

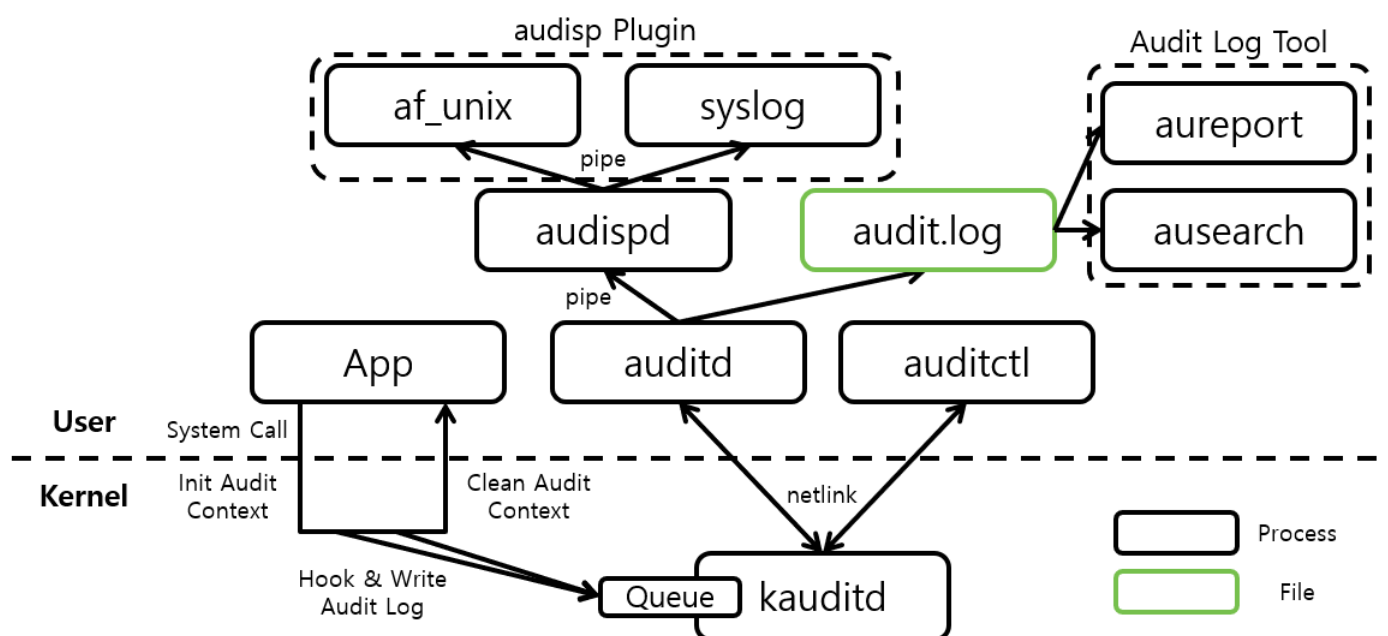
Unix

- [Настройка AuditD на Unix системах](#)
- [Настройка Syslog-ng на Unix системах](#)
- [Сбор событий AuditD с помощью Rsyslog](#)

Настройка AuditD на Unix системах

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

Архитектура Auditd



Настройка AuditD

Для начала необходимо проверить установлена ли нужная служба `auditd`, посмотрим активные правила:

```
auditctl -l
```

В случае наличия подобной ошибки:

```
[root@cn4 ~]# auditctl -l
-bash: auditctl: command not found
[root@cn4 ~]#
```

Необходимо установить следующие пакеты:

```
apt-get install auditd audispd-plugins
```

Либо (если RHEL подобные ОС):

```
yum install audit audispd-plugins
```

Рекомендуем использовать следующие правила для аудита:

```
wget -O audit.rules https://raw.githubusercontent.com/Neo23x0/auditd/master/audit.rules
```

Загрузить файл с правилами аудита с портала box.kaspersky.com - [тут](#).

Другие правила аудита можно найти в этой статье - <https://kb.kuma-community.ru/link/14#bkmrk-linux>

Рекомендуем добавить записи в конец файла `audit.rules`, для быстрого добавления используйте команду ниже (после выполните `systemctl restart auditd.service`):

```
cat << EOF >> /etc/audit/rules.d/audit.rules
# root authorized_keys
-w /root/.ssh/authorized_keys -p wa -k rootkey

# motd audit
-w /etc/update-motd.d/ -p wa -k motd

# udev audit
-w /etc/udev/rules.d/ -p wa -k udev

# xdg audit
-w /etc/xdg/autostart/ -p wa -k xdg
-w /usr/share/autostart/ -p wa -k xdg

# Package Manager (APT/YUM/DNF)
-w /etc/yum/pluginconf.d/ -p wa -k package_man
-w /etc/apt/apt.conf.d/ -p wa -k package_man
```

```
-w /etc/dnf/plugins/dnfcon.conf -p wa -k package_man
```

```
# extra systemd
```

```
-w /usr/lib/systemd/ -p wa -k systemd
```

```
-w /lib/systemd/ -p wa -k systemd
```

```
-w /usr/local/lib/systemd/ -p wa -k systemd
```

```
-w /usr/local/share/systemd/user -p wa -k systemd_user
```

```
-w /usr/share/systemd/user -p wa -k systemd_user
```

```
# setcap audit
```

```
-w /usr/sbin/setcap -p x -k setcap
```

```
# rc audit
```

```
-w /etc/rc.local -p wa -k rclocal
```

```
## extra Shell/profile configurations
```

```
-w /etc/bash.bashrc -p wa -k shell_profiles
```

```
-w /etc/bash.bash_logout -p wa -k shell_profiles
```

```
-w /root/.profile -p wa -k shell_profiles
```

```
-w /root/.bashrc -p wa -k shell_profiles
```

```
-w /root/.bash_logout -p wa -k shell_profiles
```

```
-w /root/.bash_profile -p wa -k shell_profiles
```

```
-w /root/.bash_login -p wa -k shell_profiles
```

```
# extra search files
```

```
-w /usr/bin/find -p x -k T1083_File_And_Directory_Discovery
```

```
## Kernel Related Events
```

```
-w /usr/sbin/modprobe -p x -k T1547_Boot_or_Logon_Autostart_Execution
```

```
-w /usr/sbin/insmod -p x -k T1547_Boot_or_Logon_Autostart_Execution
```

```
-w /usr/sbin/lsmmod -p x -k T1547_Boot_or_Logon_Autostart_Execution
```

```
-w /usr/sbin/rmmmod -p x -k T1547_Boot_or_Logon_Autostart_Execution
```

```
-w /usr/sbin/modinfo -p x -k T1547_Boot_or_Logon_Autostart_Execution
```

```
-w /etc/modprobe.conf -p wa -k T1547.006_6
```

```
-w /etc/sysctl.conf -p wa -k sysctl
```

```
# extra file manipulation
```

```
-w /usr/bin/ftp -p x -k T1105_remote_file_copy
```

```
-w /usr/bin/sftp -p x -k T1105_remote_file_copy
```

```
-w /usr/bin/rsync -p x -k T1105_remote_file_copy
```

```
-w /usr/bin/cp -p x -k T1005_Data_from_Local_System
-w /usr/bin/dd -p x -k T1005_Data_from_Local_System
-a always,exit -F arch=b32 -S execve -S execveat -F exe=/usr/bin/shred -F -k T1070.004_1
-a always,exit -F arch=b64 -S execve -S execveat -F exe=/usr/bin/shred -F -k T1070.004_2

# split cmd audit
-w /usr/bin/split -p x -k split

EOF
```

Другие правила аудита и полезные материалы по AuditD можно найти - [тут](#).

Далее нужно переместить правила в директорию по умолчанию и применить правила перезапуском сервиса:

```
cp audit.rules /etc/audit/rules.d/
systemctl restart auditd.service
systemctl enable auditd.service
```

В случае ошибки рестарта службы auditd (Failed to restart auditd.service)

На RHEL подобных ОС, может встретиться следующая ошибка:

*Failed to restart auditd.service: Operation refused, unit auditd.service may be requested by dependency only (it is configured to refuse manual start/stop).
See system logs and 'systemctl status auditd.service' for details.*

```
nano /usr/lib/systemd/system/auditd.service
```

Измените параметр `RefuseManualStop` на:

```
RefuseManualStop=no
```

Затем обновите параметры службы:

```
systemctl daemon-reload
```

Для проверки убедитесь что следующий лог наполняется информацией:

```
tail -f /var/log/audit/audit.log
```

Рекомендуемый парсер (без агрегации/склейки событий) для правил корреляции Community - **[2024-09-23] Unix AuditD (REGEX)** (из Community-Pack)

Для использования агрегации логов используйте коробочный парсер **[OOTB] Linux auditd syslog for KUMA 3.2** с включенным переключателем "auditd", который доступен в KUMA 3.2, подробнее: <https://support.kaspersky.com/help/KUMA/3.2/ru-RU/220739.htm>

Известные проблемы

Бывают случаи, когда из-за ротации самого себя auditd (собственная ротация) падает в статусе сервиса:

Sep 24 00:11:42 example.org auditd[756]: Audit daemon rotating log files

В таком статусе лог файл не пополняется, рекомендуется использовать системную ротацию logrotate.

Сначала отключается собственная ротация auditd, правим конфиг:

```
nano /etc/audit/auditd.conf
```

Правим значение (выделено жирным): `max_log_file_action = ignore`

Затем настраивается системная ротация logrotate.

```
touch /etc/logrotate.d/auditd
chmod 644 /etc/logrotate.d/auditd; chown root:root /etc/logrotate.d/auditd
nano /etc/logrotate.d/auditd
```

Пишем в файле auditd:

```
# daily rotation keep last 2 days and compress old
/var/log/audit/audit.log {
    daily
    missingok
    notifempty
    sharedscripts
    rotate 2
    compress
    delaycompress
```

```
postrotate
    /usr/bin/systemctl kill -s USR1 auditd.service >/dev/null 2>&1 || true
endscript
}
```

Перезапускаем службы logrotate и auditd:

```
systemctl restart logrotate.service; systemctl restart auditd.service
```

Классический сбор событий auditd с помощью Rsyslog

Проведите настройку по этой инструкции: <https://kb.kuma-community.ru/books/podkliucenie-istocnikov/page/sbor-sobytii-auditd-s-pomoshhiu-rsyslog>

Удаленная отправка логов auditd

Не поддерживается коробочным парсером [OOTB] Linux auditd syslog for KUMA 3.2

Иногда **если место на сервере ограничено и хранить объемный лог auditd нет возможности**, для этого можно настроить отправку логов сразу на удаленный сервер, для этого будем использовать плагин audispd-plugins, который мы загружали выше.

Отключим локальное ведение логов аудита в файле `/etc/audit/auditd.conf` выставляем значение **write_logs = no**:

```
root@kuma# nano /etc/audit/auditd.conf

local_events = yes
write_logs = no
name_format = HOSTNAME
```

Не прописывайте `name_format = HOSTNAME` если планируете использоватькоробочный парсер**[OOTB] Linux auditd syslog for KUMA 3.2**

Теперь нам нужно исправить файл по примеру ниже для отправки логов на удаленный сервер:

```
root@kuma# nano /etc/audit/plugins.d/au-remote.conf

active = yes
direction = out
path = /sbin/audisp-remote
type = always
#args =
format = string
```

Далее нужно отредактировать файл `/etc/audit/audisp-remote.conf` следующим образом:

```
root@kuma# nano /etc/audit/audisp-remote.conf

#
# This file controls the configuration of the audit remote
# logging subsystem, audisp-remote.
#

remote_server = 192.168.0.100
port = 16666
transport = tcp
queue_file = /var/spool/audit/remote.log
mode = immediate
queue_depth = 10240
format = ascii
network_retry_time = 2
max_tries_per_record = 3
max_time_per_record = 5
heartbeat_timeout = 0

network_failure_action = stop
disk_low_action = ignore
disk_full_action = warn_once
disk_error_action = warn_once
```



```
remote_ending_action = reconnect
generic_error_action = syslog
generic_warning_action = syslog
queue_error_action = stop
overflow_action = syslog
startup_failure_action = warn_once_continue

##krb5_principal =
##krb5_client_name = auditd
##krb5_key_file = /etc/audisp/audisp-remote.key
```

Теперь нужно перезапустить сервис auditd для применения обновленных конфигураций :

```
systemctl restart auditd.service
```

Сырые события будут без заголовка syslog, парсер Unix из комьюнити-пака обрабатывает корректно такие логи:

```
node=kuma-aio.local type=PROCTITLE msg=audit(1704808440.087:50482):
proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C6573
```

Настройка Syslog-ng на Unix системах

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

Для начала необходимо проверить установлена ли нужная служба Syslog-ng, посмотрим статус службы:

```
systemctl status syslog-ng
```

В случае отсутствия службы необходимо установить следующие пакеты:

```
apt-get install syslog-ng
```

В случае если служба не запущена:

```
sudo systemctl start syslog-ng  
sudo systemctl enable syslog-ng
```

Настройка источника

Далее на источнике нужно создать файл с параметрами работы службы и изменить конфигурационный файл службы Syslog-ng.

Сначала создается файл с параметрами работы службы:

Создайте файл `/etc/syslog-ng/1-unixLogging.conf`, например с помощью nano:

```
nano /etc/syslog-ng/1-unixLogging.conf
```

Добавьте в файл строки для отправки по UDP на порт 5140:

```
filter unix_filter {  
    not facility(cron, lpr, mail, news, uucp);
```

```
};

destination to_kuma_udp {
    udp("<IP_KUMA_Collector>" port(5140));
};

log {
    source(s_src);
    filter(unix_filter);
    destination(to_kuma_udp);
};
```

Добавьте в файл строки для отправки по TCP на порт 5140:

```
filter unix_filter {
    not facility(cron, lpr, mail, news, uucp);
};

destination to_kuma_tcp {
    tcp("<IP_KUMA_Collector>" port(5140) log-fifo-size(1000));
};

log {
    source(s_src);
    filter(unix_filter);
    destination(to_kuma_tcp);
    flags(flow-control);
};
```

Чтобы настроить конфигурационный файл службы с использованием настроек сделанных выше, отредактируйте файл `/etc/syslog-ng/syslog-ng.conf`, добавив в файл строку:

```
@include "1-unixLogging.conf"
```

Перезапустите службу syslog-ng:

```
systemctl restart syslog-ng
```

Проверка отправки сообщения

Для проверки получения и отправки сообщения можно воспользоваться командой с тестовым сообщением:

```
logger "testTest"
```

Это сообщение должно появиться в системном журнале, например `/var/log/messages`:

```
Oct 4 10:22:41 test-kuma systemd[1]: kuma-collector-2d8ccbfd-3990-4e
Oct 4 10:22:41 test-kuma systemd[1]: Failed to start KUMA collector.
Oct 4 10:22:43 test-kuma root[4032724]: testTest
Oct 4 10:22:44 test-kuma kuma[4393]: 2023/10/04 10:22:44 WARN: You s
Oct 4 10:22:44 test-kuma systemd[1]: kuma-collector-28a4fb00-f0e3-4f
Oct 4 10:22:44 test-kuma systemd[1]: kuma-collector-28a4fb00-f0e3-4f
```

Дополнительная информация

Обычно в конфигурации `/etc/syslog-ng/syslog-ng.conf` в `s_src` содержится 2 типа журналов

```
source s_src {
    system(); # системный журнал
    internal(); # внутренние сообщения журнала syslog-ng
};
```

Для задания шаблона сообщения можно использовать следующее:

```
template LogglyFormat { template("<${PRI}>1 ${ISODATE} ${HOST} ${PROGRAM} ${PID} ${MSGID}
[TOKEN@41058 tag=\"TAG\" ] $MSG\n");
    template_escape(no);
};
```

```
destination d_loggly {
    tcp("logs-01.loggly.com" port(514) template(LogglyFormat));
};
```

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](#) >
Services

Add service

Refresh

ReloadRestartCopy IDGo to eventsGo to active listsGo to partitionsReset certificateRemove

<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](#) >

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	path	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
```