

# **Лабораторная работа №15**

**Настройка сетевого журналирования**

Ромицына Анастасия Романовна

# Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	13
4	Ответы на контрольные вопросы:	14
	Список литературы	16

## Список иллюстраций

2.1	Создание на сервере файла конфигурации сетевого хранения журналов. . . . .	6
2.2	Включение в файле конфигурации <code>/etc/rsyslog.d/netlog-server.conf</code> приёма записей журнала по TCP-порту 514. . . . .	6
2.3	Перезапуск службы <code>rsyslog</code> и просмотр прослушиваемых портов, связанных с <code>rsyslog</code> . . . . .	6
2.4	Настройка на сервере межсетевого экрана для приёма сообщений по TCP-порту 514. . . . .	7
2.5	Создание на клиенте файла конфигурации сетевого хранения журналов. . . . .	7
2.6	Включение в файле конфигурации <code>/etc/rsyslog.d/netlog-client.conf</code> перенаправления сообщений журнала на 514 TCP-порт сервера. .	7
2.7	Перезапуск службы <code>rsyslog</code> . . . . .	7
2.8	Просмотр на сервере одного из файлов журнала. . . . .	8
2.9	Запуск на сервере под пользователем <code>arromichina</code> графической программы для просмотра журналов. . . . .	8
2.10	Установка на сервере просмотрщика журналов системных сообщений. . . . .	9
2.11	Просмотр логов. . . . .	9
2.12	Переход на виртуальной машине <code>server</code> в каталог для внесения изменений в настройки внутреннего окружения <code>/vagrant/provision/server/</code> , создание в нём каталога <code>netlog</code> , в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге <code>/vagrant/provision/server</code> исполняемого файла <code>netlog.sh</code> . .	10
2.13	Открытие файла на редактирование и добавление в него скрипта. .	10
2.14	Переход на виртуальной машине <code>client</code> в каталог для внесения изменений в настройки внутреннего окружения <code>/vagrant/provision/client/</code> , создание в нём каталога <code>netlog</code> , в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге <code>/vagrant/provision/client</code> исполняемого файла <code>netlog.sh</code> . .	11
2.15	Открытие файла на редактирование и добавление в него скрипта. .	11
2.16	Добавление конфигураций в конфигурационном файле <code>Vagrantfile</code> для сервера и клиента. . . . .	12

## Список таблиц

# 1 Цель работы

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

## 2 Выполнение лабораторной работы

На сервере создадим файл конфигурации сетевого хранения журналов(рис. 2.1).

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

Рис. 2.1: 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. 2.2).

```
netlog-server.conf [-----] 22 L: [ 1* 1 2/ 2] *(37 / 37b) <EOF>
$ModLoad imtcp
$InputTCPServerRun 514
```

Рис. 2.2: 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. 2.3).

```
[root@server.arromichina.net rsyslog.d]# systemctl restart rsyslog
[root@server.arromichina.net rsyslog.d]# ss -ltn | grep TCP
ss: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
Output information may be incomplete.
ss: WARNING: can't stat() fuse.portal file system /run/user/1001/doc
Output information may be incomplete.
systemd 1 root 42u IPv4 5512 0t0 TCP *:sunrpc (LISTEN)
systemd 1 root 44u IPv6 5526 0t0 TCP *:sunrpc (LISTEN)
```

Рис. 2.3: Перезапуск службы rsyslog и просмотр прослушиваемых портов, связанных с rsyslog.

На сервере настроим межсетевого экран для приёма сообщений по TCP-порту 514(рис. 2.4).

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

Рис. 2.4: Настройка на сервере межсетевого экрана для приёма сообщений по TCP-порту 514.

На клиенте создадим файл конфигурации сетевого хранения журналов (рис. 2.5).

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

Рис. 2.5: 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. 2.6).

```
netlog-client.conf [-M--] 25 L:[ 1* 0 1/ 1] *(25 / 25b) <EOF>
*.* @server.user.net:514
```

Рис. 2.6: Включение в файле конфигурации /etc/rsyslog.d/netlog-client.conf перенаправления сообщений журнала на 514 TCP-порт сервера.

Перезапустим службу rsyslog (рис. 2.7).

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

Рис. 2.7: Перезапуск службы rsyslog.

На сервере посмотрим один из файлов журнала(рис. 2.8).

```
[root@server.arromichina.net rsyslog.d]# tail -f /var/log/messages
Dec 10 13:24:36 server named[1358]: timed out resolving 'ns4.dnsnadeeasy.com/A/IN': 127.0.0.1#53
Dec 10 13:24:36 server named[1358]: timed out resolving 'ns4.dnsnadeeasy.com/AAAA/IN': 127.0.0.1#53
Dec 10 13:24:36 server named[1358]: timed out resolving 'ns2.dnsnadeeasy.com/AAAA/IN': 127.0.0.1#53
Dec 10 13:24:36 server named[1358]: timed out resolving 'ns2.dnsnadeeasy.com/A/IN': 127.0.0.1#53
Dec 10 13:24:36 server named[1358]: timed out resolving 'ns0.dnsnadeeasy.com/A/IN': 127.0.0.1#53
Dec 10 13:24:36 server named[1358]: timed out resolving 'ns0.dnsnadeeasy.com/AAAA/IN': 127.0.0.1#53
Dec 10 13:24:37 server named[1358]: timed out resolving 'user.net/D5/IN': 127.0.0.1#53
Dec 10 13:24:42 server NetworkManager[4948]: <info> [1765373082.1385] agent-manager: agent[b4b1c00d5069170,:1.206/org.gnome.Shell.NetworkAgent/1001]: agent registered
Dec 10 13:24:42 server gnome-shell[7970]: Glib::Error: org.freedesktop.DBus.Error.Failed: Set global engine failed: Operation was cancelled#012Stack trace:#012 _promisify/proto[asyncFunc]/</@resource:///org/gnome/gjs/modules/core/overrides/Gio.js:453:45#012 @resource:///org/gnome/shell/ui/init.js:21:20#012 ### Promise created here: ####
012 _setEngine@resource:///org/gnome/shell/misc/ibusManager.js:286:30#012 setEngine@resource:///org/gnome/shell/misc/ibusManager.js:299:24#012 activateInputSource@resource:///org/gnome/shell/ui/status/keyboard.js:523:27#012 _callHandler
s@resource:///org/gnome/gjs/modules/core/_signals.js:130:42#012 _emit@resource:///org/gnome/gjs/modules/core/_signals.js:119:10#012 activate@resource:///org/gnome/shell/ui/status/keyboard.js:66:14#012 _inputSourcesChanged@resource:///org/gnome/shell/ui/status/keyboard.js:394:14#012 _ibusSetContentType@resource:///org/gnome/shell/ui/status/keyboard.js:736:14#012 _callHandlers@resource:///org/gnome/gjs/modules/core/_signals.js:130:42#012 _emit@resource:///org/gnome/gjs/modules/core/_signals.js:119:10#012 _setContentType@resource:///org/gnome/shell/misc/ibusManager.js:264:14#012 @resource:///org/gnome/shell/ui/init.js:21:20#012
```

Рис. 2.8: Просмотр на сервере одного из файлов журнала.

На сервере под пользователем arromichina запустим графическую программу для просмотра журналов (рис. 2.9).

Process Name	User	% CPU	ID	Memory	Disk read total	Disk write
at-spi2-registryd	arromichina	0.00	8013	131.1 kB	299.0 kB	
at-spi-bus-launcher	arromichina	0.00	8005	131.1 kB	323.6 kB	
bash	arromichina	0.00	8878	393.2 kB	9.3 MB	
bash	arromichina	0.00	10594	2.0 MB	892.9 kB	
catatonit	arromichina	0.00	8776	N/A	663.6 kB	
dbus-broker	arromichina	0.00	7890	1.2 MB	1.4 MB	
dbus-broker	arromichina	0.00	8012	N/A	N/A	
dbus-broker-launch	arromichina	0.00	7888	131.1 kB	N/A	
dbus-broker-launch	arromichina	0.00	8011	131.1 kB	N/A	
dconf-service	arromichina	0.00	8031	262.1 kB	495.6 kB	20.0
evolution-addressbook-factory	arromichina	0.00	8328	131.1 kB	2.9 MB	53.0
evolution-alarm-notify	arromichina	0.00	8095	258.0 kB	1.7 MB	
evolution-calendar-factory	arromichina	0.00	8269	917.5 kB	3.9 MB	
evolution-source-registry	arromichina	0.00	8049	1.0 MB	4.7 MB	
firefox	arromichina	1.89	8674	210.6 MB	412.1 MB	140.0
gdm-wayland-session	arromichina	0.00	7884	131.1 kB	4.1 kB	
gjs	arromichina	0.00	8050	102.4 kB	192.5 kB	
nis	arromichina	0.00	8267	3.3 MB	4.8 MB	

Рис. 2.9: Запуск на сервере под пользователем arromichina графической программы для просмотра журналов.

На сервере установим просмотрщик журналов системных сообщений(рис. 2.10).



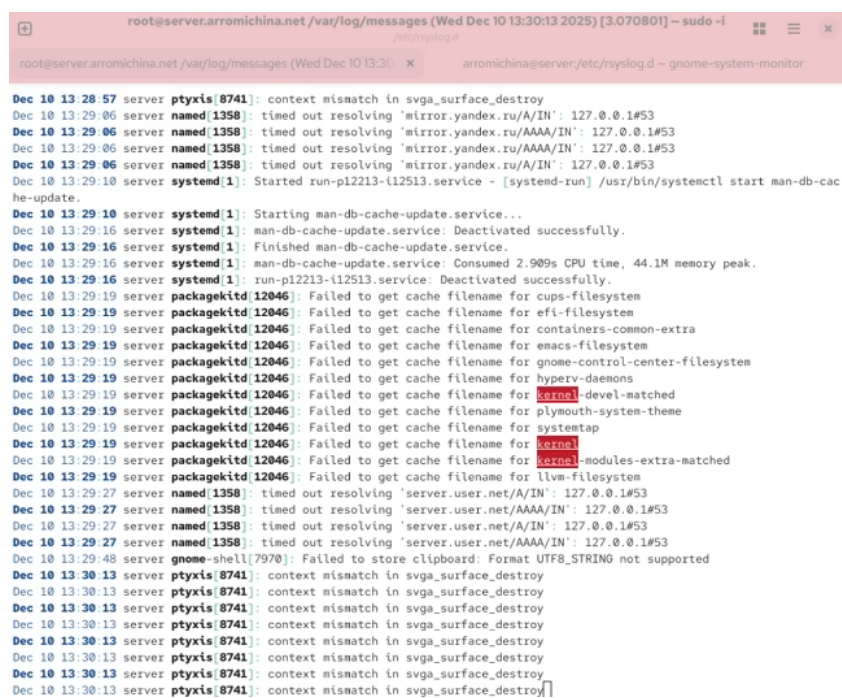
```
[root@server.arromichina.net rsyslog.d]# sudo dnf install -y multitail
Last metadata expiration check: 0:50:41 ago on Wed 10 Dec 2025 12:38:23 PM UTC.
Dependencies resolved.
=====
Package                        Architecture      Version           Repository
=====
Installing:
multitail                      x86_64            7.1.3-2.el10_0    epel

Transaction Summary
=====
Install 1 Package

Total download size: 148 k
Installed size: 326 k
Downloading Packages:
multitail-7.1.3-2.el10_0.x86_64.rpm                                108 kB/s | 148 kB
-----
Total                                                                73 kB/s | 148 kB
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :
  Installing     : multitail-7.1.3-2.el10_0.x86_64
  Running scriptlet: multitail-7.1.3-2.el10_0.x86_64
```

Рис. 2.10: Установка на сервере просмотрщика журналов системных сообщений.

Посмотрим логи(рис. 2.11).



```
root@server.arromichina.net /var/log/messages (Wed Dec 10 13:30:13 2025) [3.070801] -- sudo -i
root@server.arromichina.net /var/log/messages (Wed Dec 10 13:30:13 2025) [3.070801] -- sudo -i
arromichina@server/etc/rsyslog.d - gnome-system-monitor

Dec 10 13:28:57 server ptyxis[8741]: context mismatch in svga_surface_destroy
Dec 10 13:29:06 server named[1358]: timed out resolving 'mirror.yandex.ru/A/IN': 127.0.0.1#53
Dec 10 13:29:06 server named[1358]: timed out resolving 'mirror.yandex.ru/AAAA/IN': 127.0.0.1#53
Dec 10 13:29:06 server named[1358]: timed out resolving 'mirror.yandex.ru/AAAA/IN': 127.0.0.1#53
Dec 10 13:29:06 server named[1358]: timed out resolving 'mirror.yandex.ru/A/IN': 127.0.0.1#53
Dec 10 13:29:10 server systemd[1]: Started run-p12213-12513.service - [systemd-run] /usr/bin/systemctl start man-db-cache-update.
Dec 10 13:29:10 server systemd[1]: Starting man-db-cache-update.service...
Dec 10 13:29:16 server systemd[1]: man-db-cache-update.service: Deactivated successfully.
Dec 10 13:29:16 server systemd[1]: Finished man-db-cache-update.service.
Dec 10 13:29:16 server systemd[1]: man-db-cache-update.service: Consumed 2.909s CPU time, 44.1M memory peak.
Dec 10 13:29:16 server systemd[1]: run-p12213-12513.service: Deactivated successfully.
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for cups-filesystem
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for efi-filesystem
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for containers-common-extra
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for emacs-filesystem
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for gnome-control-center-filesystem
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for hyperv-daemons
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for kernel-devel-matched
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for plymouth-system-theme
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for systemd
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for kernel-modules-extra-matched
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for llvm-filesystem
Dec 10 13:29:27 server named[1358]: timed out resolving 'server.user.net/A/IN': 127.0.0.1#53
Dec 10 13:29:27 server named[1358]: timed out resolving 'server.user.net/AAAA/IN': 127.0.0.1#53
Dec 10 13:29:27 server named[1358]: timed out resolving 'server.user.net/A/IN': 127.0.0.1#53
Dec 10 13:29:27 server named[1358]: timed out resolving 'server.user.net/AAAA/IN': 127.0.0.1#53
Dec 10 13:29:48 server gnome-shell[7970]: Failed to store clipboard: Format UTF8_STRING not supported
Dec 10 13:30:13 server ptyxis[8741]: context mismatch in svga_surface_destroy
Dec 10 13:30:13 server ptyxis[8741]: context mismatch in svga_surface_destroy
Dec 10 13:30:13 server ptyxis[8741]: context mismatch in svga_surface_destroy
Dec 10 13:30:13 server ptyxis[8741]: context mismatch in svga_surface_destroy
Dec 10 13:30:13 server ptyxis[8741]: context mismatch in svga_surface_destroy
Dec 10 13:30:13 server ptyxis[8741]: context mismatch in svga_surface_destroy
Dec 10 13:30:13 server ptyxis[8741]: context mismatch in svga_surface_destroy
```

Рис. 2.11: Просмотр логов.

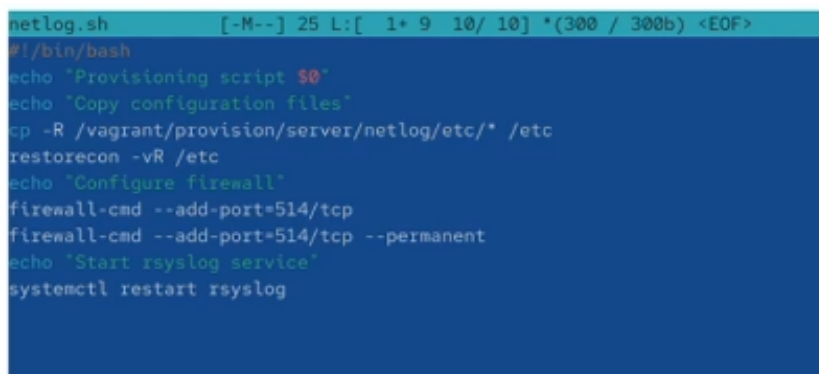
На виртуальной машине server перейдём в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создадим в нём

каталог netlog, в который поместим в соответствующие подкаталоги конфигурационные файлы. В каталоге /vagrant/provision/server создадим исполняемый файл netlog.sh(рис. 2.12).

```
[root@server.arrowichina.net rsyslog.d]# cd /vagrant/provision/server
[root@server.arrowichina.net server]# mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.arrowichina.net server]# cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.arrowichina.net server]# cd /vagrant/provision/server
[root@server.arrowichina.net server]# touch netlog.sh
[root@server.arrowichina.net server]# chmod +x netlog.sh
[root@server.arrowichina.net server]#
```

Рис. 2.12: 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. 2.13).



```
netlog.sh [-M--] 25 L:[ 1* 9 10/ 10] *(300 / 300b) <EOF>
#!/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. 2.13: 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. 2.14).

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

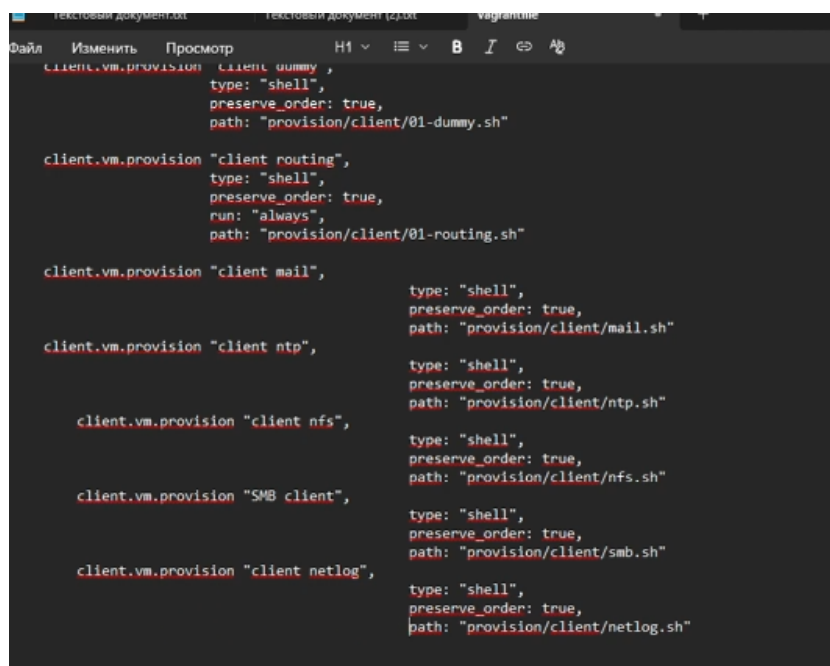
Рис. 2.14: Переход на виртуальной машине client в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создание в нём каталога netlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге /vagrant/provision/client исполняемого файла netlog.sh.

Открыв его на редактирование, пропишем в нём скрипт (рис. 2.15).

```
netlog.sh [-M--] 25 L: [ 1* 8 9/ 9] *(249 / 249b) <EOF>
#!/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. 2.15: 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 и клиента (рис. 2.16).



```
client.vm.provision "client dummy",
  type: "shell",
  preserve_order: true,
  path: "provision/client/01-dummy.sh"

client.vm.provision "client routing",
  type: "shell",
  preserve_order: true,
  run: "always",
  path: "provision/client/01-routing.sh"

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

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

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

client.vm.provision "SMB client",
  type: "shell",
  preserve_order: true,
  path: "provision/client/smb.sh"

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

Рис. 2.16: Добавление конфигураций в конфигурационном файле Vagrantfile для сервера и клиента.

## **3 Выводы**

В ходе выполнения лабораторной работы были получены 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 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`

## **Список литературы**