

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
```

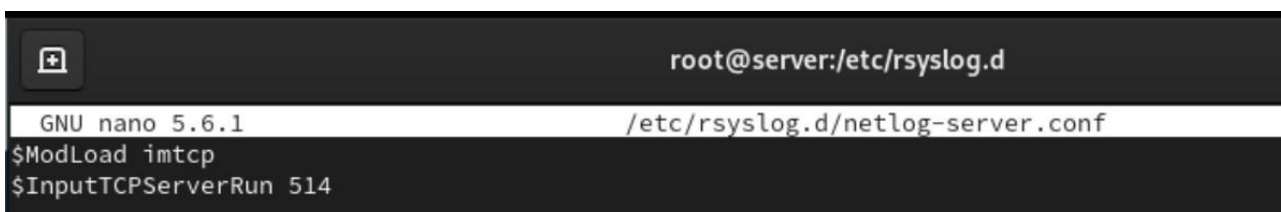


```
root@server:/etc/rsyslog.d

[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):



```
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.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      30060      0t0      TCP server.user.net:38
```

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
```

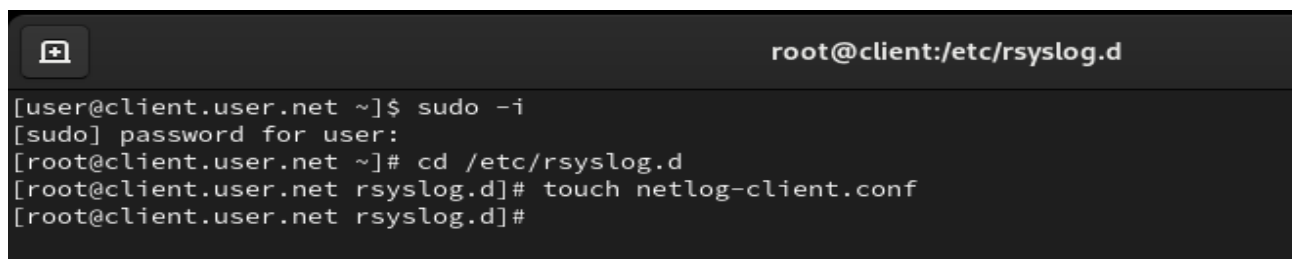
```
root@server:/etc/rsyslog.d
[root@server.user.net rsyslog.d]# firewall-cmd --add-port=514/tcp
success
[root@server.user.net rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent
success
[root@server.user.net rsyslog.d]#
```

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
```

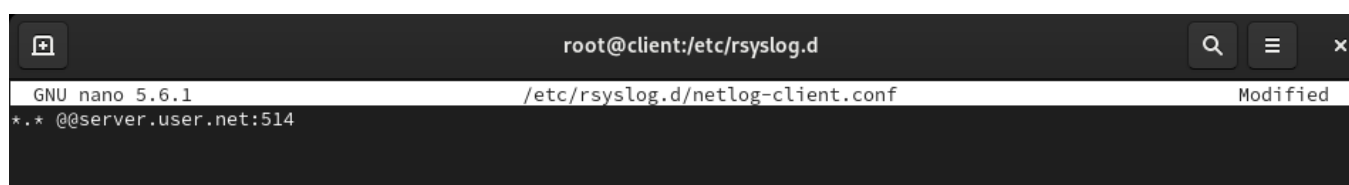
```
netlog-client.conf
```

A terminal window titled 'root@client:/etc/rsyslog.d' showing a user switching to root via 'sudo -i', navigating to '/etc/rsyslog.d', and creating 'netlog-client.conf' with 'touch'.

```
root@client:/etc/rsyslog.d
[user@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):

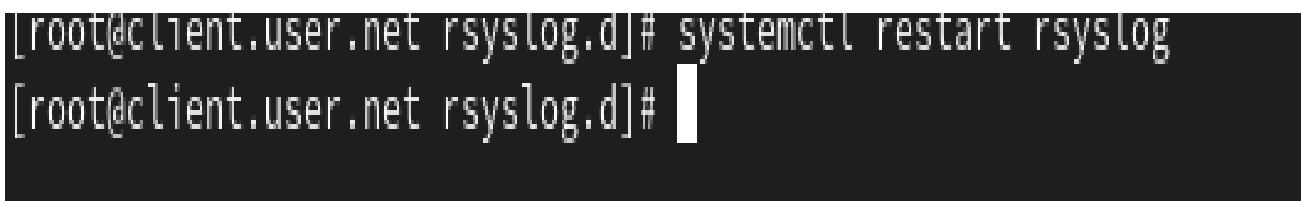
A terminal window titled 'root@client:/etc/rsyslog.d' showing the nano editor editing '/etc/rsyslog.d/netlog-client.conf'. The content '@server.user.net:514' is visible.

```
root@client:/etc/rsyslog.d
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
```

A terminal window showing the command 'systemctl restart rsyslog' being executed as root.

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

Рис. 2.3. Перезапуск службы rsyslog.

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

```
root@server:~  
[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

Process Name	User	% CPU	ID	Memory	Disk read tota	Disk writ
accounts-daemon	root	0.00	566	102.4 kB	7.9 MB	
acpi_thermal_pm	root	0.00	52	N/A	N/A	
alsactl	root	0.00	597	N/A	5.0 MB	
ata_sff	root	0.00	341	N/A	N/A	
atd	root	0.00	1349	N/A	462.8 kB	
auditd	root	0.00	533	196.6 kB	16.0 MB	577
bash	root	0.00	52085	393.2 kB	44.1 MB	4
bash	root	0.00	52215	2.0 MB	606.2 kB	
blkcg_punt_bio	root	0.00	35	N/A	N/A	
config	root	0.00	1380	N/A	180.2 kB	
cpuhp/0	root	0.00	20	N/A	N/A	
crond	root	0.00	1351	N/A	32.1 MB	
cryptd	root	0.00	32	N/A	N/A	
cupsd	root	0.00	783	N/A	11.3 MB	28
dovecot	root	0.00	1333	N/A	2.0 MB	4
edac-poller	root	0.00	39	N/A	N/A	
firewalld	root	0.00	49112	65.5 kB	77.5 MB	32

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`

```
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 ~]#
```

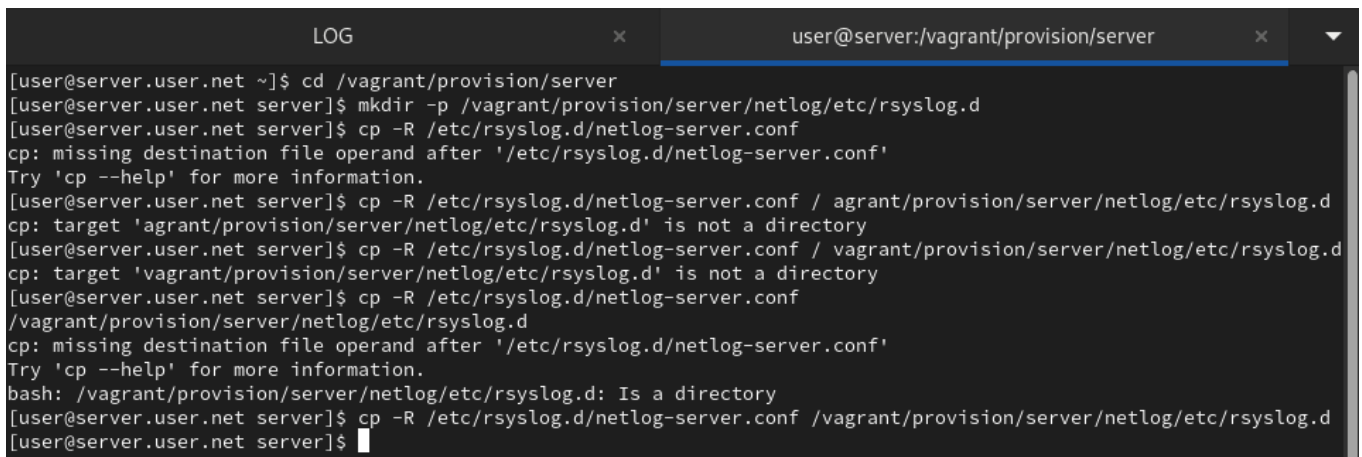
Рис. 3.3. Установка на сервере просмотрщика журналов системных сообщений lnav.

Просмотрим логи с помощью lnav (Рис. 3.4):

lnav

Рис. 3.4. Просмотр логов с помощью lnav.

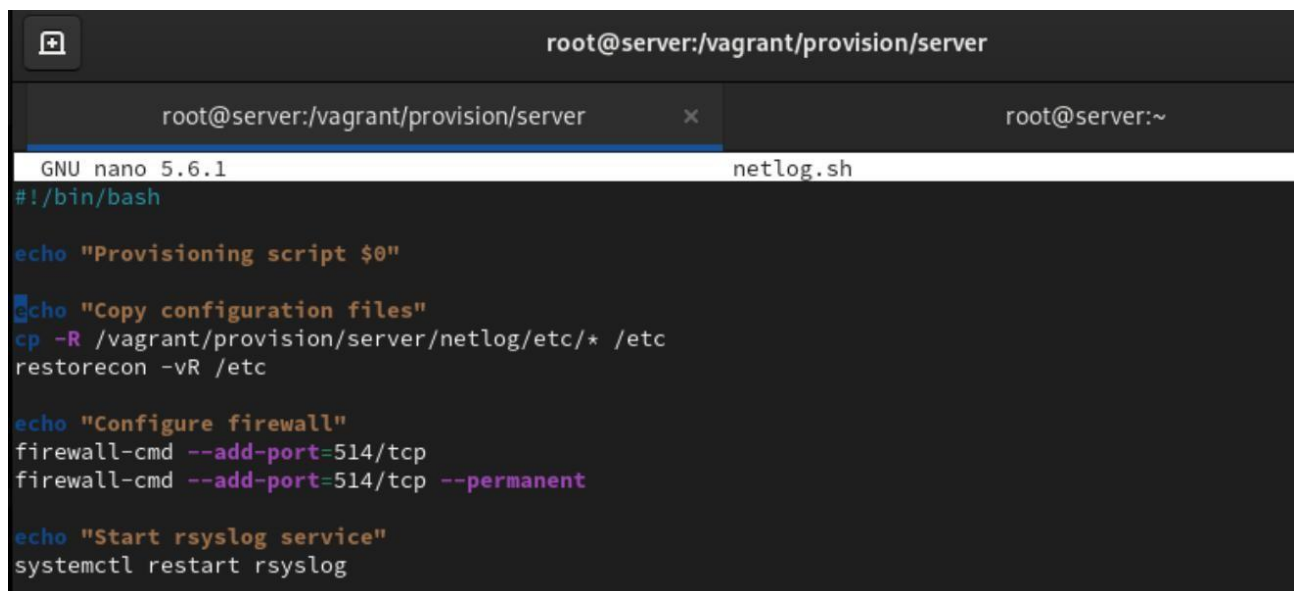
На виртуальной машине server перейдём в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создадим в нём каталог `netlog`, в который поместим в соответствующие подкаталоги конфигурационные файлы. В каталоге `/vagrant/provision/server` создадим исполняемый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



```
LOG x user@server:/vagrant/provision/server x
[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 /agrant/provision/server/netlog/etc/rsyslog.d
cp: target 'agrant/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:~
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

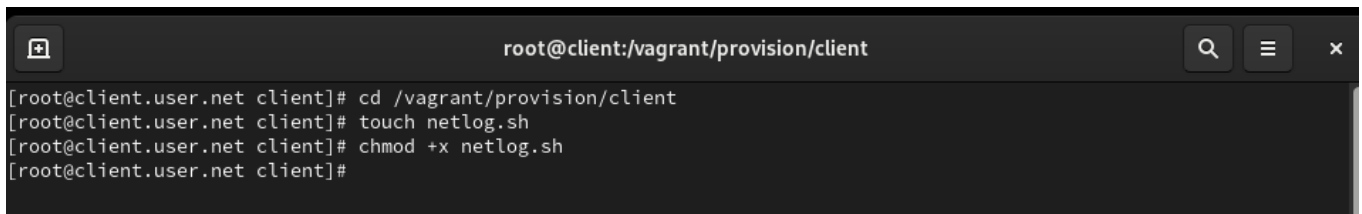
echo "Configure firewall"
firewall-cmd --add-port=514/tcp
firewall-cmd --add-port=514/tcp --permanent

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

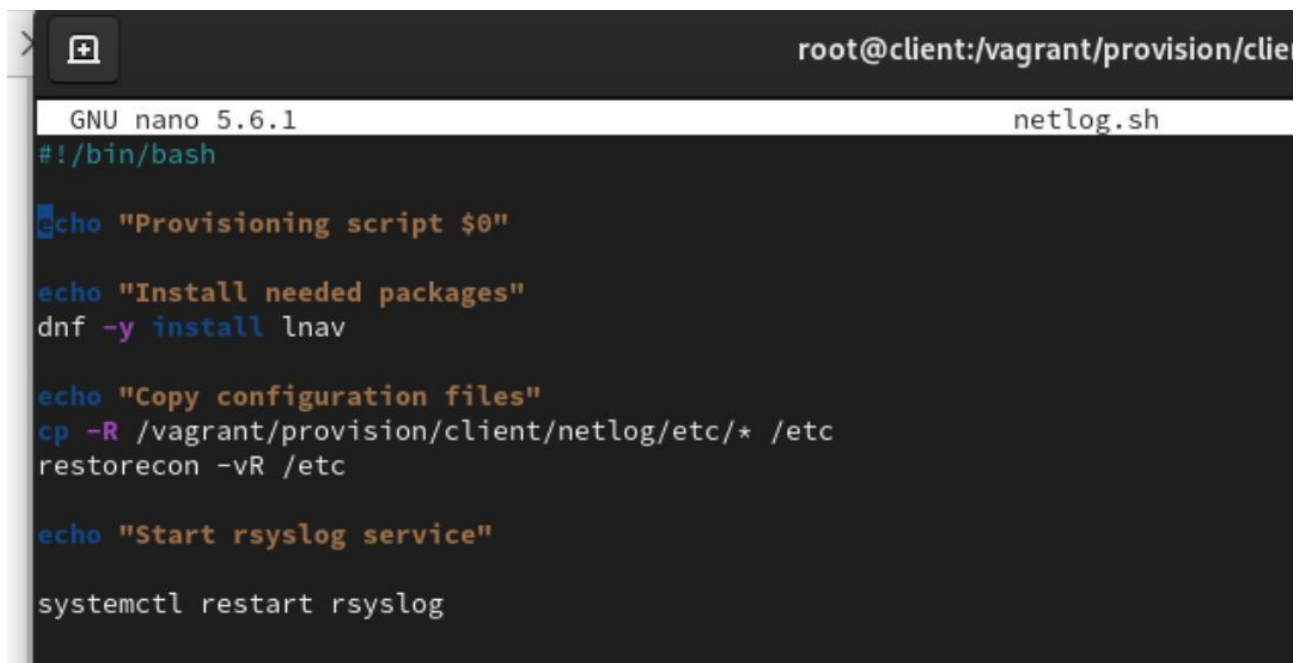
каталог `nentlog`, в который поместим в соответствующие подкаталоги конфигурационные файлы. В каталоге `/vagrant/provision/client` создадим исполняемый файл `netlog.sh` (Рис. 4.3):

A terminal window titled 'root@client:/vagrant/provision/client'. The prompt is '[root@client.user.net client]#'. The user enters 'cd /vagrant/provision/client', then 'touch netlog.sh', then 'chmod +x netlog.sh', and finally a new prompt '[root@client.user.net client]#'.

```
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 `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):

A terminal window titled 'root@client:/vagrant/provision/client' showing the GNU nano 5.6.1 editor editing 'netlog.sh'. The editor shows a bash script with several commands: 'echo', 'dnf install', 'cp', 'restorecon', and 'systemctl restart'.

```
GNU nano 5.6.1 netlog.sh
#!/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",  
  type: "shell",  
  preserve_order: true,  
  path: "provision/server/netlog.sh"
```

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

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