Лабораторная работа №15

Настройка сетевого журналирования

Студент: Пакавира Арсениу Висенте Луиш

Группа: Нфибд 02 –23

дисциплина: **Администрирование сетевых подсистем (Lab 15)**

Цель работы

- Целью данной работы является получение навыков по работе с журналами системных событий.

Настройка сервера сетевого журнала

Рис. 1.1. Создание на сервере файла конфигурации сетевого хранения журналов.

Настройка сервера сетевого журнала

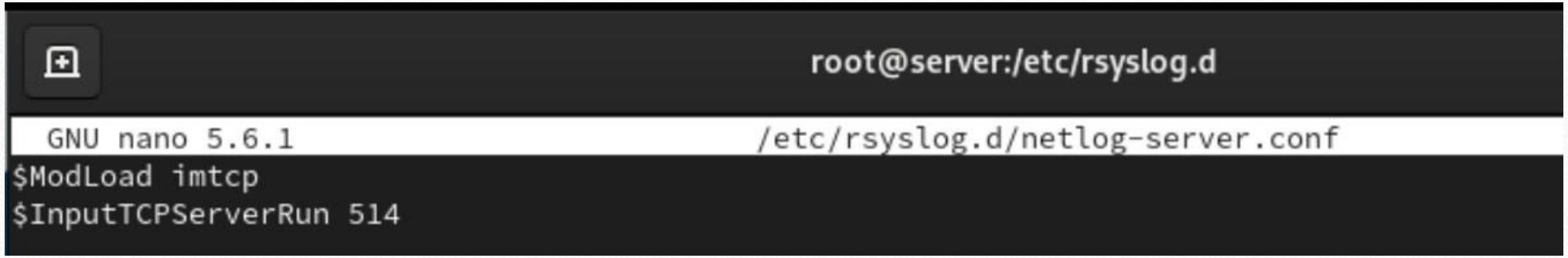

Рис. 1.2. Включение в файле конфигурации /etc/rsyslog.d/netlog-server.conf приёма записей журнала по TCP-порту 514.

Настройка сервера сетевого журнала

```
[root@server.user.net rsyslog.d]# systemctl restart rsyslog
[root@server.user.net rsyslog.d]# lsof | grep TCP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
      Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/doc
      Output information may be incomplete.
cupsd      986                          root    6u     IPv6              23702       0t0        TCP localhost:ipp (LIS
TEN)
cupsd      986                          root    7u     IPv4              23703       0t0        TCP localhost:ipp (LIS
TEN)
sshd       988                          root    3u     IPv4              23717       0t0        TCP *:ssh (LISTEN)
sshd       988                          root    4u     IPv6              23719       0t0        TCP *:ssh (LISTEN)
master    1293                          root   13u     IPv4              23894       0t0        TCP localhost:smtp (LI
STEN)
smbd      1321                          root   27u     IPv6              24053       0t0        TCP *:microsoft-ds (LI
STEN)
smbd      1321                          root   28u     IPv6              24054       0t0        TCP *:netbios-ssn (LIS
TEN)
smbd      1321                          root   29u     IPv4              24056       0t0        TCP *:microsoft-ds (LI
STEN)
smbd      1321                          root   30u     IPv4              24057       0t0        TCP *:netbios-ssn (LIS
TEN)
firefox   2665                          user  125u     IPv4              30969       0t0        TCP server.user.net:38
```

Рис. 1.3. Перезапуск службы rsyslog и просмотр прослушиваемых портов, связанных с rsyslog.

Настройка сервера сетевого журнала

Рис. 1.4. Настройка на сервере межсетевого экрана для приёма сообщений по TCP-порту 514.

Настройка клиента сетевого журнала

Рис. 2.1. Создание на клиенте файла конфигурации сетевого хранения журналов.

Настройка клиента сетевого журнала

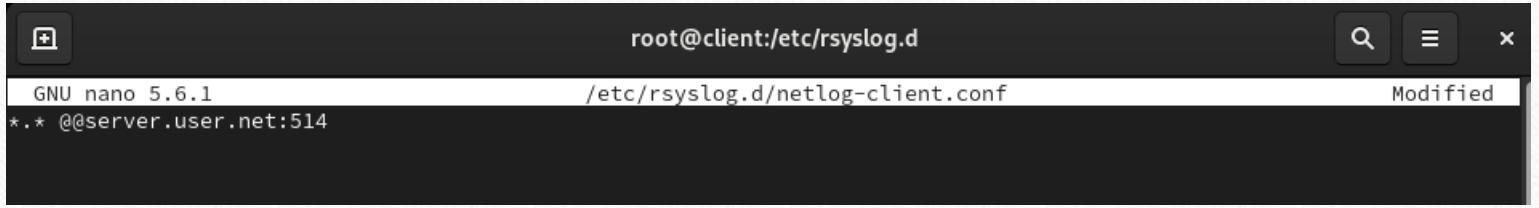

Рис. 2.2. Включение в файле конфигурации /etc/rsyslog.d/netlog-client.conf перенаправления сообщений журнала на 514 TCP-порт сервера.

Настройка клиента сетевого журнала

```
[root@client.user.net rsyslog.d]# systemctl restart rsyslog
[root@client.user.net rsyslog.d]#
```

Просмотр журнала

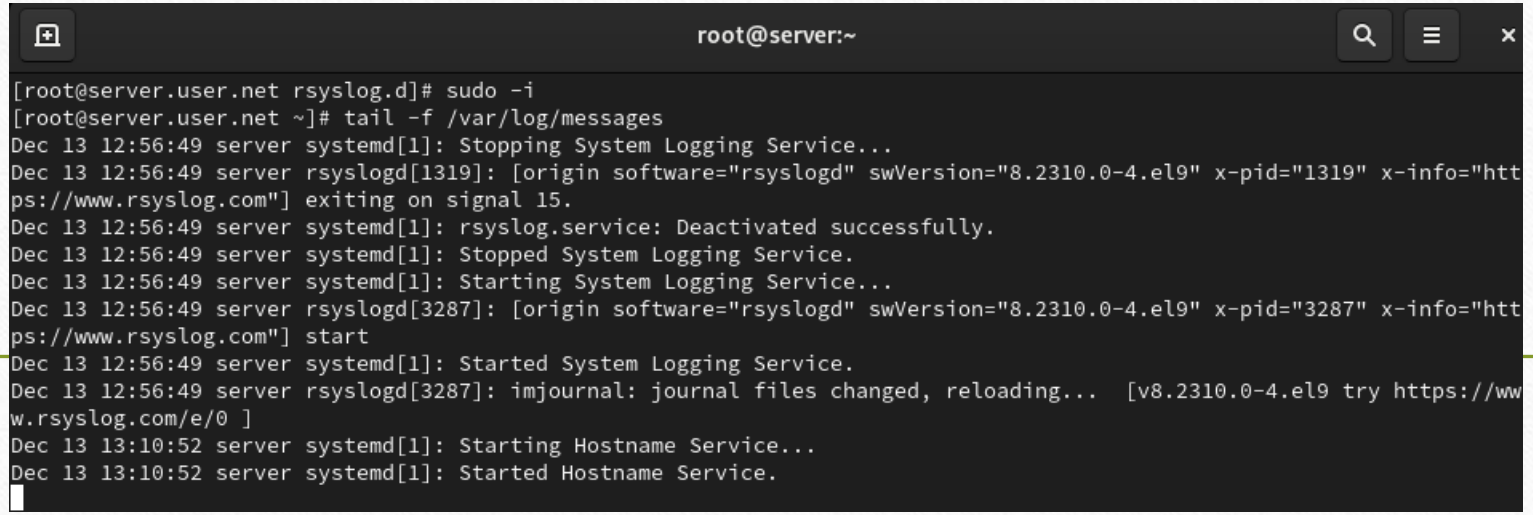

Рис. 3.1. Просмотр на сервере одного из файлов журнала.

Просмотр журнала

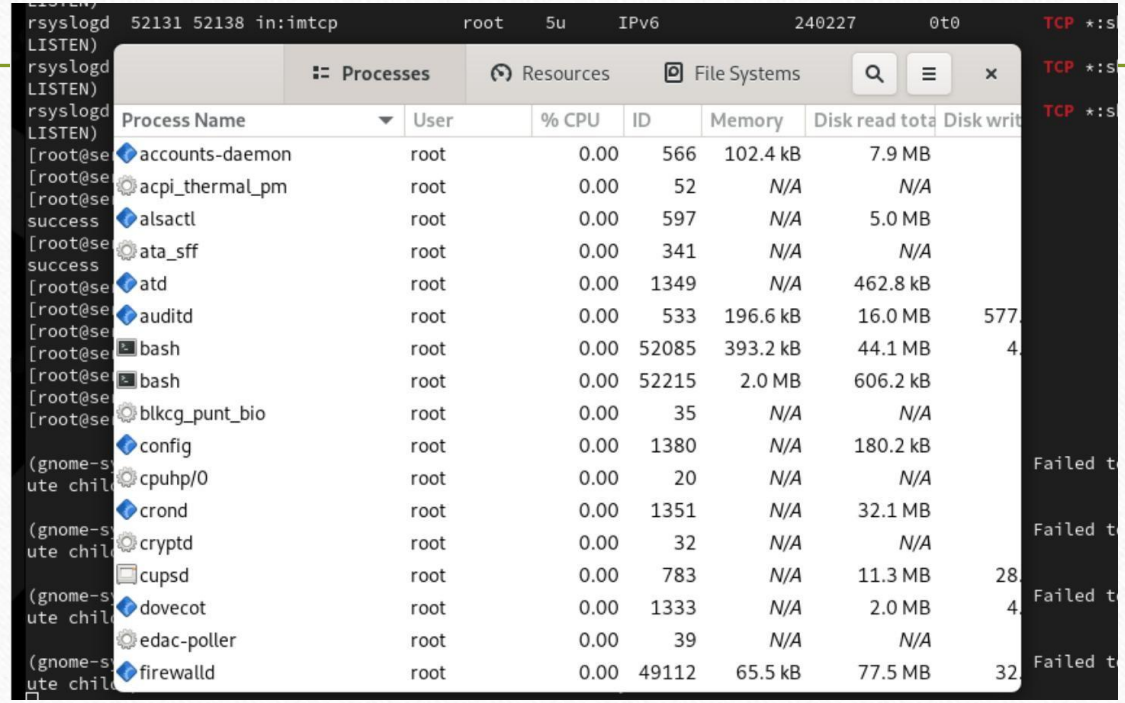

Рис. 3.2. Запуск на сервере под пользователем claudely графической программы для просмотра журналов.

Просмотр журнала

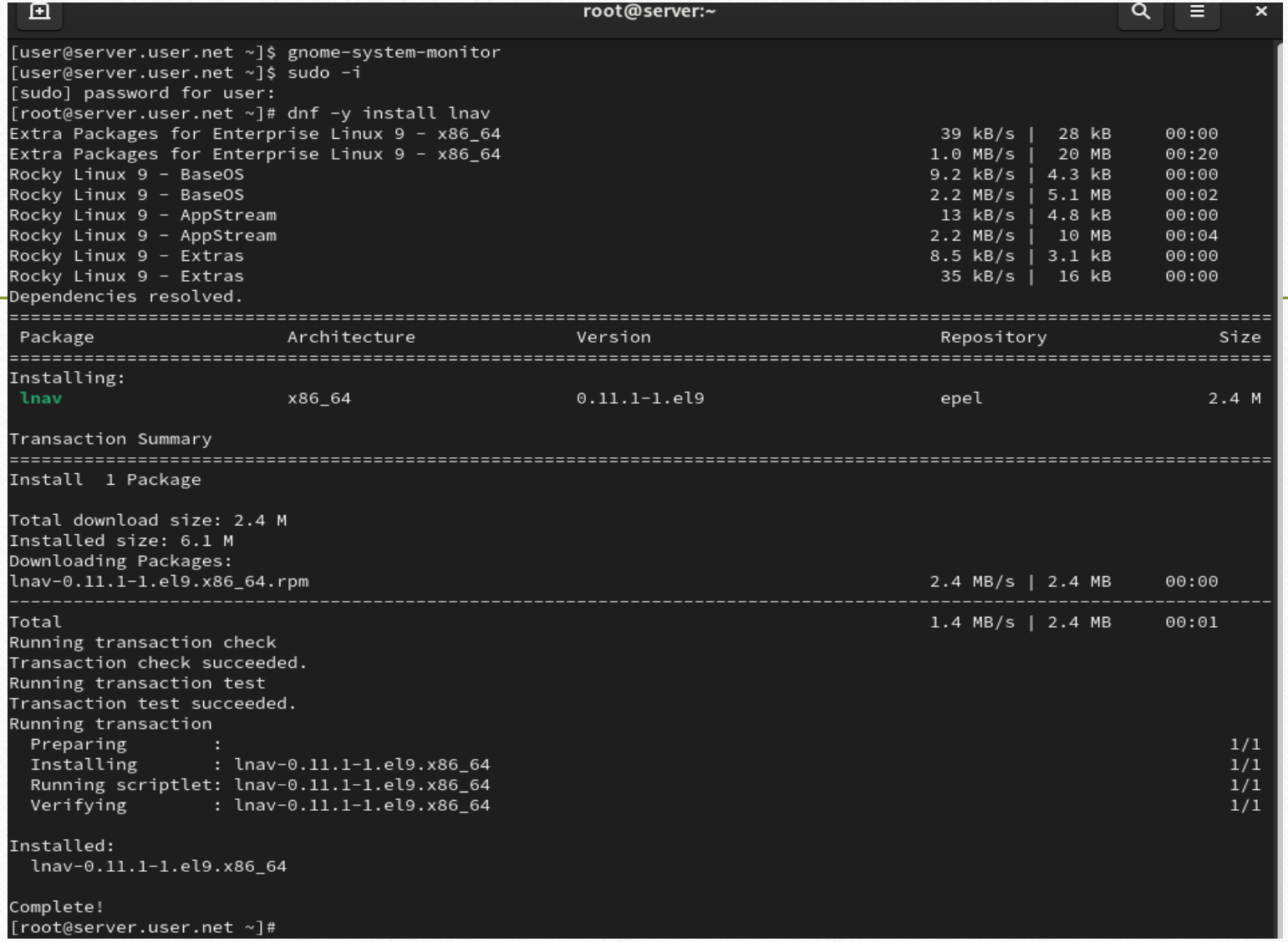
root@server:~
[user@server.user.net ~]$ gnome-system-monitor
[user@server.user.net ~]$ sudo -i
[sudo] password for user:
[root@server.user.net ~]# dnf -y install lnav
Extra Packages for Enterprise Linux 9 - x86_64 39 kB/s | 28 kB 00:00
Extra Packages for Enterprise Linux 9 - x86_64 1.0 MB/s | 20 MB 00:20
Rocky Linux 9 - BaseOS 9.2 kB/s | 4.3 kB 00:00
Rocky Linux 9 - BaseOS 2.2 MB/s | 5.1 MB 00:02
Rocky Linux 9 - AppStream 13 kB/s | 4.8 kB 00:00
Rocky Linux 9 - AppStream 2.2 MB/s | 10 MB 00:04
Rocky Linux 9 - Extras 8.5 kB/s | 3.1 kB 00:00
Rocky Linux 9 - Extras 35 kB/s | 16 kB 00:00
Dependencies resolved.
Package Architecture Version Repository Size
Installing:
lnav x86_64 0.11.1-1.el9 epel 2.4 M
Transaction Summary
Install 1 Package
Total download size: 2.4 M
Installed size: 6.1 M
Downloading Packages:
lnav-0.11.1-1.el9.x86_64.rpm 2.4 MB/s | 2.4 MB 00:00
Total 1.4 MB/s | 2.4 MB 00:01
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing : 1/1
Installing : lnav-0.11.1-1.el9.x86_64 1/1
Running scriptlet: lnav-0.11.1-1.el9.x86_64 1/1
Verifying : lnav-0.11.1-1.el9.x86_64 1/1
Installed:
lnav-0.11.1-1.el9.x86_64
Complete!
[root@server.user.net ~]#

Рис. 3.3. Установка на сервере просмотрщика журналов системных сообщений lnav.

Просмотр журнала

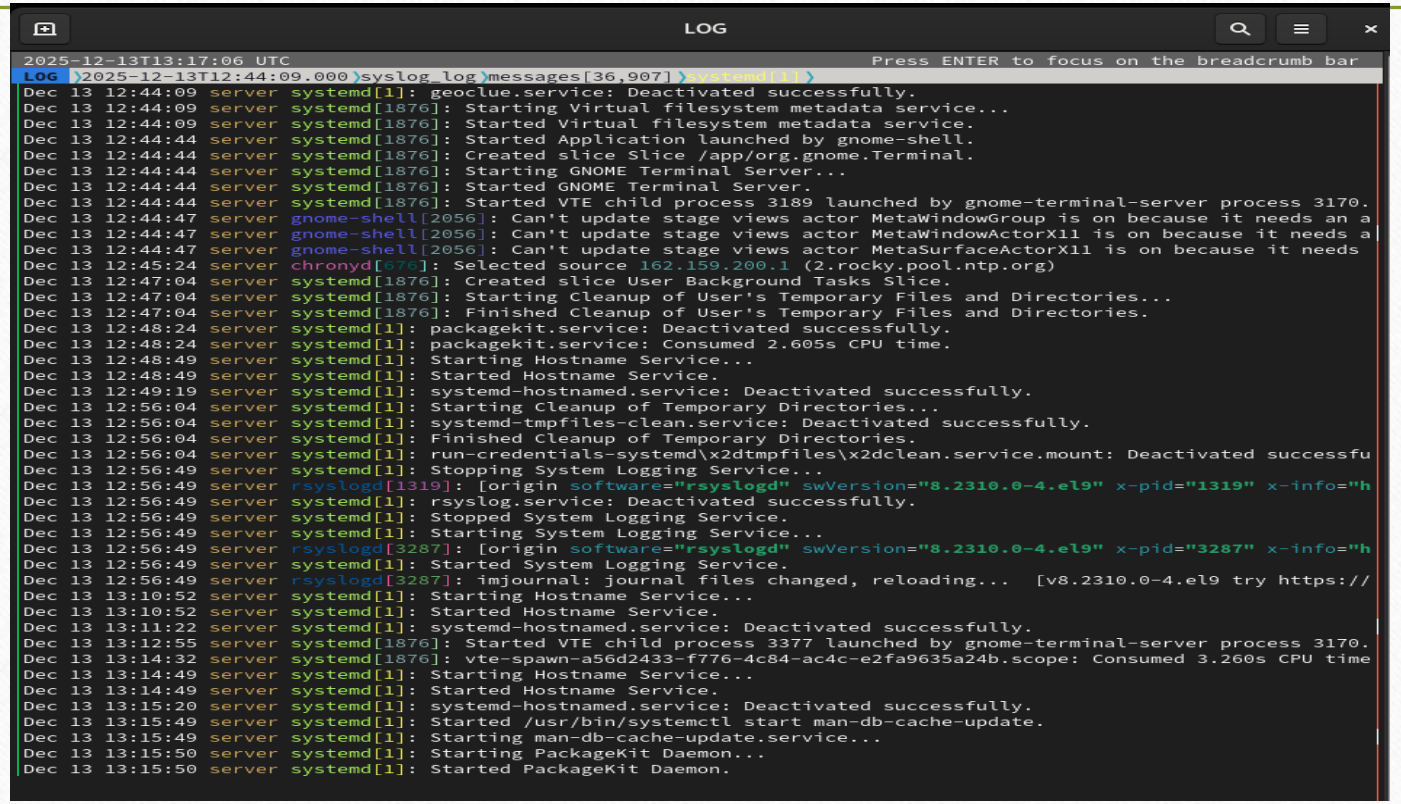

Рис. 3.4. Просмотр логов с помощью lnav.

Внесение изменений в настройки внутреннего окружения виртуальных машин

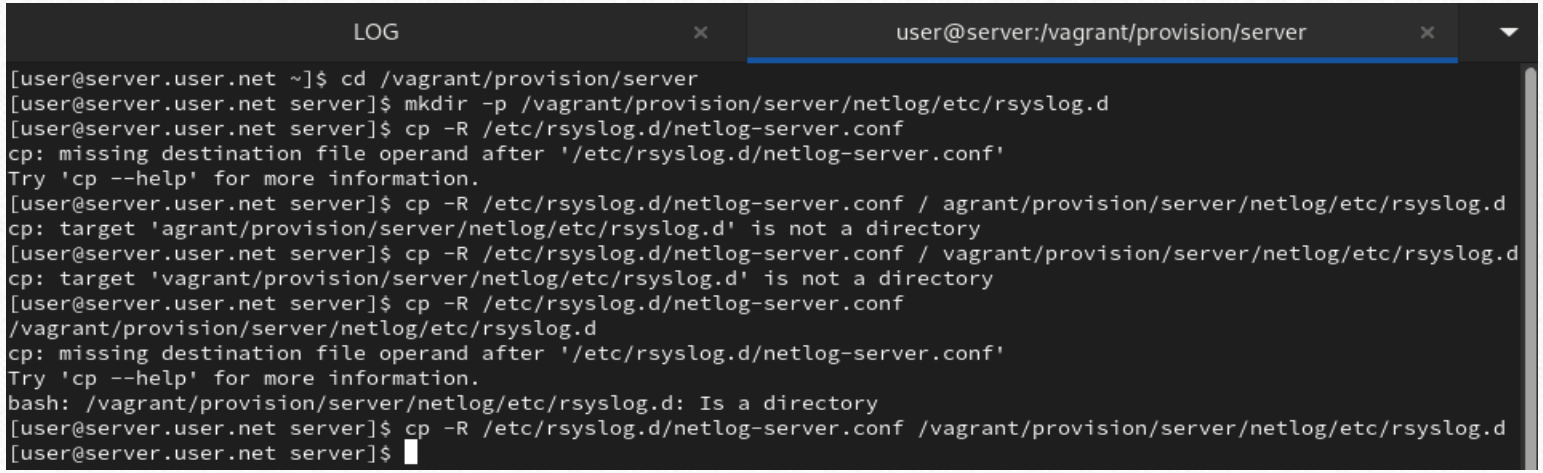

Рис. 4.1. Переход на виртуальной машине server в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога netlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге /vagrant/provision/server исполняемого файла netlog.sh.

Внесение изменений в настройки внутреннего окружения виртуальных машин

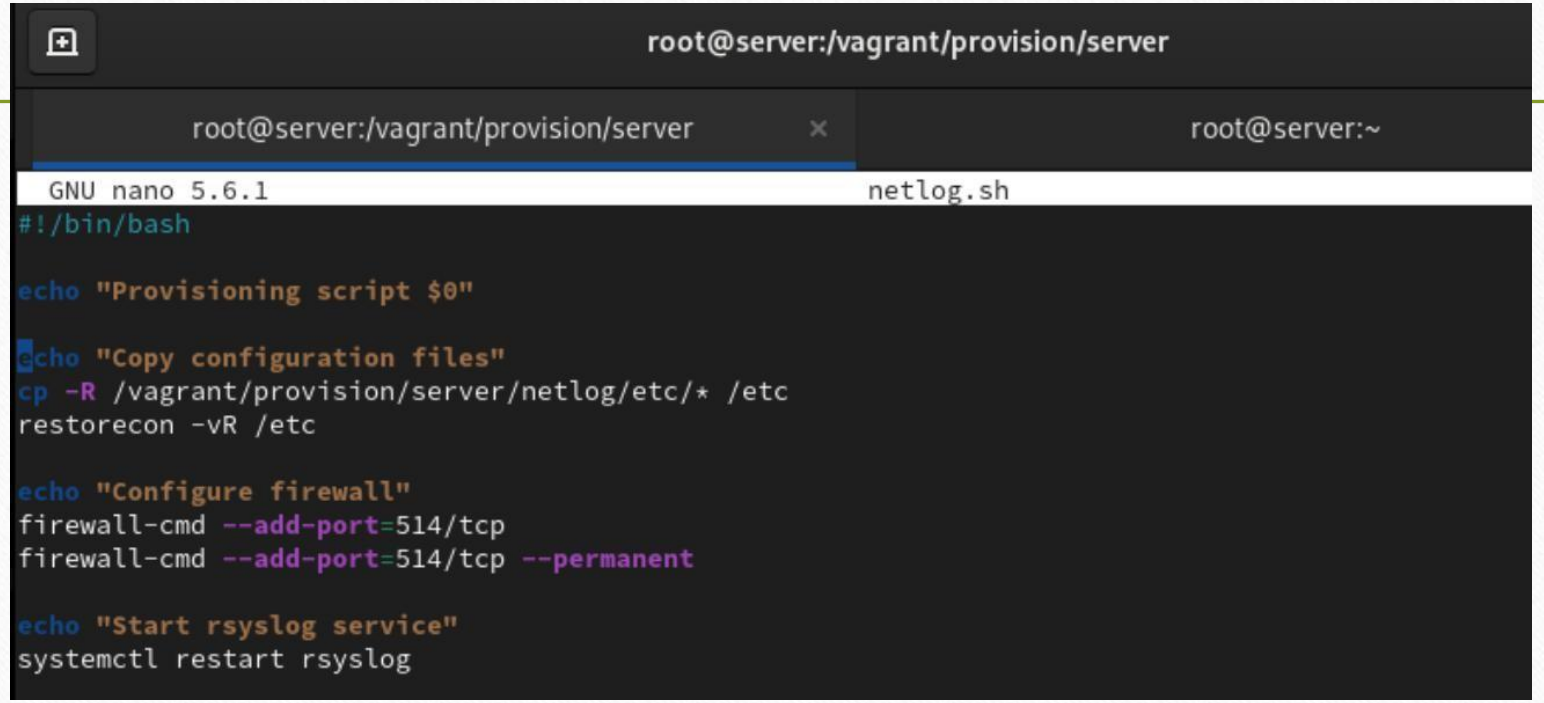

Рис. 4.2. Открытие файла на редактирование и добавление в него скрипта.

Внесение изменений в настройки внутреннего окружения виртуальных машин

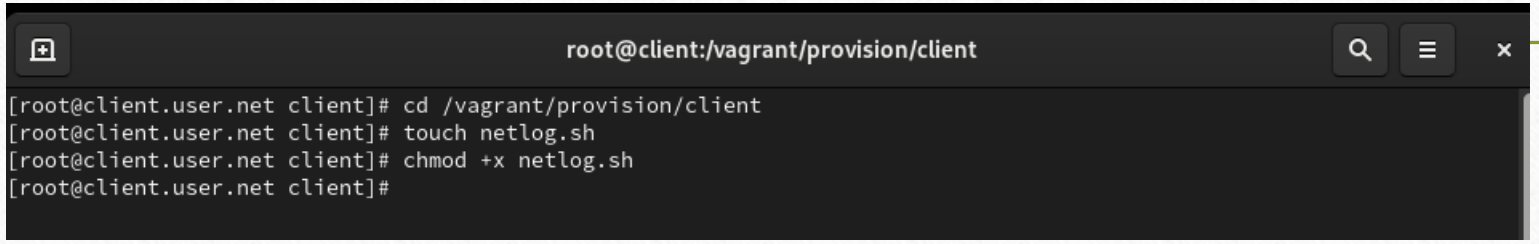

Рис. 4.3. Переход на виртуальной машине client в каталог для внесения изменений в настройки внутреннего окружения

/vagrant/provision/client/, создание в нём каталога nentlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге /vagrant/provision/client исполняемого файла netlog.sh.

Внесение изменений в настройки внутреннего окружения виртуальных машин

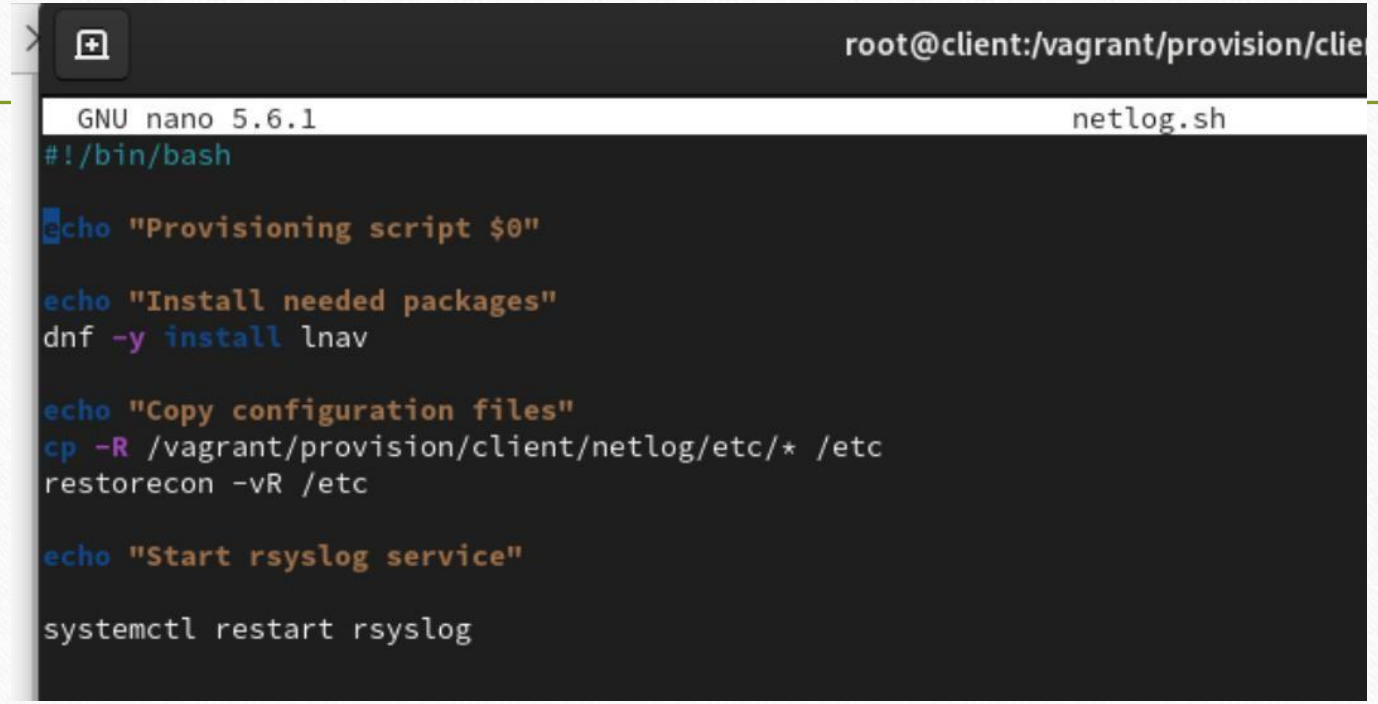

Рис. 4.4. Открытие файла на редактирование и добавление в него скрипта.

Внесение изменений в настройки внутреннего окружения виртуальных машин

```
                    preserve_order: true,
                    path: "provision/server/smb.sh"
server.vm.provision "server netlog",
                    type: "shell",
                    preserve_order: true,
                    path: "provision/server/netlog.sh"
```

Рис. 4.5. Добавление конфигураций в конфигурационном файле Vagrantfile для сервера.

Внесение изменений в настройки внутреннего окружения виртуальных машин

```
                        preserve_order: true,
                        path: "provision/client/smb.sh"
client.vm.provision "client netlog",
                        type: "shell",
                        preserve_order: true,
                        path: "provision/client/netlog.sh"
```

Рис. 4.6. Добавление конфигураций в конфигурационном файле Vagrantfile для клиента.

Вывод

- В ходе выполнения лабораторной работы были получены навыки по работе с журналами системных событий.

Спасибо за внимание!