

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 15

«Настройка сетевого журналирования»

Дисциплина: Администрирование сетевых подсистем

Студент: Карташова А.С.

Группа: НФИбд-03-18

МОСКВА

2020 г.

Оглавление

Цель работы	2
Задачи.....	2
Ход работы	2
Настройка сервера сетевого журнала	2
Настройка клиента сетевого журнала.....	4
Просмотр журнала.....	4
Внесение изменений в настройки внутреннего окружения виртуальных машин	6
Заключение.....	8
Контрольные вопросы.....	8

Цель работы

Получение навыков по работе с журналами системных событий.

Задачи

1. Настроить сервер сетевого журналирования событий
2. Настроить клиент для передачи системных сообщений в сетевой журнал на сервере
3. Просмотреть журналы системных событий с помощью нескольких программ
4. Написать скрипты для Vagrant, фиксирующие действия по установке и настройке сетевого сервера журналирования

Ход работы

Настройка сервера сетевого журнала

На сервере создадим файл конфигурации сетевого хранения журналов:

В файле конфигурации `/etc/rsyslog.d/netlog-server.conf` включим приём записей журнала по TCP-порту 514:

```
root@server:/etc/rsyslog.d
File Edit View Search Terminal Tabs Help
root@server:/etc/dhcp x root@server:/etc/rsyslog.d x
GNU nano 2.9.8 netlog-server.conf Modified
$ModLoad imtcp
$InputTCPServerRun 514
```

Перезапустим службу rsyslog и посмотрим, какие порты, связанные с rsyslog, прослушиваются:

Команды: *systemctl restart rsyslog*

lsof | grep TCP

```
Activities Terminal Jan 8 11:18 en
root@server:/etc/rsyslog.d
File Edit View Search Terminal Tabs Help
root@server:/etc/dhcp x root@server:/etc/rsyslog.d x
named 7355 7358 isc-socket named 27u IPv6 77471 0t0 TCP localhost:rn
dc (LISTEN)
rsyslogd 8165 root 4u IPv4 85759 0t0 TCP *:shell (LIS
TEN)
rsyslogd 8165 root 5u IPv6 85760 0t0 TCP *:shell (LIS
TEN)
rsyslogd 8165 8167 in:imjour root 4u IPv4 85759 0t0 TCP *:shell (LIS
TEN)
rsyslogd 8165 8167 in:imjour root 5u IPv6 85760 0t0 TCP *:shell (LIS
TEN)
rsyslogd 8165 8168 in:imtcp root 4u IPv4 85759 0t0 TCP *:shell (LIS
TEN)
rsyslogd 8165 8168 in:imtcp root 5u IPv6 85760 0t0 TCP *:shell (LIS
TEN)
rsyslogd 8165 8169 in:imtcp root 4u IPv4 85759 0t0 TCP *:shell (LIS
TEN)
rsyslogd 8165 8169 in:imtcp root 5u IPv6 85760 0t0 TCP *:shell (LIS
TEN)
rsyslogd 8165 8170 in:imtcp root 4u IPv4 85759 0t0 TCP *:shell (LIS
TEN)
rsyslogd 8165 8170 in:imtcp root 5u IPv6 85760 0t0 TCP *:shell (LIS
TEN)
rsyslogd 8165 8171 in:imtcp root 4u IPv4 85759 0t0 TCP *:shell (LIS
TEN)
rsyslogd 8165 8171 in:imtcp root 5u IPv6 85760 0t0 TCP *:shell (LIS
TEN)
rsyslogd 8165 8172 in:imtcp root 4u IPv4 85759 0t0 TCP *:shell (LIS
TEN)
rsyslogd 8165 8172 in:imtcp root 5u IPv6 85760 0t0 TCP *:shell (LIS
TEN)
rsyslogd 8165 8173 rs:main root 4u IPv4 85759 0t0 TCP *:shell (LIS
TEN)
rsyslogd 8165 8173 rs:main root 5u IPv6 85760 0t0 TCP *:shell (LIS
TEN)
[root@server.askartashova.net rsyslog.d]#
```

На сервере настроим межсетевой экран для приёма сообщений по TCP-порту 514:

Команды: *firewall-cmd --add-port=514/tcp*

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

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

Настройка клиента сетевого журнала

На клиенте создадим файл конфигурации сетевого хранения журналов:

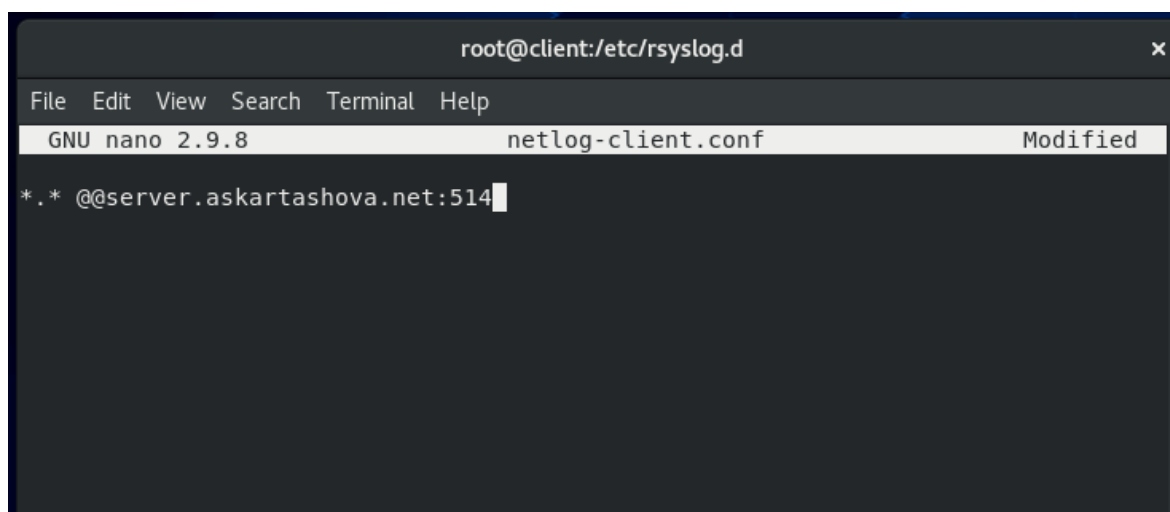
Команды: `cd /etc/rsyslog.d`

`touch netlog-client.conf`

```
[root@client.askartashova.net ~]# cd /etc/rsyslog.d
[root@client.askartashova.net rsyslog.d]# touch netlog-client.conf
[root@client.askartashova.net rsyslog.d]# nano netlog-client.conf
```

На клиенте в файле конфигурации `/etc/rsyslog.d/netlog-client.conf` включим перенаправление сообщения журнала на 514 TCP-порт

`*.* @@server.user.net:514`



Перезапустим службу rsyslog:

Команда: `systemctl restart rsyslog`

```
[root@client.askartashova.net rsyslog.d]# nano netlog-client.conf
[root@client.askartashova.net rsyslog.d]# systemctl restart rsyslog
[root@client.askartashova.net rsyslog.d]#
```

Просмотр журнала

На сервере откроем еще одно окно терминала и посмотрим один из файлов журнала

Команда: `tail -f /var/log/messages`

Обратим внимание, что имя хоста client.

```
[root@server.askartashova.net ~]# tail -f /var/log/messages
Jan 8 15:50:27 client NetworkManager[3371]: <info> [1610110226.6452] dhcp4 (eth1): option requested_routers
=> '1'
Jan 8 15:50:27 client NetworkManager[3371]: <info> [1610110226.6453] dhcp4 (eth1): option requested_static_r
tes => '1'
Jan 8 15:50:27 client NetworkManager[3371]: <info> [1610110226.6453] dhcp4 (eth1): option requested_subnet_m
k => '1'
Jan 8 15:50:27 client NetworkManager[3371]: <info> [1610110226.6453] dhcp4 (eth1): option requested_time_off
t => '1'
Jan 8 15:50:27 client NetworkManager[3371]: <info> [1610110226.6453] dhcp4 (eth1): option requested_wpad
=> '1'
Jan 8 15:50:27 client NetworkManager[3371]: <info> [1610110226.6453] dhcp4 (eth1): option routers
=> '192.168.1.1'
Jan 8 15:50:27 client NetworkManager[3371]: <info> [1610110226.6453] dhcp4 (eth1): option subnet_mask
=> '255.255.255.0'
Jan 8 15:50:27 client NetworkManager[3371]: <info> [1610110226.6455] dhcp4 (eth1): state changed extended ->
extended
Jan 8 15:50:27 client systemd[1]: Starting Network Manager Script Dispatcher Service...
Jan 8 15:50:27 client systemd[1]: Started Network Manager Script Dispatcher Service.
```

На сервере запустим графическую программу для просмотра журналов:

Команда: `gnome-system-log` (не получилось установить)

На сервере установим просмотрщик журналов системных сообщений `lnav`:

Команда: `dnf -y install lnav`

Посмотрим логи с помощью `lnav`:

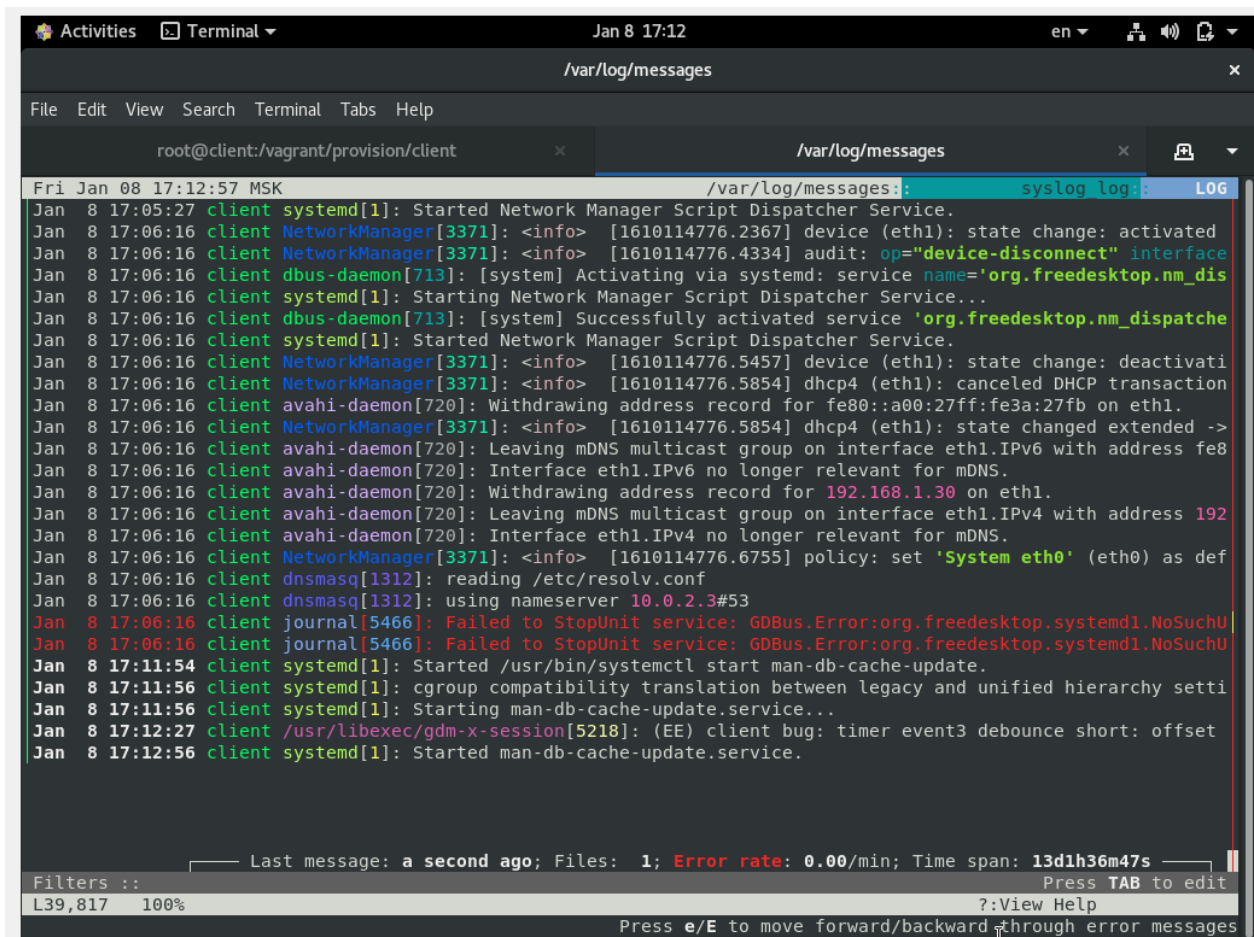
Команда: `lnav`

Посмотрим записи с сервера и клиента.

```

Fri Jan 08 13:50:25 UTC                               /var/log/messages: syslog log: LOG
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7820] dhcp4 (eth1): option domain_name
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7821] dhcp4 (eth1): option domain_name_server
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7821] dhcp4 (eth1): option expiry
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7821] dhcp4 (eth1): option ip_address
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7822] dhcp4 (eth1): option requested_broadcast
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7822] dhcp4 (eth1): option requested_domain_n
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7822] dhcp4 (eth1): option requested_domain_n_s
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7822] dhcp4 (eth1): option requested_host_nam
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7823] dhcp4 (eth1): option requested_host_nam
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7823] dhcp4 (eth1): option requested_interface
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7823] dhcp4 (eth1): option requested_ip_class
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7823] dhcp4 (eth1): option requested_nis_doma
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7823] dhcp4 (eth1): option requested_nis_serv
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7824] dhcp4 (eth1): option requested_ntp_serv
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7824] dhcp4 (eth1): option requested_ntp_serv
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7824] dhcp4 (eth1): option requested_rfc3442
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7824] dhcp4 (eth1): option requested_root_pat
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7824] dhcp4 (eth1): option requested_routers
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7825] dhcp4 (eth1): option requested_static_r
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7825] dhcp4 (eth1): option requested_subnet_m
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7825] dhcp4 (eth1): option requested_time_off
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7825] dhcp4 (eth1): option requested_wpad
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7825] dhcp4 (eth1): option routers
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7826] dhcp4 (eth1): option subnet_mask
Jan 8 16:45:26 client NetworkManager[3371]: <info> [1610113526.7826] dhcp4 (eth1): state changed extended ->
Jan 8 16:45:26 client systemd[1]: Starting Network Manager Script Dispatcher Service...
Jan 8 16:45:26 client systemd[1]: Started Network Manager Script Dispatcher Service.
Jan 8 13:48:04 server dbus-daemon[707]: [system] Activating via systemd: service name='net.reactivated.Fprint
Jan 8 13:48:04 server systemd[1]: Starting Fingerprint Authentication Daemon...
Jan 8 13:48:04 server dbus-daemon[707]: [system] Successfully activated service 'net.reactivated.Fprint'
Jan 8 13:48:04 server systemd[1]: Started Fingerprint Authentication Daemon.
Filters :: Press TAB to edit
L1,432 99% ?::View Help
Press e/E to move forward/backward through error messages

```



```
Activities Terminal Jan 8 17:12 en /var/log/messages
File Edit View Search Terminal Tabs Help
root@client:/vagrant/provision/client /var/log/messages
Fri Jan 08 17:12:57 MSK /var/log/messages: syslog log: LOG
Jan 8 17:05:27 client systemd[1]: Started Network Manager Script Dispatcher Service.
Jan 8 17:06:16 client NetworkManager[3371]: <info> [1610114776.2367] device (eth1): state change: activated
Jan 8 17:06:16 client NetworkManager[3371]: <info> [1610114776.4334] audit: op="device-disconnect" interface
Jan 8 17:06:16 client dbus-daemon[713]: [system] Activating via systemd: service name='org.freedesktop.nm_dis
Jan 8 17:06:16 client systemd[1]: Starting Network Manager Script Dispatcher Service...
Jan 8 17:06:16 client dbus-daemon[713]: [system] Successfully activated service 'org.freedesktop.nm_dispatche
Jan 8 17:06:16 client systemd[1]: Started Network Manager Script Dispatcher Service.
Jan 8 17:06:16 client NetworkManager[3371]: <info> [1610114776.5457] device (eth1): state change: deactivati
Jan 8 17:06:16 client NetworkManager[3371]: <info> [1610114776.5854] dhcp4 (eth1): canceled DHCP transaction
Jan 8 17:06:16 client avahi-daemon[720]: Withdrawing address record for fe80::a00:27ff:fe3a:27fb on eth1.
Jan 8 17:06:16 client NetworkManager[3371]: <info> [1610114776.5854] dhcp4 (eth1): state changed extended ->
Jan 8 17:06:16 client avahi-daemon[720]: Leaving mDNS multicast group on interface eth1.IPv6 with address fe8
Jan 8 17:06:16 client avahi-daemon[720]: Interface eth1.IPv6 no longer relevant for mDNS.
Jan 8 17:06:16 client avahi-daemon[720]: Withdrawing address record for 192.168.1.30 on eth1.
Jan 8 17:06:16 client avahi-daemon[720]: Leaving mDNS multicast group on interface eth1.IPv4 with address 192
Jan 8 17:06:16 client avahi-daemon[720]: Interface eth1.IPv4 no longer relevant for mDNS.
Jan 8 17:06:16 client NetworkManager[3371]: <info> [1610114776.6755] policy: set 'System eth0' (eth0) as def
Jan 8 17:06:16 client dnsmasq[1312]: reading /etc/resolv.conf
Jan 8 17:06:16 client dnsmasq[1312]: using nameserver 10.0.2.3#53
Jan 8 17:06:16 client journal[5466]: Failed to StopUnit service: GDBus.Error:org.freedesktop.systemd1.NoSuchU
Jan 8 17:06:16 client journal[5466]: Failed to StopUnit service: GDBus.Error:org.freedesktop.systemd1.NoSuchU
Jan 8 17:11:54 client systemd[1]: Started /usr/bin/systemctl start man-db-cache-update.
Jan 8 17:11:56 client systemd[1]: cgroup compatibility translation between legacy and unified hierarchy setti
Jan 8 17:11:56 client systemd[1]: Starting man-db-cache-update.service...
Jan 8 17:12:27 client /usr/libexec/gdm-x-session[5218]: (EE) client bug: timer event3 debounce short: offset
Jan 8 17:12:56 client systemd[1]: Started man-db-cache-update.service.
Last message: a second ago; Files: 1; Error rate: 0.00/min; Time span: 13d1h36m47s
Filters :: Press TAB to edit
L39,817 100% ? :View Help
Press e/E to move forward/backward through error messages
```

Внесение изменений в настройки внутреннего окружения виртуальных машин

На виртуальной машине server перейдем в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создадим в нём каталог `netlog`, в который поместите в соответствующие подкаталоги конфигурационные файлы:

```
^C[C[root@server.askartashova.net rsyslog.d]# cd /vagrant/provision/server
[root@server.askartashova.net server]# mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.askartashova.net server]# cp -R /etc/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog
g.d
cp: cannot stat '/etc/netlog-server.conf': No such file or directory
[root@server.askartashova.net server]# cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/
etc/rsyslog.d
```

В каталоге `/vagrant/provision/server` создадим исполняемый файл `netlog.sh`, открыв его на редактирование, пропишем в нём следующий скрипт

```
[root@server.askartashova.net server]# cd /vagrant/provision/server
[root@server.askartashova.net server]# touch netlog.sh
[root@server.askartashova.net server]# chmod +x netlog.sh
```

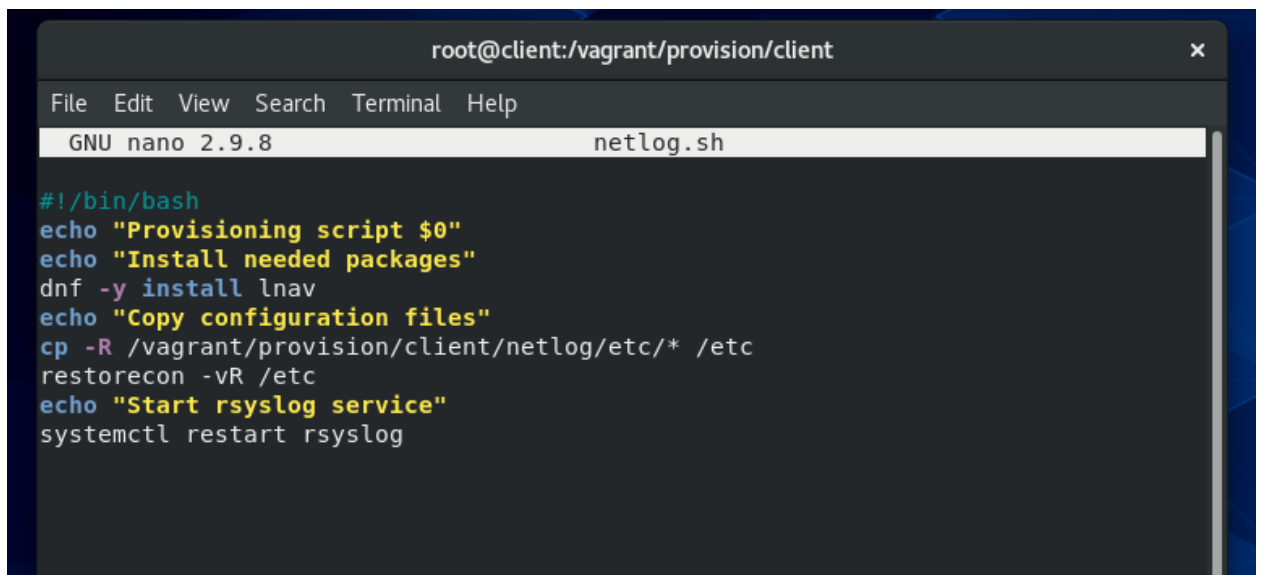
```
root@server:/vagrant/provision/server
File Edit View Search Terminal Tabs Help
root@server:/etc/dhcp x root@server:/vagrant/provision/ser... x /var/log/message
GNU nano 2.9.8 netlog.sh
#!/bin/bash
echo "Provisioning script $0"
echo "Copy configuration files"
cp -R /vagrant/provision/server/netlog/etc/* /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
```

На виртуальной машине client перейдем в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создадим в нём каталог netlog, в который поместим в соответствующие подкаталоги конфигурационные файлы

```
rtt min/avg/max/mdev = 0.619/0.678/0.719/0.052 ms
[root@client.askartashova.net rsyslog.d]# cd /vagrant/provision/client
[root@client.askartashova.net client]# mkdir -p /vagrant/provision/client/netlog
/etc/rsyslog.d
[root@client.askartashova.net client]# cp -R /etc/rsyslog.d/netlog-client.conf /
vagrant/provision/client/netlog/etc/rsyslog.d/
[root@client.askartashova.net client]# S
```

В каталоге /vagrant/provision/client создадим исполняемый файл netlog.sh:

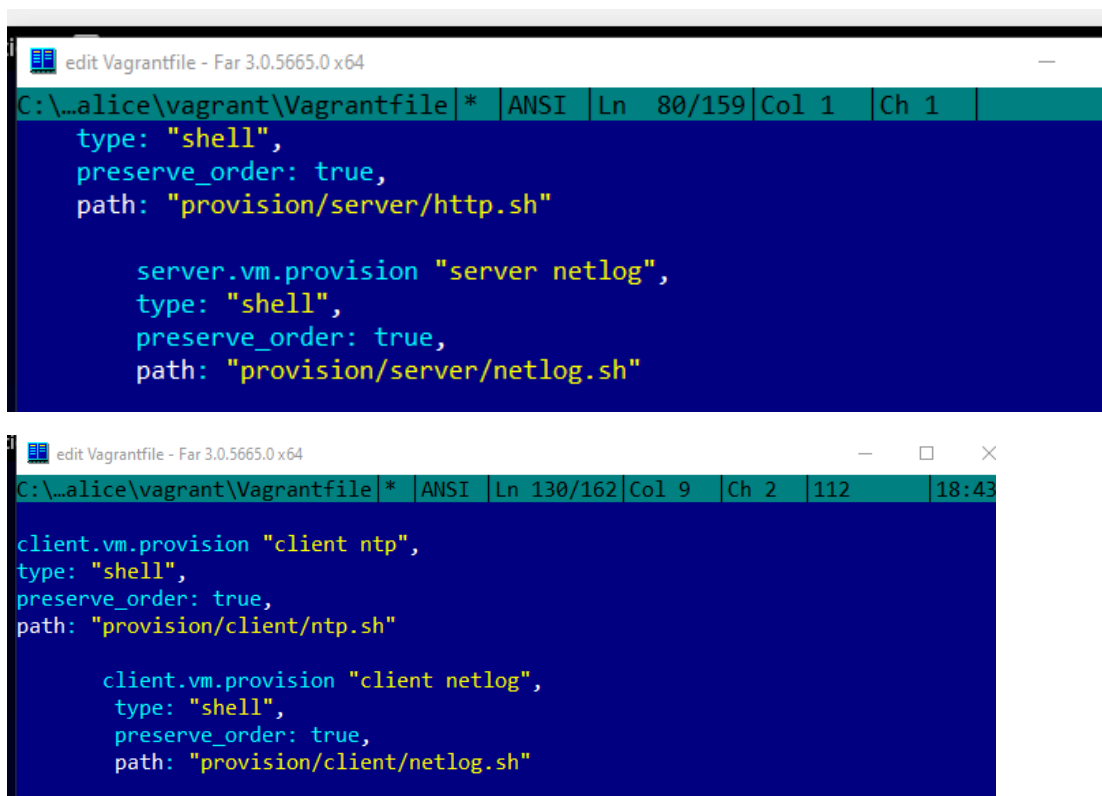
```
[root@client.askartashova.net client]# cd /vagrant/provision/client
[root@client.askartashova.net client]# touch netlog.sh
[root@client.askartashova.net client]# chmod +x netlog.sh
[root@client.askartashova.net client]#
```



```
root@client:/vagrant/provision/client
File Edit View Search Terminal Help
GNU nano 2.9.8 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
```

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



```
edit Vagrantfile - Far 3.0.5665.0 x64
C:\...alice\vagrant\Vagrantfile |*| ANSI | Ln 80/159 | Col 1 | Ch 1 |
type: "shell",
preserve_order: true,
path: "provision/server/http.sh"

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

edit Vagrantfile - Far 3.0.5665.0 x64
C:\...alice\vagrant\Vagrantfile |*| ANSI | Ln 130/162 | Col 9 | Ch 2 | 112 | 18:43
client.vm.provision "client ntp",
type: "shell",
preserve_order: true,
path: "provision/client/ntp.sh"

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

Заключение

Мы приобрели навыки нпо работе с журналами системных событий

Контрольные вопросы

1. Какой модуль rsyslog вы должны использовать для приёма

сообщений от journald?

Модуль imjournal был специально разработан для интеграции rsyslogd и journald.

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

Модуль imuxsock

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

В rsyslog.conf для правильной обработки приема журнала необходимы две строки: В rsyslog.conf для правильной обработки приема журнала необходимы две строки:

\$OmitLocalLogging on

\$IMJournalStateFile imjournal.state

Первая отключает прием логов через модуль imuxsocks. Вторая строка определяет имя файла состояния, который rsyslogd использует для отслеживания состояния синхронизации между rsyslogd и journald.

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

Файл /etc/rsyslog.conf.

5. Каким параметром управляется пересылка сообщений из journald в rsyslog?
6. Какой модуль rsyslog вы можете использовать для включения сообщений из файла журнала, не созданного rsyslog?

Модуль: *imjournal*.

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

Модуль: *ommysql*

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

\$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 --permanen