

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:

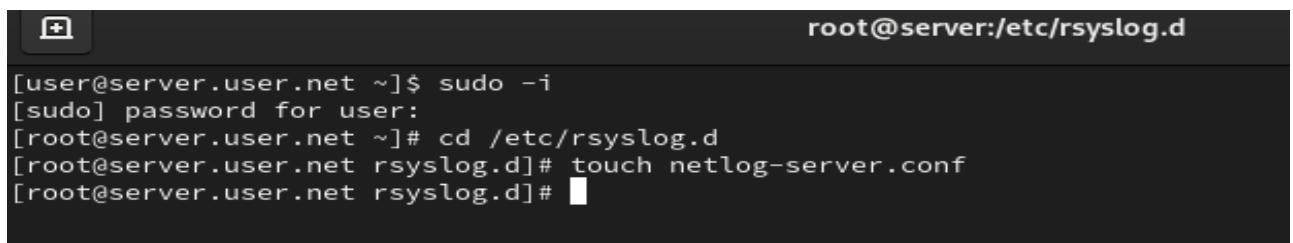
Целью данной работы является получение навыков по работе с журналами системных событий.

Выполнение работы:

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

```
cd /etc/rsyslog.d
```

```
touch netlog-server.conf
```

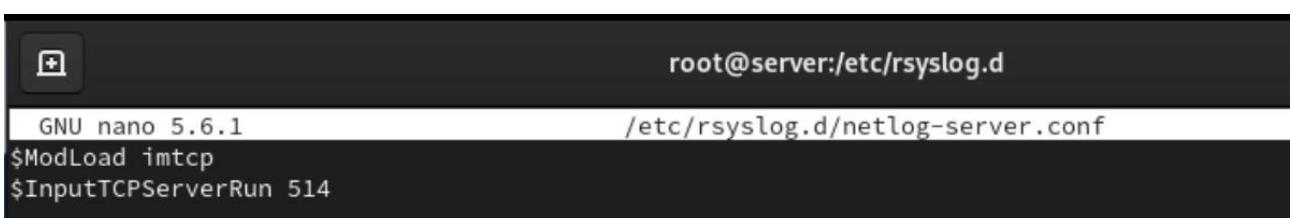


The screenshot shows a terminal window with a dark background and light-colored text. At the top right, it says "root@server:/etc/rsyslog.d". The terminal prompt is "[user@server.user.net ~]\$ sudo -i". The user enters their password. Then, they type "cd /etc/rsyslog.d" and "touch netlog-server.conf". Finally, they press the Enter key. The terminal window has a small icon in the top-left corner.

```
[user@server.user.net ~]$ sudo -i
[sudo] password for user:
[root@server.user.net ~]# cd /etc/rsyslog.d
[root@server.user.net rsyslog.d]# touch netlog-server.conf
[root@server.user.net rsyslog.d]#
```

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):



The screenshot shows a terminal window with a dark background and light-colored text. At the top right, it says "root@server:/etc/rsyslog.d". The terminal prompt is "/etc/rsyslog.d/netlog-server.conf". The user is using the nano editor to edit the file. The screen shows the command "GNU nano 5.6.1" followed by the configuration code: "\$ModLoad imtcp" and "\$InputTCPServerRun 514". The terminal window has a small icon in the top-left corner.

```
GNU nano 5.6.1
$ModLoad imtcp
$InputTCPServerRun 514
```

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):

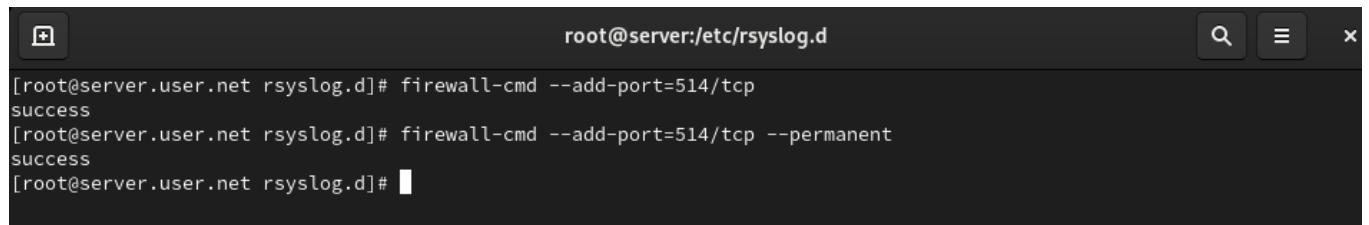
```
[root@server.user.net rsyslog.d]# systemctl restart rsyslog
[root@server.user.net rsyslog.d]# lsof | grep TCP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
      Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/doc
      Output information may be incomplete.
cupsd    986                      root   6u    IPv6          23702    0t0      TCP  localhost:ipp (LISTEN)
cupsd    986                      root   7u    IPv4          23703    0t0      TCP  localhost:ipp (LISTEN)
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 (LISTEN)
smbd   1321                      root   27u   IPv6          24053    0t0      TCP  *:microsoft-ds (LISTEN)
smbd   1321                      root   28u   IPv6          24054    0t0      TCP  *:netbios-ssn (LISTEN)
smbd   1321                      root   29u   IPv4          24056    0t0      TCP  *:microsoft-ds (LISTEN)
smbd   1321                      root   30u   IPv4          24057    0t0      TCP  *:netbios-ssn (LISTEN)
firefox 2665                     user   125u  IPv4          20060    0t0      TCP  server_user_port:2665
```

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
```



The screenshot shows a terminal window with a dark background and light-colored text. At the top, it says "root@server:/etc/rsyslog.d". The command "firewall-cmd --add-port=514/tcp" is entered twice, followed by "success" each time. The terminal ends with a "#".

```
[root@server.user.net rsyslog.d]# firewall-cmd --add-port=514/tcp
success
[root@server.user.net rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent
success
[root@server.user.net rsyslog.d]#
```

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
```

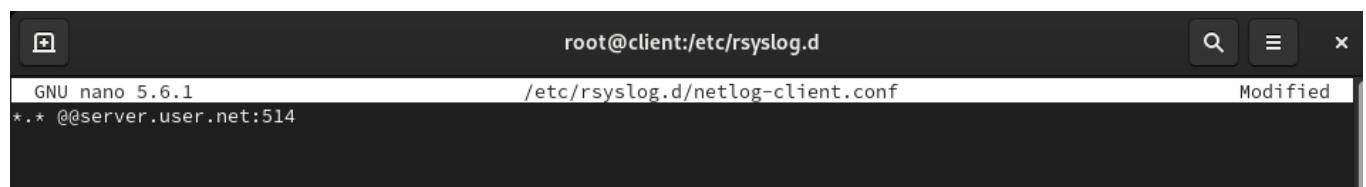
```
netlog-client.conf
```



```
[root@client user.net ~]$ sudo -i  
[sudo] password for user:  
[root@client user.net ~]# cd /etc/rsyslog.d  
[root@client user.net rsyslog.d]# touch netlog-client.conf  
[root@client user.net rsyslog.d]#
```

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):



```
GNU nano 5.6.1          /etc/rsyslog.d/netlog-client.conf      Modified  
.* @server.user.net:514
```

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
```



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

Рис. 2.3. Перезапуск службы rsyslog.

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

```
[root@server.user.net rsyslog.d]# sudo -i
[root@server.user.net ~]# tail -f /var/log/messages
Dec 13 12:56:49 server systemd[1]: Stopping System Logging Service...
Dec 13 12:56:49 server rsyslogd[1319]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="1319" x-info="https://www.rsyslog.com"] exiting on signal 15.
Dec 13 12:56:49 server systemd[1]: rsyslog.service: Deactivated successfully.
Dec 13 12:56:49 server systemd[1]: Stopped System Logging Service.
Dec 13 12:56:49 server systemd[1]: Starting System Logging Service...
Dec 13 12:56:49 server rsyslogd[3287]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="3287" x-info="https://www.rsyslog.com"] start
Dec 13 12:56:49 server systemd[1]: Started System Logging Service.
Dec 13 12:56:49 server rsyslogd[3287]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
Dec 13 13:10:52 server systemd[1]: Starting Hostname Service...
Dec 13 13:10:52 server systemd[1]: Started Hostname Service.
```

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

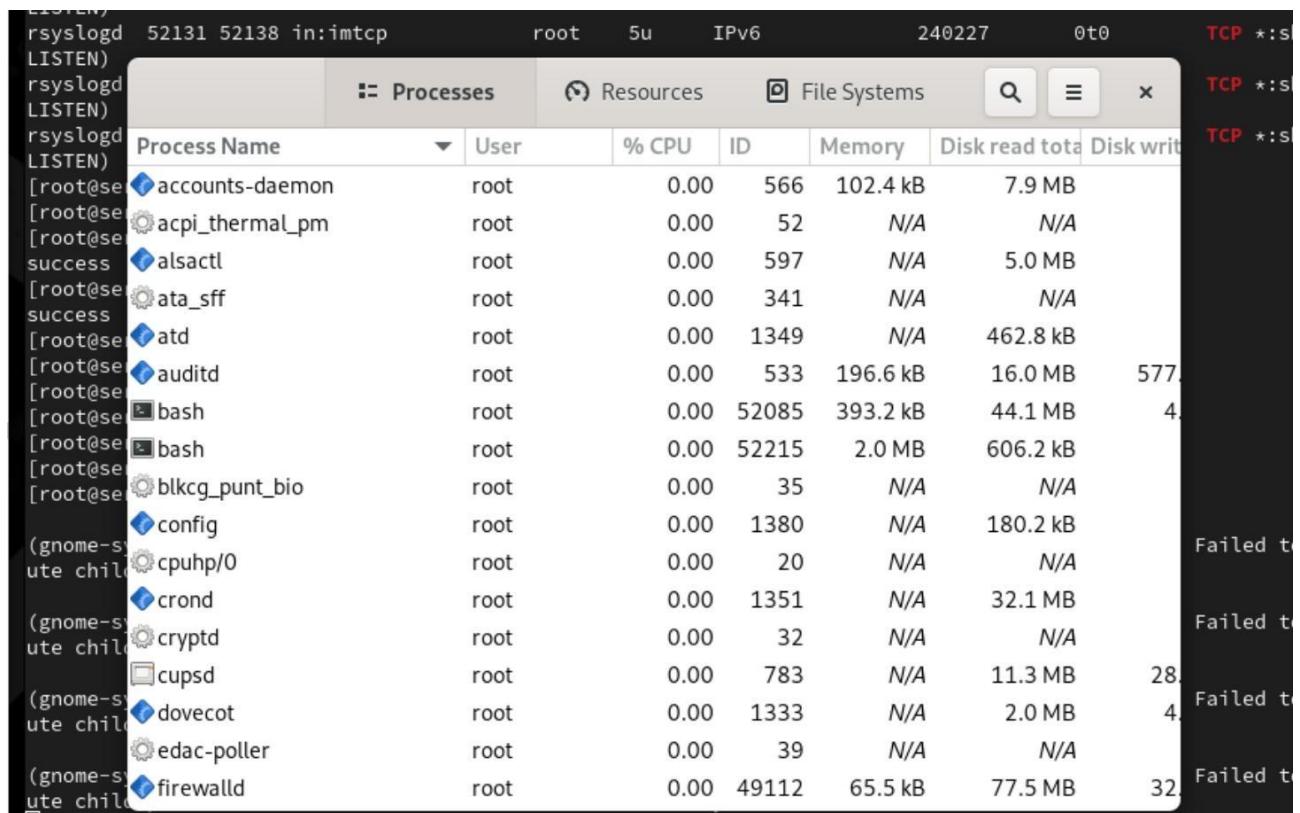
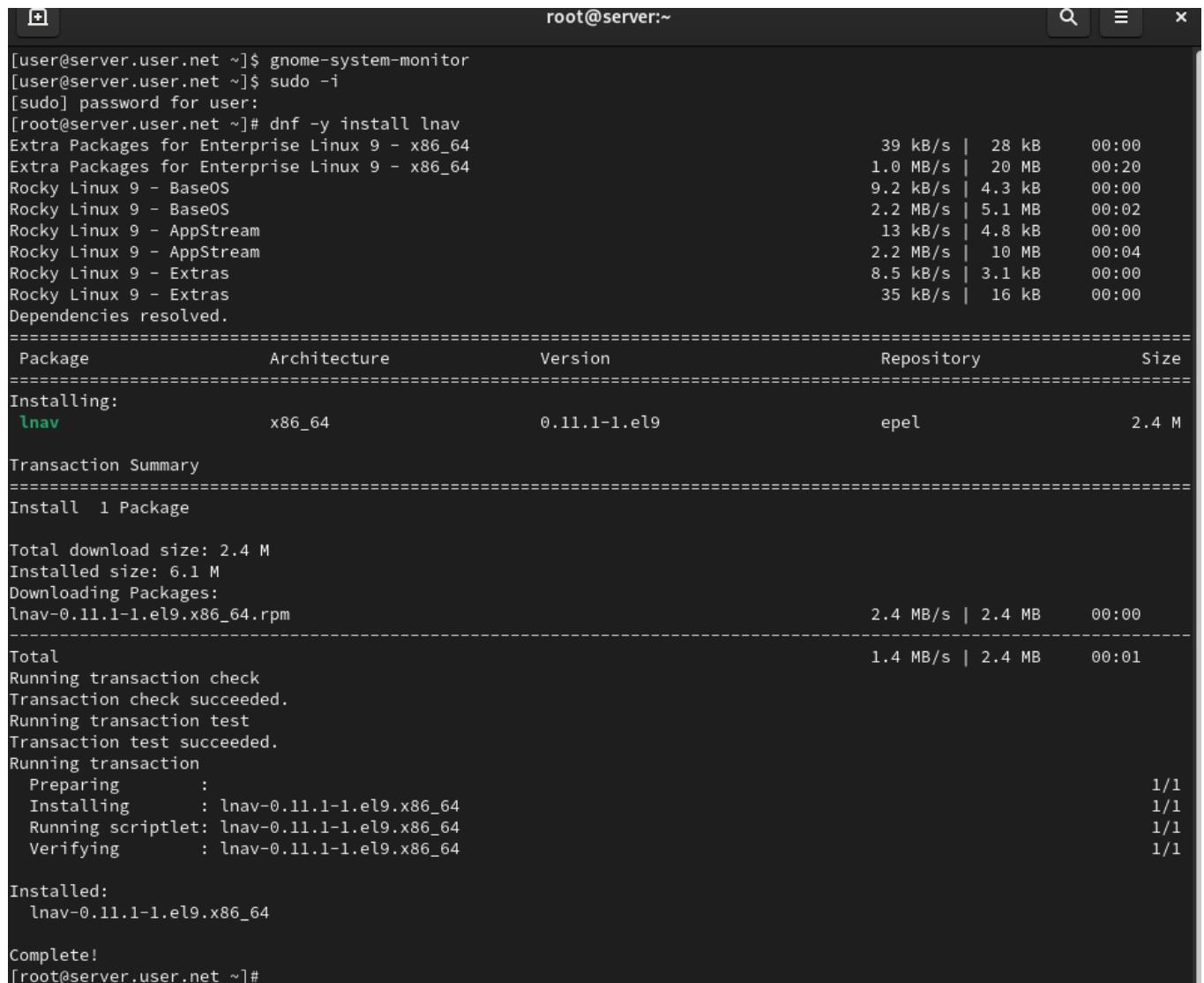


Рис. 3.2. Запуск на сервере под пользователем server графической программы для просмотра журналов.

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

```
dnf -y install lnav
```



```
[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
Extra Packages for Enterprise Linux 9 - x86_64
Rocky Linux 9 - BaseOS
Rocky Linux 9 - BaseOS
Rocky Linux 9 - AppStream
Rocky Linux 9 - AppStream
Rocky Linux 9 - Extras
Rocky Linux 9 - Extras
Dependencies resolved.
=====
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
Total
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.

Просмотрим логи с помощью lnav (Рис. 3.4):

```
lnav
```

```
2025-12-13T13:17:06 UTC
LOG >2025-12-13T12:44:09.000>syslog_log>messages[36,907]>systemd[1]>
Dec 13 12:44:09 server systemd[1]: geoclue.service: Deactivated successfully.
Dec 13 12:44:09 server systemd[1876]: Starting Virtual filesystem metadata service...
Dec 13 12:44:09 server systemd[1876]: Started Virtual filesystem metadata service.
Dec 13 12:44:44 server systemd[1876]: Started Application launched by gnome-shell.
Dec 13 12:44:44 server systemd[1876]: Created slice Slice /app/org.gnome.Terminal.
Dec 13 12:44:44 server systemd[1876]: Starting GNOME Terminal Server...
Dec 13 12:44:44 server systemd[1876]: Started GNOME Terminal Server.
Dec 13 12:44:44 server systemd[1876]: Started VTE child process 3189 launched by gnome-terminal-server process 3170.
Dec 13 12:44:47 server gnome-shell[2056]: Can't update stage views actor MetaWindowGroup is on because it needs an a
Dec 13 12:44:47 server gnome-shell[2056]: Can't update stage views actor MetaWindowActorX11 is on because it needs a
Dec 13 12:44:47 server gnome-shell[2056]: Can't update stage views actor MetaSurfaceActorX11 is on because it needs
Dec 13 12:45:24 server chrony[676]: Selected source 162.159.200.1 (2.rocky.pool.ntp.org)
Dec 13 12:47:04 server systemd[1876]: Created slice User Background Tasks Slice.
Dec 13 12:47:04 server systemd[1876]: Starting Cleanup of User's Temporary Files and Directories...
Dec 13 12:47:04 server systemd[1876]: Finished Cleanup of User's Temporary Files and Directories.
Dec 13 12:48:24 server systemd[1]: packagekit.service: Deactivated successfully.
Dec 13 12:48:24 server systemd[1]: packagekit.service: Consumed 2.605s CPU time.
Dec 13 12:48:49 server systemd[1]: Starting Hostname Service...
Dec 13 12:48:49 server systemd[1]: Started Hostname Service.
Dec 13 12:49:19 server systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Dec 13 12:56:04 server systemd[1]: Starting Cleanup of Temporary Directories...
Dec 13 12:56:04 server systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
Dec 13 12:56:04 server systemd[1]: Finished Cleanup of Temporary Directories.
Dec 13 12:56:04 server systemd[1]: run-credentials-systemd\x2dtmpfiles\x2dclean.service.mount: Deactivated successfu
Dec 13 12:56:49 server systemd[1]: Stopping System Logging Service...
Dec 13 12:56:49 server rsyslogd[1319]: [origin software="rsyslog" swVersion="8.2310.0-4.el9" x-pid="1319" x-info="h
Dec 13 12:56:49 server systemd[1]: rsyslog.service: Deactivated successfully.
Dec 13 12:56:49 server systemd[1]: Stopped System Logging Service.
Dec 13 12:56:49 server systemd[1]: Starting System Logging Service...
Dec 13 12:56:49 server rsyslogd[3287]: [origin software="rsyslog" swVersion="8.2310.0-4.el9" x-pid="3287" x-info="h
Dec 13 12:56:49 server systemd[1]: Started System Logging Service.
Dec 13 12:56:49 server rsyslogd[3287]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try https://
Dec 13 13:10:52 server systemd[1]: Starting Hostname Service...
Dec 13 13:10:52 server systemd[1]: Started Hostname Service.
Dec 13 13:11:22 server systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Dec 13 13:12:55 server systemd[1876]: Started VTE child process 3377 launched by gnome-terminal-server process 3170.
Dec 13 13:14:32 server systemd[1876]: vte-spawn-a56d2433-f776-4c84-ac4c-e2fa9635a24b.scope: Consumed 3.260s CPU time
Dec 13 13:14:49 server systemd[1]: Starting Hostname Service...
Dec 13 13:14:49 server systemd[1]: Started Hostname Service.
Dec 13 13:15:20 server systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Dec 13 13:15:49 server systemd[1]: Started /usr/bin/systemctl start man-db-cache-update.
Dec 13 13:15:49 server systemd[1]: Starting man-db-cache-update.service...
Dec 13 13:15:50 server systemd[1]: Starting PackageKit Daemon...
Dec 13 13:15:50 server systemd[1]: Started PackageKit Daemon.
```

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):

```
[user@server.user.net ~]$ cd /vagrant/provision/server
[user@server.user.net server]$ mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
[user@server.user.net server]$ cp -R /etc/rsyslog.d/netlog-server.conf
cp: missing destination file operand after '/etc/rsyslog.d/netlog-server.conf'
Try 'cp --help' for more information.
[user@server.user.net server]$ cp -R /etc/rsyslog.d/netlog-server.conf / vagrant/provision/server/netlog/etc/rsyslog.d
cp: target 'vagrant/provision/server/netlog/etc/rsyslog.d' is not a directory
[user@server.user.net server]$ cp -R /etc/rsyslog.d/netlog-server.conf / vagrant/provision/server/netlog/etc/rsyslog.d
cp: target 'vagrant/provision/server/netlog/etc/rsyslog.d' is not a directory
[user@server.user.net server]$ cp -R /etc/rsyslog.d/netlog-server.conf
/vagrant/provision/server/netlog/etc/rsyslog.d
cp: missing destination file operand after '/etc/rsyslog.d/netlog-server.conf'
Try 'cp --help' for more information.
bash: /vagrant/provision/server/netlog/etc/rsyslog.d: Is a directory
[user@server.user.net server]$ cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog.d
[user@server.user.net server]$
```

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):

```
root@server:/vagrant/provision/server
root@server:/vagrant/provision/server          x      root@server:~
root@server:/vagrant/provision/server          netlog.sh
GNU nano 5.6.1
#!/bin/bash

echo "Provisioning script $0"

echo "Copy configuration files"
cp -R /vagrant/provision/server/netlog/etc/* /etc
restorecon -vR /etc

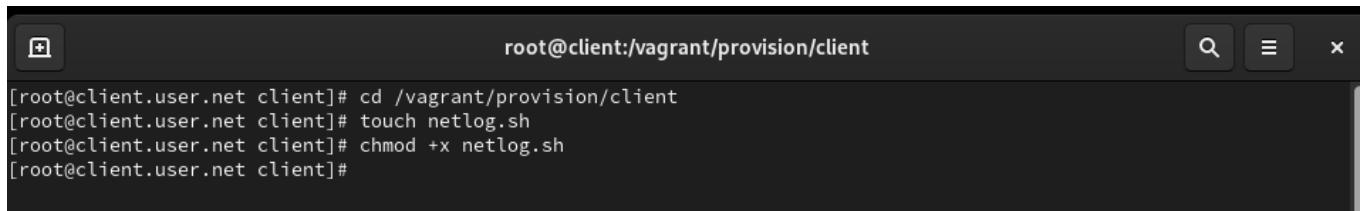
echo "Configure firewall"
firewall-cmd --add-port=514/tcp
firewall-cmd --add-port=514/tcp --permanent

echo "Start rsyslog service"
systemctl restart rsyslog
```

Рис. 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

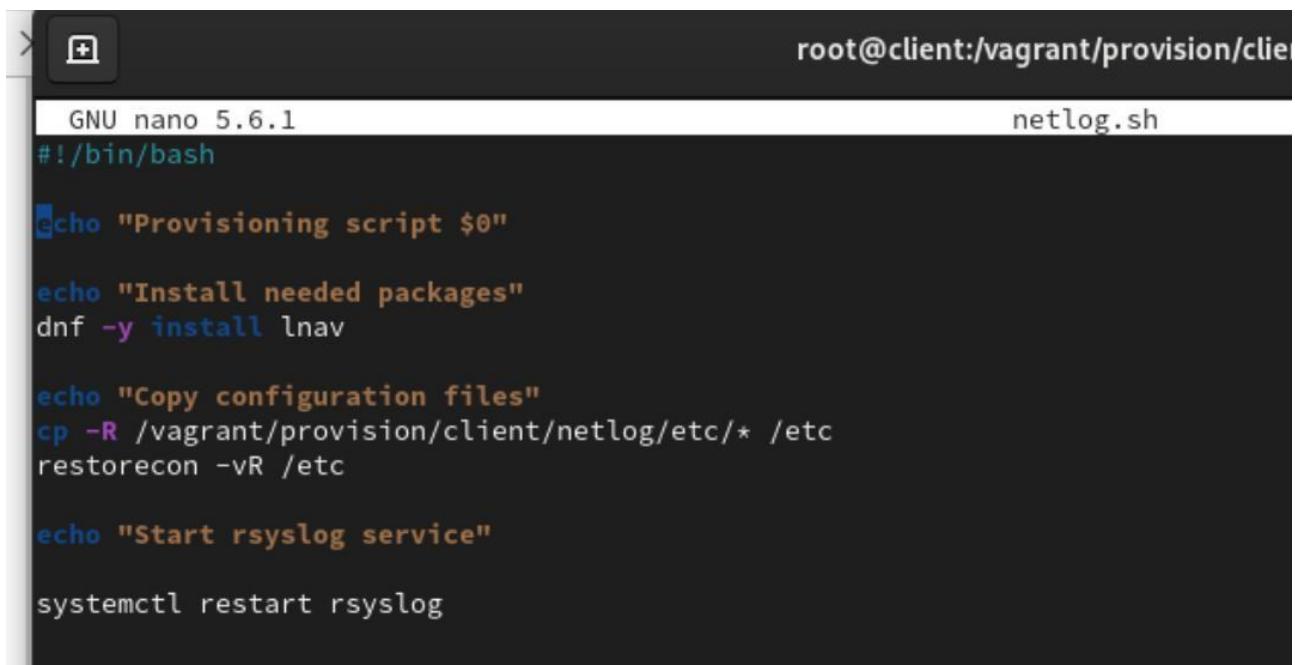
каталог netlog, в который поместим в соответствующие подкаталоги конфигурационные файлы. В каталоге /vagrant/provision/client создадим исполняемый файл netlog.sh (Рис. 4.3):



```
root@client:/vagrant/provision/client
[root@client.user.net client]# cd /vagrant/provision/client
[root@client.user.net client]# touch netlog.sh
[root@client.user.net client]# chmod +x netlog.sh
[root@client.user.net client]#
```

Рис. 4.3. Переход на виртуальной машине client в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создание в нём каталога netlog, 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):



```
root@client:/vagrant/provision/client
GNU nano 5.6.1
#!/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. 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 **ommysqlops**.

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