Администрирование сетевых подсистем

Настройка сетевого журналирования (rsyslog)

Метвалли Ахмед Фарг Набеех

1 декабря 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Цель лабораторной работы

Получить практические навыки по настройке сетевого журналирования с использованием rsyslog и интеграции с journald.

Выполнение лабораторной работы

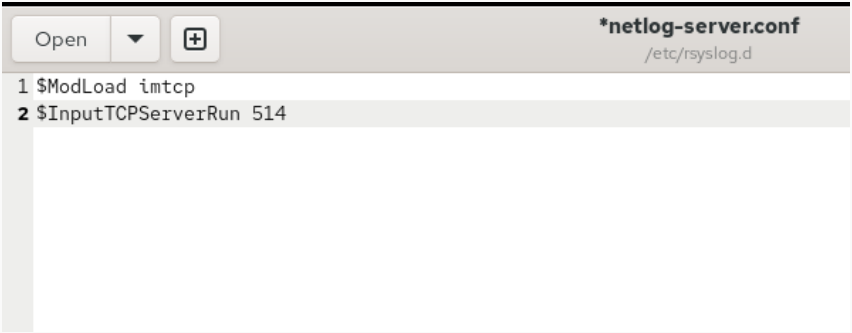


Рис. 1: Конфигурация netlog-server.conf

Проверка работы сервера

```
rsyslogd  10224 10227 in:imtcp            root    4u     IPv4               52678       0t0       TCP *:shell (LISTEN)
rsyslogd  10224 10227 in:imtcp            root    5u     IPv6               52679       0t0       TCP *:shell (LISTEN)
rsyslogd  10224 10228 in:imtcp            root    4u     IPv4               52678       0t0       TCP *:shell (LISTEN)
rsyslogd  10224 10228 in:imtcp            root    5u     IPv6               52679       0t0       TCP *:shell (LISTEN)
rsyslogd  10224 10229 in:imtcp            root    4u     IPv4               52678       0t0       TCP *:shell (LISTEN)
rsyslogd  10224 10229 in:imtcp            root    5u     IPv6               52679       0t0       TCP *:shell (LISTEN)
rsyslogd  10224 10230 in:imtcp            root    4u     IPv4               52678       0t0       TCP *:shell (LISTEN)
rsyslogd  10224 10230 in:imtcp            root    5u     IPv6               52679       0t0       TCP *:shell (LISTEN)
rsyslogd  10224 10231 in:imtcp            root    4u     IPv4               52678       0t0       TCP *:shell (LISTEN)
rsyslogd  10224 10231 in:imtcp            root    5u     IPv6               52679       0t0       TCP *:shell (LISTEN)
rsyslogd  10224 10232 rs:main             root    4u     IPv4               52678       0t0       TCP *:shell (LISTEN)
rsyslogd  10224 10232 rs:main             root    5u     IPv6               52679       0t0       TCP *:shell (LISTEN)
[root@server.ahmedfarg.net rsyslog.d]# firewall-cmd --add-port=514/tcp
success
[root@server.ahmedfarg.net rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent
success
[root@server.ahmedfarg.net rsyslog.d]#
```

Рис. 2: Порты rsyslog и firewall

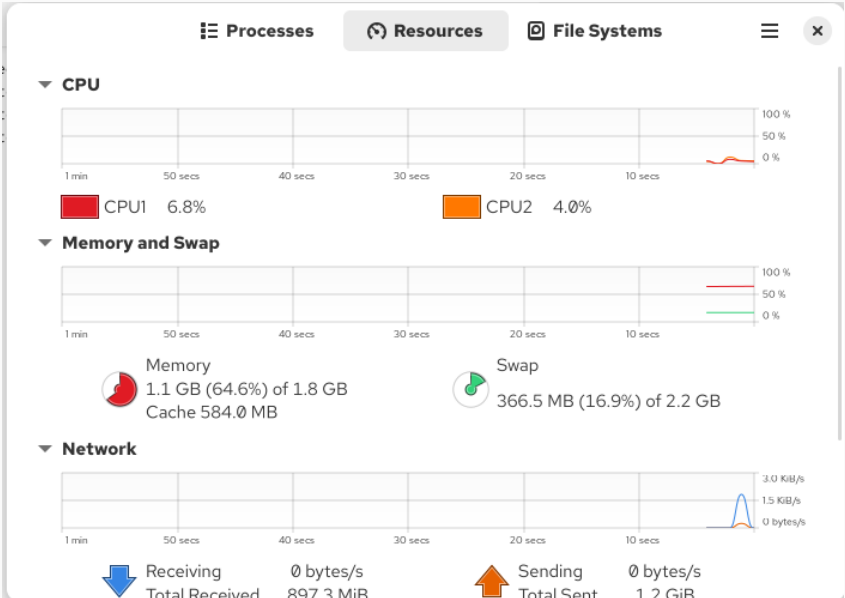
Рис. 3: Конфигурация клиента netlog-client.conf

Просмотр системных журналов

```
Nov  5 09:26:28 client systemd[1]: Started systemd-coredump@85-30245-0.service - Process Core Dump (PID 30245/UID 0).
Nov  5 09:26:28 client systemd-coredump[30246]: Process 30241 (VBoxClient) of user 1001 dumped core.#012#012Module libXa
u.so.6 from rpm 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 libX11-1.8.10-1.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 30244:#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  0x00007f2fd6699b68 start_thread (libc.so.6 + 0x94b68)#012#5  0x00007f2fd670a6bc __clone3 (libc.so.6 +
0x1056bc)#012#012Stack trace of thread 30242:#012#0  0x00007f2fd67084bd syscall (libc.so.6 + 0x1034bd)#012#1  0x00000000
00434c30 n/a (n/a + 0x0)#012#2  0x000000000450bfb n/a (n/a + 0x0)#012#3  0x000000000043566a n/a (n/a + 0x0)#012#4  0x00
0000000045041c n/a (n/a + 0x0)#012#5  0x00000000004355d0 n/a (n/a + 0x0)#012#6  0x00007f2fd6699b68 start_thread (libc.so
.6 + 0x94b68)#012#7  0x00007f2fd670a6bc __clone3 (libc.so.6 + 0x1056bc)#012#012Stack trace of thread 30243:#012#0  0x000
07f2fd67084bd syscall (libc.so.6 + 0x1034bd)#012#1  0x00000000004344e2 n/a (n/a + 0x0)#012#2  0x000000000450066 n/a (n/
a + 0x0)#012#3  0x0000000000416559 n/a (n/a + 0x0)#012#4  0x000000000041838a n/a (n/a + 0x0)#012#5  0x00000000417d6a n
/a (n/a + 0x0)#012#6  0x0000000000404860 n/a (n/a + 0x0)#012#7  0x000000000045041c n/a (n/a + 0x0)#012#8  0x000000000043
55d0 n/a (n/a + 0x0)#012#9  0x00007f2fd6699b68 start_thread (libc.so.6 + 0x94b68)#012#10 0x00007f2fd670a6bc __clone3 (li
bc.so.6 + 0x1056bc)#012#012Stack trace of thread 30241:#012#0  0x00007f2fd67084bd syscall (libc.so.6 + 0x1034bd)#012#1
0x00000000004344e2 n/a (n/a + 0x0)#012#2  0x000000000450066 n/a (n/a + 0x0)#012#3  0x0000000000405123 n/a (n/a + 0x0)#0
12#4  0x00007f2fd662f30e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5  0x00007f2fd662f3c9 __libc_start_main@@GLIBC
_2.34 (libc.so.6 + 0x2a3c9)#012#6  0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Nov  5 09:26:28 client systemd[1]: systemd-coredump@85-30245-0.service: Deactivated successfully.
Nov  5 09:26:31 server kernel: traps: VBoxClient[10726] trap int3 ip:41dd1b sp:7f4ab3e35cd0 error:0 in VBoxClient[1dd1b,
400000+bb000]
Nov  5 09:26:31 server systemd-coredump[10727]: Process 10723 (VBoxClient) of user 1001 terminated abnormally with signa
l 5/TRAP, processing...
Nov  5 09:26:31 server systemd[1]: Started systemd-coredump@115-10727-0.service - Process Core Dump (PID 10727/UID 0).
```

Рис. 4: Просмотр журнала через tail

Мониторинг системных сообщений



Настройка provisioning (сервер)

```
#!/bin/bash
echo "Provisioning script $0"
echo "Copy configuration files"
cp -R /vagrant/provision/server/netlog/etc/* /etc
restorecon -vR /etc
echo "Configure firewall"
firewall-cmd --add-port=514/tcp
firewall-cmd --add-port=514/tcp --permanent
echo "Start rsyslog service"
systemctl restart rsyslog
```

Рис. 6: Provisioning серверной части

```
#!/bin/bash
echo "Provisioning script $0"
echo "Install needed packages"
#dnf -y install lnav
echo "Copy configuration files"
cp -R /vagrant/provision/client/netlog/etc/* /etc
restorecon -vR /etc
echo "Start rsyslog service"
systemctl restart rsyslog

```

Рис. 7: Provisioning клиентской части

Итоги лабораторной работы

Вывод

Система сетевого журналирования успешно настроена: сервер принимает сообщения по TCP, клиент перенаправляет системные логи, результаты подтверждены просмотром журналов. Подготовлены provisioning-скрипты, автоматизирующие развёртывание и конфигурацию обеих машин.