

Администрирование сетевых подсистем

Настройка сетевого журналирования (Лабораторная работа №15)

Заур Мустафаев

12 декабря 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Цель лабораторной работы

Получение практических навыков настройки сетевого журналирования с использованием службы **rsyslog**.

Выполнение лабораторной работы

Настройка сервера сетевого журнала

```
netlog-server.conf [----] 22 L:[ 1+ 1 2/ 2] *(37
$ModLoad imtcp
$InputTCPServerRun 514
```

Рис. 1: Конфигурация netlog-server.conf

Активация TCP-приёма сообщений

```
rsyslogd 11220                           root  4u   IPv4          58857  0t0      TCP *:shell (LISTEN)
rsyslogd 11220                           root  5u   IPv6          58858  0t0      TCP *:shell (LISTEN)
rsyslogd 11220 11222 in:imjour          root  4u   IPv4          58857  0t0      TCP *:shell (LISTEN)
rsyslogd 11220 11222 in:imjour          root  5u   IPv6          58858  0t0      TCP *:shell (LISTEN)
rsyslogd 11220 11223 in:imtcp           root  4u   IPv4          58857  0t0      TCP *:shell (LISTEN)
rsyslogd 11220 11223 in:imtcp           root  5u   IPv6          58858  0t0      TCP *:shell (LISTEN)
rsyslogd 11220 11224 in:imtcp           root  4u   IPv4          58857  0t0      TCP *:shell (LISTEN)
rsyslogd 11220 11224 in:imtcp           root  5u   IPv6          58858  0t0      TCP *:shell (LISTEN)
rsyslogd 11220 11225 in:imtcp           root  4u   IPv4          58857  0t0      TCP *:shell (LISTEN)
rsyslogd 11220 11225 in:imtcp           root  5u   IPv6          58858  0t0      TCP *:shell (LISTEN)
rsyslogd 11220 11226 in:imtcp           root  4u   IPv4          58857  0t0      TCP *:shell (LISTEN)
rsyslogd 11220 11226 in:imtcp           root  5u   IPv6          58858  0t0      TCP *:shell (LISTEN)
rsyslogd 11220 11227 in:imtcp           root  4u   IPv4          58857  0t0      TCP *:shell (LISTEN)
rsyslogd 11220 11227 in:imtcp           root  5u   IPv6          58858  0t0      TCP *:shell (LISTEN)
rsyslogd 11220 11228 rs:main            root  4u   IPv4          58857  0t0      TCP *:shell (LISTEN)
rsyslogd 11220 11228 rs:main            root  5u   IPv6          58858  0t0      TCP *:shell (LISTEN)
[root@server.zmustafaev.net rsyslog.d]# firewall-cmd --add-port=514/tcp
success
[root@server.zmustafaev.net rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent
success
[root@server.zmustafaev.net rsyslog.d]#
```

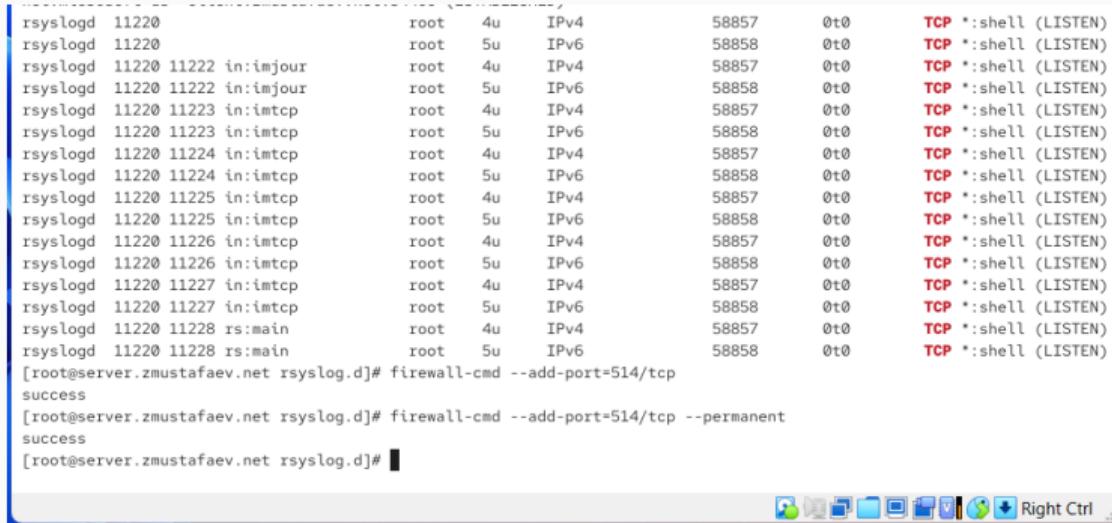
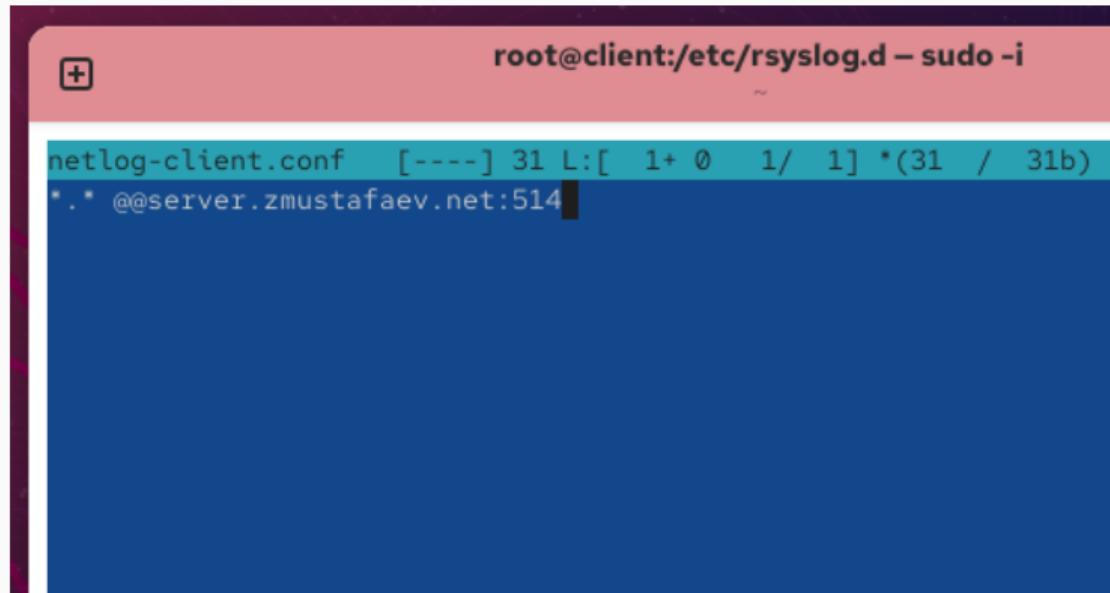


Рис. 2: Проверка прослушиваемых портов rsyslog

Настройка межсетевого экрана



The screenshot shows a terminal window with a red header bar. The header bar contains the text "root@client:/etc/rsyslog.d – sudo -i". Below the header, there is a command-line interface with a blue background. The command shown is:

```
netlog-client.conf [----] 31 L:[ 1+ 0 1/ 1] *(31 / 31b) <
*. * @server.zmustafaev.net:514
```

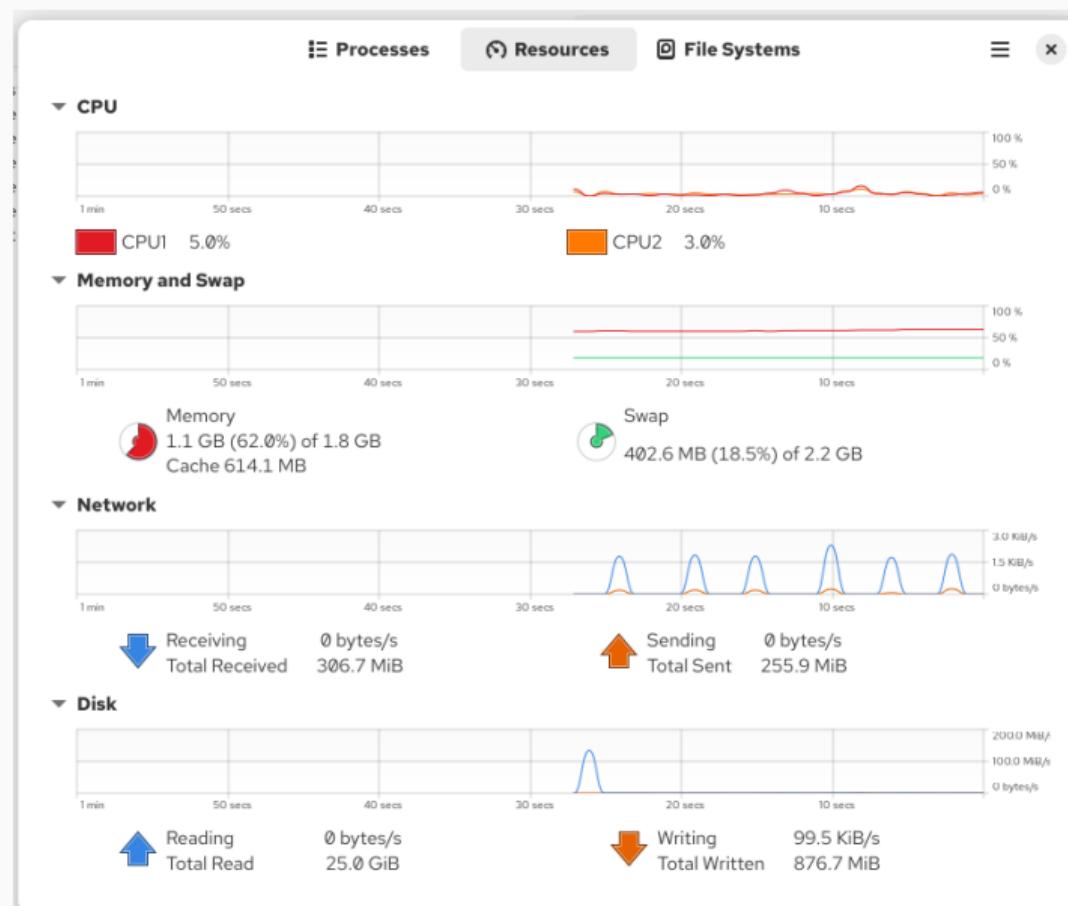
Рис. 3: Настройка firewall для порта 514

Настройка клиента сетевого журнала

```
Dec 12 14:05:56 server systemd[1]: systemd-coredump@105-11594-0.service: Deactivated successfully.  
Dec 12 14:05:54 client kernel: traps: VBoxClient[14015] trap int3 ip:41dd1b sp:7f5a61a35cd0 error:0 in VBoxClient[1dd1  
b,400000+bb000]  
Dec 12 14:05:54 client systemd-coredump[14016]: Process 14012 (VBoxClient) of user 1001 terminated abnormally with sig  
nal 5/TRAP, processing...  
Dec 12 14:05:54 client systemd[1]: Started systemd-coredump@86-14016-0.service - Process Core Dump (PID 14016/UID 0).  
Dec 12 14:05:54 client systemd-coredump[14017]: Process 14012 (VBoxClient) of user 1001 dumped core.#012#012Module lib  
Xau.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 lib  
X11.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 libw  
ayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 14015:#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 0x0000000000043
```

Рис. 4: Конфигурация netlog-client.conf

Проверка приёма журналов на сервере



Мониторинг системы

```
[root@server.zmustafaev.net rsyslog.d]#  
[root@server.zmustafaev.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 - BaseOS  
Rocky Linux 10 - AppStream  
Rocky Linux 10 - AppStream  
Rocky Linux 10 - CRB  
Rocky Linux 10 - CRB  
Rocky Linux 10 - Extras  
Rocky Linux 10 - Extras  
No match for argument: lnav  
Error: Unable to find a match: lnav  
[root@server.zmustafaev.net rsyslog.d]#
```

Рис. 6: Мониторинг ресурсов системы

Просмотр журналов

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

Рис. 7: Попытка установки Inav

Автоматизация настройки сервера

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

Рис. 8: Provisioning-скрипт сервера

Автоматизация настройки клиента

Выводы по проделанной работе

Вывод

В ходе лабораторной работы был настроен сервер сетевого журналирования на основе **rsyslog**. Реализован приём сообщений по TCP-протоколу, настроена пересылка журналов с клиента, выполнена проверка корректности работы и подготовлены provisioning-скрипты для автоматизации развёртывания.