

Лабораторная работа №15

Настройка сетевого журналирования

Ромицина А. Р.

12 декабря 2025

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Ромицына Анастасия Романовна
- НПИбд-02-23 Студ. билет: 1132236132
- Российский университет дружбы народов
- 1132236132@pfur.ru

Вводная часть

Цель работы

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

Основная часть

Настройка сервера сетевого журнала

- Создание на сервере файла конфигурации сетевого хранения журналов.

```
[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]# █
```

Настройка сервера сетевого журнала

- Включение в файле конфигурации /etc/rsyslog.d/netlog-server.conf приёма записей журнала по TCP-порту 514

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

Настройка сервера сетевого журнала

- Перезапуск службы rsyslog и просмотр прослушиваемых портов, связанных с rsyslog.

```
[root@server.arromichina.net rsyslog.d]# systemctl restart rsyslog
[root@server.arromichina.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.
lsof: 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)
```

Настройка сервера сетевого журнала

- Настройка на сервере межсетевого экрана для приёма сообщений по TCP-порту 514

```
[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]# █
```

Настройка клиента сетевого журнала

- Создание на клиенте файла конфигурации сетевого хранения журналов.

```
[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]# █
```

Настройка клиента сетевого журнала

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

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

Настройка клиента сетевого журнала

- Перезапуск службы rsyslog.

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

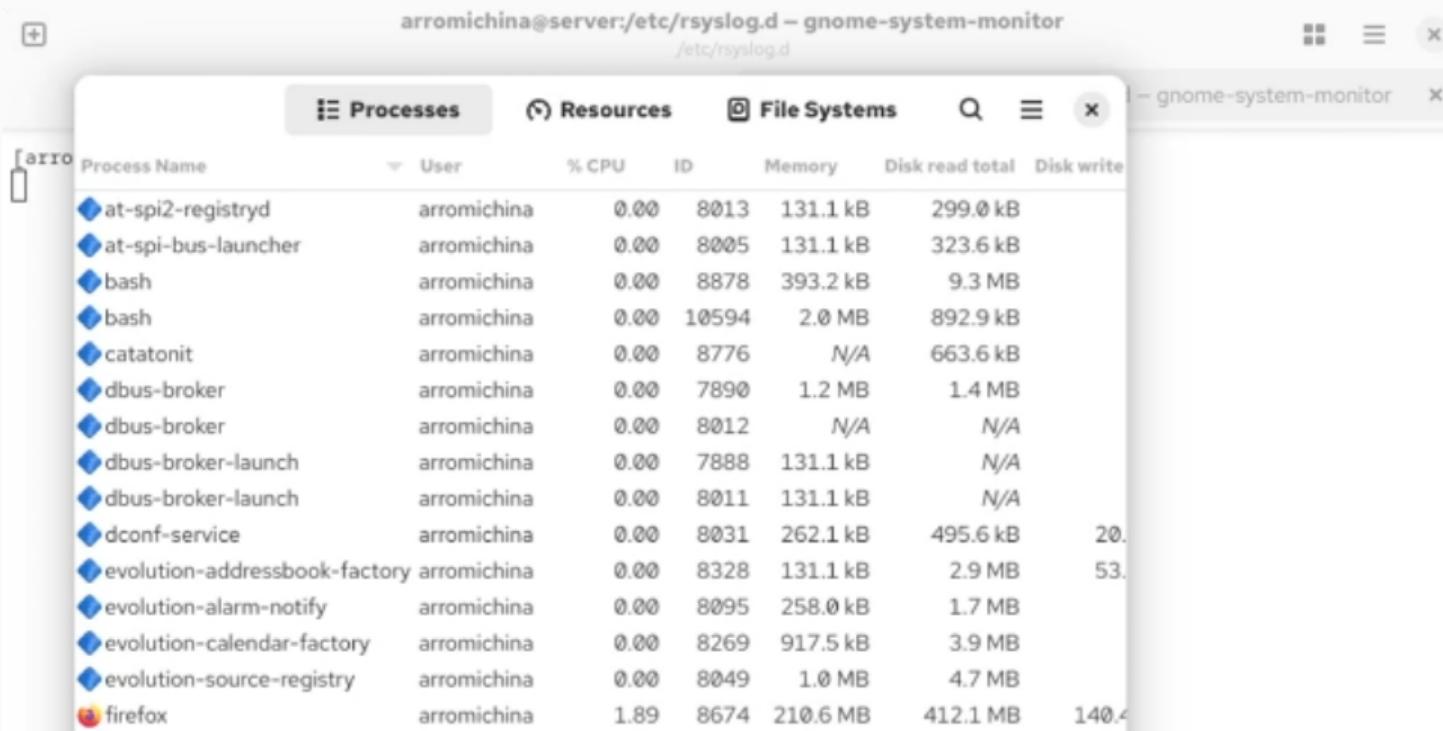
Просмотр журнала

- Просмотр на сервере одного из файлов журнала.

```
[root@server.arromichina.net rsyslog.d]# tail -f /var/log/messages
Dec 10 13:24:36 server named[1358]: timed out resolving 'ns4.dnsmadeeasy.com/A/IN': 127.0.0.1#53
Dec 10 13:24:36 server named[1358]: timed out resolving 'ns4.dnsmadeeasy.com/AAAA/IN': 127.0.0.1#53
Dec 10 13:24:36 server named[1358]: timed out resolving 'ns2.dnsmadeeasy.com/AAAA/IN': 127.0.0.1#53
Dec 10 13:24:36 server named[1358]: timed out resolving 'ns2.dnsmadeeasy.com/A/IN': 127.0.0.1#53
Dec 10 13:24:36 server named[1358]: timed out resolving 'ns0.dnsmadeeasy.com/A/IN': 127.0.0.1#53
Dec 10 13:24:36 server named[1358]: timed out resolving 'ns0.dnsmadeeasy.com/AAAA/IN': 127.0.0.1#53
Dec 10 13:24:37 server named[1358]: timed out resolving 'user.net/DS/IN': 127.0.0.1#53
Dec 10 13:24:37 server named[1358]: timed out resolving 'user.net/DS/IN': 127.0.0.1#53
Dec 10 13:24:42 server NetworkManager[4948]: <info> [1765373082.1385] agent-manager: agent[bc4b1c00d5069170,:1.206/org.gnome.Shell.NetworkAgent/1001]: agent registered
Dec 10 13:24:42 server gnome-shell[7970]: Gio.DBusError: GDBus.Error:org.freedesktop.DBus.Error.Failed: Set global engine failed: Operation was cancelled#012#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 _callHandlers@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:661:33#012 reload@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 _setContent-Type@resource:///org/gnome/shell/misc/ibusManager.js:264:14#012 @resource:///org/gnome/shell/ui/init.js:21:20#012
```

Просмотр журнала

- Запуск на сервере под пользователем arromichina графической программы для просмотра журналов.



The screenshot shows the 'Processes' tab of the gnome-system-monitor application. The window title is 'arromichina@server:/etc/rsyslog.d – gnome-system-monitor'. The table lists various system processes running under the user 'arromichina'. The columns are: Process Name, User, % CPU, ID, Memory, Disk read total, and Disk write. The data includes:

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.
evolution-addressbook-factory	arromichina	0.00	8328	131.1 kB	2.9 MB	53.
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.

Просмотр журнала

- Установка на сервере просмотрщика журналов системных сообщений.

```
[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

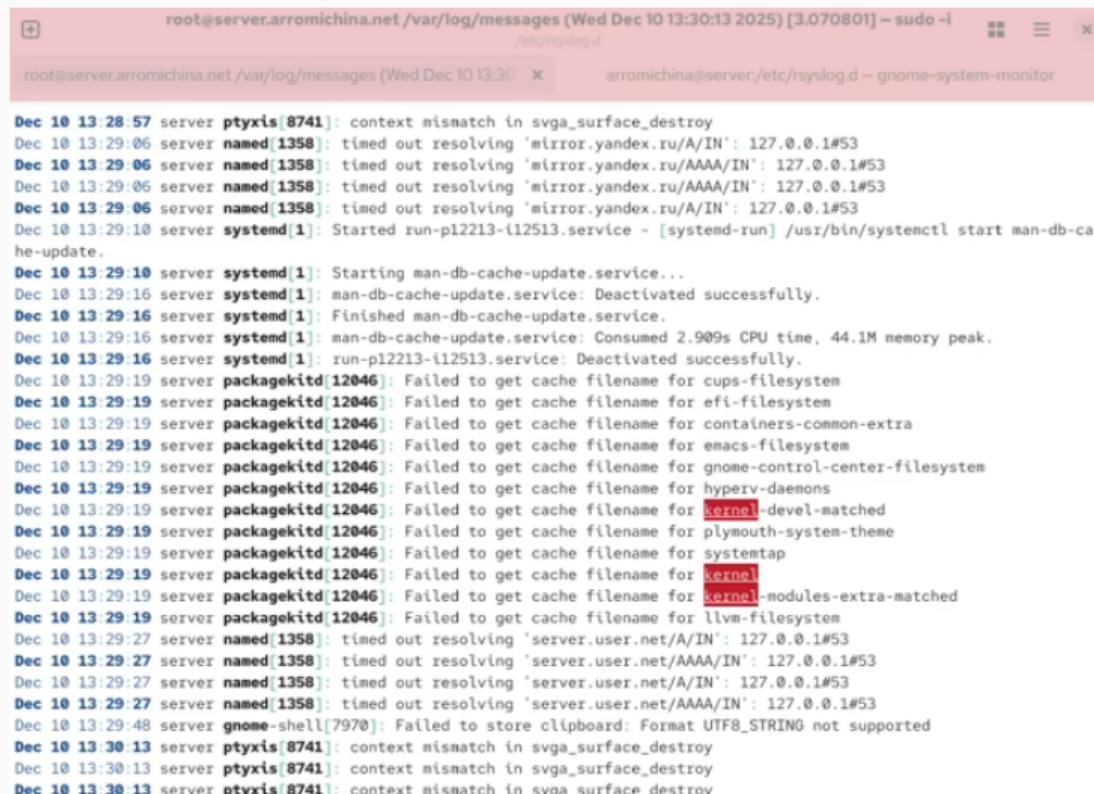
Transaction Summary
=====
Install 1 Package

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
```

Просмотр журнала

- Просмотр логов



The screenshot shows a terminal window with the following details:

- Terminal title: root@server.arromichina.net /var/log/messages (Wed Dec 10 13:30:13 2025) [3.070801] – sudo -i /etc/nylog.d
- Current directory: /var/log/messages
- Log entries (partial list):

```
Dec 10 13:28:57 server ptyxix[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/AAAAA/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-i12513.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-i12513.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 systemtap
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for kernel
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 ptyxix[8741]: context mismatch in svga_surface_destroy
Dec 10 13:30:13 server ptyxix[8741]: context mismatch in svga_surface_destroy
Dec 10 13:30:13 server ptxix[8741]: context mismatch in svga_surface_destroy
```

Внесение изменений в настройки внутреннего окружения виртуальных машин

- 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.

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

Настройка сервера NFSv4

- Открытие файла на редактирование и добавление в него скрипта.

```
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
```

Мониторинг NFS на клиенте

- 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.

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

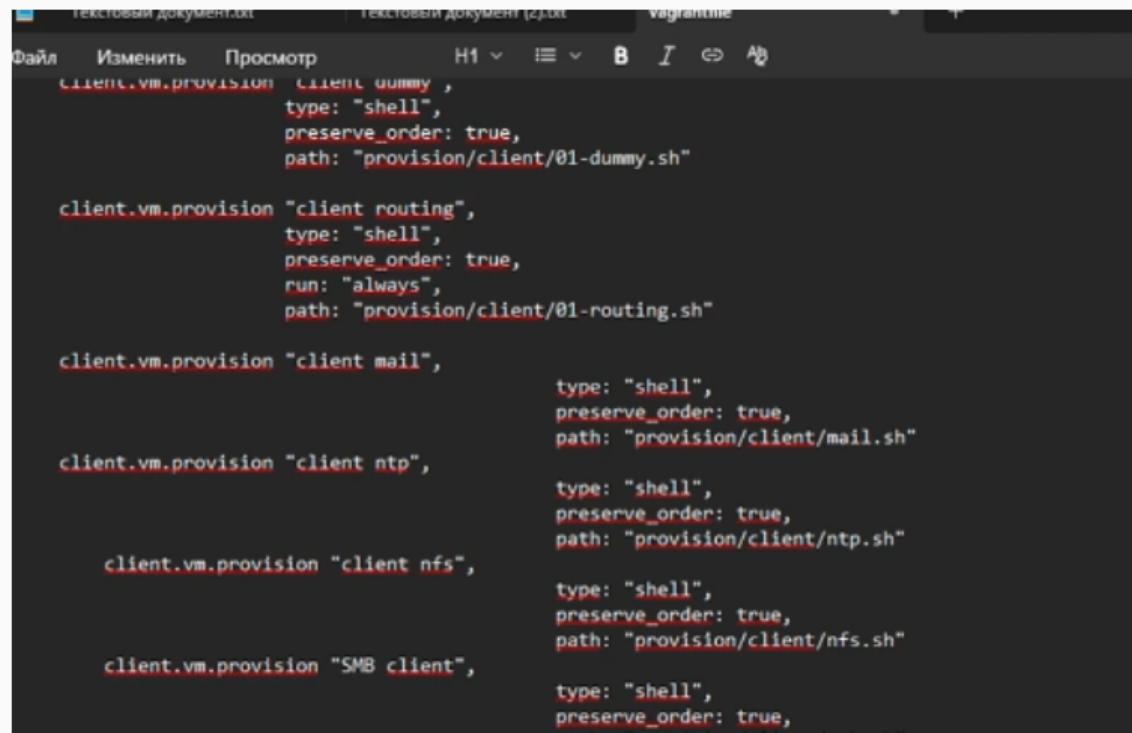
Мониторинг NFS на клиенте

- Открытие файла на редактирование и добавление в него скрипта.

```
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
```

Мониторинг NFS на клиенте

- Добавление конфигураций в конфигурационном файле Vagrantfile для сервера и клиента.



The screenshot shows a Windows Notepad window with the title "Vagrantfile". The content of the file is a Vagrant configuration script:

```
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,
```

Вывод

Вывод

- В ходе выполнения лабораторной работы были получены навыки по работе с журналами системных событий.