

Отчёт по лабораторной работе №15

Дисциплина: Администрирование сетевых подсистем

Мишина Анастасия Алексеевна

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
2.1	Настройка сервера сетевого журнала	6
2.2	Настройка клиента сетевого журнала	7
2.3	Просмотр журнала	8
2.4	Внесение изменений в настройки внутреннего окружения виртуальной машины	10
3	Выводы	14
4	Ответы на контрольные вопросы	15

Список иллюстраций

2.1	Редактирование файла конфигурации сетевого хранения журналов /etc/rsyslog.d/netlog-server.conf	6
2.2	Перезапуск rsyslog и просмотр прослушиваемых портов .	7
2.3	Настройка межсетевого экрана для работы с TCP-портом 514	7
2.4	Редактирование файла конфигурации сетевого хранения журналов на клиенте: включение перенаправления на 514 порт	8
2.5	Просмотр файла журнала на сервере	8
2.6	Запуск графической программы для просмотра журналов	9
2.7	Использование lnav для просмотра логов	10
2.8	Редактирование netlog.sh на сервере	11
2.9	Редактирование netlog.sh на клиенте	12

Список таблиц

1 Цель работы

Получение навыков по работе с журналами системных событий.

2 Выполнение лабораторной работы

2.1 Настройка сервера сетевого журнала

На сервере создаем файл конфигурации сетевого хранения журналов: `cd /etc/rsyslog.d` и `touch netlog-server.conf`.

В данном файле включаем прием записей журнала по TCP-порту 514 (рис. 2.1).

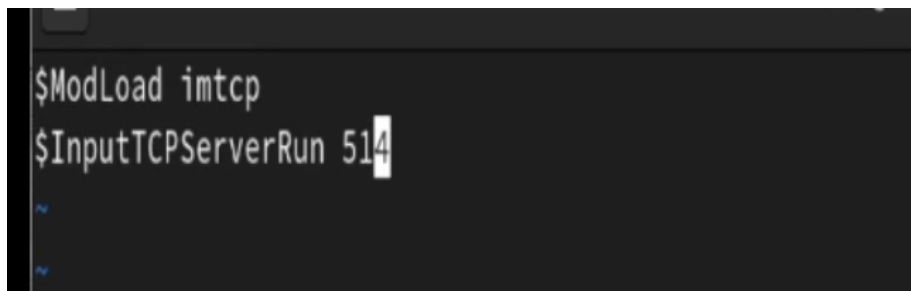


Рис. 2.1: Редактирование файла конфигурации сетевого хранения журналов `/etc/rsyslog.d/netlog-server.conf`

Перезапускаем службу `rsyslog` - `systemctl restart rsyslog` и просматриваем прослушиваемые порты, которые связаны со службой - `lsof | grep TCP` (рис. 2.2).

```

rsyslogd 6677          root 4u IPv4 42173 0t0 TCP *:shell (LISTEN)
rsyslogd 6677          root 5u IPv6 42174 0t0 TCP *:shell (LISTEN)
rsyslogd 6677 6679 in:imjour root 4u IPv4 42173 0t0 TCP *:shell (LISTEN)
rsyslogd 6677 6679 in:imjour root 5u IPv6 42174 0t0 TCP *:shell (LISTEN)
rsyslogd 6677 6680 in:imtcp root 4u IPv4 42173 0t0 TCP *:shell (LISTEN)
rsyslogd 6677 6680 in:imtcp root 5u IPv6 42174 0t0 TCP *:shell (LISTEN)
rsyslogd 6677 6681 in:imtcp root 4u IPv4 42173 0t0 TCP *:shell (LISTEN)
rsyslogd 6677 6681 in:imtcp root 5u IPv6 42174 0t0 TCP *:shell (LISTEN)
rsyslogd 6677 6682 in:imtcp root 4u IPv4 42173 0t0 TCP *:shell (LISTEN)
rsyslogd 6677 6682 in:imtcp root 5u IPv6 42174 0t0 TCP *:shell (LISTEN)
rsyslogd 6677 6683 in:imtcp root 4u IPv4 42173 0t0 TCP *:shell (LISTEN)
rsyslogd 6677 6683 in:imtcp root 5u IPv6 42174 0t0 TCP *:shell (LISTEN)
rsyslogd 6677 6684 in:imtcp root 4u IPv4 42173 0t0 TCP *:shell (LISTEN)
rsyslogd 6677 6684 in:imtcp root 5u IPv6 42174 0t0 TCP *:shell (LISTEN)
rsyslogd 6677 6685 rs:main root 4u IPv4 42173 0t0 TCP *:shell (LISTEN)
rsyslogd 6677 6685 rs:main root 5u IPv6 42174 0t0 TCP *:shell (LISTEN)
[root@server.aamishina.net ~]#

```

Рис. 2.2: Перезапуск rsyslog и просмотр прослушиваемых портов

На сервере настраиваем межсетевой экран для работы с TCP-портом 514 (рис. 2.3).

```

[root@server.aamishina.net ~]# firewall-cmd --add-port=514/tcp
success
[root@server.aamishina.net ~]# firewall-cmd --add-port=514/tcp --permanent
success
[root@server.aamishina.net ~]#

```

Рис. 2.3: Настройка межсетевого экрана для работы с TCP-портом 514

2.2 Настройка клиента сетевого журнала

На клиенте создаем файл конфигурации сетевого хранения журналов:

```

cd /etc/rsyslog.d
touch netlog-client.conf

```

В данном файле включаем перенаправление сообщений журнала на 514 TCP-порт сервера и перезапускаем службу (рис. 2.4).

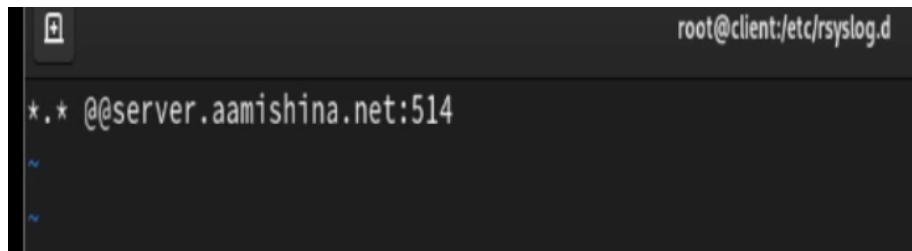


Рис. 2.4: Редактирование файла конфигурации сетевого хранения журналов на клиенте: включение перенаправления на 514 порт

2.3 Просмотр журнала

На сервере просматриваем один из файлов журнала. Обращаем внимание, что выводятся сообщения как с сервера, так и с клиента (рис. 2.5).



Рис. 2.5: Просмотр файла журнала на сервере

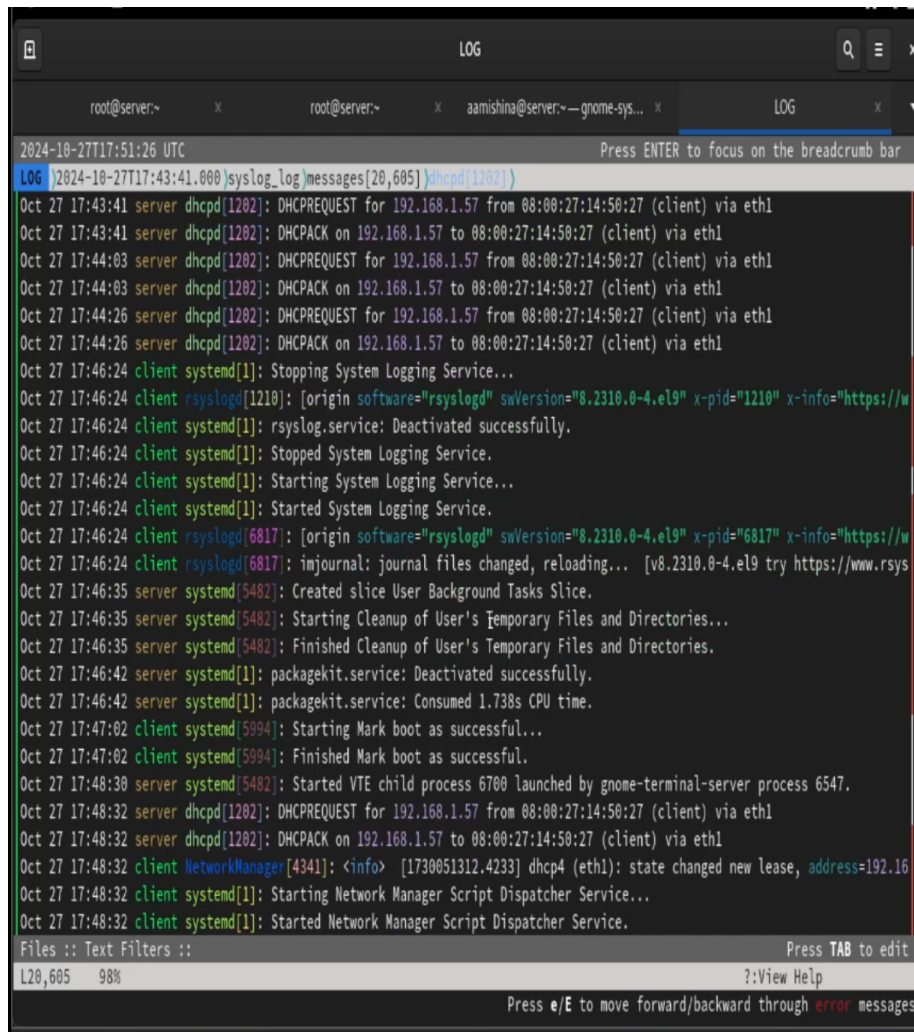
На сервере под пользователем aamishina запускаем графическую программу для просмотра журналов (рис. 2.6).

Process Name	User	% CPU	ID	Memory	Disk read tot	Disk write tot	Disk read	Disk write	Priority
at-spi2-registrd	aamishina	0.00	5716	262.1 kB	184.3 kB	N/A	N/A	N/A	Normal
at-spi-bus-launcher	aamishina	0.00	5685	81.9 kB	491.5 kB	N/A	N/A	N/A	Normal
bash	aamishina	0.00	6566	2.0 MB	10.6 MB	N/A	N/A	N/A	Normal
bash	aamishina	0.00	6700	2.0 MB	958.5 kB	N/A	N/A	N/A	Normal
bash	aamishina	0.00	6774	2.0 MB	N/A	N/A	N/A	N/A	Normal
dbus-broker	aamishina	0.00	5579	917.5 kB	671.7 kB	N/A	N/A	N/A	Normal
dbus-broker	aamishina	0.00	5691	131.1 kB	81.9 kB	N/A	N/A	N/A	Normal
dbus-broker-launch	aamishina	0.00	5564	131.1 kB	1.6 MB	N/A	N/A	N/A	Normal
dbus-broker-launch	aamishina	0.00	5690	N/A	8.2 kB	N/A	N/A	N/A	Normal
dconf-service	aamishina	0.00	6060	393.2 kB	692.2 kB	16.4 kB	N/A	N/A	Normal
evolution-addressbook-factory	aamishina	0.00	6063	655.4 kB	6.4 MB	36.9 kB	N/A	N/A	Normal
evolution-alarm-notify	aamishina	0.00	6227	499.7 kB	8.2 MB	N/A	N/A	N/A	Normal
evolution-calendar-factory	aamishina	0.00	6037	131.1 kB	2.5 MB	N/A	N/A	N/A	Normal
evolution-source-registry	aamishina	0.00	6022	N/A	3.1 MB	N/A	N/A	N/A	Normal
gjs	aamishina	0.00	6139	2.0 MB	4.0 MB	N/A	N/A	N/A	Normal
gjs	aamishina	0.00	6283	2.7 MB	2.8 MB	N/A	N/A	N/A	Normal
gnome-keyring-daemon	aamishina	0.00	5544	507.9 kB	N/A	N/A	N/A	N/A	Normal
gnome-session-binary	aamishina	0.00	5549	65.5 kB	9.1 MB	N/A	N/A	N/A	Normal

Рис. 2.6: Запуск графической программы для просмотра журналов

Устанавливаем просмотрщик журналов системных событий `lnav: dnf -y install lnav`.

Используем `lnav` для просмотра логов (рис. 2.7).



```
LOG
root@server:~ x root@server:~ x aamishina@server:~ - gnome-sys... x LOG x
2024-10-27T17:51:26 UTC Press ENTER to focus on the breadcrumb bar
LOG 2024-10-27T17:43:41.000/syslog_log/messages[20,605]dhcpd[1202]
Oct 27 17:43:41 server dhcpd[1202]: DHCPREQUEST for 192.168.1.57 from 08:00:27:14:50:27 (client) via eth1
Oct 27 17:43:41 server dhcpd[1202]: DHCPACK on 192.168.1.57 to 08:00:27:14:50:27 (client) via eth1
Oct 27 17:44:03 server dhcpd[1202]: DHCPREQUEST for 192.168.1.57 from 08:00:27:14:50:27 (client) via eth1
Oct 27 17:44:03 server dhcpd[1202]: DHCPACK on 192.168.1.57 to 08:00:27:14:50:27 (client) via eth1
Oct 27 17:44:26 server dhcpd[1202]: DHCPREQUEST for 192.168.1.57 from 08:00:27:14:50:27 (client) via eth1
Oct 27 17:44:26 server dhcpd[1202]: DHCPACK on 192.168.1.57 to 08:00:27:14:50:27 (client) via eth1
Oct 27 17:46:24 client systemd[1]: Stopping System Logging Service...
Oct 27 17:46:24 client rsyslogd[1210]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="1210" x-info="https://w
Oct 27 17:46:24 client systemd[1]: rsyslog.service: Deactivated successfully.
Oct 27 17:46:24 client systemd[1]: Stopped System Logging Service.
Oct 27 17:46:24 client systemd[1]: Starting System Logging Service...
Oct 27 17:46:24 client systemd[1]: Started System Logging Service.
Oct 27 17:46:24 client rsyslogd[6817]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="6817" x-info="https://w
Oct 27 17:46:24 client rsyslogd[6817]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try https://www.rsys
Oct 27 17:46:35 server systemd[5482]: Created slice User Background Tasks Slice.
Oct 27 17:46:35 server systemd[5482]: Starting Cleanup of User's Temporary Files and Directories...
Oct 27 17:46:35 server systemd[5482]: Finished Cleanup of User's Temporary Files and Directories.
Oct 27 17:46:42 server systemd[1]: packagekit.service: Deactivated successfully.
Oct 27 17:46:42 server systemd[1]: packagekit.service: Consumed 1.738s CPU time.
Oct 27 17:47:02 client systemd[5994]: Starting Mark boot as successful...
Oct 27 17:47:02 client systemd[5994]: Finished Mark boot as successful.
Oct 27 17:48:30 server systemd[5482]: Started VTE child process 6700 launched by gnome-terminal-server process 6547.
Oct 27 17:48:32 server dhcpd[1202]: DHCPREQUEST for 192.168.1.57 from 08:00:27:14:50:27 (client) via eth1
Oct 27 17:48:32 server dhcpd[1202]: DHCPACK on 192.168.1.57 to 08:00:27:14:50:27 (client) via eth1
Oct 27 17:48:32 client NetworkManager[4341]: <info> [1730051312.4233] dhcp4 (eth1): state changed new lease, address=192.16
Oct 27 17:48:32 client systemd[1]: Starting Network Manager Script Dispatcher Service...
Oct 27 17:48:32 client systemd[1]: Started Network Manager Script Dispatcher Service.
Files :: Text Filters :: Press TAB to edit
L20,605 98% ?::View Help
Press e/E to move forward/backward through error messages
```

Рис. 2.7: Использование `lnav` для просмотра логов

2.4 Внесение изменений в настройки внутреннего окружения виртуальной машины

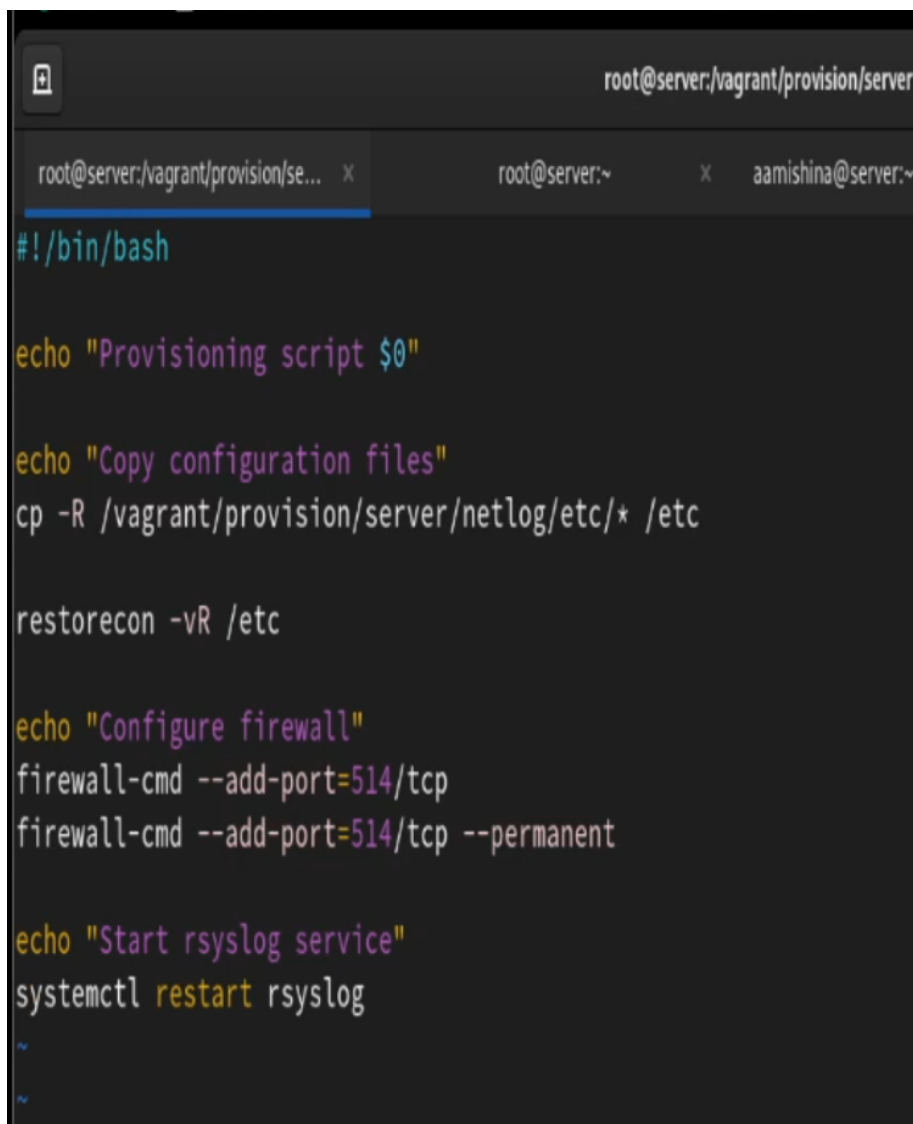
На VM server переходим в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/` и копируем в соответствующие каталоги конфигурационные файлы:

```
cd /vagrant/provision/server
```

```
mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
```

```
cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netl
```

Вносим изменения в файл `/vagrant/provision/server/netlog.sh` (рис. 2.8).

A screenshot of a terminal window with a dark background. The title bar at the top shows the path `root@server:/vagrant/provision/server`. Below the title bar, there are three tabs: `root@server:/vagrant/provision/se...`, `root@server:~`, and `aamishina@server:~`. The first tab is active. The terminal content shows a shell prompt `#!/bin/bash` followed by several `echo` commands and system configuration commands. The commands are: `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"`, and `systemctl restart rsyslog`. The terminal ends with two tilde characters `~` on separate lines.

```
#!/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

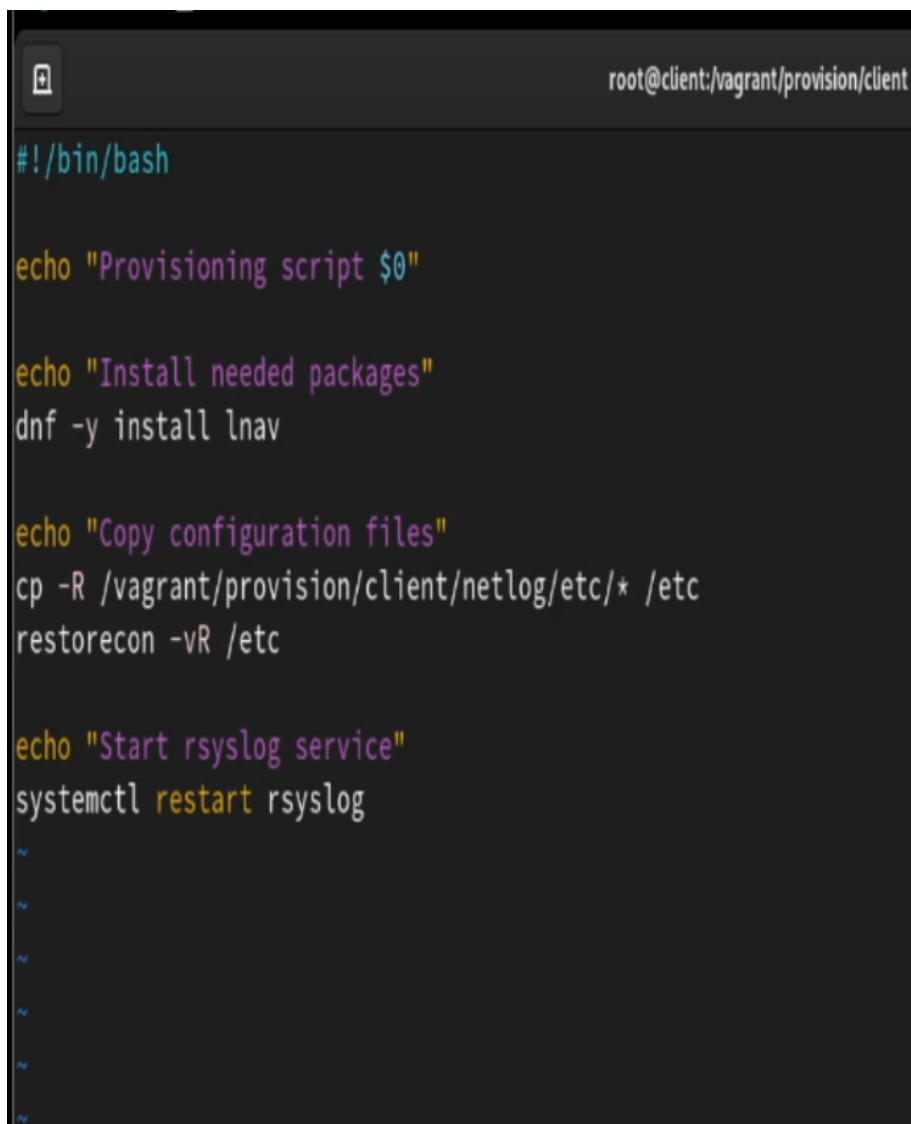
~
~
```

Рис. 2.8: Редактирование `netlog.sh` на сервере

На `VM client` переходим в каталог для внесения изменений в настройки внутреннего окружения и копируем в соответствующие каталоги конфигурационные файлы:

```
cd /vagrant/provision/client
mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d
cp -R /etc/rsyslog.d/netlog-client.conf /vagrant/provision/client/netl
```

Создаем и редактируем скрипт `/vagrant/provision/client/netlog.sh` (рис. 2.9).

A terminal window with a dark background. The title bar shows a window icon and the text 'root@client:/vagrant/provision/client'. The terminal content is a shell script with syntax highlighting: a shebang line, an echo statement, an echo statement followed by a dnf command, an echo statement followed by cp and restorecon commands, and an echo statement followed by a systemctl command. There are also several tilde characters at the bottom.

```
#!/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. 2.9: Редактирование `netlog.sh` на клиенте

Для отработки созданных скриптов во время загрузки виртуальных машин `server` и `client` в конфигурационном файле `Vagrantfile` добавляем записи в соответствующих разделах конфигураций для сервера и клиента:

```
server.vm.provision "server netlog",
type: "shell",
preserve_order: true,
path: "provision/server/netlog.sh"
```

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

3 Выводы

В результате выполнения работы были приобретены навыки по работе с журналами системных событий.

4 Ответы на контрольные вопросы

1. Какой модуль `rsyslog` вы должны использовать для приёма сообщений от `journald`?

Для приёма сообщений от `journald` следует использовать модуль `imjournal`.

2. Как называется устаревший модуль, который можно использовать для включения приёма сообщений журнала в `rsyslog`?

`imklog`

3. Чтобы убедиться, что устаревший метод приёма сообщений из `journald` в `rsyslog` не используется, какой дополнительный параметр следует использовать?

Следует использовать параметр `SystemCallFilter[include:omusrmsg.conf?]` в конфигурационном файле `rsyslog.conf`.

4. В каком конфигурационном файле содержатся настройки, которые позволяют вам настраивать работу журнала?

Настройки, позволяющие настраивать работу журнала, содержатся в конфигурационном файле `rsyslog.conf`.

5. Каким параметром управляется пересылка сообщений из `journald` в `rsyslog`?

Пересылка сообщений из `journald` в `rsyslog` управляется параметром “`ForwardToSyslog`” в файле конфигурации `journald.conf`.

6. Какой модуль `rsyslog` вы можете использовать для включения сообщений из файла журнала, не созданного `rsyslog`?

Модуль `rsyslog`, который можно использовать для включения сообщений из файла журнала, не созданного `rsyslog`, называется `imfile`.

7. Какой модуль `rsyslog` вам нужно использовать для пересылки сообщений в базу данных `MariaDB`?

Для пересылки сообщений в базу данных `MariaDB` следует использовать модуль `ommysql`.

8. Какие две строки вам нужно включить в `rsyslog.conf`, чтобы позволить текущему журнальному серверу получать сообщения через TCP?

Для позволения текущему журнальному серверу получать сообщения через TCP нужно включить две строки в `rsyslog.conf`:

```
$ModLoad imtcp  
$InputTCPServerRun 514
```

9. Как настроить локальный брандмауэр, чтобы разрешить приём сообщений журнала через порт TCP 514?

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