

**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ ИМЕНИ  
ПАТРИСА ЛУМУМБЫ**

**Факультет физико-математических и естественных наук**

**Кафедра теории вероятностей и кибербезопасности**

**ОТЧЕТ  
ПО ЛАБОРАТОРНОЙ РАБОТЕ № 15**

*Дисциплина «Администрирование сетевых подсистем»*

*Тема «Настройка сетевого журналирования»*

Студент: Щербак Маргарита Романовна

Ст. билет: 1032216537

Группа: НПИбд-02-21

**МОСКВА**

2023 г.

## Цель работы

Получение навыков по работе с журналами системных событий.

## Задание

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. При наличии сообщений о некорректной работе сервисов исправить ошибки в настройках соответствующих служб.
4. Написать скрипты для Vagrant, фиксирующие действия по установке и настройке сетевого сервера журналирования.

## Выполнение

### 1. Настройка сервера сетевого журнала

1. На сервере создала файл конфигурации сетевого хранения журналов и в нем включила приём записей журнала по TCP-порту 514, после чего перезапустила службу rsyslog и посмотрела, какие порты, связанные с rsyslog, прослушиваются. Действия представлены на рис.1.1 – рис.1.3. Служба rsyslog порт shell 514.

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

[root@server.mrshcherbak.net rsyslog.d]# systemctl restart rsyslog
[root@server.mrshcherbak.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.
systemd      1             root    34u    IPv4        18260      0t0      TCP *:sunrpc (LISTEN)
systemd      1             root    36u    IPv6        18276      0t0      TCP *:sunrpc (LISTEN)
systemd      1             root    58u    IPv6       21243      0t0      TCP *:websm (LISTEN)
rpcbind     579           rpc      4u    IPv4        18260      0t0      TCP *:sunrpc (LISTEN)
rpcbind     579           rpc      6u    IPv6        18276      0t0      TCP *:sunrpc (LISTEN)
cupsd       963           root     6u    IPv6       22907      0t0      TCP localhost:ipp (LISTEN)
cupsd       963           root     7u    IPv4       22908      0t0      TCP localhost:ipp (LISTEN)
sshd        979           root     3u    IPv4       22976      0t0      TCP *:down (LISTEN)
sshd        979           root     4u    IPv6       22996      0t0      TCP *:down (LISTEN)
sshd        979           root     5u    IPv4       22998      0t0      TCP *:ssh (LISTEN)
sshd        979           root     6u    IPv6       23000      0t0      TCP *:ssh (LISTEN)
named       1002          named    17u    IPv4       23087      0t0      TCP localhost:domain (LISTEN)
named       1002          named    21u    IPv6       23089      0t0      TCP localhost:domain (LISTEN)
named       1002          named    22u    IPv4       23163      0t0      TCP localhost:rndc (LISTEN)
named       1002          named    23u    IPv6       23164      0t0      TCP localhost:rndc (LISTEN)
named       1002          named    24u    IPv4       24455      0t0      TCP server.mrshcherbak.net:domain (LISTEN)
named       1002          named    26u    IPv4       33404      0t0      TCP www.mrshcherbak.net:domain (LISTEN)
named       1002 1003 isc-net-0  named    17u    IPv4       23087      0t0      TCP localhost:domain (LISTEN)
named       1002 1003 isc-net-0  named    21u    IPv6       23089      0t0      TCP localhost:domain (LISTEN)
named       1002 1003 isc-net-0  named    22u    IPv4       23163      0t0      TCP localhost:rndc (LISTEN)
named       1002 1003 isc-net-0  named    23u    IPv6       23164      0t0      TCP localhost:rndc (LISTEN)
```

Рис.1.1. Выполнение команд

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

httpd 1617 1814 httpd apache 4u IPv6 25377 0t0 TCP *:http (LISTEN)
httpd 1617 1814 httpd apache 5u sock 0,8 0t0 25388 protocol: TCP
httpd 1617 1814 httpd apache 6u IPv6 25389 0t0 TCP *:https (LISTEN)
httpd 1617 1814 httpd apache 23u sock 0,8 0t0 27008 protocol: TCP
httpd 1617 1815 httpd apache 3u sock 0,8 0t0 25376 protocol: TCP
httpd 1617 1815 httpd apache 4u IPv6 25377 0t0 TCP *:http (LISTEN)
httpd 1617 1815 httpd apache 5u sock 0,8 0t0 25388 protocol: TCP
httpd 1617 1815 httpd apache 6u IPv6 25389 0t0 TCP *:https (LISTEN)
httpd 1617 1815 httpd apache 23u sock 0,8 0t0 27008 protocol: TCP
rsyslogd 7366 root 4u IPv4 45747 0t0 TCP *:shell (LISTEN)
rsyslogd 7366 root 5u IPv6 45748 0t0 TCP *:shell (LISTEN)
rsyslogd 7366 7368 in:imjour root 4u IPv4 45747 0t0 TCP *:shell (LISTEN)
rsyslogd 7366 7368 in:imjour root 5u IPv6 45748 0t0 TCP *:shell (LISTEN)
rsyslogd 7366 7369 in:imtcp root 4u IPv4 45747 0t0 TCP *:shell (LISTEN)
rsyslogd 7366 7369 in:imtcp root 5u IPv6 45748 0t0 TCP *:shell (LISTEN)
rsyslogd 7366 7370 in:imtcp root 4u IPv4 45747 0t0 TCP *:shell (LISTEN)
rsyslogd 7366 7370 in:imtcp root 5u IPv6 45748 0t0 TCP *:shell (LISTEN)
rsyslogd 7366 7371 in:imtcp root 4u IPv4 45747 0t0 TCP *:shell (LISTEN)
rsyslogd 7366 7371 in:imtcp root 5u IPv6 45748 0t0 TCP *:shell (LISTEN)
rsyslogd 7366 7372 in:imtcp root 4u IPv4 45747 0t0 TCP *:shell (LISTEN)
rsyslogd 7366 7372 in:imtcp root 5u IPv6 45748 0t0 TCP *:shell (LISTEN)
rsyslogd 7366 7373 in:imtcp root 4u IPv4 45747 0t0 TCP *:shell (LISTEN)
rsyslogd 7366 7373 in:imtcp root 5u IPv6 45748 0t0 TCP *:shell (LISTEN)
rsyslogd 7366 7374 rs:main root 4u IPv4 45747 0t0 TCP *:shell (LISTEN)
rsyslogd 7366 7374 rs:main root 5u IPv6 45748 0t0 TCP *:shell (LISTEN)
[root@server.mrshcherbak.net rsyslog.d]# cat /etc/services | grep shell
shell 514/tcp cmd # no passwords used
kshell 544/tcp krcmd # Kerberized 'rsh' (v5)
kshell 544/udp # krcmd
chshell 562/tcp # chcmd
chshell 562/udp # chcmd
sshell 614/tcp # SSLshell
sshell 614/udp # SSLshell
carrius-rshell 1197/tcp # Carrius Remote Access
carrius-rshell 1197/udp # Carrius Remote Access
nim-vdrshell 6420/tcp # NIM_VDRShell
nim-vdrshell 6420/udp # NIM_VDRShell
tnos-dp 7902/tcp # TNOS shell Protocol
tnos-dp 7902/udp # TNOS shell Protocol
dai-shell 45824/tcp # Server for the DAI family of client-server products
[root@server.mrshcherbak.net rsyslog.d]#
```

Рис.1.2. Просмотр портов, связанных с rsyslog

```
mc [root@server.mrshcherbak.net]:/etc/rsyslog.d
netlog-s~er.conf [----] 22 L:[ 1+ 1 2/ 2] *(37 / 37b) <E[*][X]
$ModLoad imtcp
$InputTCPServerRun 514
```

Рис.1.3. Содержимое файла /etc/rsyslog.d/netlog-server.conf

2. На сервере настроила межсетевой экран для приёма сообщений по TCP-порту 514 (рис.1.4).

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

Рис.1.4. Настройка межсетевого экрана для приёма сообщений по TCP-порту 514

## 2. Настройка клиента сетевого журнала

1. На клиенте создала файл конфигурации сетевого хранения журналов и в нем включила перенаправление сообщений журнала на 514 TCP-порт сервера. После чего перезапустила службу rsyslog. Действия представлены на рис.2.1 – рис.2.2.

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

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

Рис.2.1. Выполнение команд

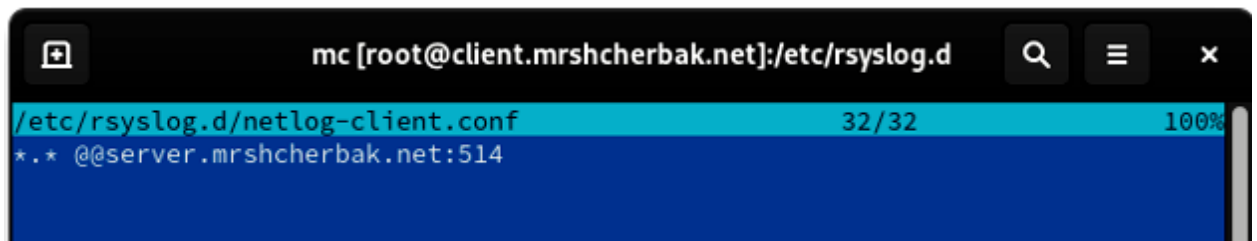


Рис.2.2. Содержимое файла /etc/rsyslog.d/netlog-client.conf

## 3. Просмотр журнала

1. На сервере просмотрела один из файлов журнала (рис.3.1).

```
[root@server.mrshcherbak.net rsyslog.d]# tail -f /var/log/messages
Dec 20 19:55:56 server dhcpd[1443]: DHCPREQUEST for 192.168.1.142 from 08:00:27:df:b4:e0 (client) via eth1
Dec 20 19:55:56 server dhcpd[1443]: DHCPACK on 192.168.1.142 to 08:00:27:df:b4:e0 (client) via eth1
Dec 20 16:56:37 client systemd[1]: Stopping System Logging Service...
Dec 20 16:56:37 client rsyslogd[569]: [origin software="rsyslogd" swVersion="8.2102.0-113.el9_2.1" x-pid="569" x-info="https://www.rsyslog.com"] exiting on signal 15.
Dec 20 16:56:37 client systemd[1]: rsyslog.service: Deactivated successfully.
Dec 20 16:56:37 client systemd[1]: Stopped System Logging Service.
Dec 20 16:56:37 client systemd[1]: Starting System Logging Service...
Dec 20 16:56:37 client systemd[1]: Started System Logging Service.
Dec 20 16:56:37 client rsyslogd[6585]: [origin software="rsyslogd" swVersion="8.2102.0-113.el9_2.1" x-pid="6585" x-info="https://www.rsyslog.com"] start
Dec 20 16:56:37 client rsyslogd[6585]: imjournal: journal files changed, reloading... [v8.2102.0-113.el9_2.1 try https://www.rsyslog.com/e/0 ]
```

Рис.3.1. Просмотр одного из файлов журнала

2. На сервере под пользователем mrshcherbak запустила графическую программу для просмотра журналов (рис.3.2).

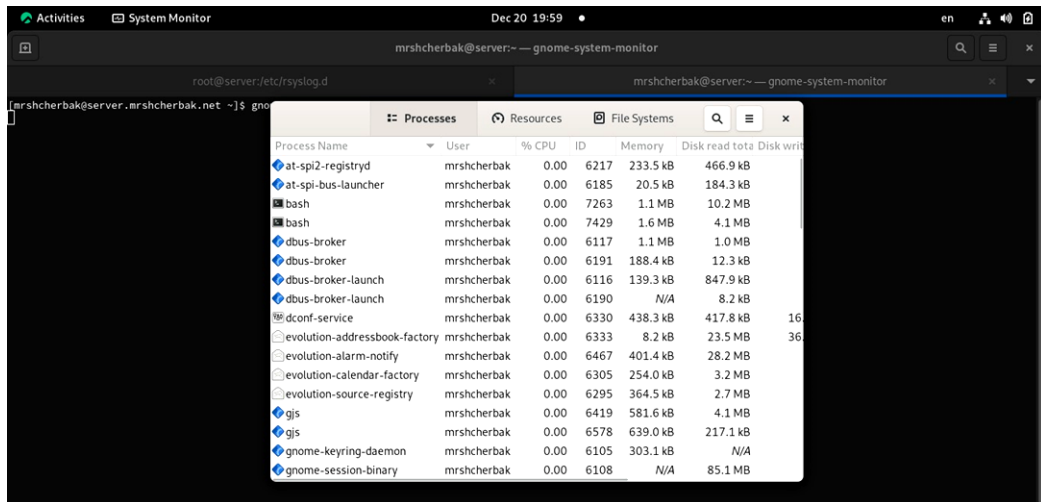


Рис.3.2. Запуск графической программы для просмотра журналов

3. На сервере установила просмотрщик журналов системных сообщений lnav (рис.3.3).

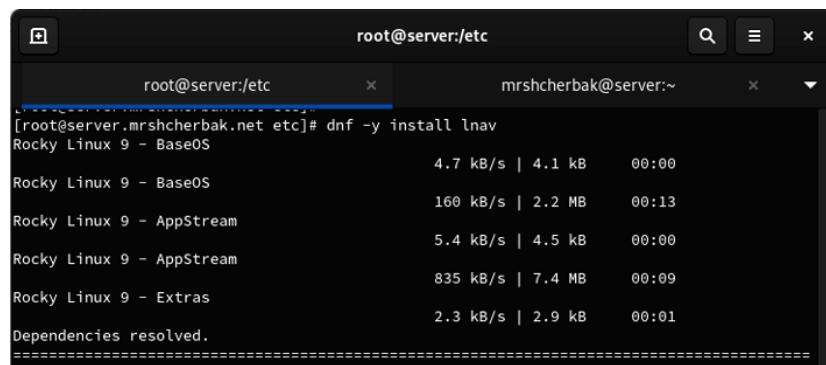


Рис.3.3. Установка просмотрщика журналов системных сообщений

4. Просмотрела логи с помощью lnav (рис.3.4 – рис.3.6).

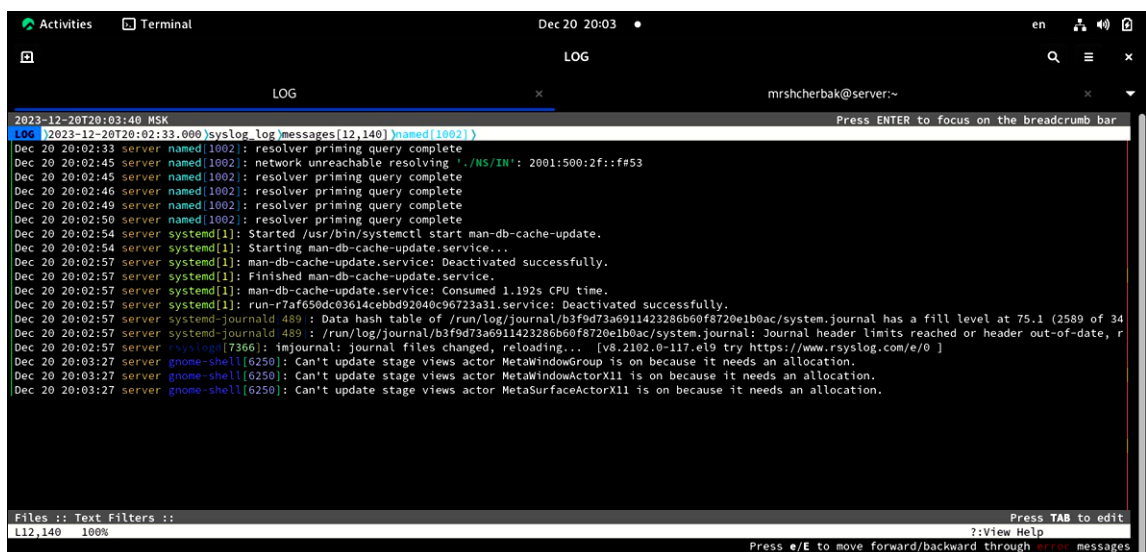
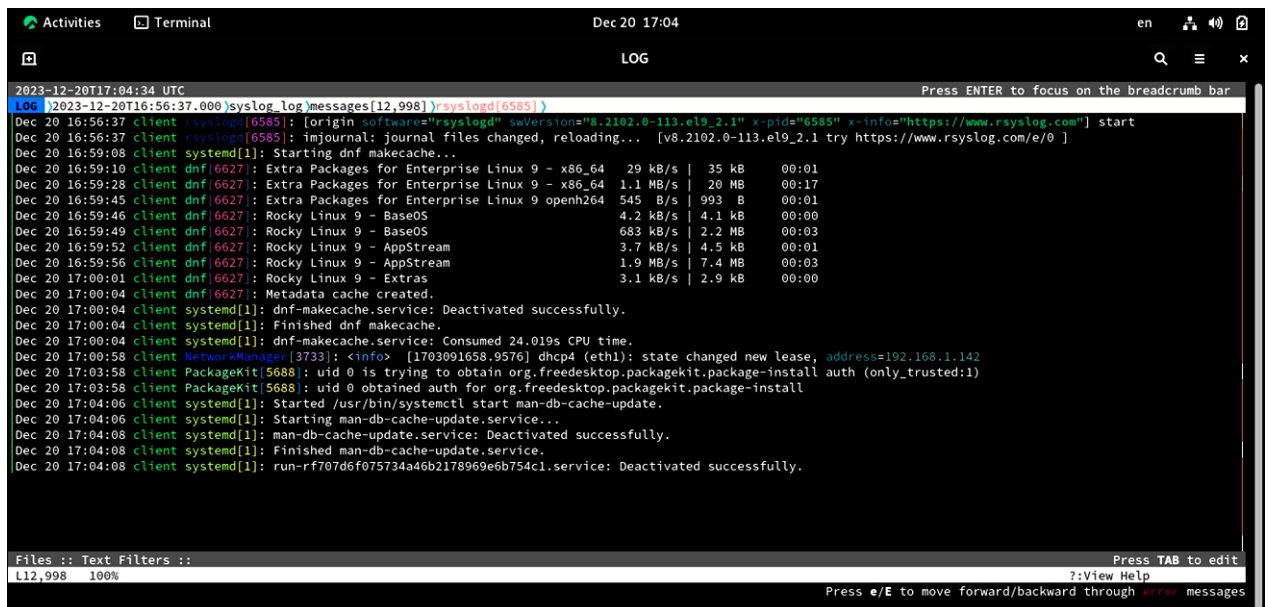
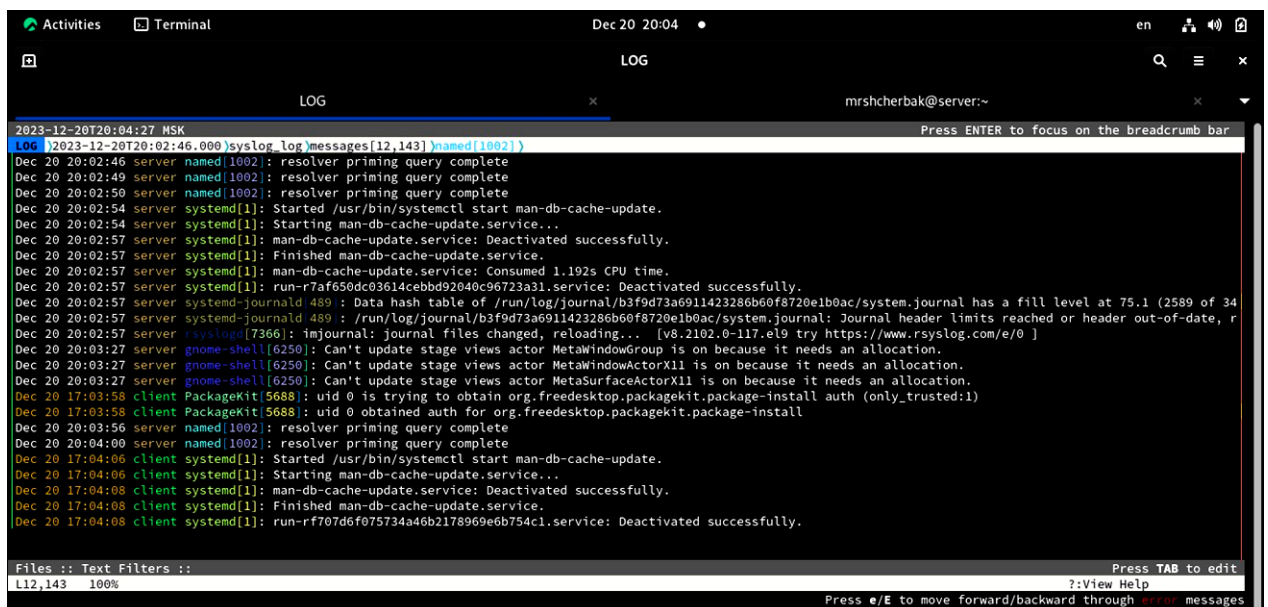


Рис.3.4. Просмотр логов



```
2023-12-20T17:04:34 UTC
LOG 2023-12-20T16:56:37.000 syslog_log/messages[12,998] rsyslogd[6585]
Dec 20 16:56:37 client rsyslogd[6585]: [origin software="rsyslogd" swVersion="8.2102.0-113.el9_2.1" x-pid="6585" x-info="https://www.rsyslog.com/"] start
Dec 20 16:59:08 client systemd[1]: Starting dnf makecache...
Dec 20 16:59:10 client dnf[6627]: Extra Packages for Enterprise Linux 9 - x86_64 29 kB/s | 35 kB 00:01
Dec 20 16:59:28 client dnf[6627]: Extra Packages for Enterprise Linux 9 - x86_64 1.1 MB/s | 20 MB 00:17
Dec 20 16:59:45 client dnf[6627]: Extra Packages for Enterprise Linux 9 openh264 545 B/s | 993 B 00:01
Dec 20 16:59:46 client dnf[6627]: Rocky Linux 9 - BaseOS 4.2 kB/s | 4.1 kB 00:00
Dec 20 16:59:49 client dnf[6627]: Rocky Linux 9 - BaseOS 683 kB/s | 2.2 MB 00:03
Dec 20 16:59:52 client dnf[6627]: Rocky Linux 9 - AppStream 3.7 kB/s | 4.5 kB 00:01
Dec 20 16:59:56 client dnf[6627]: Rocky Linux 9 - AppStream 1.9 MB/s | 7.4 MB 00:03
Dec 20 17:00:01 client dnf[6627]: Rocky Linux 9 - Extras 3.1 kB/s | 2.9 kB 00:00
Dec 20 17:00:04 client dnf[6627]: Metadata cache created.
Dec 20 17:00:04 client systemd[1]: dnf-makecache.service: Deactivated successfully.
Dec 20 17:00:04 client systemd[1]: Finished dnf makecache.
Dec 20 17:00:04 client systemd[1]: dnf-makecache.service: Consumed 24.019s CPU time.
Dec 20 17:00:58 client NetworkManager[3733]: <info> [1703091658.9576] dhcp4 (eth1): state changed new lease, address=192.168.1.142
Dec 20 17:03:58 client PackageKit[5688]: uid 0 is trying to obtain org.freedesktop.packagekit.package-install auth (only_trusted:1)
Dec 20 17:03:58 client PackageKit[5688]: uid 0 obtained auth for org.freedesktop.packagekit.package-install
Dec 20 17:04:06 client systemd[1]: Started /usr/bin/systemctl start man-db-cache-update.
Dec 20 17:04:06 client systemd[1]: Starting man-db-cache-update.service...
Dec 20 17:04:08 client systemd[1]: man-db-cache-update.service: Deactivated successfully.
Dec 20 17:04:08 client systemd[1]: Finished man-db-cache-update.service.
Dec 20 17:04:08 client systemd[1]: run-rf707d6f075734a46b2178969e6b754c1.service: Deactivated successfully.
```

Рис.3.5. Просмотр логов



```
2023-12-20T20:04:27 MSK
LOG 2023-12-20T20:02:46.000 syslog_log/messages[12,143] named[1002]
Dec 20 20:02:46 server named[1002]: resolver priming query complete
Dec 20 20:02:49 server named[1002]: resolver priming query complete
Dec 20 20:02:50 server named[1002]: resolver priming query complete
Dec 20 20:02:54 server systemd[1]: Started /usr/bin/systemctl start man-db-cache-update.
Dec 20 20:02:54 server systemd[1]: Starting man-db-cache-update.service...
Dec 20 20:02:57 server systemd[1]: man-db-cache-update.service: Deactivated successfully.
Dec 20 20:02:57 server systemd[1]: Finished man-db-cache-update.service.
Dec 20 20:02:57 server systemd[1]: man-db-cache-update.service: Consumed 1.192s CPU time.
Dec 20 20:02:57 server systemd-journal[489]: Data hash table of /run/log/journal/b3f9d73a6911423286b60f8720e1b0ac/system.journal has a fill level at 75.1 (2589 of 34
Dec 20 20:02:57 server rsyslogd[7366]: imjournal: journal files changed, reloading... [v8.2102.0-117.el9 try https://www.rsyslog.com/e/0 ]
Dec 20 20:03:27 server gnome-shell[6250]: Can't update stage views actor MetaWindowGroup is on because it needs an allocation.
Dec 20 20:03:27 server gnome-shell[6250]: Can't update stage views actor MetaSurfaceActorX11 is on because it needs an allocation.
Dec 20 17:03:58 client PackageKit[5688]: uid 0 is trying to obtain org.freedesktop.packagekit.package-install auth (only_trusted:1)
Dec 20 17:03:58 client PackageKit[5688]: uid 0 obtained auth for org.freedesktop.packagekit.package-install
Dec 20 20:03:56 server named[1002]: resolver priming query complete
Dec 20 20:04:00 server named[1002]: resolver priming query complete
Dec 20 17:04:06 client systemd[1]: Started /usr/bin/systemctl start man-db-cache-update.
Dec 20 17:04:06 client systemd[1]: Starting man-db-cache-update.service...
Dec 20 17:04:08 client systemd[1]: man-db-cache-update.service: Deactivated successfully.
Dec 20 17:04:08 client systemd[1]: Finished man-db-cache-update.service.
Dec 20 17:04:08 client systemd[1]: run-rf707d6f075734a46b2178969e6b754c1.service: Deactivated successfully.
```

Рис.3.6. Просмотр логов

## 4. Внесение изменений в настройки внутреннего окружения виртуальных машин

1. На виртуальной машине server перешла в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создала в нём каталог netlog, в который поместила в соответствующие подкаталоги конфигурационные файлы и в каталоге /vagrant/provision/server создала исполняемый файл netlog.sh, в котором прописала скрипт (рис.4.2). Действия представлены на рис.4.1.

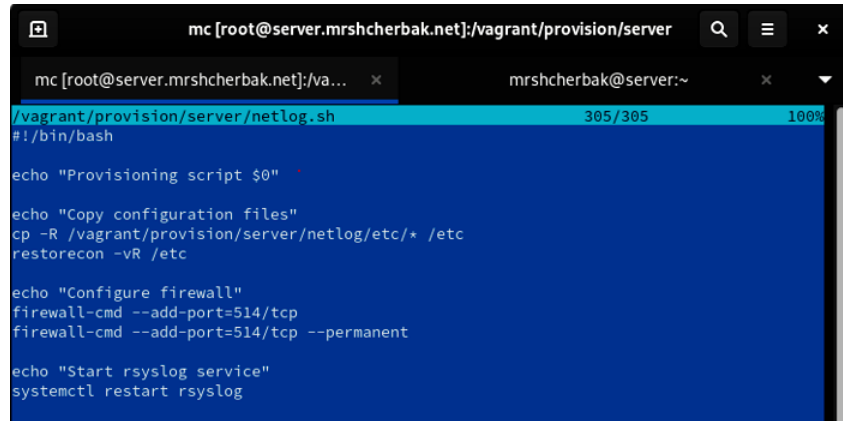


```

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

```

Рис.4.1. Выполнение команд



```

mc [root@server.mrshcherbak.net]:/vagrant/provision/server
/vagrant/provision/server/netlog.sh 305/305 100%
#!/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. Содержимое файла netlog.sh на сервере

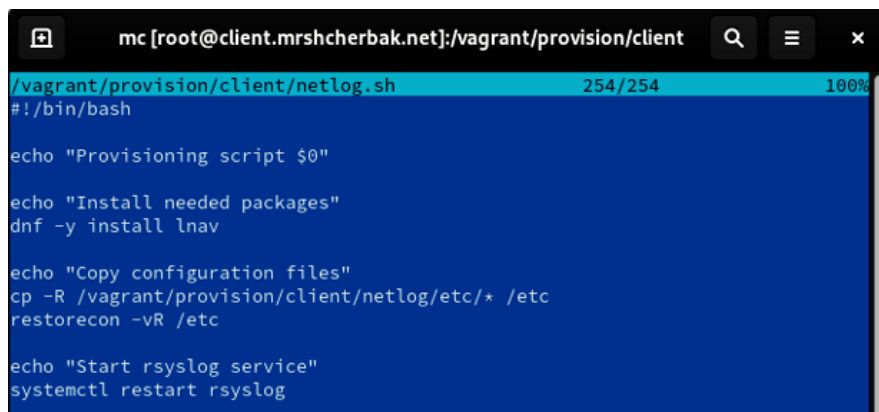
2. На виртуальной машине client перешла в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создала в нём каталог netlog, в который поместила в соответствующие подкаталоги конфигурационные файлы и в каталоге /vagrant/provision/client создала исполняемый файл netlog.sh, в котором прописала скрипт (рис.4.4). Действия представлены на рис.4.3.

```

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

```

Рис.4.3. Выполнение команд



```

mc [root@client.mrshcherbak.net]:/vagrant/provision/client
/vagrant/provision/client/netlog.sh 254/254 100%
#!/bin/bash

echo "Provisioning script $0"

echo "Install needed packages"
dnf -y install lnav

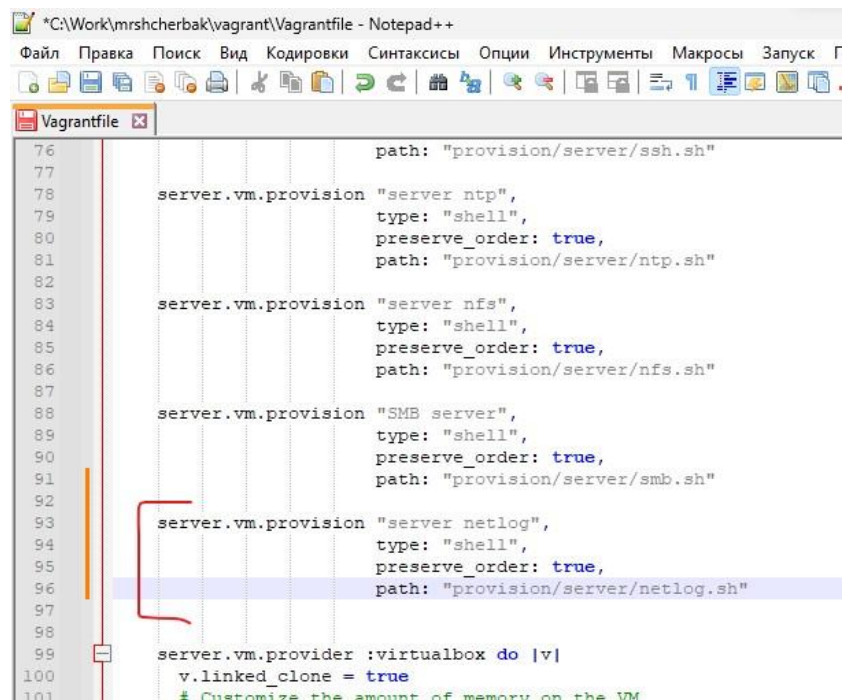
echo "Copy configuration files"
cp -R /vagrant/provision/client/netlog/etc/* /etc
restorecon -vR /etc

echo "Start rsyslog service"
systemctl restart rsyslog

```

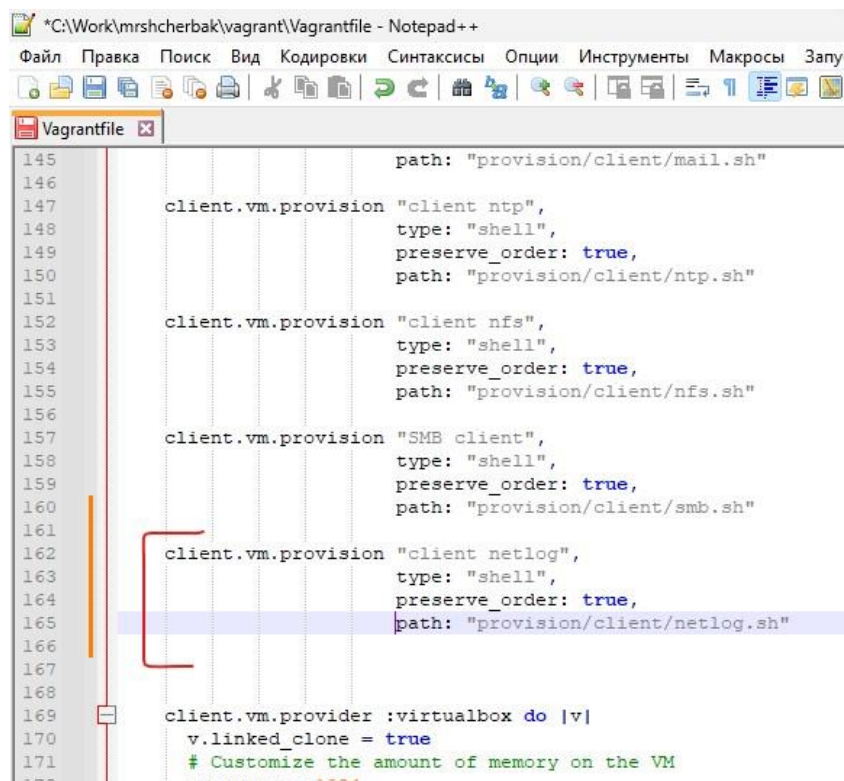
Рис.4.4. Содержимое файла netlog.sh на клиенте

3. Для отработки созданных скриптов во время загрузки виртуальных машин server и client в конфигурационном файле Vagrantfile добавила в соответствующих разделах конфигураций для сервера и клиента записи (рис.4.5 – рис.4.6).



```
76                                     path: "provision/server/ssh.sh"
77
78     server.vm.provision "server ntp",
79         type: "shell",
80         preserve_order: true,
81         path: "provision/server/ntp.sh"
82
83     server.vm.provision "server nfs",
84         type: "shell",
85         preserve_order: true,
86         path: "provision/server/nfs.sh"
87
88     server.vm.provision "SMB server",
89         type: "shell",
90         preserve_order: true,
91         path: "provision/server/smb.sh"
92
93     server.vm.provision "server netlog",
94         type: "shell",
95         preserve_order: true,
96         path: "provision/server/netlog.sh"
97
98
99     server.vm.provider :virtualbox do |v|
100         v.linked_clone = true
101         # Customize the amount of memory on the VM
```

Рис.4.5. Содержимое файла Vagrantfile



```
145                                     path: "provision/client/mail.sh"
146
147     client.vm.provision "client ntp",
148         type: "shell",
149         preserve_order: true,
150         path: "provision/client/ntp.sh"
151
152     client.vm.provision "client nfs",
153         type: "shell",
154         preserve_order: true,
155         path: "provision/client/nfs.sh"
156
157     client.vm.provision "SMB client",
158         type: "shell",
159         preserve_order: true,
160         path: "provision/client/smb.sh"
161
162     client.vm.provision "client netlog",
163         type: "shell",
164         preserve_order: true,
165         path: "provision/client/netlog.sh"
166
167
168     client.vm.provider :virtualbox do |v|
169         v.linked_clone = true
170         # Customize the amount of memory on the VM
171         v.memory = 1024
```

Рис.4.6. Содержимое файла Vagrantfile



**Вывод:** таким образом, в ходе выполнения л/р №15 я получила навыки по работе с журналами системных событий.

### Контрольные вопросы

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

Для приёма сообщений от journald следует использовать модуль imjournal. Этот модуль предназначен для чтения сообщений из журнала journald и передачи их в rsyslog для дальнейшей обработки.

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

Модули imjournallegacy и imuxsock считаются устаревшими. imjournallegacy предназначен для приёма сообщений из журнала, а imuxsock — для приёма через Unix-сокеты. Для современных систем рекомендуется использовать более актуальный imjournal.

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

В моем файле rsyslog.conf не используется устаревший метод приёма сообщений из journald. Модуль imjournal настроен с использованием параметра UsePid="system", что указывает на современный метод интеграции с журналом journald. Таким образом, в данном случае, дополнительный параметр для отключения устаревшего метода не требуется, так как уже используется актуальный модуль imjournal.

Для убедительности в том, что устаревший метод приёма сообщений из journald в rsyslog не используется, следует добавить следующую строку в файл конфигурации /etc/rsyslog.conf:

```
$IMJOURNALLEGACY_OPTIONS --no-imjournallegacy
```

Это явно указывает rsyslog не использовать устаревший метод (--no-imjournallegacy) для приёма сообщений из journald. Или установить LegacyFormat в значение off при наличии данной строки.

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

Все настройки rsyslog находятся в файле /etc/rsyslog.conf. В этот же файл

подключаются дополнительные файлы настройки из каталога /etc/rsyslog.d/.

В /etc/systemd/journald.conf содержатся различные настройки journald.

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

Пересылка сообщений из journald в rsyslog управляется параметром "ForwardToSyslog".

```
/etc/systemd/journald.conf
```

```
ForwardToSyslog=yes
```

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, можно использовать модуль imfile.

```
$ModLoad imfile
```

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

Для пересылки сообщений в базу данных MariaDB используйте модуль ommysql.

```
# Подключение модуля mysql
```

```
$ModLoad 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?

В л/р я на сервере создавала файл конфигурации сетевого хранения журналов и в нем включала приём записей журнала по TCP-порту 514, после чего перезапускала службу rsyslog и настраивала межсетевой экран для приёма сообщений по TCP-порту 514.

Так сервер должен принимать сообщения журнала через TCP-порт 514, а брандмауэр должен быть настроен на разрешение входящего трафика на этот порт.

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

[root@server.mrshcherbak.net rsyslog.d]# systemctl restart rsyslog
```

```
mc [root@server.mrshcherbak.net]:/etc/rsyslog.d
netlog-server.conf  [----] 22 L:[ 1+ 1  2/  2] *(37 / 37b) <E[*][X]
$ModLoad imtcp
$InputTCPServerRun 514
```

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