

Лабораторная работа №15

Тема «Настройка сетевого журналирования»
по дисциплине «Администрирование сетевых подсистем»

Выполнил: Щербак Маргарита Романовна

Студент группы: НПИбд-02-21

«22» декабря 2023г.

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 работы

Настройка сервера сетевого журнала

```
[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 17u      IPv4      23087    0t0      TCP localhost:domain (LISTEN)
named       1002 1003 isc-net-0 21u      IPv6      23089    0t0      TCP localhost:domain (LISTEN)
named       1002 1003 isc-net-0 22u      IPv4      23163    0t0      TCP localhost:rndc (LISTEN)
named       1002 1003 isc-net-0 23u      IPv6      23164    0t0      TCP localhost:rndc (LISTEN)
```

```
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]#
```

Просмотр портов,
связанных с 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
```

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

Настройка межсетевого экрана для приёма сообщений по TCP-порту 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]#
```

Настройка клиента сетевого журнала

```
[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]#
```

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



```
mc [root@client.mrshcherbak.net]:/etc/rsyslog.d
/etc/rsyslog.d/netlog-client.conf 32/32 100%
*.* @@server.mrshcherbak.net:514
```

Просмотр журнала

```
[root@server.mrshcherbak.net rsyslog.d]# tail -f /var/log/messages
Dec 20 19:55:56 server dhcpcd[1443]: DHCPREQUEST for 192.168.1.142 from 08:00:27:df:b4:e0 (client) via eth1
Dec 20 19:55:56 server dhcpcd[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 ]
```

The screenshot shows a Linux desktop environment with the GNOME System Monitor application open. The 'Processes' tab is selected, showing a list of running processes. The background shows a terminal window with the command 'tail -f /var/log/messages' being executed.

Process Name	User	% CPU	ID	Memory	Disk read total	Disk write total
at-spi2-registr	mrshcherbak	0.00	6217	233.5 kB	466.9 kB	
at-spi-bus-launcher	mrshcherbak	0.00	6185	20.5 kB	184.3 kB	
bash	mrshcherbak	0.00	7263	1.1 MB	10.2 MB	
bash	mrshcherbak	0.00	7429	1.6 MB	4.1 MB	
dbus-broker	mrshcherbak	0.00	6117	1.1 MB	1.0 MB	
dbus-broker	mrshcherbak	0.00	6191	188.4 kB	12.3 kB	
dbus-broker-launch	mrshcherbak	0.00	6116	139.3 kB	847.9 kB	
dbus-broker-launch	mrshcherbak	0.00	6190	N/A	8.2 kB	
dconf-service	mrshcherbak	0.00	6330	438.3 kB	417.8 kB	16.0 kB
evolution-addressbook-factory	mrshcherbak	0.00	6333	8.2 kB	23.5 MB	36.0 kB
evolution-alarm-notify	mrshcherbak	0.00	6467	401.4 kB	28.2 MB	
evolution-calendar-factory	mrshcherbak	0.00	6305	254.0 kB	3.2 MB	
evolution-source-registry	mrshcherbak	0.00	6295	364.5 kB	2.7 MB	
gjs	mrshcherbak	0.00	6419	581.6 kB	4.1 MB	
gjs	mrshcherbak	0.00	6578	639.0 kB	217.1 kB	
gnome-keyring-daemon	mrshcherbak	0.00	6105	303.1 kB	N/A	
gnome-session-binary	mrshcherbak	0.00	6108	N/A	85.1 MB	

Запуск графической программы для просмотра журналов

```
root@server:/etc
root@server:/etc x mrshcherbak@server:~ x
[roo@server.mrshcherbak.net etc]# dnf -y install lnav
Rocky Linux 9 - BaseOS
Rocky Linux 9 - BaseOS 4.7 kB/s | 4.1 kB 00:00
Rocky Linux 9 - AppStream 160 kB/s | 2.2 MB 00:13
Rocky Linux 9 - AppStream 5.4 kB/s | 4.5 kB 00:00
Rocky Linux 9 - Extras 835 kB/s | 7.4 MB 00:09
Rocky Linux 9 - Extras 2.3 kB/s | 2.9 kB 00:01
Dependencies resolved.
=====
Package Architecture Version
Repository Size
=====
Installing:
lnav x86_64 0.11.1-1.el9
epel 2.4 M
Transaction Summary
=====
```

Просмотр логов

```
Activities Terminal Dec 20 20:03 en
LOG
LOG mrshcherbak@server:~
2023-12-20T20:03:40 MSK
LOG 2023-12-20T20:02:33.000 syslog_log messages[12,140] named[1002]
Dec 20 20:02:33 server named[1002]: resolver priming query complete
Dec 20 20:02:45 server named[1002]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
Dec 20 20:02:45 server named[1002]: resolver priming query complete
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[1]: run-r7af650dc03614cebbd92040c96723a31.service: Deactivated successfully.
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 systemd-journal[489]: /run/log/journal/b3f9d73a6911423286b60f8720e1b0ac/system.journal: Journal header limits reached or header out-of-date, r
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 MetaWindowActorX11 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.
Files :: Text Filters :: Press TAB to edit
L12,140 100% ?::View Help
Press e/E to move forward/backward through error messages
```



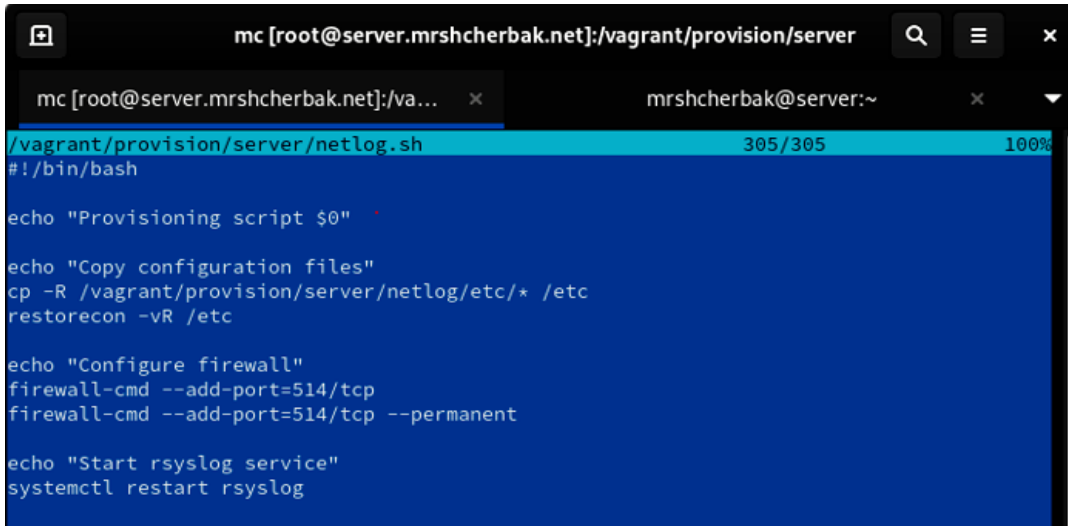
```
Activities Terminal Dec 20 17:04 en en LOG
2023-12-20T17:04:34 UTC Press ENTER to focus on the breadcrumb bar
LOG | 2023-12-20T16:56:37.000 syslog log messages[12,998] rsyslogd[6585]
Dec 20 16:56:37 client rsyslogd[6585]: [origin software="rsyslogd" swVersion="8.2102.0-113.el9_2.1" x-pid="6585" x-info="https://www.rsyslog.com"] start
Dec 20 16:56:37 client rsyslogd[6585]: imjournal: journal files changed, reloading... [v8.2102.0-113.el9_2.1 try https://www.rsyslog.com/e/0 ]
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.
Files :: Text Filters :: Press TAB to edit
L12,998 100% ? : View Help
Press e/E to move forward/backward through error messages
```

Внесение изменений в настройки внутреннего окружения виртуальных машин

```
[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
```

```
[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
```

Содержимое файла netlog.sh на сервере



The screenshot shows a terminal window with the title bar "mc [root@server.mrshcherbak.net]:/vagrant/provision/server". The terminal displays the execution of the script `/vagrant/provision/server/netlog.sh`, which is 305/305 bytes and 100% complete. The script content is as follows:

```
#!/bin/bash

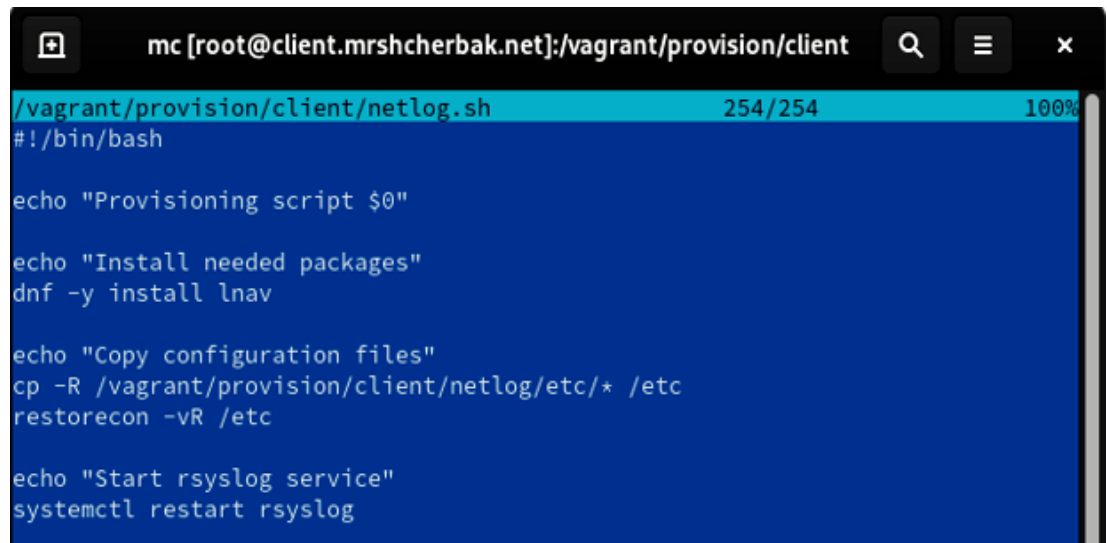
echo "Provisioning script $0"

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
```

Содержимое файла netlog.sh на клиенте



The screenshot shows a terminal window with the title bar "mc [root@client.mrshcherbak.net]:/vagrant/provision/client". The terminal displays the execution of the script `/vagrant/provision/client/netlog.sh`, which is 254/254 bytes and 100% complete. The script content is as follows:

```
#!/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
```

```
*C:\Work\mrshcherbak\vagrant\Vagrantfile - Notepad++
Файл Правка Поиск Вид Кодировки Синтаксисы Опции Инструменты Макросы Запуск Г
Vagrantfile x
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
```

```
*C:\Work\mrshcherbak\vagrant\Vagrantfile - Notepad++
Файл Правка Поиск Вид Кодировки Синтаксисы Опции Инструменты Макросы Запу
Vagrantfile x
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|
```

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