

Лабораторная работа №15

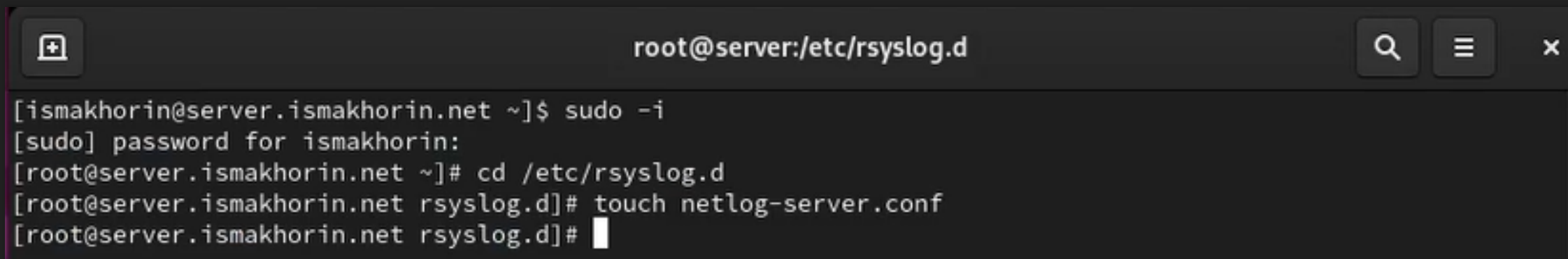
Настройка сетевого журналирования

Махорин Иван Сергеевич

1032211221

НПИБД-02-21

Настройка сервера сетевого журнала



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

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

Настройка сервера сетевого журнала

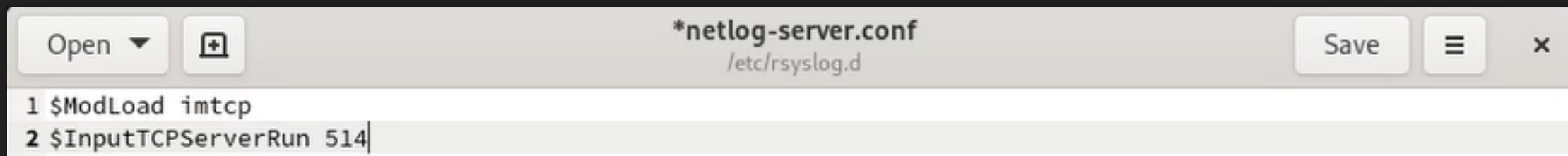
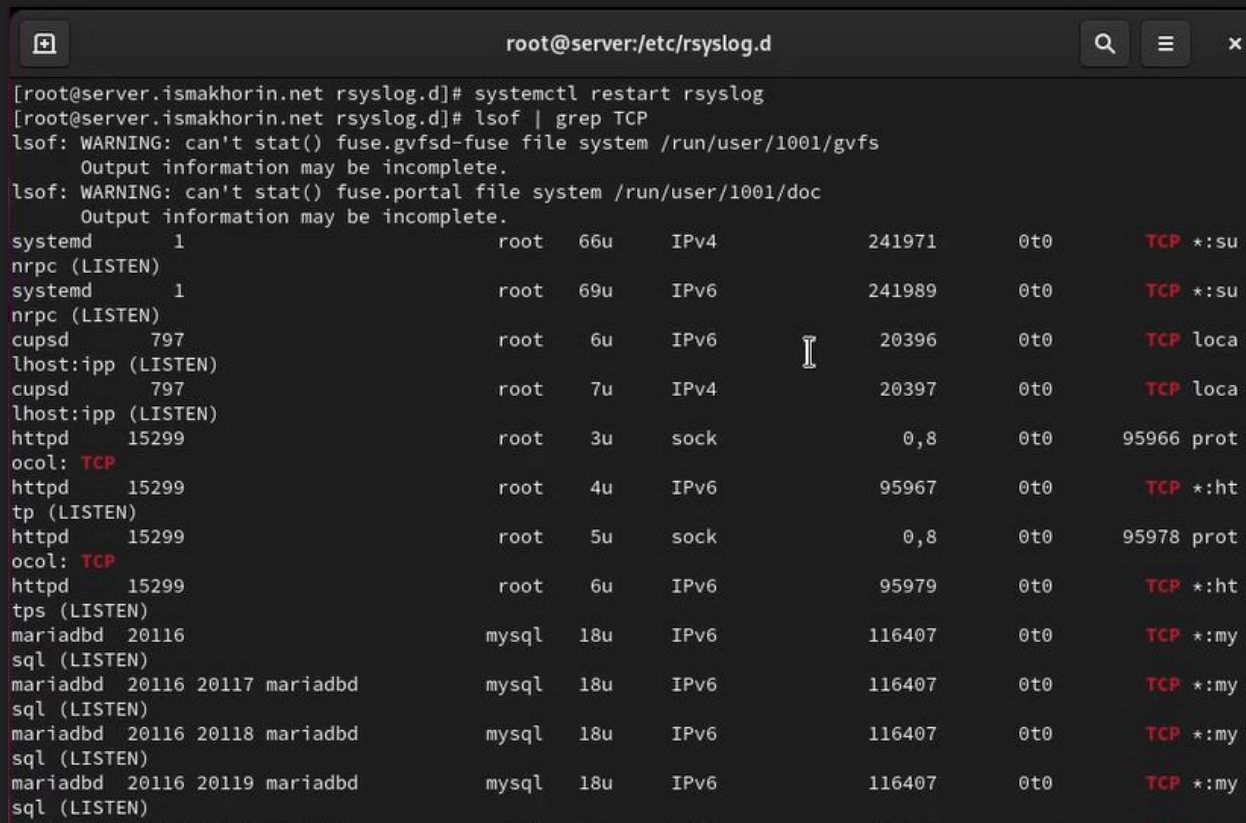


Рис. 1.2. Включение в файле конфигурации `/etc/rsyslog.d/netlog-server.conf` приёма записей журнала по TCP-порту 514.

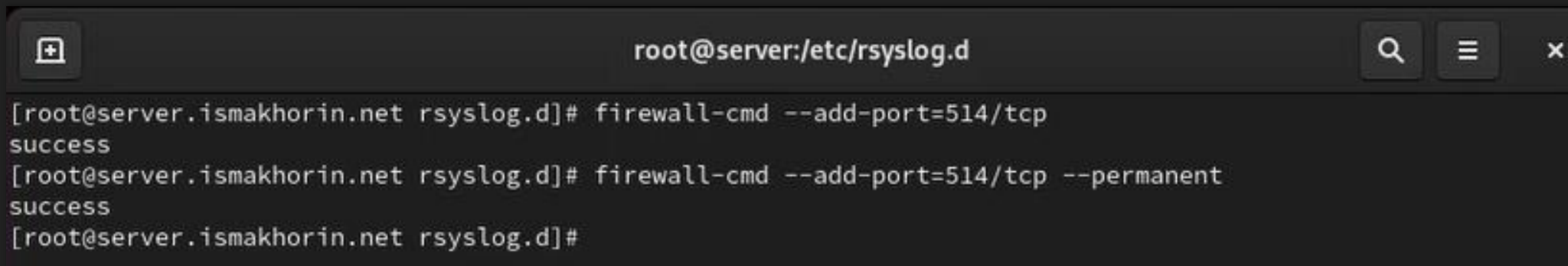
Настройка сервера сетевого журнала



```
root@server:/etc/rsyslog.d
[root@server.ismakhorin.net rsyslog.d]# systemctl restart rsyslog
[root@server.ismakhorin.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.
systemd      1      root    66u    IPv4      241971      0t0      TCP *:su
nrpc (LISTEN)
systemd      1      root    69u    IPv6      241989      0t0      TCP *:su
nrpc (LISTEN)
cupsd        797    root     6u    IPv6      20396      0t0      TCP loca
lhost:ipp (LISTEN)
cupsd        797    root     7u    IPv4      20397      0t0      TCP loca
lhost:ipp (LISTEN)
httpd       15299   root     3u    sock      0,8        0t0      95966 prot
ocol: TCP
httpd       15299   root     4u    IPv6      95967      0t0      TCP *:ht
tp (LISTEN)
httpd       15299   root     5u    sock      0,8        0t0      95978 prot
ocol: TCP
httpd       15299   root     6u    IPv6      95979      0t0      TCP *:ht
tps (LISTEN)
mariadb     20116   mysql    18u    IPv6     116407      0t0      TCP *:my
sql (LISTEN)
mariadb     20116 20117 mariadb  mysql    18u    IPv6     116407      0t0      TCP *:my
sql (LISTEN)
mariadb     20116 20118 mariadb  mysql    18u    IPv6     116407      0t0      TCP *:my
sql (LISTEN)
mariadb     20116 20119 mariadb  mysql    18u    IPv6     116407      0t0      TCP *:my
sql (LISTEN)
```

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

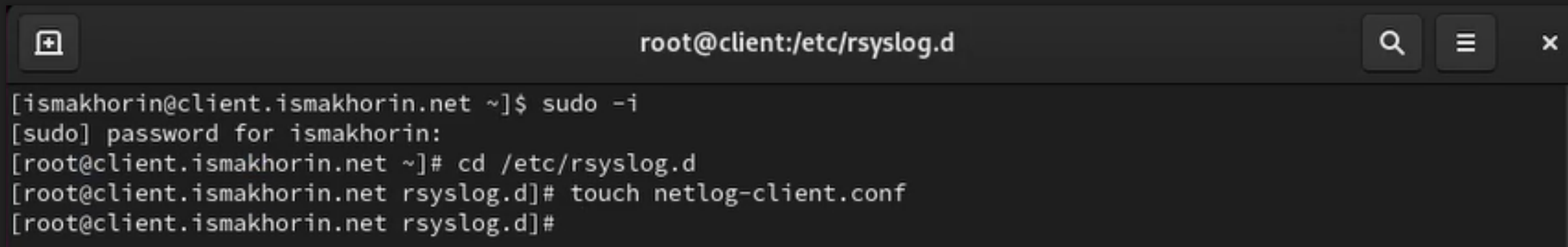
Настройка сервера сетевого журнала

A terminal window with a dark background and light text. The title bar at the top shows a window icon, the text 'root@server:/etc/rsyslog.d', and search, menu, and close buttons. The terminal content shows three lines of commands and their outputs: 'firewall-cmd --add-port=514/tcp' followed by 'success', 'firewall-cmd --add-port=514/tcp --permanent' followed by 'success', and a final prompt line.

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

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

Рис. 2.1. Создание на клиенте файла конфигурации сетевого хранения журналов.

Настройка клиента сетевого журнала

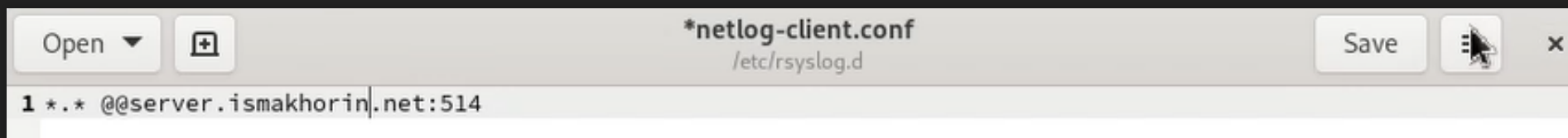
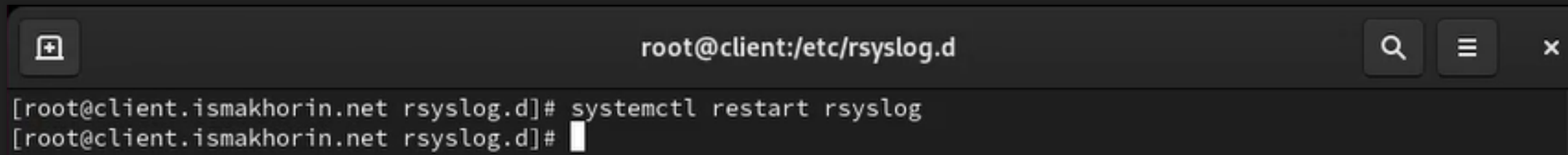


Рис. 2.2. Включение в файле конфигурации `/etc/rsyslog.d/netlog-client.conf` перенаправления сообщений журнала на 514 TCP-порт сервера.

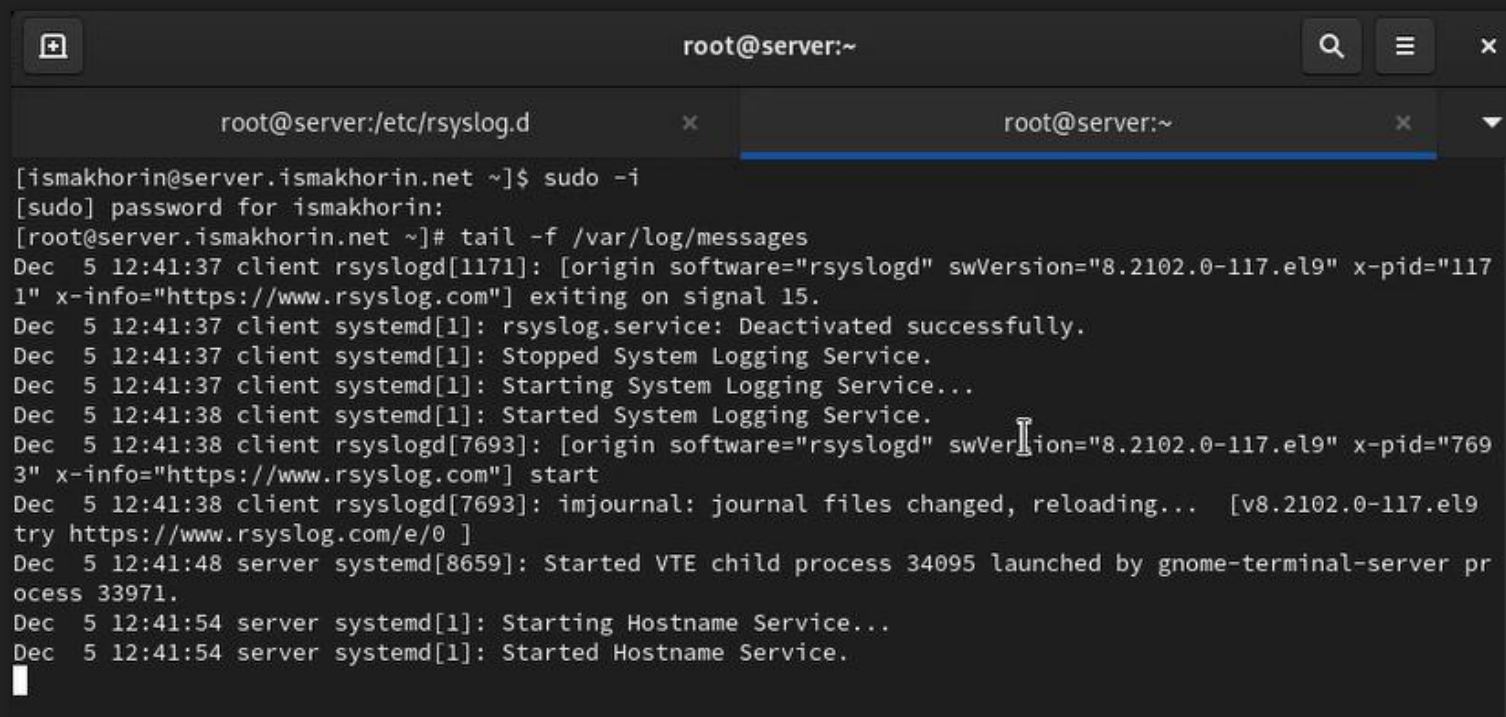
Настройка клиента сетевого журнала

A terminal window with a dark background. The title bar shows a window icon, the text 'root@client:/etc/rsyslog.d', and search, menu, and close buttons. The terminal content shows the command 'systemctl restart rsyslog' being executed in the directory '/etc/rsyslog.d' on the host 'client.ismakhorin.net'.

```
root@client:/etc/rsyslog.d  
[root@client.ismakhorin.net rsyslog.d]# systemctl restart rsyslog  
[root@client.ismakhorin.net rsyslog.d]#
```

Рис. 2.3. Перезапуск службы rsyslog.

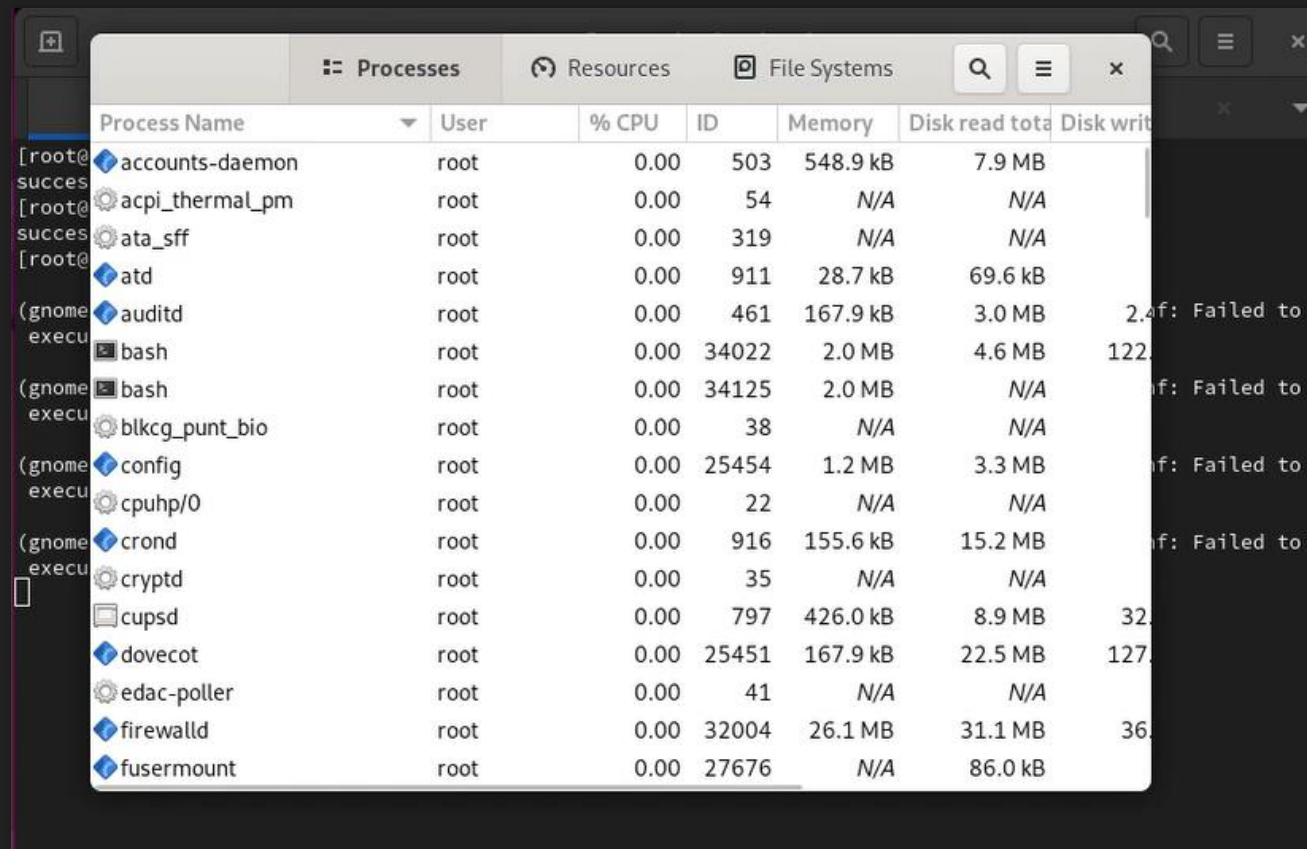
Просмотр журнала



```
root@server:~
[ismakhorin@server.ismakhorin.net ~]$ sudo -i
[sudo] password for ismakhorin:
[root@server.ismakhorin.net ~]# tail -f /var/log/messages
Dec  5 12:41:37 client rsyslogd[1171]: [origin software="rsyslogd" swVersion="8.2102.0-117.el9" x-pid="1171" x-info="https://www.rsyslog.com"] exiting on signal 15.
Dec  5 12:41:37 client systemd[1]: rsyslog.service: Deactivated successfully.
Dec  5 12:41:37 client systemd[1]: Stopped System Logging Service.
Dec  5 12:41:37 client systemd[1]: Starting System Logging Service...
Dec  5 12:41:38 client systemd[1]: Started System Logging Service.
Dec  5 12:41:38 client rsyslogd[7693]: [origin software="rsyslogd" swVersion="8.2102.0-117.el9" x-pid="7693" x-info="https://www.rsyslog.com"] start
Dec  5 12:41:38 client rsyslogd[7693]: imjournal: journal files changed, reloading... [v8.2102.0-117.el9 try https://www.rsyslog.com/e/0 ]
Dec  5 12:41:48 server systemd[8659]: Started VTE child process 34095 launched by gnome-terminal-server process 33971.
Dec  5 12:41:54 server systemd[1]: Starting Hostname Service...
Dec  5 12:41:54 server systemd[1]: Started Hostname Service.
```

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

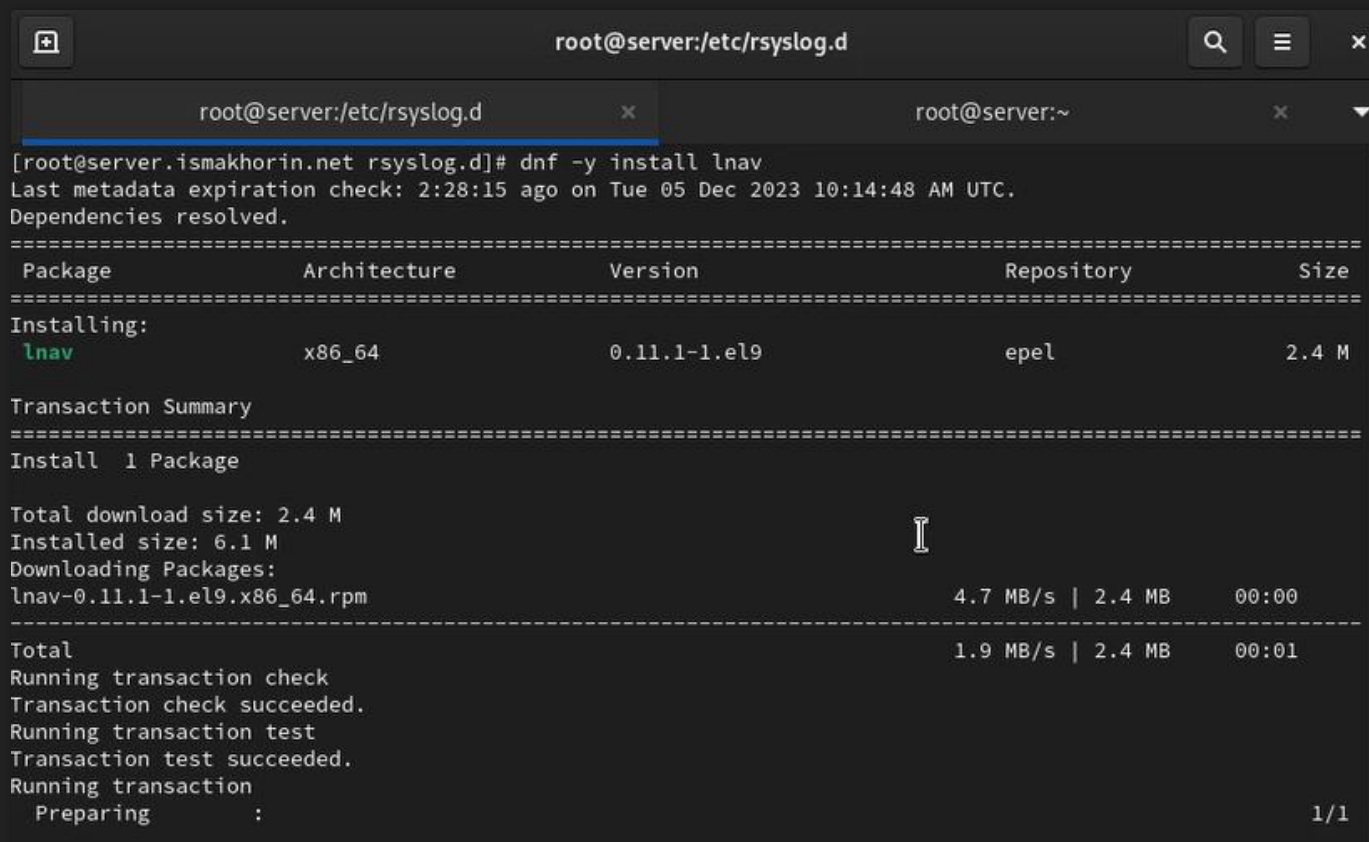
Просмотр журнала



Process Name	User	% CPU	ID	Memory	Disk read total	Disk write total
accounts-daemon	root	0.00	503	548.9 kB	7.9 MB	
acpi_thermal_pm	root	0.00	54	N/A	N/A	
ata_sff	root	0.00	319	N/A	N/A	
atd	root	0.00	911	28.7 kB	69.6 kB	
auditd	root	0.00	461	167.9 kB	3.0 MB	2.4f: Failed to
bash	root	0.00	34022	2.0 MB	4.6 MB	122
bash	root	0.00	34125	2.0 MB	N/A	f: Failed to
blkcg_punt_bio	root	0.00	38	N/A	N/A	
config	root	0.00	25454	1.2 MB	3.3 MB	f: Failed to
cpuhp/0	root	0.00	22	N/A	N/A	
crond	root	0.00	916	155.6 kB	15.2 MB	f: Failed to
cryptd	root	0.00	35	N/A	N/A	
cupsd	root	0.00	797	426.0 kB	8.9 MB	32
dovecot	root	0.00	25451	167.9 kB	22.5 MB	127
edac-poller	root	0.00	41	N/A	N/A	
firewalld	root	0.00	32004	26.1 MB	31.1 MB	36
fusermount	root	0.00	27676	N/A	86.0 kB	

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

Просмотр журнала



The image shows a terminal window titled 'root@server:/etc/rsyslog.d'. The user has executed the command 'dnf -y install lnav'. The terminal output shows the package details for 'lnav' (version 0.11.1-1.el9, repository epel, size 2.4 M) and a transaction summary. The transaction summary indicates that 1 package will be installed, with a total download size of 2.4 M and an installed size of 6.1 M. The download progress for 'lnav-0.11.1-1.el9.x86_64.rpm' is shown as 4.7 MB/s | 2.4 MB | 00:00. The total download progress is 1.9 MB/s | 2.4 MB | 00:01. The transaction check and test are successful, and the transaction is currently preparing.

```
root@server:/etc/rsyslog.d
[root@server.ismakhorin.net rsyslog.d]# dnf -y install lnav
Last metadata expiration check: 2:28:15 ago on Tue 05 Dec 2023 10:14:48 AM 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:
lnav-0.11.1-1.el9.x86_64.rpm                4.7 MB/s | 2.4 MB    00:00
-----
Total                                         1.9 MB/s | 2.4 MB    00:01
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :
1/1
```

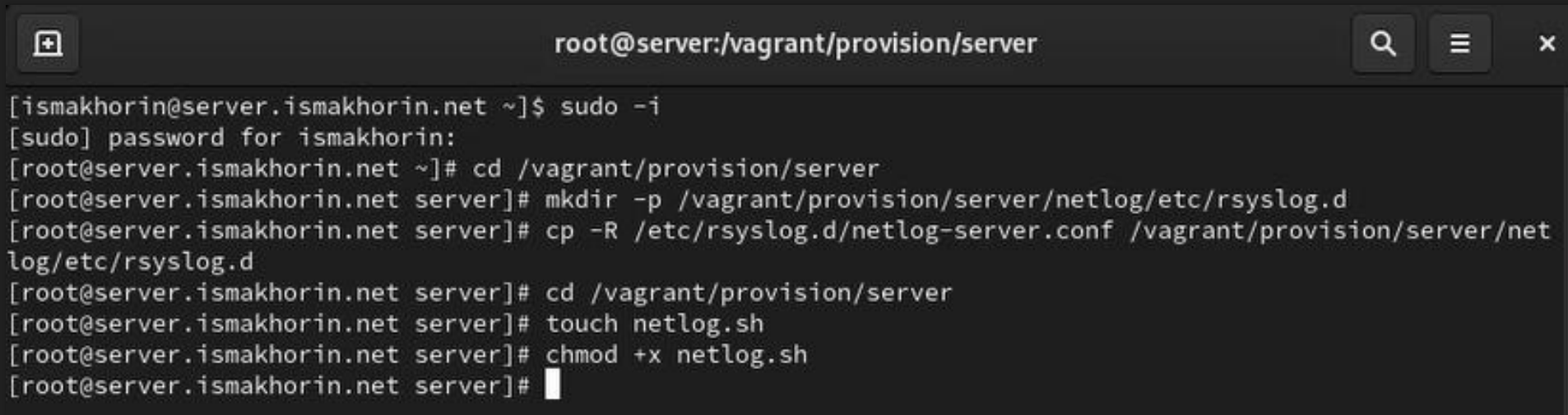
Рис. 3.3. Установка на сервере просмотрщика журналов системных сообщений lnav.

Просмотр журнала

```
LOG 2023-12-05T12:43:40.000 >syslog_log>messages[19,855] >avahi-daemon[495]>
Dec 5 12:43:40 server avahi-daemon[495]: Joining mDNS multicast group on interface eth0.IPv6 with addre
Dec 5 12:43:40 server avahi-daemon[495]: New relevant interface eth0.IPv6 for mDNS.
Dec 5 12:43:40 server avahi-daemon[495]: Registering new address record for fe80::a00:27ff:fe80:c28f on
Dec 5 12:43:40 server NetworkManager[10196]: <info> [1701780220.8657] device (eth0): state change: ip-
Dec 5 12:43:40 server NetworkManager[10196]: <info> [1701780220.8770] device (eth0): state change: sec
Dec 5 12:43:40 server NetworkManager[10196]: <info> [1701780220.8899] manager: NetworkManager state is
Dec 5 12:43:40 server NetworkManager[10196]: <info> [1701780220.9090] device (eth0): Activation: succe
Dec 5 12:43:40 server NetworkManager[10196]: <info> [1701780220.9182] manager: NetworkManager state is
Dec 5 12:43:41 server systemd[1]: iscsi.service: Unit cannot be reloaded because it is inactive.
Dec 5 12:43:41 server chrynyd[28314]: Source 195.3.254.2 online
Dec 5 12:43:41 server chrynyd[28314]: Source 188.225.9.167 online
Dec 5 12:43:41 server chrynyd[28314]: Source 83.217.206.10 online
Dec 5 12:43:41 server chrynyd[28314]: Source 91.209.94.10 online
Dec 5 12:43:41 server systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@13.servi
Dec 5 12:43:41 server chrynyd[28314]: Selected source 91.209.94.10 (2.rocky.pool.ntp.org)
```

Рис. 3.4. Просмотр логов с помощью Inav.

Внесение изменений в настройки внутреннего окружения виртуальных машин

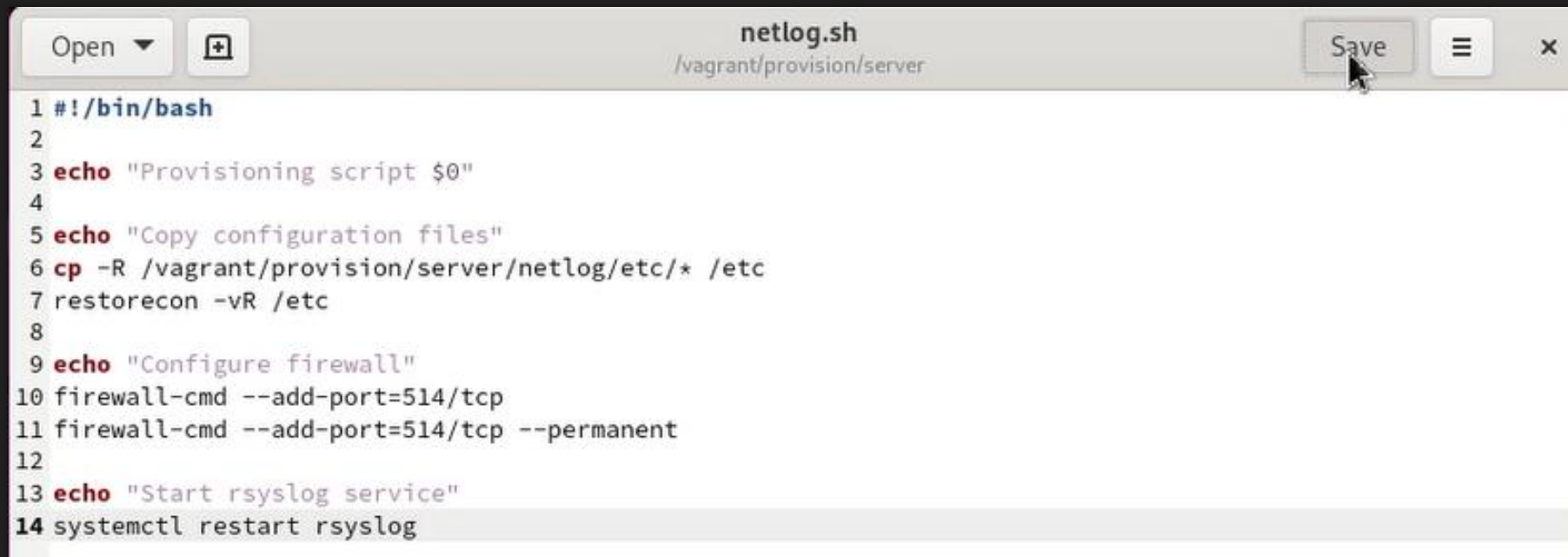


```
root@server:/vagrant/provision/server

[ismakhorin@server.ismakhorin.net ~]$ sudo -i
[sudo] password for ismakhorin:
[root@server.ismakhorin.net ~]# cd /vagrant/provision/server
[root@server.ismakhorin.net server]# mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.ismakhorin.net server]# cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.ismakhorin.net server]# cd /vagrant/provision/server
[root@server.ismakhorin.net server]# touch netlog.sh
[root@server.ismakhorin.net server]# chmod +x netlog.sh
[root@server.ismakhorin.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

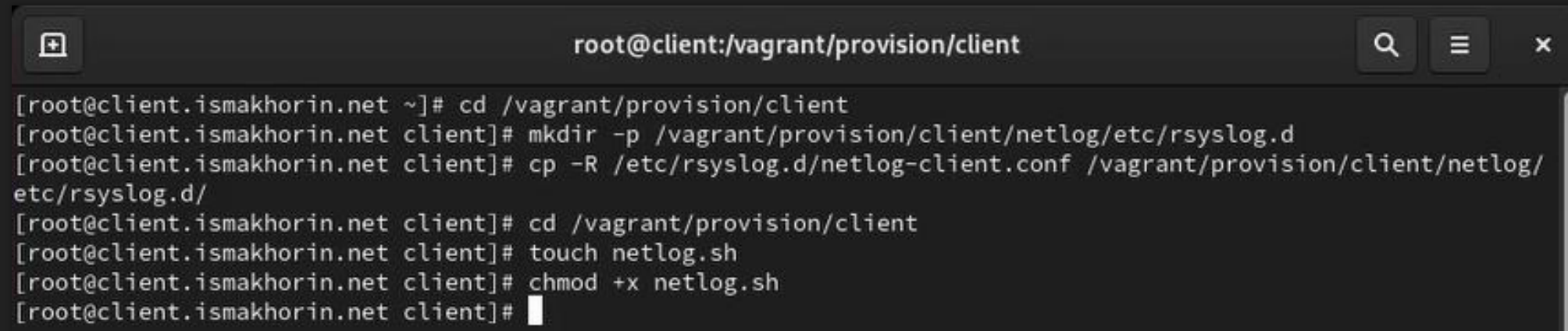


The screenshot shows a text editor window with the title bar "netlog.sh" and the file path "/vagrant/provision/server". The window contains a shell script with 14 lines of code. A mouse cursor is hovering over the "Save" button in the top right corner of the editor window.

```
1 #!/bin/bash
2
3 echo "Provisioning script $0"
4
5 echo "Copy configuration files"
6 cp -R /vagrant/provision/server/netlog/etc/* /etc
7 restorecon -vR /etc
8
9 echo "Configure firewall"
10 firewall-cmd --add-port=514/tcp
11 firewall-cmd --add-port=514/tcp --permanent
12
13 echo "Start rsyslog service"
14 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.ismakhorin.net ~]# cd /vagrant/provision/client
[root@client.ismakhorin.net client]# mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d
[root@client.ismakhorin.net client]# cp -R /etc/rsyslog.d/netlog-client.conf /vagrant/provision/client/netlog/
etc/rsyslog.d/
[root@client.ismakhorin.net client]# cd /vagrant/provision/client
[root@client.ismakhorin.net client]# touch netlog.sh
[root@client.ismakhorin.net client]# chmod +x netlog.sh
[root@client.ismakhorin.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`.

Внесение изменений в настройки внутреннего окружения виртуальных машин

A screenshot of a text editor window. The title bar shows the filename as `*netlog.sh` and the path as `/vagrant/provision/client`. The window has standard buttons: 'Open', a plus icon, 'Save', a hamburger menu, and a close 'x' button. The editor contains a shell script with 13 lines of code. The code includes comments, package installation using `dnf`, file copying, and service management using `systemctl`.

```
1 #!/bin/bash
2
3 echo "Provisioning script $0"
4
5 echo "Install needed packages"
6 dnf -y install lnav
7
8 echo "Copy configuration files"
9 cp -R /vagrant/provision/client/netlog/etc/* /etc
10 restorecon -vR /etc
11
12 echo "Start rsyslog service"
13 systemctl restart rsyslog
```

Рис. 4.4. Открытие файла на редактирование и добавление в него скрипта.

Внесение изменений в настройки внутреннего окружения виртуальных машин

```
92  
93     server.vm.provision "server netlog",  
94                         type: "shell",  
95                         preserve_order: true,  
96                         path: "provision/server/netlog.sh"  
97
```

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

Внесение изменений в настройки внутреннего окружения виртуальных машин

```
159             path: "provision/client/smb.sh"
160
161     client.vm.provision "client netlog",
162                       type: "shell",
163                       preserve_order: true,
164                       path: "provision/client/netlog.sh"
165
```

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!