

Администрирование системных подсистем

Настройка сетевого журналирования rsyslog

Сейдалиев Тагиетдин Ровшенович

11 декабря 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

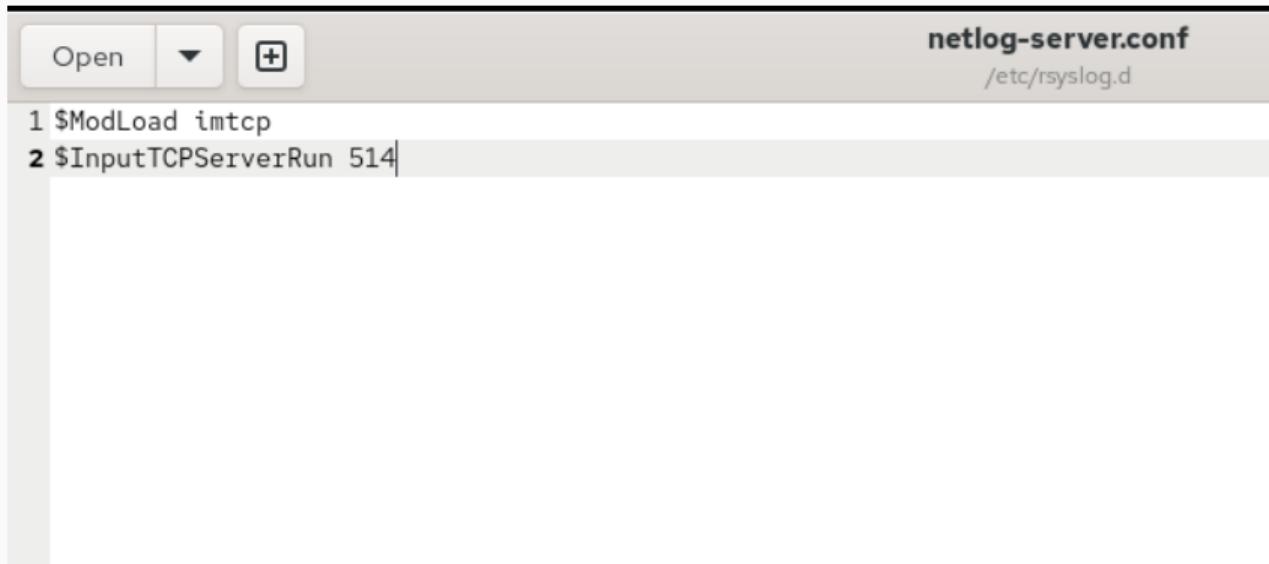
Основная цель

Получить навыки настройки сетевого журналирования с использованием rsyslog, пересылки логов по TCP и автоматизации конфигурации с помощью Vagrant.

Настройка сервера

Конфигурация rsyslog

Создание файла `netlog-server.conf` и включение модуля `imtcp` для приёма сообщений по TCP-порту 514.



The screenshot shows a text editor window with the title bar "netlog-server.conf /etc/rsyslog.d". On the left, there are standard file operations buttons: "Open", a dropdown menu, and a "+" button. The main area contains two lines of configuration code:

```
1 $ModLoad imtcp
2 $InputTCPServerRun 514
```

Рис. 1: Конфигурация сервера

Перезапуск и проверка портов

Анализ открытых TCP-соединений, связанных с rsyslog, и проверка работы firewall.

```
s->client.trseidaliev.net:41294 (ESTABLISHED)
rsyslogd 14018                               root      4u      IPv4          58014      0t0      TCP *:shell (LISTEN)
rsyslogd 14018                               root      5u      IPv6          58015      0t0      TCP *:shell (LISTEN)
rsyslogd 14018 14021 in:imjour              root      4u      IPv4          58014      0t0      TCP *:shell (LISTEN)
rsyslogd 14018 14021 in:imjour              root      5u      IPv6          58015      0t0      TCP *:shell (LISTEN)
rsyslogd 14018 14022 in:imtcp               root      4u      IPv4          58014      0t0      TCP *:shell (LISTEN)
rsyslogd 14018 14022 in:imtcp               root      5u      IPv6          58015      0t0      TCP *:shell (LISTEN)
rsyslogd 14018 14023 in:imtcp               root      4u      IPv4          58014      0t0      TCP *:shell (LISTEN)
rsyslogd 14018 14023 in:imtcp               root      5u      IPv6          58015      0t0      TCP *:shell (LISTEN)
rsyslogd 14018 14024 in:imtcp               root      4u      IPv4          58014      0t0      TCP *:shell (LISTEN)
rsyslogd 14018 14024 in:imtcp               root      5u      IPv6          58015      0t0      TCP *:shell (LISTEN)
rsyslogd 14018 14025 in:imtcp               root      4u      IPv4          58014      0t0      TCP *:shell (LISTEN)
rsyslogd 14018 14025 in:imtcp               root      5u      IPv6          58015      0t0      TCP *:shell (LISTEN)
rsyslogd 14018 14026 in:imtcp               root      4u      IPv4          58014      0t0      TCP *:shell (LISTEN)
rsyslogd 14018 14026 in:imtcp               root      5u      IPv6          58015      0t0      TCP *:shell (LISTEN)
rsyslogd 14018 14027 rs:main                root      4u      IPv4          58014      0t0      TCP *:shell (LISTEN)
rsyslogd 14018 14027 rs:main                root      5u      IPv6          58015      0t0      TCP *:shell (LISTEN)

[root@server.trseidaliev.net rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent
success
[root@server.trseidaliev.net rsyslog.d]# firewall-cmd --add-port=514/tcp
success
[root@server.trseidaliev.net rsyslog.d]#
```

Рис. 2: Порты rsyslog

Настройка клиента

Пересылка сообщений

Создание файла `netlog-client.conf` и указание отправки всех сообщений на сервер `server.trseidaliev.net:514`.



Рис. 3: Конфигурация клиента

Перезапуск службы

Активация новых настроек путём перезапуска rsyslog.

Просмотр логов

Просмотр `/var/log/messages` и подтверждение получения сообщений как с сервера, так и с клиента.

```
Dec 11 10:52:50 server systemd[1]: systemd-coredump@113-14434-0.service: Deactivated successfully.
Dec 11 10:52:51 client kernel: traps: VBoxClient[14264] trap int3 ip:41dd1b sp:7f49912cfcd0 error:0 in VBoxClient[1dd1b,400000+bb000]
Dec 11 10:52:51 client systemd-coredump[14265]: Process 14261 (VBoxClient) of user 1001 terminated abnormally with signal 5/TRAP, pro
cessing...
Dec 11 10:52:51 client systemd[1]: Started systemd-coredump@103-14265-0.service - Process Core Dump (PID 14265/UID 0).
Dec 11 10:52:51 client systemd-coredump[14266]: Process 14261 (VBoxClient) of user 1001 dumped core.#012#012Module libXau.so.6 from r
pm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Module libX11.so.6 from rpm libX11-1.8.1
0-1.el10.x86_64#012Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.
el10.x86_64#012Stack trace of thread 14264:#012#0 0x000000000041dd1b n/a (n/a + 0x0)#012#1 0x000000000041dc94 n/a (n/a + 0x0)#012#2
0x000000000045041c n/a (n/a + 0x0)#012#3 0x00000000004355d0 n/a (n/a + 0x0)#012#4 0x00007f499f98bb68 start_thread (libc.so.6 + 0x
```

Рис. 4: Просмотр журнала

Запуск `gnome-system-monitor` для наблюдения за процессами и ресурсами.

Process Name	User	% CPU	ID	Memory	Disk read total	Disk write
at-spi2-registryd	trseidaliev	0.00	10156	262.1 kB	241.7 kB	
at-spi-bus-launcher	trseidaliev	0.00	10116	262.1 kB	282.6 kB	
bash	trseidaliev	0.00	13502	2.0 MB	3.3 MB	
bash	trseidaliev	0.00	14478	2.0 MB	20.5 kB	
catatonit	trseidaliev	0.00	13463	N/A	679.9 kB	
dbus-broker	trseidaliev	0.00	9766	2.0 MB	143.4 kB	
dbus-broker	trseidaliev	0.00	10132	131.1 kB	102.4 kB	
dbus-broker-launch	trseidaliev	0.00	9760	262.1 kB	4.1 kB	
dbus-broker-launch	trseidaliev	0.00	10131	131.1 kB	N/A	
dconf-service	trseidaliev	0.00	12696	262.1 kB	135.2 kB	36.1 kB
evolution-addressbook-factory	trseidaliev	0.00	10792	1.7 MB	3.6 MB	53.1 kB
evolution-alarm-notify	trseidaliev	0.00	10365	7.0 MB	2.7 MB	
evolution-calendar-factory	trseidaliev	0.00	10674	1.0 MB	2.6 MB	
evolution-source-registry	trseidaliev	0.00	10473	2.9 MB	2.8 MB	
gdm-wayland-session	trseidaliev	0.00	9757	262.1 kB	233.5 kB	
gjs	trseidaliev	0.00	10271	3.0 MB	4.1 kB	
gjs	trseidaliev	0.00	10593	405.5 kB	692.2 kB	
gnome-keyring-daemon	trseidaliev	0.00	8374	323.6 kB	766.0 kB	

Попытка установки `lnav`, отсутствующего в репозиториях.

```
[root@server.trseidaliev.net rsyslog.d]#  
[root@server.trseidaliev.net rsyslog.d]# dnf -y install lnav  
Extra Packages for Enterprise Linux 10 - x86_64  
Extra Packages for Enterprise Linux 10 - x86_64  
Rocky Linux 10 - BaseOS  
Rocky Linux 10 - AppStream  
Rocky Linux 10 - CRB  
Rocky Linux 10 - Extras  
No match for argument: lnav  
Error: Unable to find a match: lnav  
[root@server.trseidaliev.net rsyslog.d]#
```

Рис. 6: Ошибка установки `lnav`

Итоги работы

Основные результаты

- Настроен сервер rsyslog для приёма сетевых сообщений по TCP 514
- Настроен клиент для пересылки всех логов на сервер
- Выполнена проверка доставляемых сообщений
- Исследованы инструменты просмотра логов
- Созданы и оформлены скрипты провишивинга для автоматизации настройки
- Подготовлены конфигурационные файлы в структуре Vagrant