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

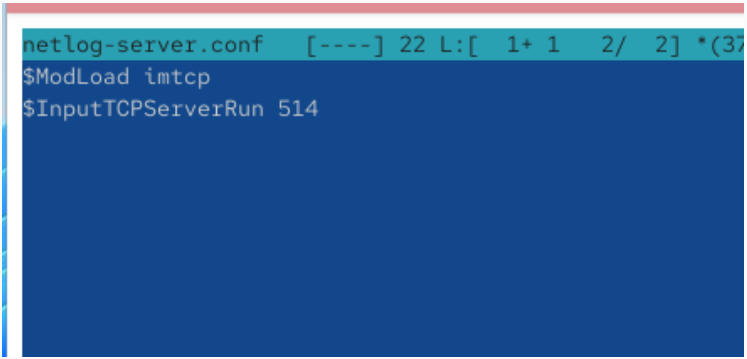


Рис. 1: Конфигурация netlog-server.conf

Активация TCP-приёма сообщений

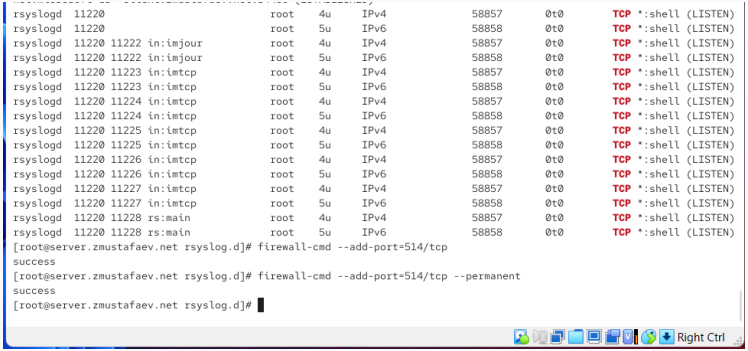


Рис. 2: Проверка прослушиваемых портов rsyslog

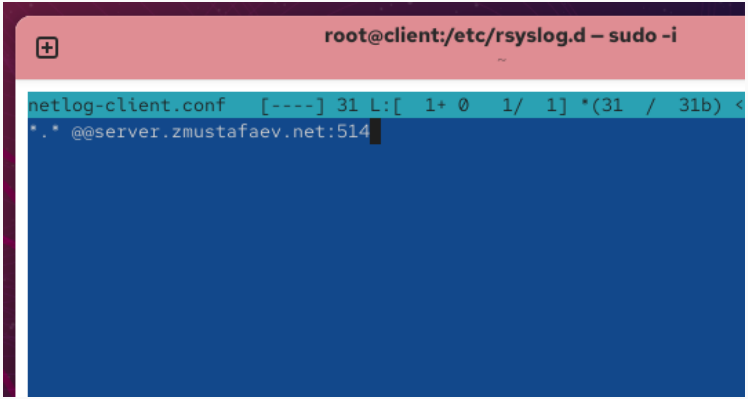


Рис. 3: Настройка firewall для порта 514

Настройка клиента сетевого журнала

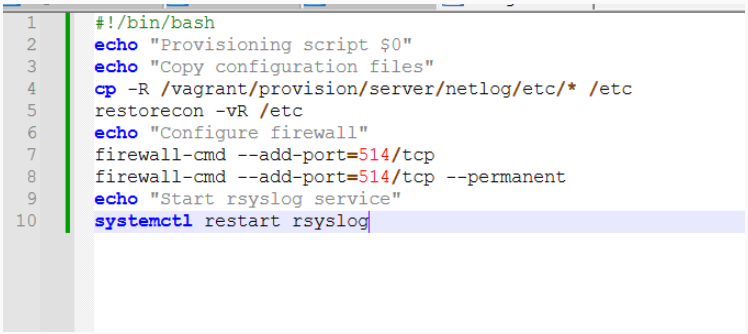
```
Dec 12 14:05:56 server systemd[1]: systemd-coredump@105-11594-0.service: Deactivated successfully.
Dec 12 14:05:54 client kernel: traps: VBoxClient[14015] trap int3 ip:41dd1b sp:7f5a61a35cd0 error:0 in VBoxClient[1dd1
b,400000+bb000]
Dec 12 14:05:54 client systemd-coredump[14016]: Process 14012 (VBoxClient) 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  0x000000000043
```

Рис. 4: Конфигурация netlog-client.conf

Проверка приёма журналов на сервере

Мониторинг системы

Рис. 6: Мониторинг ресурсов системы



```
#!/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. 7: Попытка установки lnav

Автоматизация настройки сервера

```
#!/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. 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.