

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: Бансимба Клодели Дьегра

Студ. билет № 1032215651

Группа: НПИбд-02-22

МОСКВА

2024 г.

Цель работы:

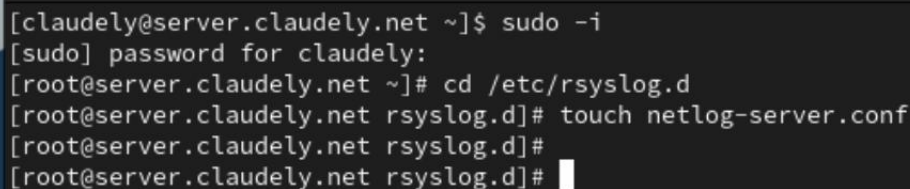
Целью данной работы является получение навыков по работе с журналами системных событий.

Выполнение работы:

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

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

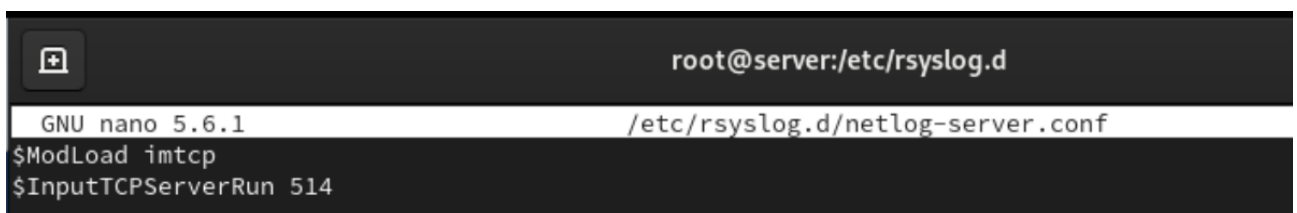
```
touch netlog-server.conf
```



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



```
root@server:/etc/rsyslog.d
GNU nano 5.6.1 /etc/rsyslog.d/netlog-server.conf
$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.claudely.net rsyslog.d]# systemctl restart rsyslog
[root@server.claudely.net rsyslog.d]# lsof | grep TCP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1002/gvfs
Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1002/doc
Output information may be incomplete.
systemd      1          root    246u      IPv4        117244      0t0      TCP *:sunrpc
systemd      1          root    249u      IPv6        117262      0t0      TCP *:sunrpc
cupsd       783          root      6u      IPv6        20625      0t0      TCP localhost
:ipp (LISTEN)
cupsd       783          root      7u      IPv4        20626      0t0      TCP localhost
:ipp (LISTEN)
sshd        798          root      3u      IPv4        20713      0t0      TCP *:down (L
ISTEN)
sshd        798          root      4u      IPv6        20733      0t0      TCP *:down (L
ISTEN)
sshd        798          root      5u      IPv4        20735      0t0      TCP *:ssh (LI

```

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

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

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

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

```

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

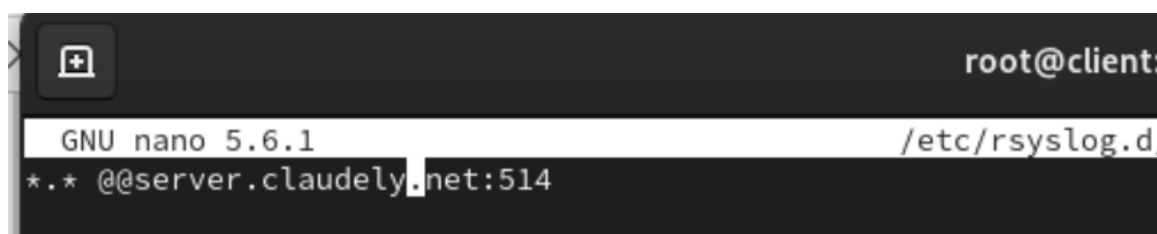
```
cd /etc/rsyslog.d
```

```
touch netlog-client.conf
```

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

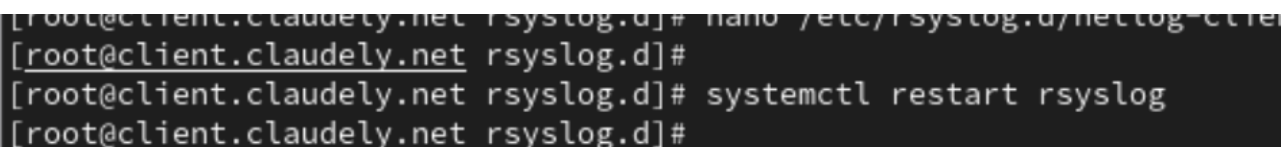


```
GNU nano 5.6.1 /etc/rsyslog.d/netlog-client.conf
*.* @@server.claudely.net:514
```

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.claudely.net rsyslog.d]# nano /etc/rsyslog.d/netlog-client.conf
[root@client.claudely.net rsyslog.d]#
[root@client.claudely.net rsyslog.d]# systemctl restart rsyslog
[root@client.claudely.net rsyslog.d]#
```

Рис. 2.3. Перезапуск службы `rsyslog`.

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

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

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

```
dnf -y install lnav
```

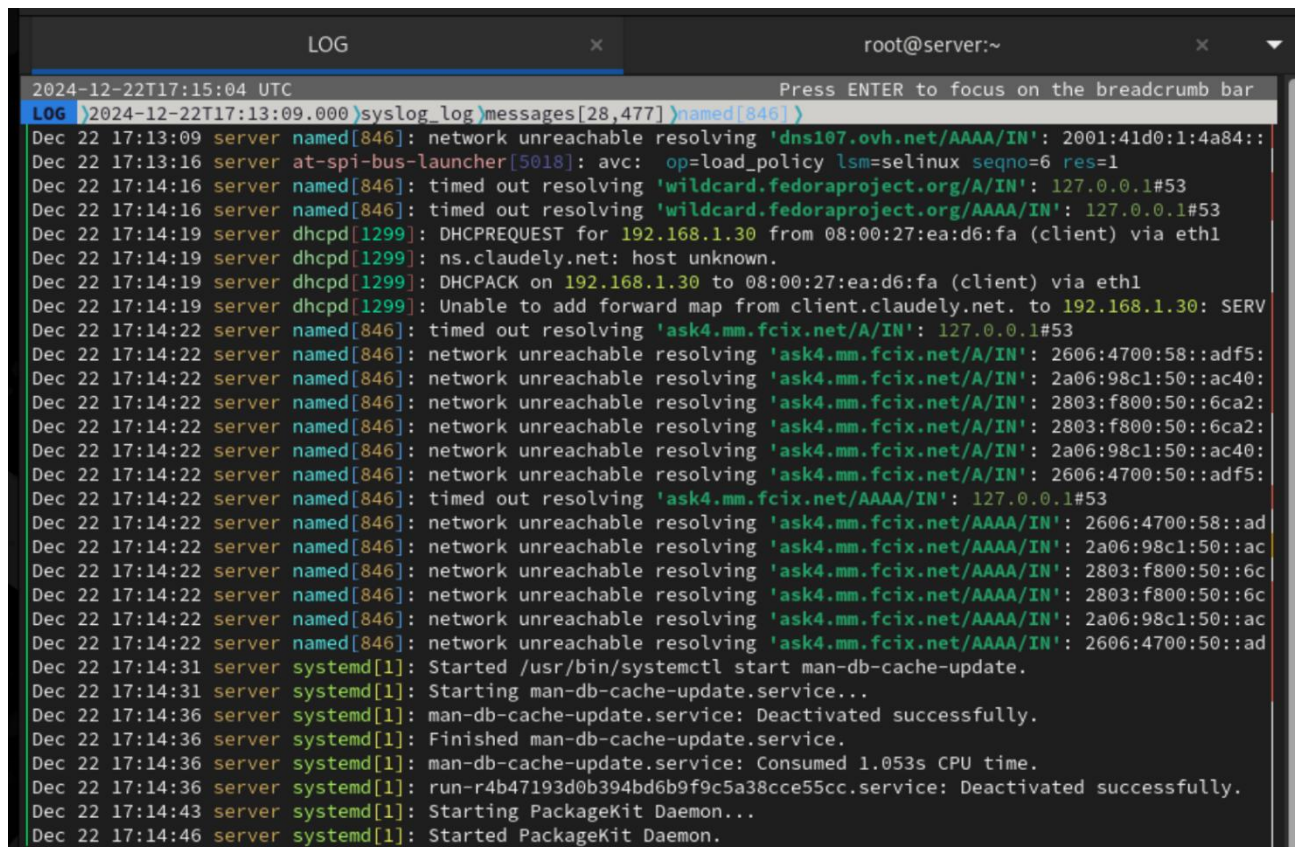
```
[root@server.claudely.net ~]# dnf -y install lnav
Last metadata expiration check: 0:01:29 ago on Sun 22 Dec 2024 05:12:42 PM UTC.
Dependencies resolved.
=====
Package                Architecture      Version           Repository        Size
=====
Installing:
lnav                    x86_64           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:
```

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

Просмотрим логи с помощью lnav (Рис. 3.4):

```
lnav
```

```
LOG 2024-12-22T17:15:04 UTC
LOG 2024-12-22T17:13:09.000 syslog_log messages[28,477] named[846]
Dec 22 17:13:09 server named[846]: network unreachable resolving 'dns107.ovh.net/AAAA/IN': 2001:41d0:1:4a84::
Dec 22 17:13:16 server at-spi-bus-launcher[5018]: avc: op=load_policy lsm=selinux seqno=6 res=1
Dec 22 17:14:16 server named[846]: timed out resolving 'wildcard.fedoraproject.org/A/IN': 127.0.0.1#53
Dec 22 17:14:16 server named[846]: timed out resolving 'wildcard.fedoraproject.org/AAAA/IN': 127.0.0.1#53
Dec 22 17:14:19 server dhcpd[1299]: DHCPREQUEST for 192.168.1.30 from 08:00:27:ea:d6:fa (client) via eth1
Dec 22 17:14:19 server dhcpd[1299]: ns.claudely.net: host unknown.
Dec 22 17:14:19 server dhcpd[1299]: DHCPACK on 192.168.1.30 to 08:00:27:ea:d6:fa (client) via eth1
Dec 22 17:14:19 server dhcpd[1299]: Unable to add forward map from client.claudely.net. to 192.168.1.30: SERV
Dec 22 17:14:22 server named[846]: timed out resolving 'ask4.mm.fcix.net/A/IN': 127.0.0.1#53
Dec 22 17:14:22 server named[846]: network unreachable resolving 'ask4.mm.fcix.net/A/IN': 2606:4700:58::adf5:
Dec 22 17:14:22 server named[846]: network unreachable resolving 'ask4.mm.fcix.net/A/IN': 2a06:98c1:50::ac40:
Dec 22 17:14:22 server named[846]: network unreachable resolving 'ask4.mm.fcix.net/A/IN': 2803:f800:50::6ca2:
Dec 22 17:14:22 server named[846]: network unreachable resolving 'ask4.mm.fcix.net/A/IN': 2803:f800:50::6ca2:
Dec 22 17:14:22 server named[846]: network unreachable resolving 'ask4.mm.fcix.net/A/IN': 2a06:98c1:50::ac40:
Dec 22 17:14:22 server named[846]: network unreachable resolving 'ask4.mm.fcix.net/A/IN': 2606:4700:50::adf5:
Dec 22 17:14:22 server named[846]: timed out resolving 'ask4.mm.fcix.net/AAAA/IN': 127.0.0.1#53
Dec 22 17:14:22 server named[846]: network unreachable resolving 'ask4.mm.fcix.net/AAAA/IN': 2606:4700:58::ad
Dec 22 17:14:22 server named[846]: network unreachable resolving 'ask4.mm.fcix.net/AAAA/IN': 2a06:98c1:50::ac
Dec 22 17:14:22 server named[846]: network unreachable resolving 'ask4.mm.fcix.net/AAAA/IN': 2803:f800:50::6c
Dec 22 17:14:22 server named[846]: network unreachable resolving 'ask4.mm.fcix.net/AAAA/IN': 2803:f800:50::6c
Dec 22 17:14:22 server named[846]: network unreachable resolving 'ask4.mm.fcix.net/AAAA/IN': 2a06:98c1:50::ac
Dec 22 17:14:22 server named[846]: network unreachable resolving 'ask4.mm.fcix.net/AAAA/IN': 2606:4700:50::ad
Dec 22 17:14:31 server systemd[1]: Started /usr/bin/systemctl start man-db-cache-update.
Dec 22 17:14:31 server systemd[1]: Starting man-db-cache-update.service...
Dec 22 17:14:36 server systemd[1]: man-db-cache-update.service: Deactivated successfully.
Dec 22 17:14:36 server systemd[1]: Finished man-db-cache-update.service.
Dec 22 17:14:36 server systemd[1]: man-db-cache-update.service: Consumed 1.053s CPU time.
Dec 22 17:14:36 server systemd[1]: run-r4b47193d0b394bd6b9f9c5a38cce55cc.service: Deactivated successfully.
Dec 22 17:14:43 server systemd[1]: Starting PackageKit Daemon...
Dec 22 17:14:46 server systemd[1]: Started PackageKit Daemon.
```

Рис. 3.4. Просмотр логов с помощью lnav.

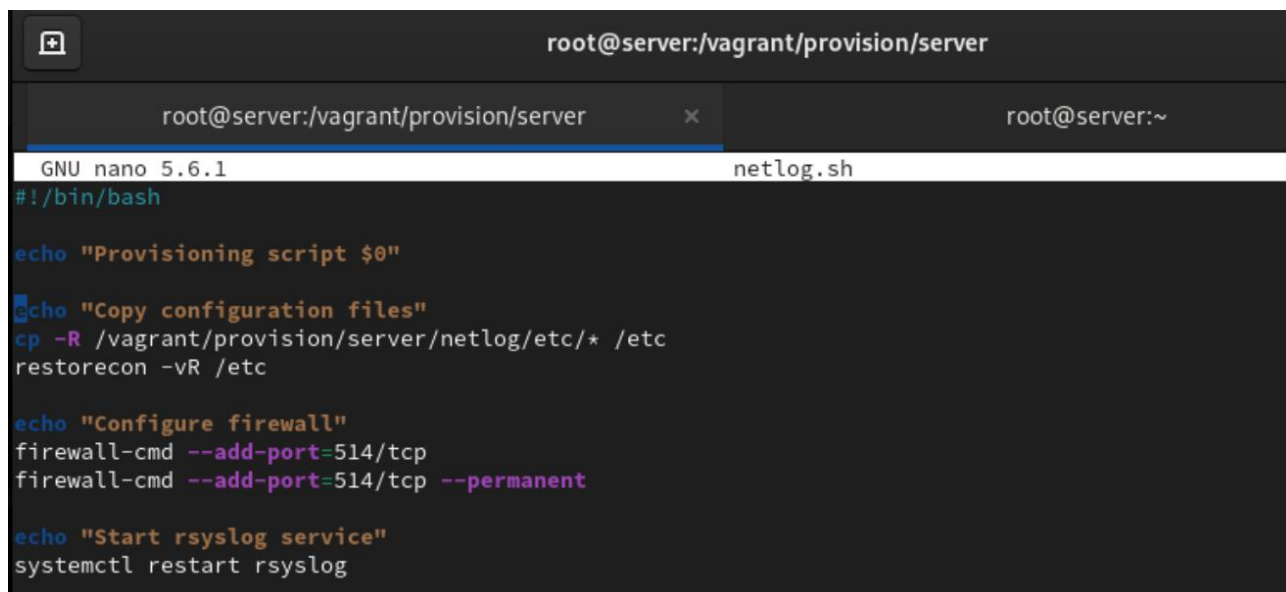
На виртуальной машине server перейдём в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создадим в нём каталог `netlog`, в который поместим в соответствующие подкаталоги конфигурационные файлы. В каталоге `/vagrant/provision/server` создадим исполняемый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



```
[root@server.claudely.net ~]#
[root@server.claudely.net ~]# cd /vagrant/provision/server
[root@server.claudely.net server]# mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.claudely.net server]# cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.claudely.net server]#
[root@server.claudely.net server]# cd /vagrant/provision/server
[root@server.claudely.net server]# touch netlog.sh
[root@server.claudely.net server]# chmod +x netlog.sh
[root@server.claudely.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):



The screenshot shows a terminal window with the title bar 'root@server:/vagrant/provision/server'. The terminal content is as follows:

```
GNU nano 5.6.1 netlog.sh
#!/bin/bash

echo "Provisioning script $0"

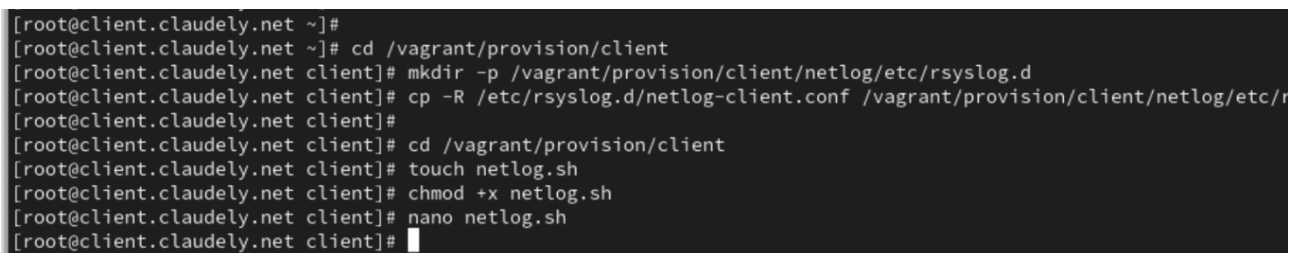
echo "Copy configuration files"
cp -R /vagrant/provision/server/netlog/etc/* /etc
restorecon -vR /etc

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):

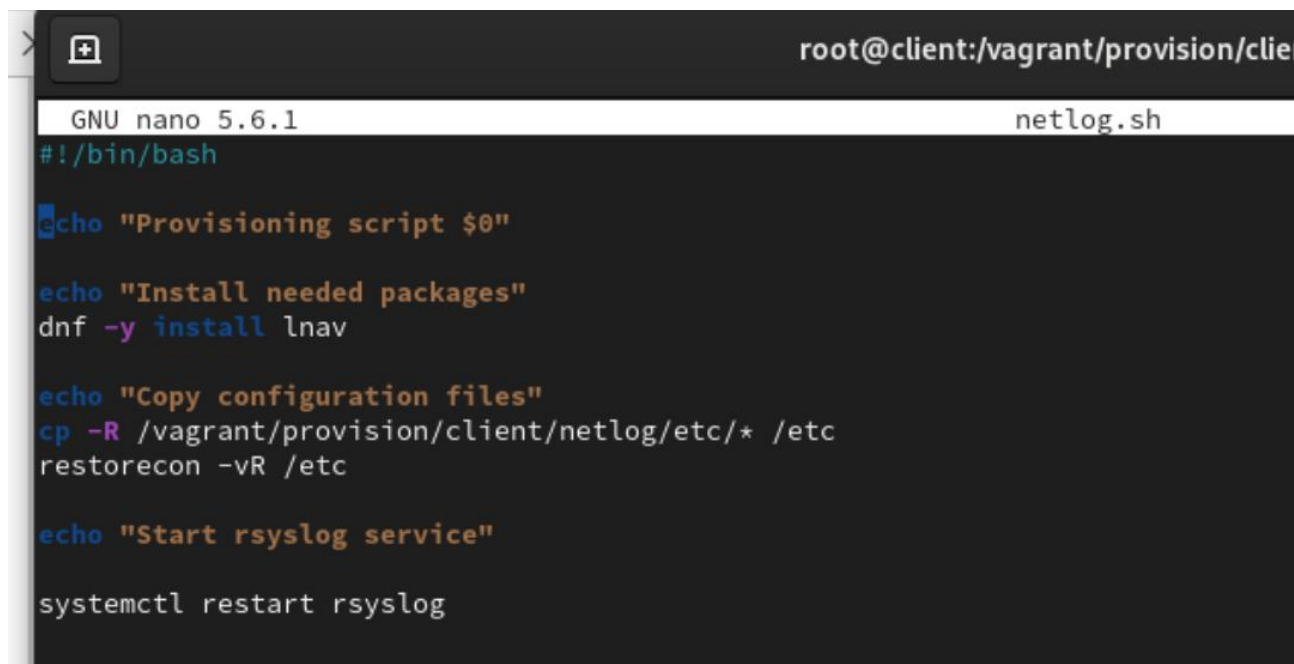


The screenshot shows a terminal window with the title bar '[root@client.claudely.net ~]#'. The terminal content is as follows:

```
[root@client.claudely.net ~]# cd /vagrant/provision/client
[root@client.claudely.net ~]# mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d
[root@client.claudely.net ~]# cp -R /etc/rsyslog.d/netlog-client.conf /vagrant/provision/client/netlog/etc/
[root@client.claudely.net ~]# cd /vagrant/provision/client
[root@client.claudely.net ~]# touch netlog.sh
[root@client.claudely.net ~]# chmod +x netlog.sh
[root@client.claudely.net ~]# nano netlog.sh
[root@client.claudely.net ~]#
```

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 netlog.sh
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):

```
server.vm.provision "server netlog",
  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