	CRED_DISP	root	/usr/bin/sudo	success
Main	28.01.2025 10:40:27.794	Unix	kuma-ai0	User-space session is started	USER_START	root	/usr/bin/sudo	success
Main	28.01.2025 10:40:27.794	Unix	kuma-ai0	removexattr			/usr/bin/vim.basic	Failed
Main	28.01.2025 10:40:27.794	Unix	kuma-ai0	User-space shell command is executed	USER_CMD	1000		success
Main	28.01.2025 10:40:27.794	Unix	kuma-ai0	User refreshes their user-space credentials	CRED_REFR	root	/usr/bin/sudo	success
Main	28.01.2025 10:40:27.794	Unix	kuma-ai0	removexattr			/usr/bin/vim.basic	Failed

???????????? ? . ?????????? ?????????? ?  
 ????????????????????? 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**.

# Редактирование коллектора

Подключение источников

Транспорт **1**

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

## Транспорт

Подключите источник, от которого хотите получать события. Подробнее см. [в онлайн-справке](#).

Основные параметры

Дополнительные параметры **2**

Отладка



Размер буфера ⓘ

Авто



Кодировка символов ⓘ



TTL буфера событий ⓘ

2000



Заголовок транспорта\*

```
type\=(?P<record_type_name>[^\s\[\]]+)\{[(?P<record_type_value>\d+)]?\s+msg\=audit\((\w+:\s)?[\d\.]+\s+(?P<event_sequence_number>\d+)\):
```

↻ Установить значение по умолчанию

Режим TLS

**3**

Включено



Сжатие

Выключено



Сохранить

Отмена

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

# Редактирование коллектора

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров **1**

## Проверка параметров

Настройка коллектора завершена, сервис добавлен в KUMA. Подробнее см. [в онлайн-справке](#).

Чтобы начать получать события, сервис этого коллектора необходимо установить на сервере, предназначенном для сбора событий (см. пример команды установки ниже). Обратите внимание, что должна быть обеспечена сетевая связность компонентов системы и открыты порты.

Подробнее см. [в онлайн-справке](#).

Сохранить и создать сервис

## Сервисы, использующие этот коллектор

Тип	Название
коллектор	LinuxAuditd Syslog-ng TCP/5152

Сохранить и перезапустить сервисы

Сохранить и обновить параметры сервисов

**2**

**3**

Сохранить

Отмена

- 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 отставку 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**.

# Редактирование коллектора

Подключение источников

Транспорт **1**

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

## Транспорт

Подключите источник, от которого хотите получать события. Подробнее см. [в онлайн-справке](#).

Основные параметры Дополнительные параметры **2**

Отладка

Размер буфера ⓘ Авто

Кодировка символов ⓘ


TTL буфера событий ⓘ 2000

Заголовок транспорта\*  
`type\=(?P<record_type_name>[^\s\[]+)\(\[(?P<record_type_value>\d+)\]\)?\s+msg\=audit\(\(\w+\.+\.+\)?\[\d\.\.+\]:(?P<event_sequence_number>\d+)\)\):`

↻ Установить значение по умолчанию

Режим TLS Нестандартный PFX **3**

Нестандартный PFX\* по умолчанию

Сжатие  
Создать **4**  
test 

Сохранить

Отмена

- 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

Тип\*

Файл PKCS\* ⓘ 2

Пароль PFX-файла\* ⓘ 3

Описание

4

Создать

Отмена

# Редактирование коллектора

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

## Транспорт

Подключите источник, от которого хотите получать события. Подробнее см. [в онлайн-справке](#).

Основные параметры [Дополнительные параметры](#)

Отладка



Размер буфера ⓘ

Авто



Кодировка символов ⓘ



TTL буфера событий ⓘ

2000



Заголовок транспорта\*

```
type\=(?P<record_type_name>[^\s\[\]]+\(\(\(?P<record_type_value>\d+\)\)?\s+msg\=audit\((\w+:\+)?[\d\.]+\:(?P<event_sequence_number>\d+)\)\):
```

Установить значение по умолчанию

Режим TLS

Нестандартный PFX



Нестандартный PFX\*



[DEMO] Auditd Collector Certificate



Сжатие

Выключено



Сохранить

Отмена

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

# Редактирование коллектора

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров **1**

## Проверка параметров

Настройка коллектора завершена, сервис добавлен в KUMA. Подробнее см. [в онлайн-справке](#).

Чтобы начать получать события, сервис этого коллектора необходимо установить на сервере, предназначенном для сбора событий (см. пример команды установки ниже). Обратите внимание, что должна быть обеспечена сетевая связность компонентов системы и открыты порты.

Подробнее см. [в онлайн-справке](#).

Сохранить и создать сервис

## Сервисы, использующие этот коллектор

Тип	Название
коллектор	LinuxAuditd Syslog-ng TCP/5152

Сохранить и перезапустить сервисы

Сохранить и обновить параметры сервисов

**2**

**3**

Сохранить

Отмена

- 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:

```
root@kuma: /etc/syslog-ng/cert# ls -la
итого 12
drwxr-xr-x 3 root root 4096 фев 10 20:27 .
drwxr-xr-x 3 root root 4096 фев 10 20:27 ..
-rw-r--r-- 1 root root 3072 фев 10 20:27 ca_auditd.pem
-rw-r--r-- 1 root root    0 фев 10 20:27 e1442ae8.0 -> ca_auditd.pem
```

- 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](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