

Лабораторная работа №15

Настройка сетевого журналирования

Студент: Пакавира Арсениу Висенте Луиш

Группа: Нфибд 02 _23

дисциплина: Администрирование сетевых подсистем (Lab 15)

Цель работы

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

Настройка сервера сетевого журнала

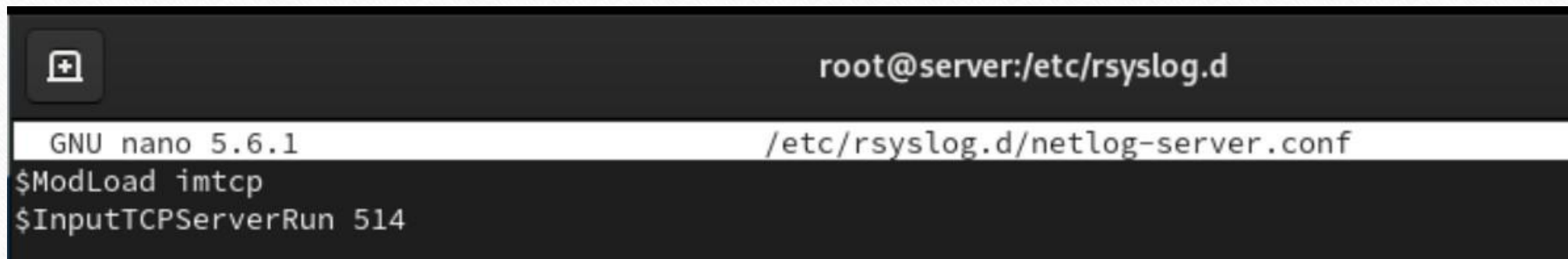


```
root@server:/etc/rsyslog.d

[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.

Настройка сервера сетевого журнала



```
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.

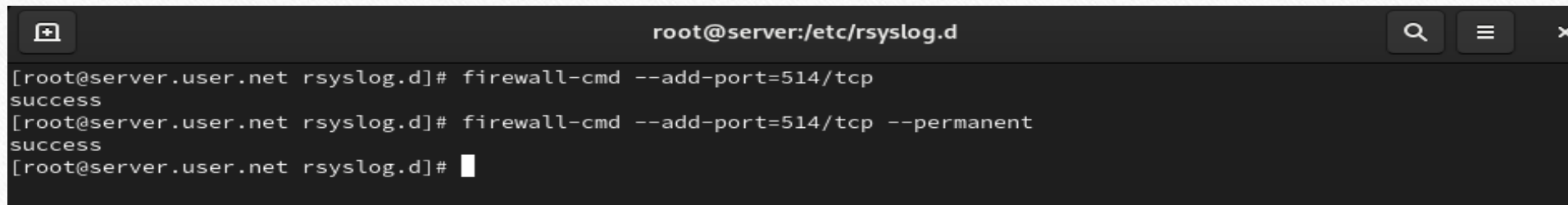
Настройка сервера сетевого журнала

```
[root@server.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.portalf 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.net:38

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

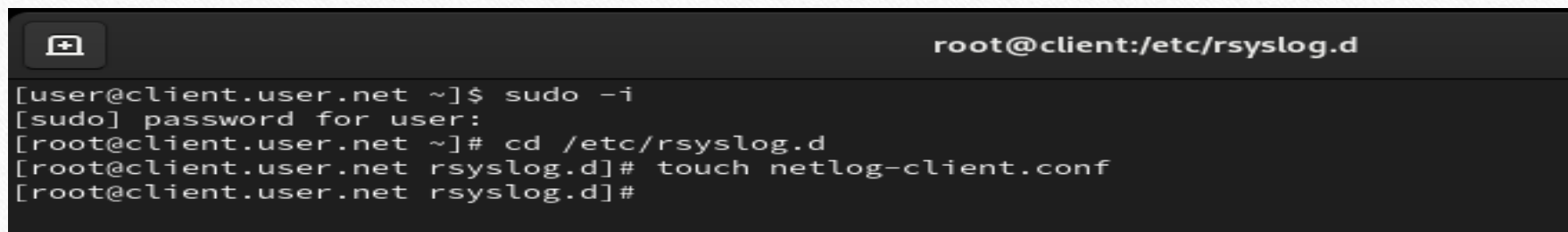
Настройка сервера сетевого журнала

A terminal window with a dark background and light text. The title bar at the top reads 'root@server:/etc/rsyslog.d' and includes search, menu, and close icons. The terminal content shows a user at the root of 'server.user.net' in the 'rsyslog.d' directory. They execute two 'firewall-cmd' commands: first to add port 514/tcp, which returns 'success', and then to make the configuration permanent, which also returns 'success'. The prompt is ready for the next command.

```
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.

Настройка клиента сетевого журнала

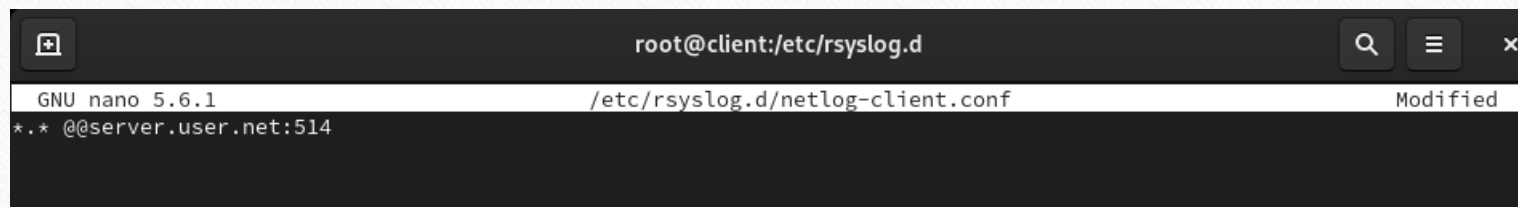


```
root@client:/etc/rsyslog.d

[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.

Настройка клиента сетевого журнала



The screenshot shows a terminal window with a dark background. The title bar at the top reads 'root@client:/etc/rsyslog.d'. Below the title bar, the text 'GNU nano 5.6.1' is on the left, '/etc/rsyslog.d/netlog-client.conf' is in the center, and 'Modified' is on the right. The main content of the terminal shows the configuration line: '*.* @@server.user.net:514'.

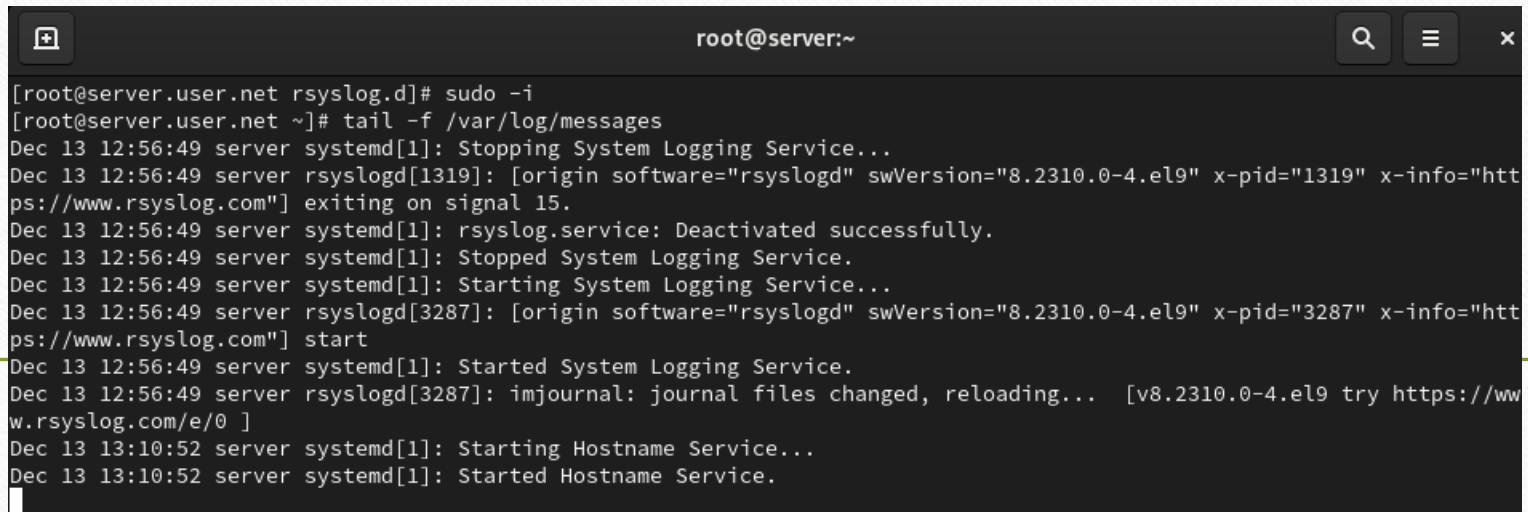
```
root@client:/etc/rsyslog.d
GNU nano 5.6.1 /etc/rsyslog.d/netlog-client.conf Modified
*.* @@server.user.net:514
```

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

Настройка клиента сетевого журнала

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

Просмотр журнала

A terminal window titled 'root@server:~' with search, menu, and close icons in the top right. The terminal shows a sequence of commands and log messages. The user runs 'sudo -i' to become root, then 'tail -f /var/log/messages' to follow the system log. The log shows the 'rsyslog.service' being stopped and then started again. It also shows 'imjournal' reloading journal files and the 'hostname' service being started.

```
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.

Просмотр журнала

Process Name	User	% CPU	ID	Memory	Disk read total	Disk write
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 to
crond	root	0.00	1351	N/A	32.1 MB	
cryptd	root	0.00	32	N/A	N/A	Failed to
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 claudely графической программы для просмотра журналов.

Просмотр журнала

```
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
lnav	x86_64	0.11.1-1.el9	epel	2.4 M

```
=====
```

Installing:

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

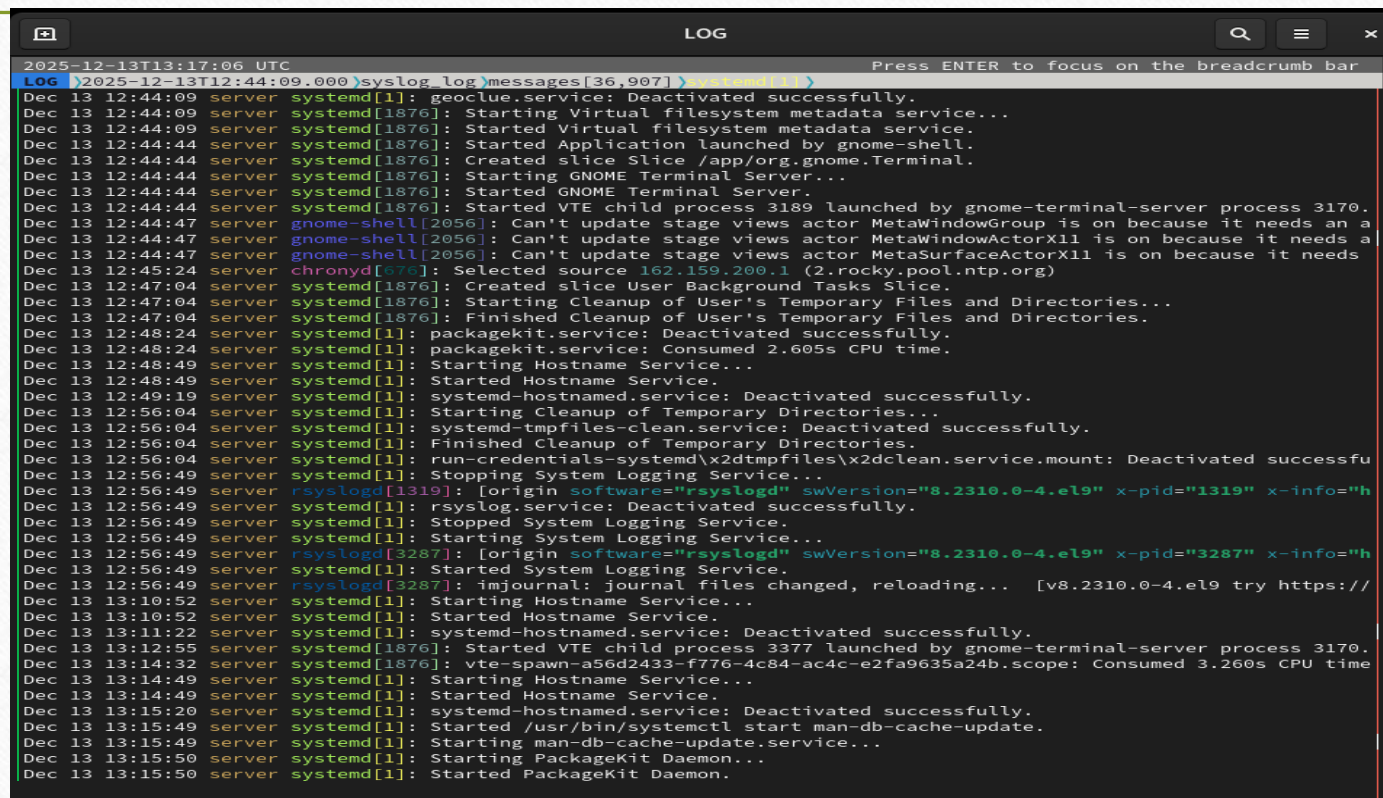
Installed:

lnav-0.11.1-1.el9.x86_64

Complete!
[root@server.user.net ~]#

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

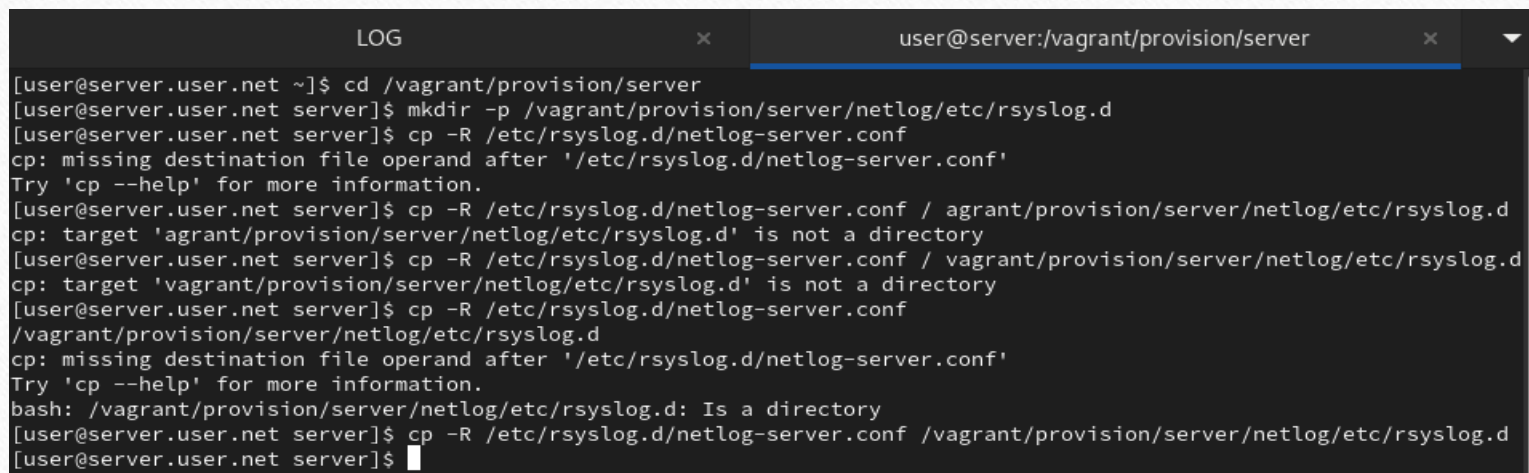
Просмотр журнала



```
LOG
2025-12-13T13:17:06 UTC
LOG 2025-12-13T12:44:09.000 syslog_log messages[36,907]
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 /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 chronyd[875]: 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="rsyslogd" 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="rsyslogd" 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.

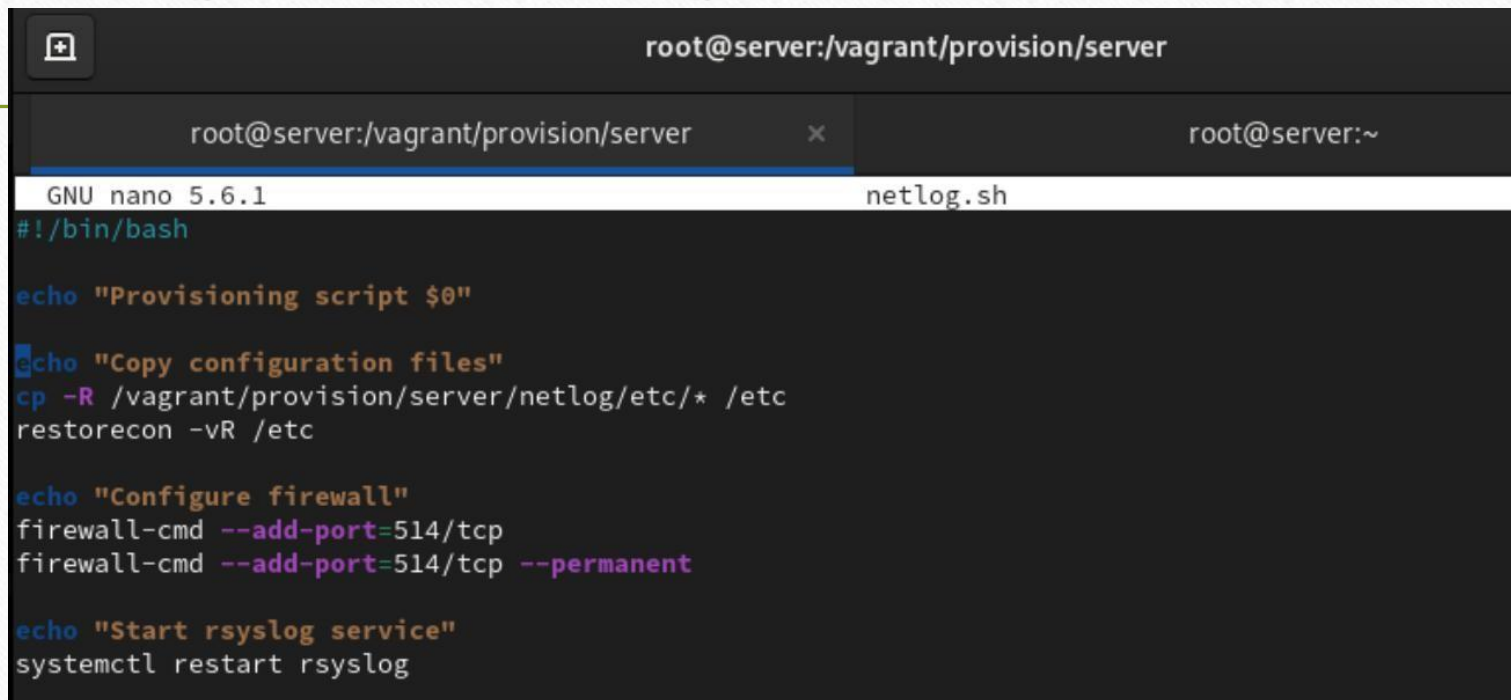
Внесение изменений в настройки внутреннего окружения виртуальных машин



```
LOG user@server:/vagrant/provision/server
[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.

Внесение изменений в настройки внутреннего окружения виртуальных машин



```
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"

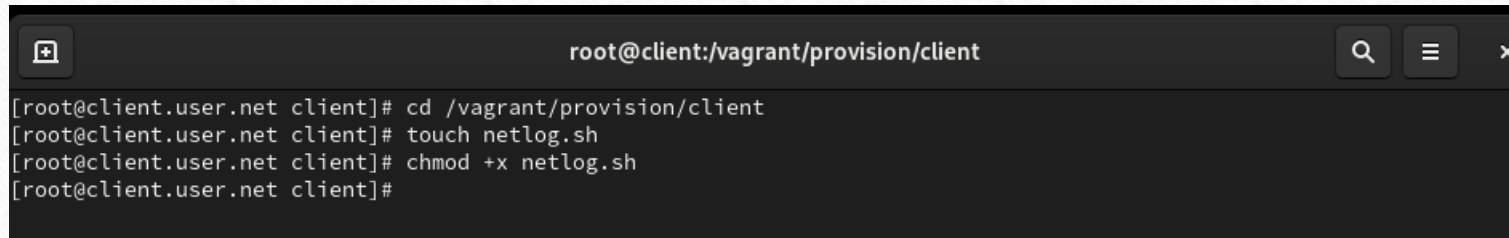
echo "Copy configuration files"
cp -R /vagrant/provision/server/netlog/etc/* /etc
restorecon -vR /etc

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.

Внесение изменений в настройки внутреннего окружения виртуальных машин

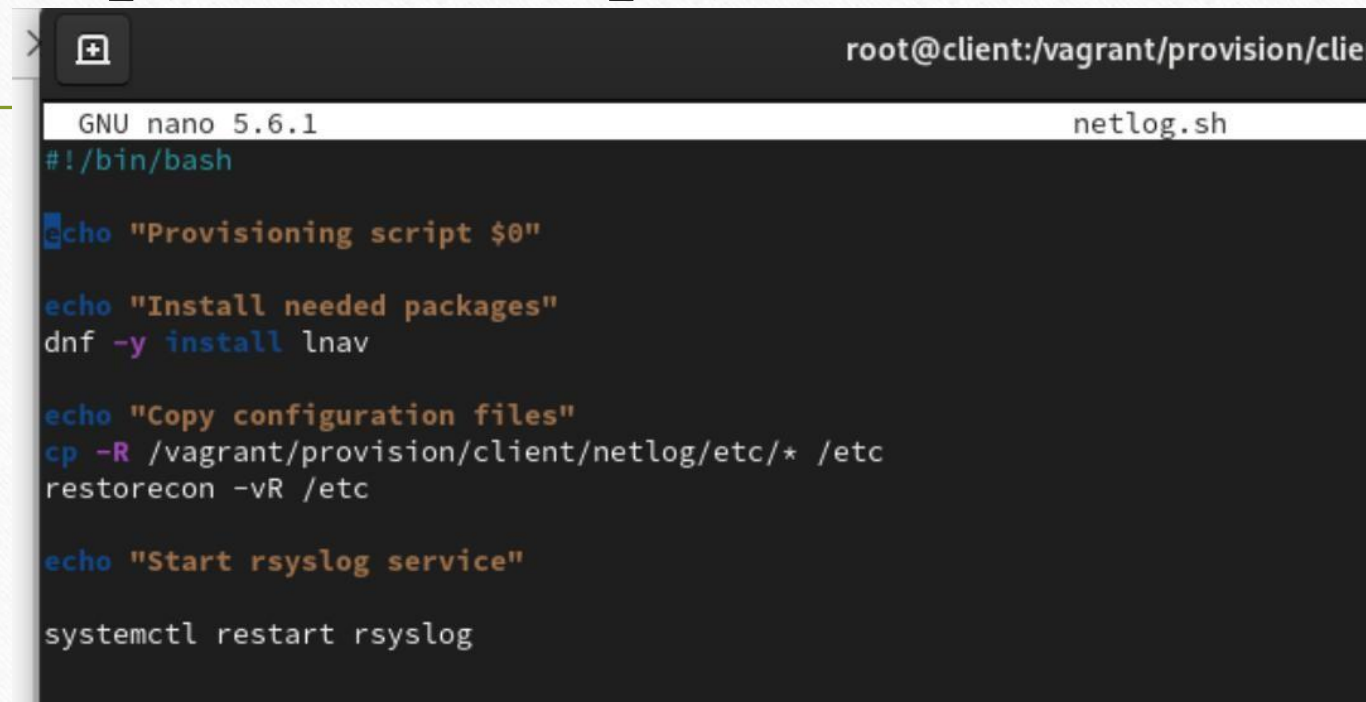


```
root@client:/vagrant/provision/client

[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.

Внесение изменений в настройки внутреннего окружения виртуальных машин

A screenshot of a terminal window. The title bar shows a window icon, a close button, and the text 'root@client:/vagrant/provision/client'. The terminal content shows the 'nano' editor interface. The top status bar indicates 'GNU nano 5.6.1' and the filename 'netlog.sh'. The editor shows a script with several lines of code: '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"', and 'systemctl restart rsyslog'. The cursor is at the end of the last line.

```
root@client:/vagrant/provision/client
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!
