РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук Кафедра теории вероятностей и кибербезопасности

ОТЧЁТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ №15

дисциплина: Администрирование сетевых подсистем

Студент: Пакавира Арсениу Висенте Луиш

Студ. билет № 1032225105

Группа: НфИбд-02-23

МОСКВА

2025 г.

Цель работы:

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

Выполнение работы:

На сервере создадим файл конфигурации сетевого хранения журналов (Рис. 1.1):

cd /etc/rsyslog.d

touch netlog-server.conf

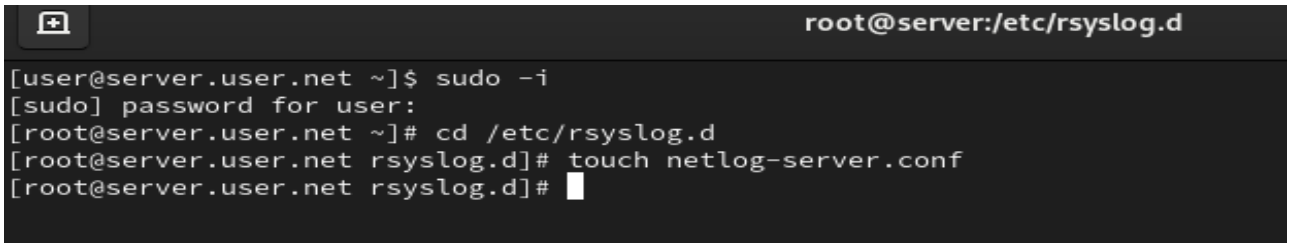

Рис. 1.1. Создание на сервере файла конфигурации сетевого хранения журналов.

В файле конфигурации /etc/rsyslog.d/netlog-server.conf включим приём записей журнала по TCP-порту 514 (Рис. 1.2):

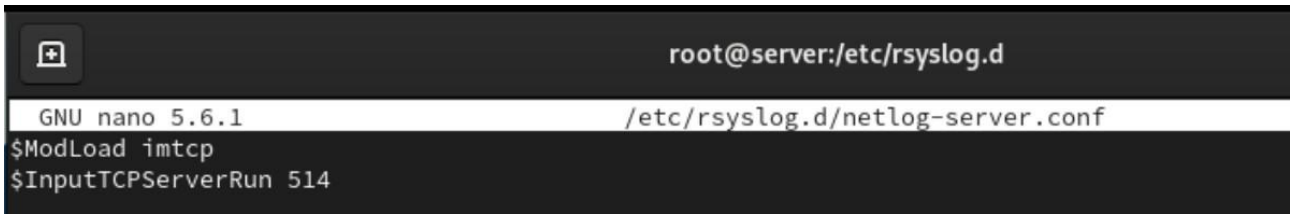

Рис. 1.2. Включение в файле конфигурации /etc/rsyslog.d/netlog-server.conf приёма записей журнала по TCP-порту 514.

Перезапустим службу rsyslog и посмотрим, какие порты, связанные с rsyslog, прослушиваются (Рис. 1.3):

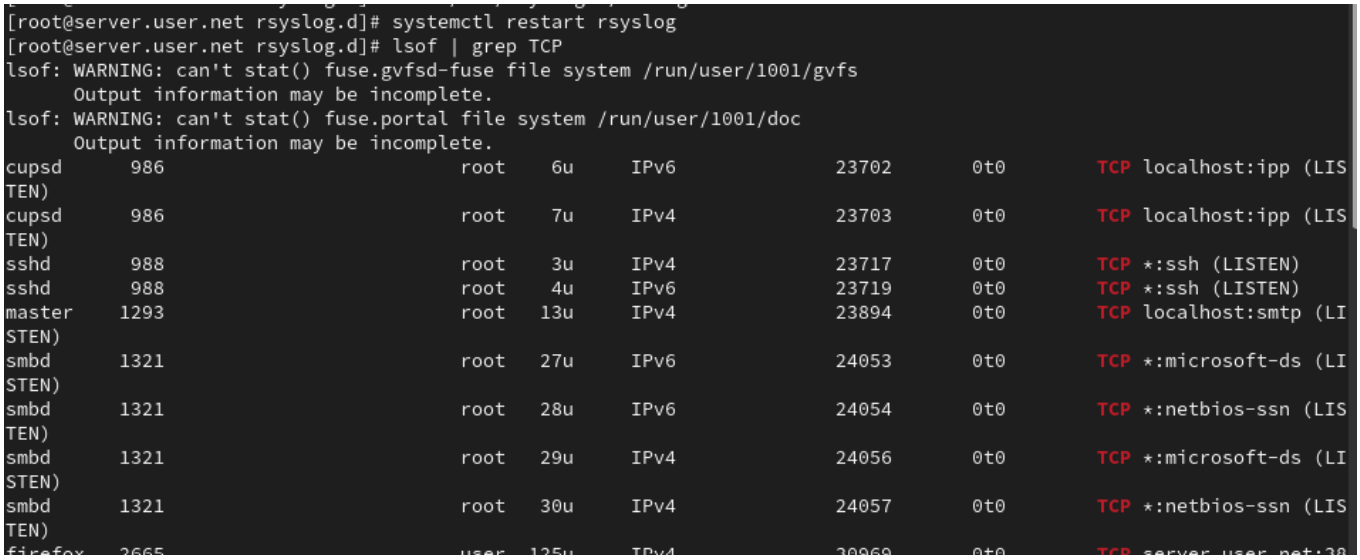

Рис. 1.3. Перезапуск службы rsyslog и просмотр прослушиваемых портов, связанных с rsyslog.

На сервере настроим межсетевой экран для приёма сообщений по TCPпорту 514 (Рис. 1.4):

firewall-cmd --add-port=514/tcp

firewall-cmd --add-port=514/tcp --permanent

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

На клиенте создадим файл конфигурации сетевого хранения журналов (Рис. 2.1):

cd /etc/rsyslog.d touch

netlog-client.conf

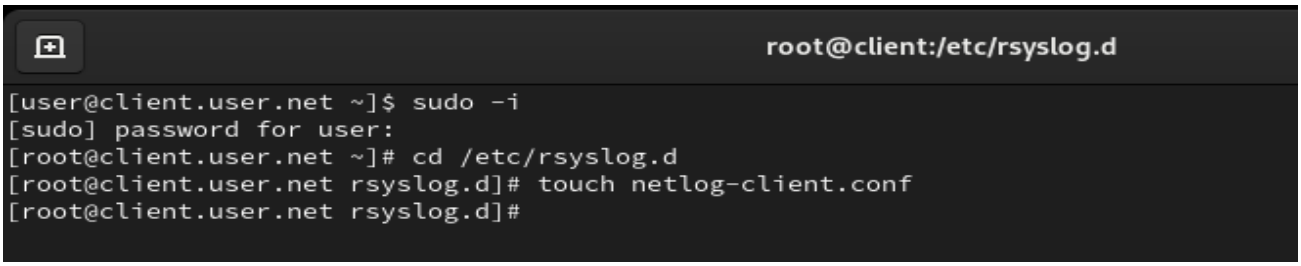

Рис. 2.1. Создание на клиенте файла конфигурации сетевого хранения журналов.

Далее в файле конфигурации /etc/rsyslog.d/netlog-client.conf включим перенаправление сообщений журнала на 514 TCP-порт сервера (Рис. 2.2):

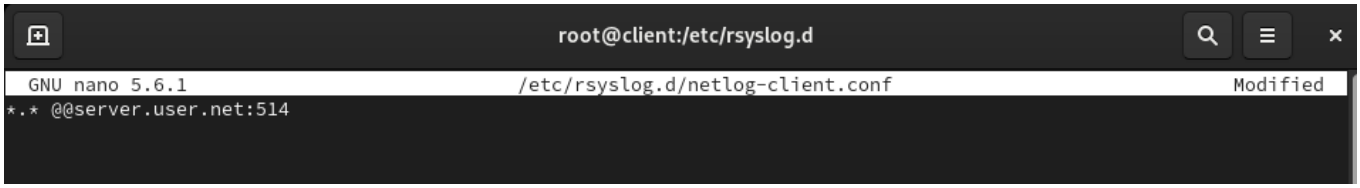

Рис. 2.2. Включение в файле конфигурации /etc/rsyslog.d/netlog-client.conf перенаправления сообщений журнала на 514 TCP-порт сервера.

Перезапустим службу rsyslog (Рис. 2.3):

systemctl restart rsyslog

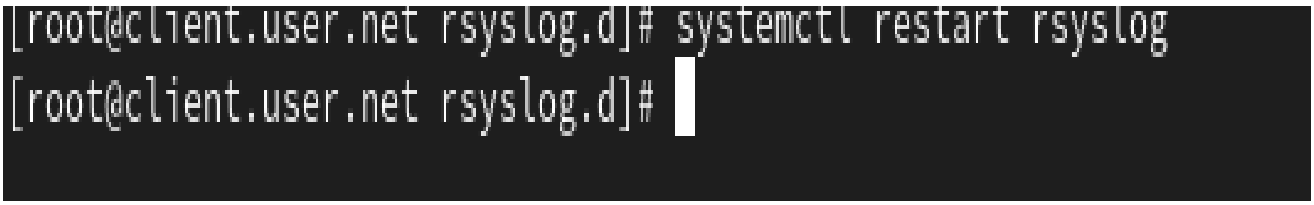

Рис. 2.3. Перезапуск службы rsyslog.

На сервере просмотрим один из файлов журнала (Рис. 3.1):

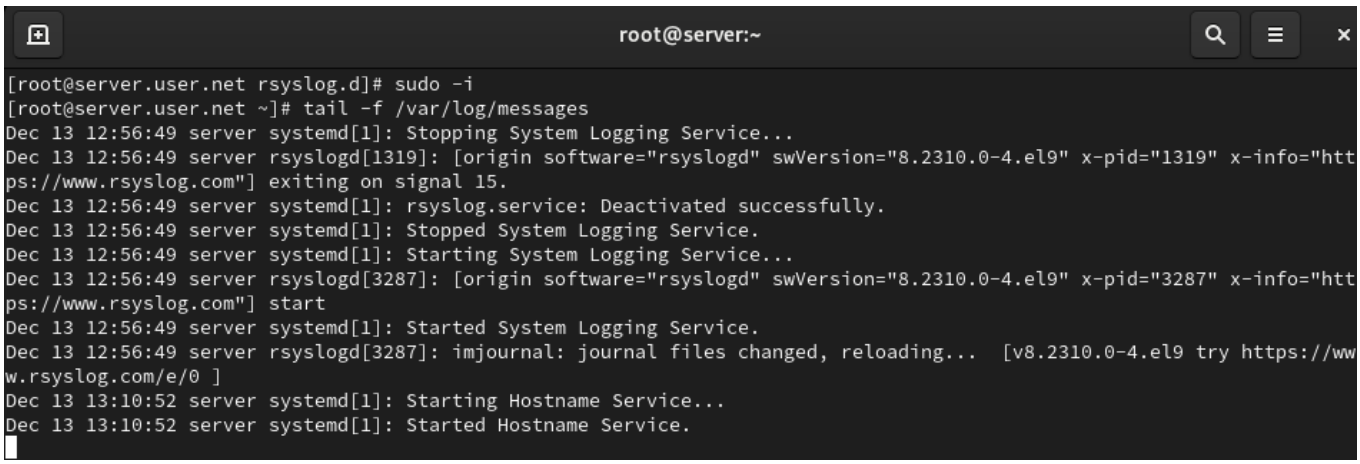

Рис. 3.1. Просмотр на сервере одного из файлов журнала.

На сервере под пользователем claudely запустим графическую программу для просмотра журналов (Рис. 3.2):

gnome-system-monitor

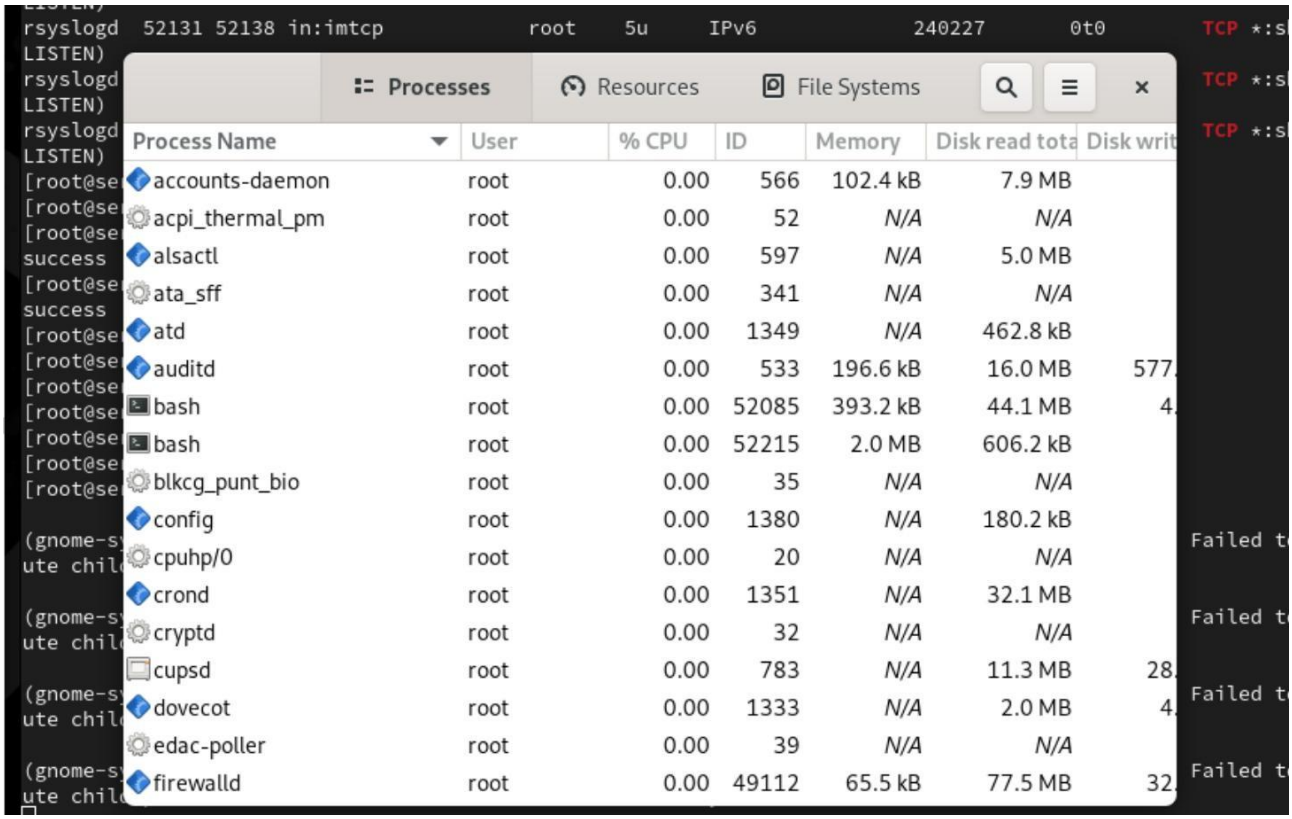

Рис. 3.2. Запуск на сервере под пользователем server графической программы для просмотра журналов.

На сервере установим просмотрщик журналов системных сообщений lnav (Рис. 3.3):

dnf -y install lnav

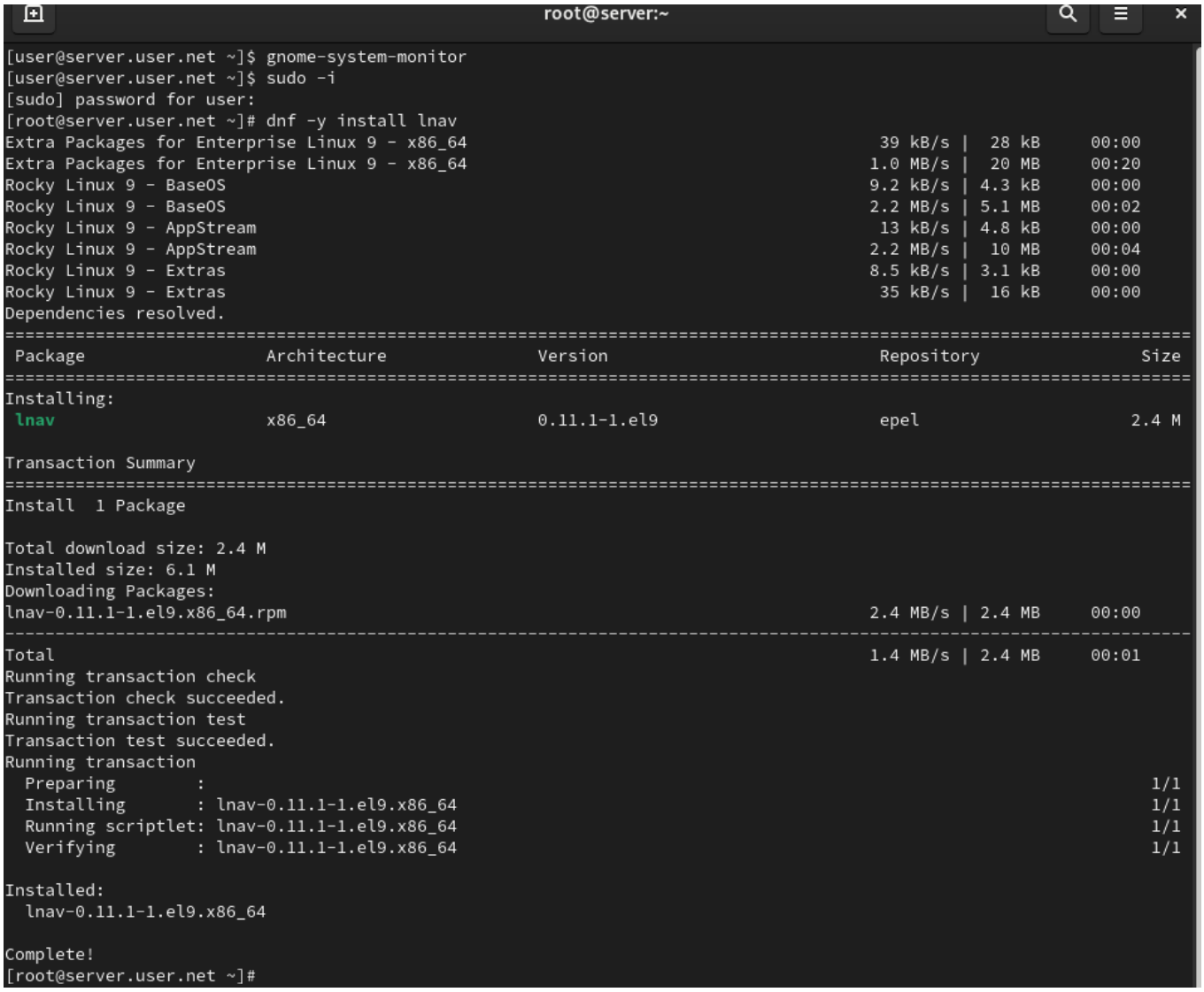

Рис. 3.3. Установка на сервере просмотрщика журналов системных сообщений lnav.

Просмотрим логи с помощью lnav (Рис. 3.4):

lnav

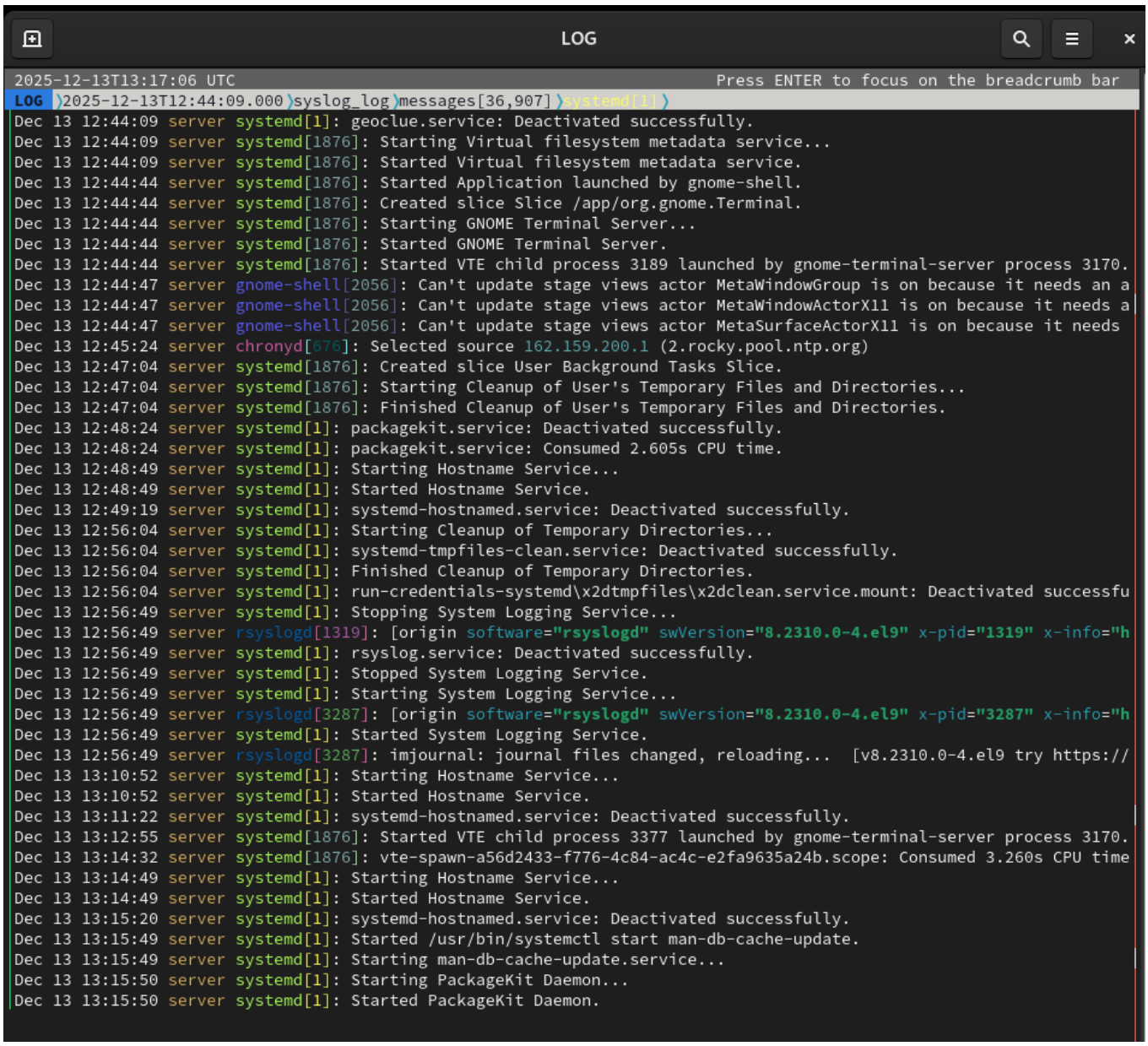

Рис. 3.4. Просмотр логов с помощью lnav.

На виртуальной машине server перейдём в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создадим в нём каталог netlog, в который поместим в соответствующие подкаталоги конфигурационные файлы. В каталоге /vagrant/provision/server создадим исполняемый файл netlog.sh (Рис. 4.1):

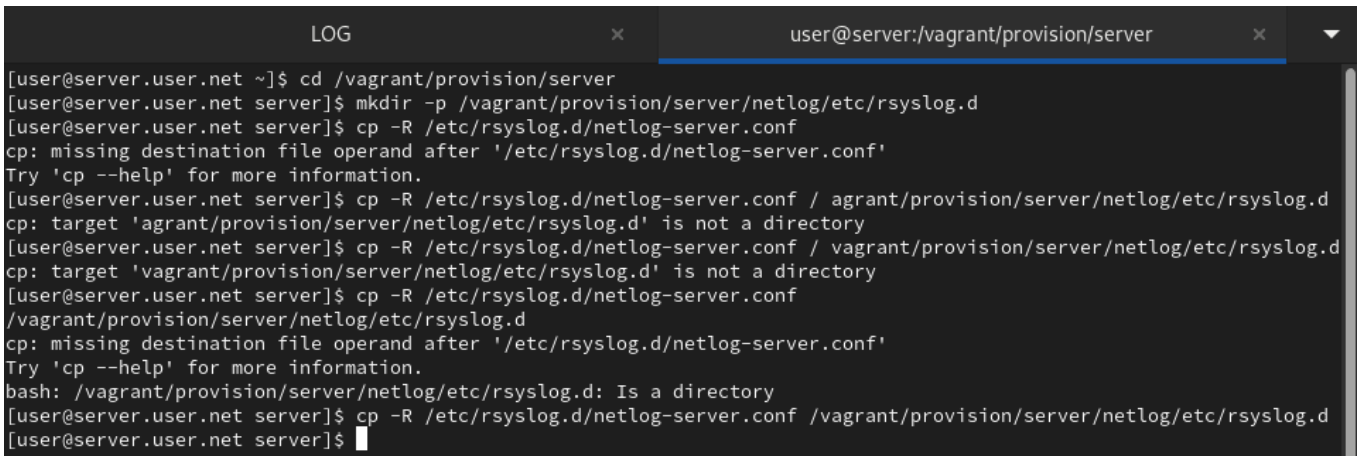

Рис. 4.1. Переход на виртуальной машине server в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога netlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге /vagrant/provision/server исполняемого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

Открыв его на редактирование, пропишем в нём скрипт (Рис. 4.2):

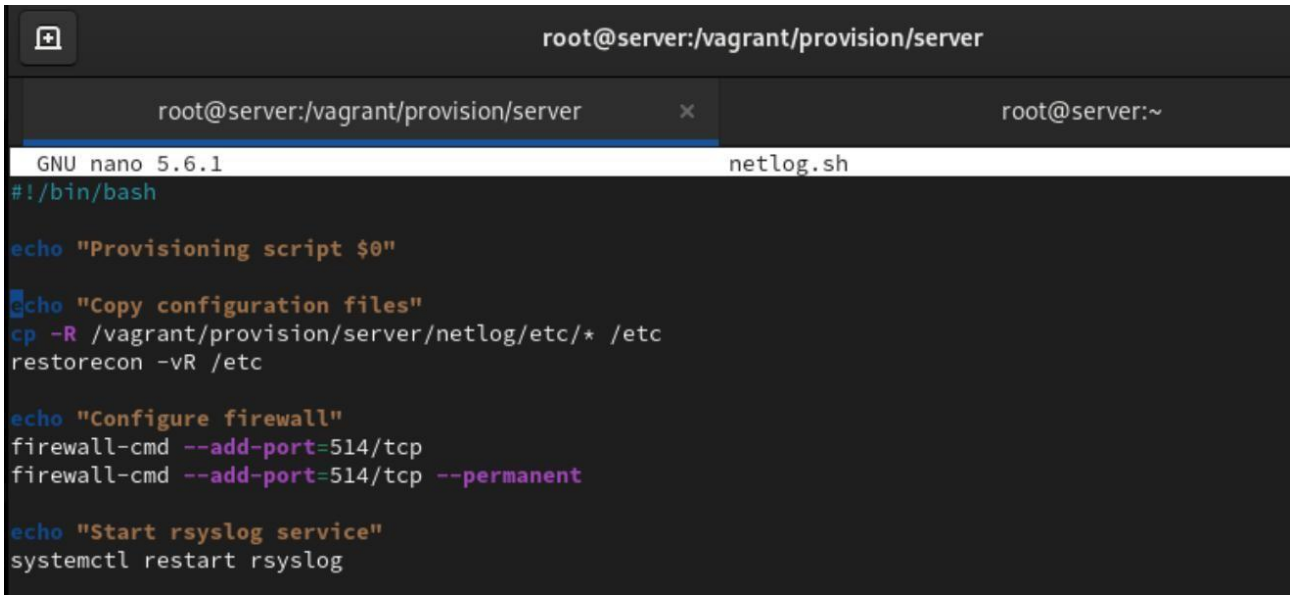

Рис. 4.2. Открытие файла на редактирование и добавление в него скрипта.

На виртуальной машине client перейдём в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создадим в нём

каталог nentlog, в который поместим в соответствующие подкаталоги конфигурационные файлы. В каталоге /vagrant/provision/client создадим исполняемый файл netlog.sh (Рис. 4.3):

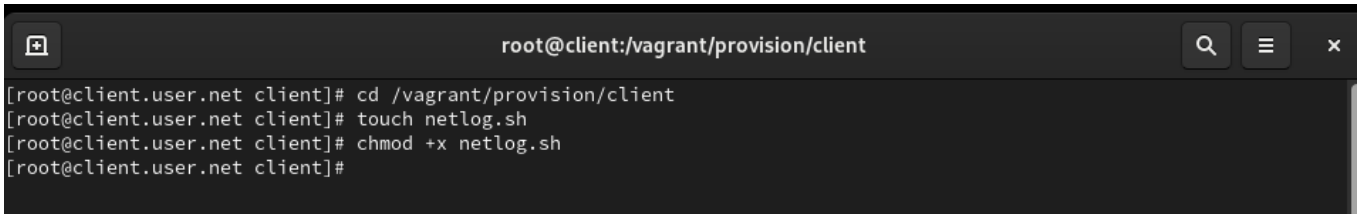

Рис. 4.3. Переход на виртуальной машине client в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создание в нём каталога nentlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге /vagrant/provision/client исполняемого файла netlog.sh.

Открыв его на редактирование, пропишем в нём скрипт (Рис. 4.4):

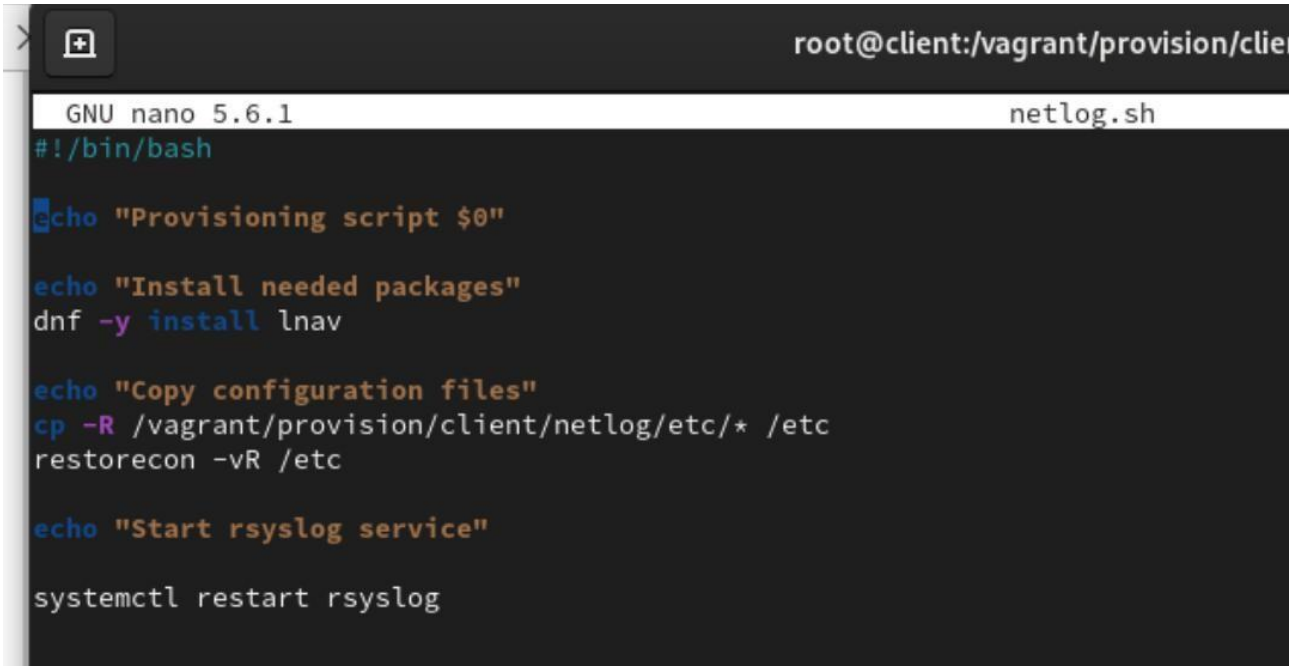

Рис. 4.4. Открытие файла на редактирование и добавление в него скрипта.

Для отработки созданных скриптов во время загрузки виртуальных машин server и client в конфигурационном файле Vagrantfile добавим в соответствующих разделах конфигураций для сервера (Рис. 4.5) и клиента (Рис.

4. 6):

```
                        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.

```
                        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.

Ответы на контрольные вопросы:

1. Какой модуль rsyslog вы должны использовать для приёма сообщений от journald? - **Для приёма сообщений от journald в rsyslog используется модуль imjournal.**
2. Как называется устаревший модуль, который можно использовать для включения приёма сообщений журнала в rsyslog? - **Устаревший модуль для приема сообщений журнала в rsyslog - imuxsock (или imuxsock_legacy).**
3. Чтобы убедиться, что устаревший метод приёма сообщений из journald в rsyslog не используется, какой дополнительный параметр следует использовать? - **Для предотвращения использования устаревшего метода можно использовать параметр SystemMaxUseForward=no в файле /etc/systemd/journald.conf.**
4. В каком конфигурационном файле содержатся настройки, которые позволяют вам настраивать работу журнала? - **Настройки, позволяющие настроить работу журнала, содержатся в файле /etc/systemd/journald.conf.**
5. Каким параметром управляется пересылка сообщений из journald в rsyslog? - **Для управления пересылкой сообщений из journald в rsyslog используется параметр ForwardToSyslog=yes в файле /etc/systemd/journald.conf.**
6. Какой модуль rsyslog вы можете использовать для включения сообщений из файла журнала, не созданного rsyslog? - **Для включения сообщений из файла журнала, не созданного rsyslog, используется модуль imfile.**
7. Какой модуль rsyslog вам нужно использовать для пересылки сообщений в базу данных MariaDB? - **Для пересылки сообщений в базу данных MariaDB используется модуль ommysql или ommysqlps.**

8. Какие две строки вам нужно включить в rsyslog.conf, чтобы позволить текущему журнальному серверу получать сообщения через TCP? - **Добавьте следующие строки в rsyslog.conf:**

   $ModLoad imtcp

   $InputTCPServerRun 514

9. Как настроить локальный брандмауэр, чтобы разрешить приём сообщений журнала через порт TCP 514? –

   Используйте команды для открытия порта: sudo

   firewall-cmd --permanent --add-port=514/tcp sudo

   firewall-cmd --reload

   Или:

   sudo iptables -A INPUT -p tcp --dport 514 -j ACCEPT
   sudo service iptables save sudo

   service iptables restart