

Лабораторная работа

№15

Настройка сетевого журналирования

Студент: БАНСИМБА КЛОДЕЛИ ДЬЕГРА

Группа: НПИбд 02–22

дисциплина: Администрирование сетевых подсистем (Lab 15)

Цель работы

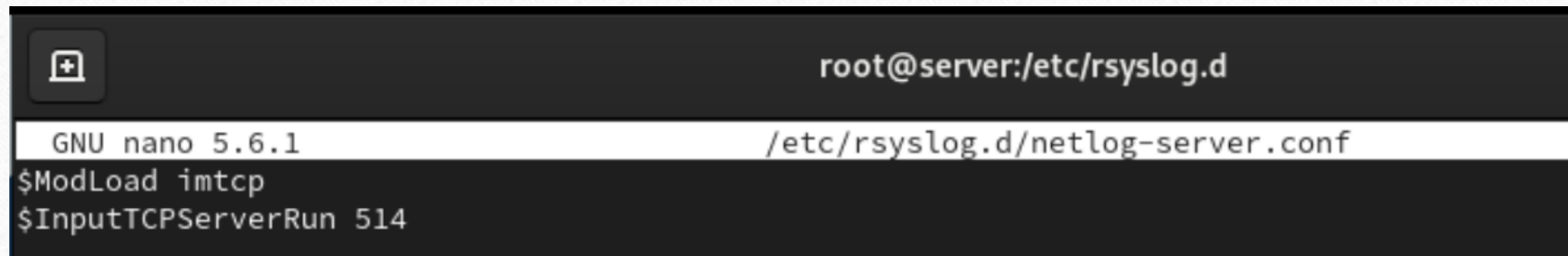
- Целью данной работы является получение навыков по работе с журналами системных событий.

Настройка сервера сетевого журнала

```
[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]#
[root@server.claudely.net rsyslog.d]#
```

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

Настройка сервера сетевого журнала



The screenshot shows a terminal window with a dark background. At the top, the prompt is 'root@server:/etc/rsyslog.d'. Below it, the title bar of the nano editor shows 'GNU nano 5.6.1' and the file path '/etc/rsyslog.d/netlog-server.conf'. The editor content shows two lines of configuration: '\$ModLoad imtcp' and '\$InputTCPServerRun 514'.

```
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.

Настройка сервера сетевого журнала

```
[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.

Настройка сервера сетевого журнала

```
[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]#
```

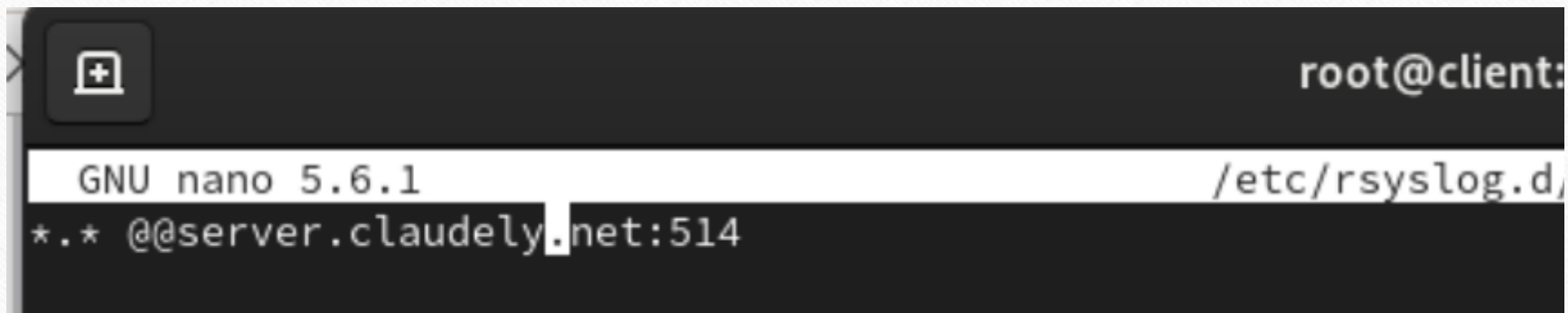
Рис. 1.4. Настройка на сервере межсетевого экрана для приёма сообщений по TCP-порту 514.

Настройка клиента сетевого журнала

```
[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.

Настройка клиента сетевого журнала



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

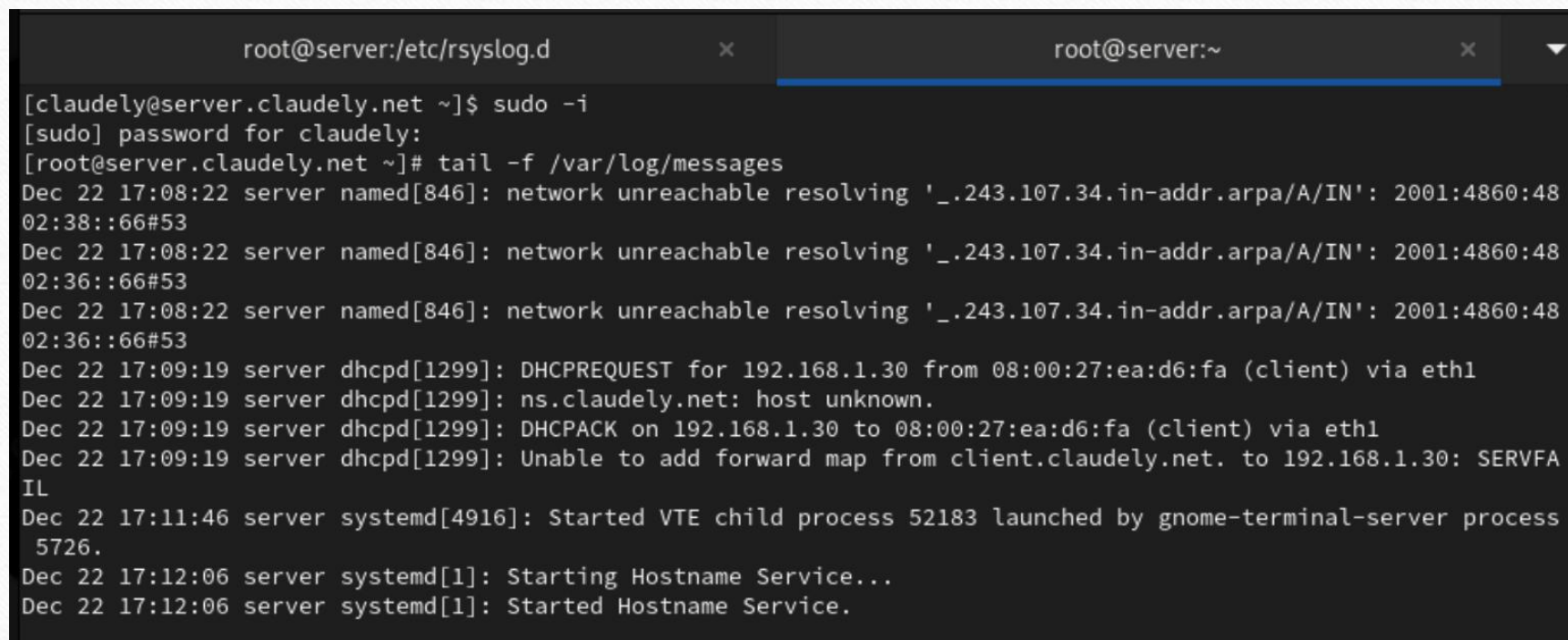
Рис. 2.2. Включение в файле конфигурации `/etc/rsyslog.d/netlog-client.conf` перенаправления сообщений журнала на 514 TCP-порт сервера.

Настройка клиента сетевого журнала

```
[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.

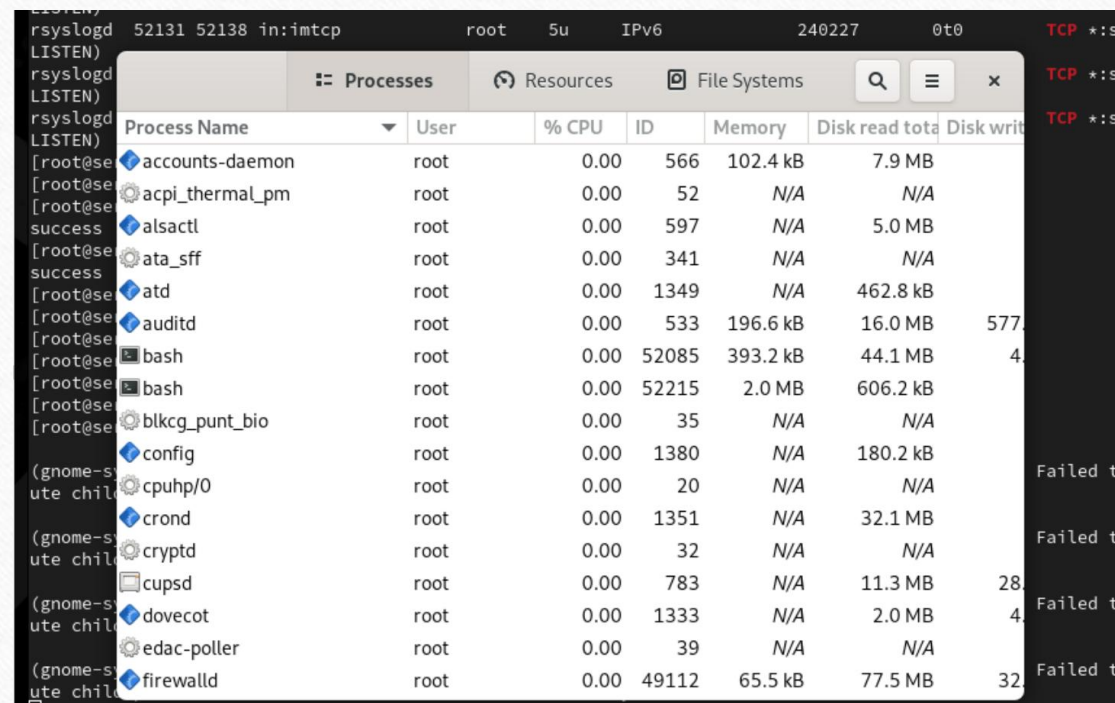
Просмотр журнала



```
root@server:/etc/rsyslog.d x root@server:~ x ▼
[claudely@server.claudely.net ~]$ sudo -i
[sudo] password for claudely:
[root@server.claudely.net ~]# tail -f /var/log/messages
Dec 22 17:08:22 server named[846]: network unreachable resolving '_243.107.34.in-addr.arpa/A/IN': 2001:4860:48
02:38::66#53
Dec 22 17:08:22 server named[846]: network unreachable resolving '_243.107.34.in-addr.arpa/A/IN': 2001:4860:48
02:36::66#53
Dec 22 17:08:22 server named[846]: network unreachable resolving '_243.107.34.in-addr.arpa/A/IN': 2001:4860:48
02:36::66#53
Dec 22 17:09:19 server dhcpd[1299]: DHCPREQUEST for 192.168.1.30 from 08:00:27:ea:d6:fa (client) via eth1
Dec 22 17:09:19 server dhcpd[1299]: ns.claudely.net: host unknown.
Dec 22 17:09:19 server dhcpd[1299]: DHCPACK on 192.168.1.30 to 08:00:27:ea:d6:fa (client) via eth1
Dec 22 17:09:19 server dhcpd[1299]: Unable to add forward map from client.claudely.net. to 192.168.1.30: SERVFA
IL
Dec 22 17:11:46 server systemd[4916]: Started VTE child process 52183 launched by gnome-terminal-server process
5726.
Dec 22 17:12:06 server systemd[1]: Starting Hostname Service...
Dec 22 17:12:06 server systemd[1]: Started Hostname Service.
```

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

Просмотр журнала



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	Failed t
crond	root	0.00	1351	N/A	32.1 MB	
cryptd	root	0.00	32	N/A	N/A	Failed t
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	Failed t
firewalld	root	0.00	49112	65.5 kB	77.5 MB	32

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

Просмотр журнала

```
[root@server.claudely.net rsyslog.d]#  
[root@server.claudely.net rsyslog.d]#  
[root@server.claudely.net rsyslog.d]# 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

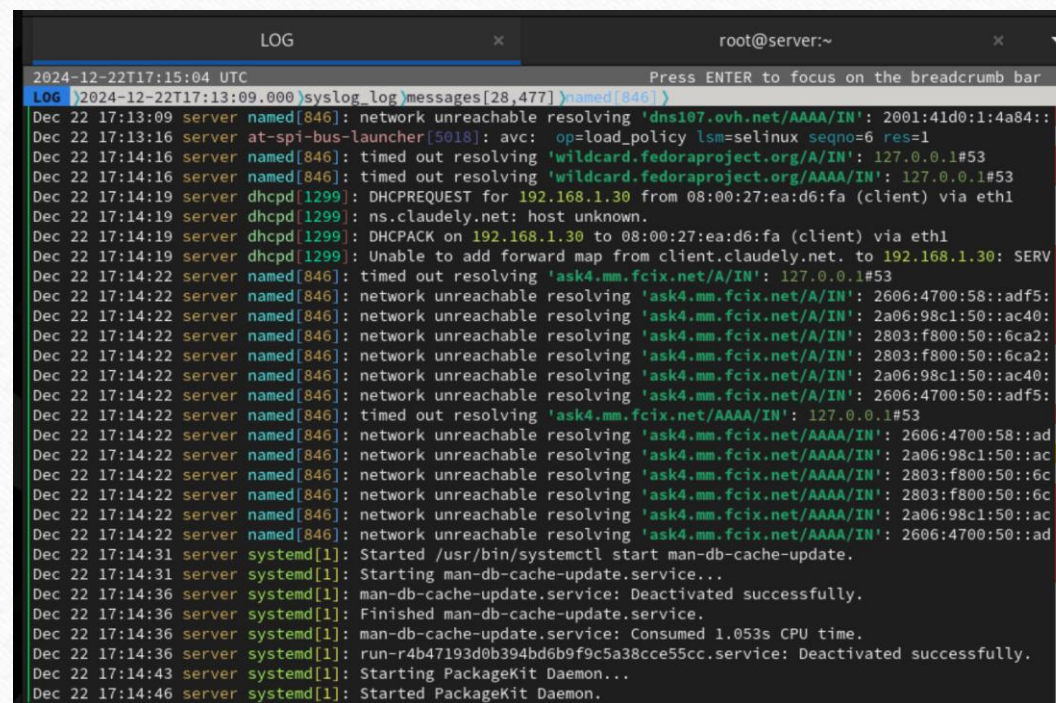
```
Transaction Summary  
=====
```

Install	1 Package
---------	-----------

```
Total download size: 2.4 M  
Installed size: 6.1 M  
Downloading Packages:  
[=====] --- B/s | 0 B --:-- ETA
```

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

Просмотр журнала



```
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.
```

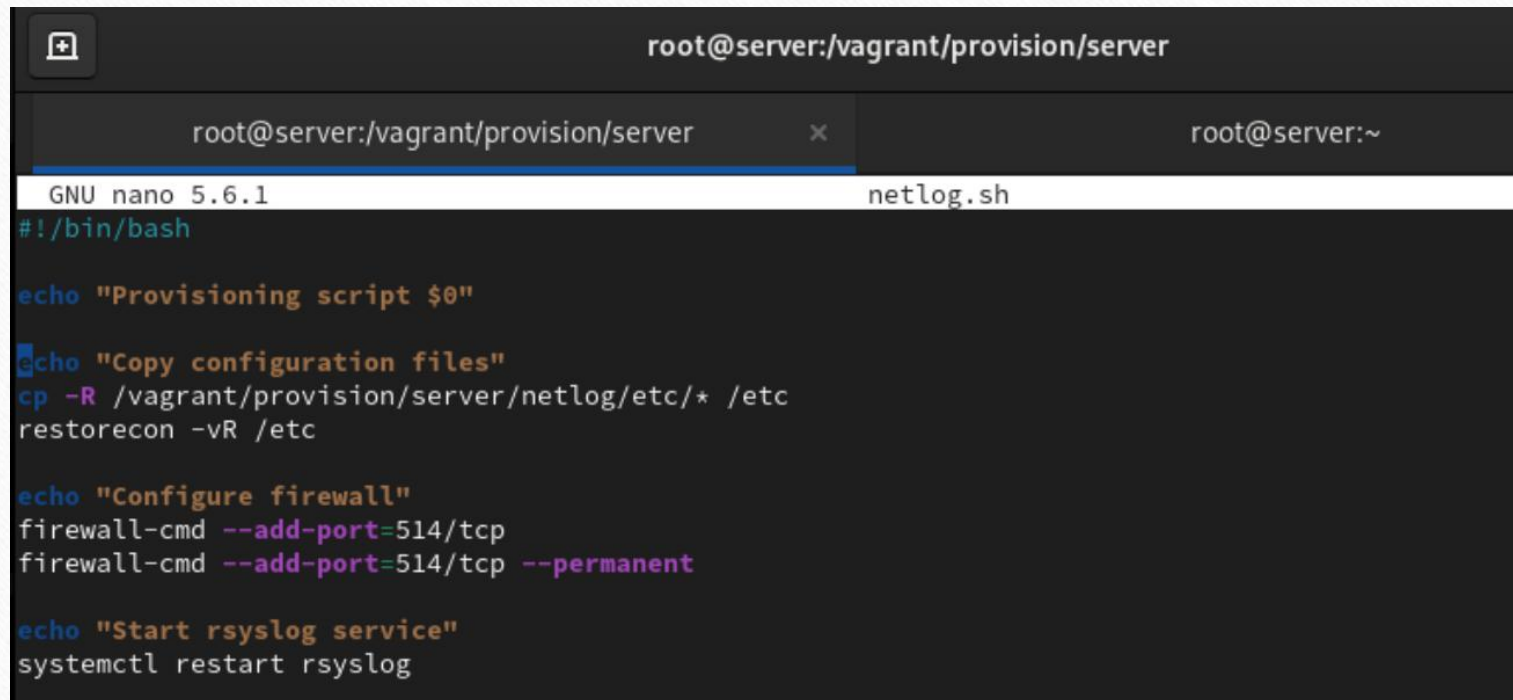
Рис. 3.4. Просмотр логов с помощью lnav.

Внесение изменений в настройки внутреннего окружения виртуальных машин

```
[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`.

Внесение изменений в настройки внутреннего окружения виртуальных машин



The screenshot shows a terminal window with two tabs. The active tab is titled 'root@server:/vagrant/provision/server' and contains the nano text editor. The editor is editing a file named 'netlog.sh'. The content of the file 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
```

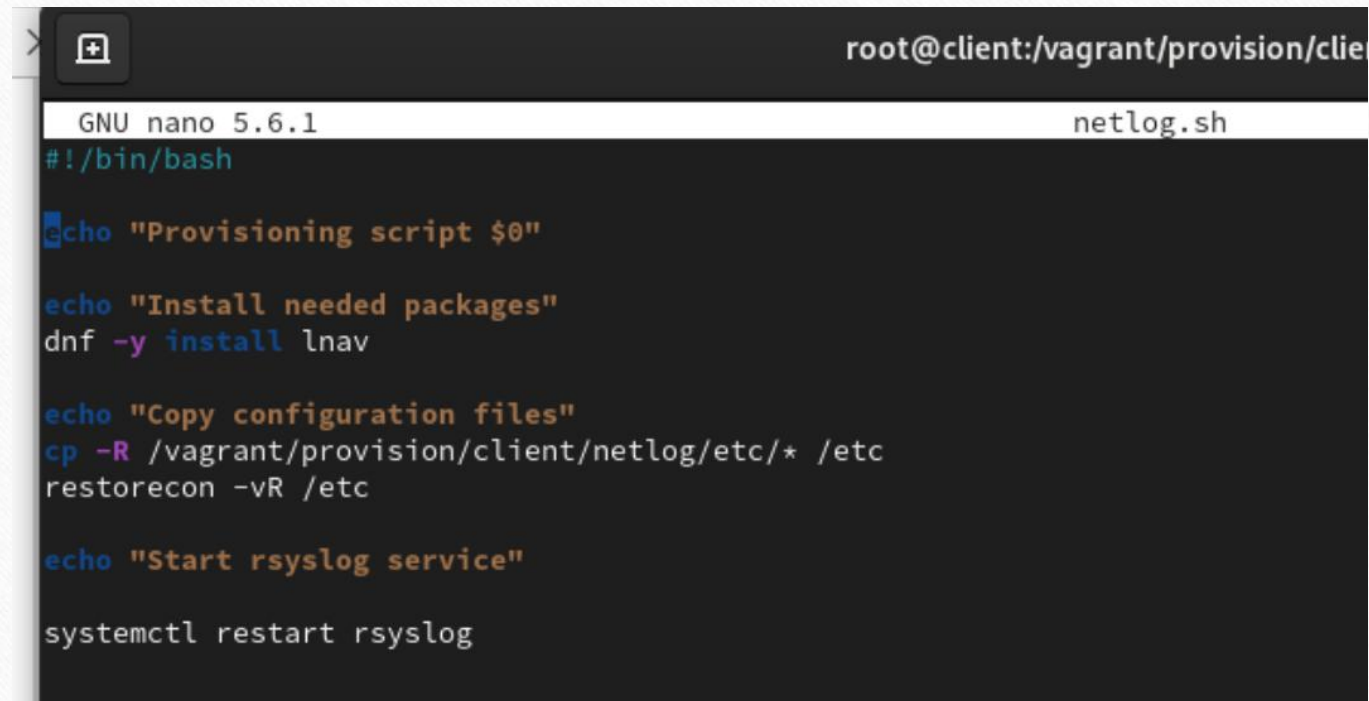
Рис. 4.2. Открытие файла на редактирование и добавление в него скрипта.

Внесение изменений в настройки внутреннего окружения виртуальных машин

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

Внесение изменений в настройки внутреннего окружения виртуальных машин



```
root@client:/vagrant/provision/client$ nano netlog.sh
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.

Внесение изменений в настройки внутреннего окружения виртуальных машин

```
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.

Внесение изменений в настройки внутреннего окружения виртуальных машин

```
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.

Спасибо за внимание!