

Лабораторная работа №15 (Настройка сетевого журналирования)

Шубина София Антоновна

11 ноября 2025

Российский университет дружбы народов

Цель работы

Получение навыков по работе с журналами системных событий.

Задание

1. Настройте сервер сетевого журналирования событий.
2. Настройте клиент для передачи системных сообщений в сетевой журнал на сервере.
3. Просмотрите журналы системных событий с помощью нескольких программ. При наличии сообщений о некорректной работе сервисов исправьте ошибки в настройках соответствующих служб.
4. Напишите скрипты для Vagrant, фиксирующие действия по установке и настройке сетевого сервера журналирования

Выполнение лабораторной работы

Настройка сервера сетевого журнала

На сервере создадим файл конфигурации сетевого хранения журналов:

```
[root@server.sashubina.net ~]# cd /etc/rsyslog.d  
[root@server.sashubina.net rsyslog.d]# touch netlog-server.conf  
[root@server.sashubina.net rsyslog.d]#
```

Рис. 1: создание файла

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

```
GNU nano 8.1          /etc/rsyslog.d/netlog-server.conf
$ModLoad imtcp
$InputTCPServerRun 514
```

Рис. 2: Включение журналирования по TCP-порту 514

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

rsyslogd	19819	root	4u	IPv4	89661	0t0	TCP *:shell (LISTEN)
rsyslogd	19819	root	5u	IPv6	89662	0t0	TCP *:shell (LISTEN)
rsyslogd	19819 19822 in:imjour	root	4u	IPv4	89661	0t0	TCP *:shell (LISTEN)
rsyslogd	19819 19822 in:imjour	root	5u	IPv6	89662	0t0	TCP *:shell (LISTEN)
rsyslogd	19819 19823 in:imtcp	root	4u	IPv4	89661	0t0	TCP *:shell (LISTEN)
rsyslogd	19819 19823 in:imtcp	root	5u	IPv6	89662	0t0	TCP *:shell (LISTEN)
rsyslogd	19819 19824 in:imtcp	root	4u	IPv4	89661	0t0	TCP *:shell (LISTEN)
rsyslogd	19819 19824 in:imtcp	root	5u	IPv6	89662	0t0	TCP *:shell (LISTEN)
rsyslogd	19819 19825 in:imtcp	root	4u	IPv4	89661	0t0	TCP *:shell (LISTEN)
rsyslogd	19819 19825 in:imtcp	root	5u	IPv6	89662	0t0	TCP *:shell (LISTEN)
rsyslogd	19819 19826 in:imtcp	root	4u	IPv4	89661	0t0	TCP *:shell (LISTEN)
rsyslogd	19819 19826 in:imtcp	root	5u	IPv6	89662	0t0	TCP *:shell (LISTEN)
rsyslogd	19819 19827 in:imtcp	root	4u	IPv4	89661	0t0	TCP *:shell (LISTEN)
rsyslogd	19819 19827 in:imtcp	root	5u	IPv6	89662	0t0	TCP *:shell (LISTEN)
rsyslogd	19819 19828 rs:main	root	4u	IPv4	89661	0t0	TCP *:shell (LISTEN)
rsyslogd	19819 19828 rs:main	root	5u	IPv6	89662	0t0	TCP *:shell (LISTEN)

Рис. 3: Просмотр прослушиваемых портов, связанных с rsyslog

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

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

Рис. 4: Настройка межсетевого экрана

Проверим 514 порт

```
[root@server.sashubina.net rsyslog.d]# sudo ss -tlnp | grep 514
LISTEN 0      25          0.0.0.0:514          0.0.0.0:*      users:(("rsyslogd",pi
d=19819,fd=4))
LISTEN 0      25          [::]:514          [::]:*      users:(("rsyslogd",pi
d=19819,fd=5))
[root@server.sashubina.net rsyslog.d]#
```

Рис. 5: Проверка 514 порта

Настройка клиента сетевого журнала

На клиенте создадим файл конфигурации сетевого хранения журналов:

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

Рис. 6: создание файла

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

```
GNU nano 8.1      /etc/rsyslog.d/netlog-client.conf
.* @server.sashubina.net:514
```

Рис. 7: Включение перенаправления сообщений журнала на 514 TCP-порт сервера

Перезапустим службу rsyslog:

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

Рис. 8: перезапустим службу

Просмотр журнала

На сервере просмотрим один из файлов журнала:

```
[root@server.sashubina.net ~]# tail -f /var/log/messages
Nov 10 17:09:36 server systemd[4167]: Finished systemd-tmpfiles-setup.service - Create User Files and Directories.
Nov 10 17:09:36 server systemd[4167]: Listening on dbus.socket - D-Bus User Message Bus Socket.
Nov 10 17:09:36 server systemd[4167]: Reached target sockets.target - Sockets.
Nov 10 17:09:36 server systemd[4167]: Reached target basic.target - Basic System.
Nov 10 17:09:36 server systemd[4167]: Reached target default.target - Main User Target.
Nov 10 17:09:36 server systemd[4167]: Startup finished in 177ms.
Nov 10 17:09:36 server systemd[1]: Started user@0.service - User Manager for UID 0.
Nov 10 17:09:36 server systemd[1]: Started session-c2.scope - Session c2 of User root.
Nov 10 17:09:36 server systemd[1]: Starting systemd-hostnamed.service - Hostname Service...
Nov 10 17:09:36 server systemd[1]: Started systemd-hostnamed.service - Hostname Service.
Nov 10 17:10:06 server systemd[1]: systemd-hostnamed.service: Deactivated successfully.
```

Рис. 9: Просмотр файла var/log/messages журнала

На сервере под пользователем sashubina запустим графическую программу для просмотра журналов с помощью команды `gnome-system-monitor`:

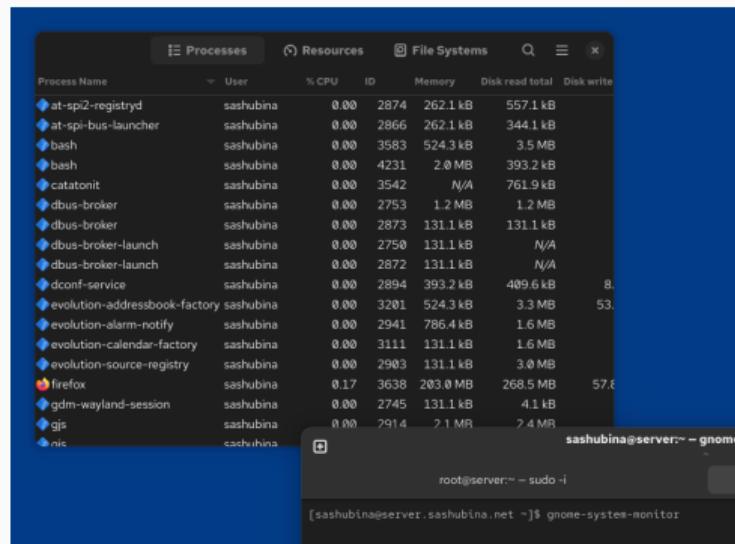


Рис. 10: Запуск графической программы для просмотра журналов

На сервере установите просмотрщик журналов системных сообщений lnav или его аналог. Я установила аналог, потому что lnav у меня не скачался

```
[root@server.sashubina.net ~]# dnf -y install multitail
Last metadata expiration check: 1:50:56 ago on Mon 10 Nov 2025 03:26:23 PM UTC.
Dependencies resolved.
=====
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                                         1.5 MB/s | 148 kB     00:00
                                                               86 kB/s | 148 kB     00:01
Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing : 1/1
Installing : multitail-7.1.3-2.el10_0.x86_64                                     1/1
Running scriptlet: multitail-7.1.3-2.el10_0.x86_64                               1/1
                                                               1/1
Installed:
multitail-7.1.3-2.el10_0.x86_64

Complete!
[root@server.sashubina.net ~]#
```



Рис. 11: загрузка

Просмотрим логи с помощью multitail на клиенте и на сервере. посмотрим /var/log/messages и /var/log/secure

```
Nov 10 17:57:14 server systemd[4240]: Starting systemd-tmpfiles-setup.service - Create User Files and Directories...
Nov 10 17:57:14 server systemd[4240]: Listening on dbus.socket - D-Bus User Message Bus Socket.
Nov 10 17:57:14 server systemd[4240]: Finished systemd-tmpfiles-setup.service - Create User Files and Directories.

Nov 10 17:57:14 server systemd[4240]: Reached target basic.target - Basic System.
Nov 10 17:57:14 server systemd[4240]: Reached target default.target - Main User Target.
Nov 10 17:57:14 server systemd[4240]: Startup finished in 172ms.
Nov 10 17:57:14 server systemd[1]: Started user@0.service - User Manager for UID 0.
Nov 10 17:57:14 server systemd[1]: Started session-c2.scope - Session c2 of User root.
Nov 10 17:57:14 server systemd[1]: Starting systemd-hostnamed.service - Hostname Service...
Nov 10 17:57:14 server systemd[1]: Started systemd-hostnamed.service - Hostname Service.
Nov 10 17:57:44 server systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Nov 10 17:58:46 server systemd[1]: packagekit.service: Deactivated successfully.
Nov 10 17:58:46 server systemd[1]: packagekit.service: Consumed 11.928s CPU time, 404.8M memory peak, 111.6M memory swap peak.
Nov 10 17:59:13 client NetworkManager[7171]: <info> [1762797553.8261] agent-manager: agent[f726fefdb8755f2cf,:1.215/org.gnome.Shell.NetworkAgent/1001]: agent registered
```

Рис. 12: Просмотр логов с сервера

Просмотрим логи с помощью multtail на клиенте и на сервере. посмотрим /var/log/messages и /var/log/secure

```
Nov 18 17:57:14 server systemd[4240]: Starting systemd-tmpfiles-setup.service - Create User Files and Directories...
Nov 18 17:57:14 server systemd[4240]: Listening on dbus.socket - D-Bus User Message Bus Socket.
Nov 18 17:57:14 server systemd[4240]: Finished systemd-tmpfiles-setup.service - Create User Files and Directories.

Nov 18 17:57:14 server systemd[4240]: Reached target basic.target - Basic System.
Nov 18 17:57:14 server systemd[4240]: Reached target default.target - Main User Target.
Nov 18 17:57:14 server systemd[4240]: Startup finished in 170ms.
Nov 18 17:57:14 server systemd[1]: Started user@.service - User Manager for UID 0.
Nov 18 17:57:14 server systemd[1]: Started session-c2.scope - Session c2 of User root.
Nov 18 17:57:14 server systemd[1]: Starting systemd-hostnamed.service - Hostname Service...
Nov 18 17:57:14 server systemd[1]: Started systemd-hostnamed.service - Hostname Service.
Nov 18 17:58:44 server systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Nov 18 17:58:46 server systemd[1]: packagekit.service: Deactivated successfully.
Nov 18 17:58:46 server systemd[1]: packagekit.service: Consumed 13.028s CPU time, 404.0M memory peak, 111.0M memory swap peak.
Nov 18 17:59:13 client NetworkManager[7171]: <info> [1762797593.826] agent-manager: agent_f726ffdf875f62cf,:1.215/org.gnome.Shell.NetworkAgent[1001]: agent registered
Nov 18 17:59:44 server vim[1248]: server listening on : port 22.
Nov 18 17:48:50 server aptetty[2147]: could not get terminal name: -22
Nov 18 17:48:50 server aptetty[21593]: could not get terminal name: +22
Nov 18 17:48:50 server aptetty[21593]: could not get terminal name: -22
Nov 18 17:48:51 server aptetty[2171]: could not get terminal name: -22
Nov 18 17:51:38 server (systemd)[2199]: pam_unix(systemd-user:session): session opened for user sashubina(uid=1001) by sashubina(uid=0)
Nov 18 17:51:38 server login[1643]: pam_unix(login:session): session opened for user sashubina(uid=1001) by sashubina(uid=0)
Nov 18 17:51:38 server login[1643]: LOGIN ON tty1 BY sashubina
Nov 18 17:52:39 server sudo[2251]: sashubina : TTY=tty1 : PWD=/home/sashubina : USER=root : COMMAND=/bin/systemctl start gdm
Nov 18 17:52:39 server sudo[2251]: pam_unix(sudo:session): session opened for user root(uid=0) by sashubina(uid=1001)
Nov 18 17:52:39 server sudo[2251]: pam_unix(sudo:session): session closed for user root
Nov 18 17:52:39 server login[1643]: pam_unix(login:session): session closed for user sashubina
Nov 18 17:52:39 server (systemd)[2277]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)
Nov 18 17:52:39 server gdm-launch-environment[2278]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=42) by (uid=0)
Nov 18 17:52:48 server gdm-password[2759]: gkr-pam: unable to locate daemon control file
Nov 18 17:52:48 server gdm-password[2759]: gkr-pam: stashed password to try later in open session
Nov 18 17:52:48 server gdm-password[2759]: pam_unix(gdm-password:session): session opened for user sashubina(uid=1001) by sashubina(uid=0)
Nov 18 17:52:48 server gdm-password[2759]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Nov 18 17:52:54 server gdm-launch-environment[2278]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Nov 18 17:57:14 server sudo[4244]: sashubina : TTY pts/0 : PWD=/root : USER=root : COMMAND=/bin/bash
Nov 18 17:57:14 server sudo[4244]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)
Nov 18 17:57:14 server sudo[4244]: pam_unix(systemd-user:session): session opened for user root(uid=0) by sashubina(uid=1001)
Nov 18 17:59:13 client gdm-password[14616]: gkr-pam: unlocked login keyring
```

Рис. 13: Просмотр логов с сервера

Просмотрим логи с помощью multitail на клиенте и на сервере. посмотрим /var/log/messages и /var/log/secure

```
Nov 10 17:49:36 client systemd[1]: setroubletd.service: Consumed 668ms CPU time, 76.8M memory peak.
Nov 10 17:49:44 client gnome-shell[11784]: Cursor update failed: drmModeAtomicCommit: Invalid argument
Nov 10 17:52:43 client NetworkManager[7171]: <info>  [1762797163.4056] dhcpc4 (eth1): state changed new lease, address=192.168.1.30
Nov 10 17:52:43 client systemd[1]: Starting NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service...
Nov 10 17:52:43 client systemd[1]: Started NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service.
Nov 10 17:52:53 client systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
Nov 10 17:59:13 client NetworkManager[7171]: <info>  [1762797553.8261] agent-manager: agent[f726fef8755f2cf,:1.215/org.gnome.Shell.NetworkAgent/1001]: agent registered
Nov 10 18:07:12 client systemd[1]: Stopping rsyslog.service - System Logging Service...
Nov 10 18:07:12 client rsyslogd[14419]: [origin software="rsyslogd" swVersion="8.2412.0-1.el10" x-pid="14419" x-info="https://www.rsyslog.com"] exiting on signal 15
Nov 10 18:07:12 client systemd[1]: rsyslog.service: Deactivated successfully.
Nov 10 18:07:12 client systemd[1]: Stopped rsyslog.service - System Logging Service.
Nov 10 18:07:12 client systemd[1]: Starting rsyslog.service - System Logging Service...
Nov 10 18:07:13 client systemd[1]: Started rsyslog.service - System Logging Service.
Nov 10 18:07:13 client rsyslogd[14745]: [origin software="rsyslogd" swVersion="8.2412.0-1.el10" x-pid="14745" x-info="https://www.rsyslog.com"] start
Nov 10 18:07:13 client rsyslogd[14745]: imjournal: journal files changed, reloading... [v8.2412.0-1.el10 try https://www.rsyslog.com/e/0 ]
Nov 10 18:07:37 client root[14753]: Test:after connection
Nov 10 18:07:43 client NetworkManager[7171]: <info>  [1762798063.4624] dhcpc4 (eth1): state changed new lease, address=192.168.1.30
Nov 10 18:07:43 client systemd[1]: Starting NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service...
Nov 10 18:07:43 client systemd[1]: Started NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service.
Nov 10 18:07:53 client systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
```

Рис. 14: Просмотр логов с клиента

Просмотрим логи с помощью multitail на клиенте и на сервере. посмотрим /var/log/messages и /var/log/secure

The screenshot shows a terminal window with the title 'multitail'. It displays two parallel log streams. The left stream shows logs from the client system, and the right stream shows logs from the server system. Both streams include timestamps, log levels (Info), and detailed log entries. The logs are color-coded for readability.

```
Nov 10 10:03:12 client system[1]: Starting NetworkManager-dnsd.service - Network Manager Dnsd Dispatcher Service
Nov 10 17:52:43 client system[1]: Started NetworkManager-dnsd.service - Network Manager Dnsd Dispatcher Service.
Nov 10 17:52:53 client system[1]: NetworkManager-dispatcher.service: Deactivated successfully.
Nov 10 17:53:13 client NetworkManager[7175]: <info> (176.27.99.53:8001) agent_manager: agent(f726febd8759f2cf.1.216/org.gnome.Shell.NetworkAgent@1801). agent_registered
Nov 10 18:07:12 client system[1]: Stopping rsyslog.service - System Logging Service...
Nov 10 18:07:12 client rsyslogd[16419]: FwdLog software="rsyslog" swVersion="8.2412.8-1.el10" x-pid="14419" x-info="https://www.rsyslog.com" exiting on signal 15
Nov 10 18:07:12 client system[1]: rsyslog.service: Deactivated successfully.

Nov 10 18:07:12 client system[1]: Starting rsyslog.service - System Logging Service
Nov 10 18:07:13 client rsyslogd[14745]: FwdLog software="rsyslog" swVersion="8.2412.8-1.el10" x-pid="14745" x-info="https://www.rsyslog.com" start
Nov 10 18:07:13 client rsyslogd[14745]: FwdLog software="rsyslog" swVersion="8.2412.8-1.el10" x-pid="14745" x-info="https://www.rsyslog.com" start
Nov 10 18:07:13 client rsyslogd[14745]: <info> [176.27.99.53:4624] dcepc (eth1) state changed new issue, address=169.1.1.1
Nov 10 18:07:43 client NetworkManager[7175]: <info> [176.27.99.53:4624] dcepc (eth1) state changed new issue, address=169.1.1.1
Nov 10 18:07:43 client system[1]: Starting NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service
Nov 10 18:07:43 client system[1]: Started NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service.
Nov 10 18:07:53 client system[1]: NetworkManager-dispatcher.service: Deactivated successfully.
Nov 10 18:08:12 client ssh[17085]: failed to create clientidc: Format UTB_PUBKEY not supported
Nov 10 16:31:47 client sudo[13139]: pam_unix(sudo session): session closed for user sashubina
Nov 10 16:32:17 client su[13354]: pam_unix(su-1-session): session opened for user sashubina(uid=1001) by sashubina(uid=0)
Nov 10 16:58:01 client gdm[13856]: gkr-pam_unlocked_login_keyring
Nov 10 16:58:01 client sudo[13856]: pam_unix(sudo-1-session): session closed for user root
Nov 10 17:30:07 client gdm-passwordd[14145]: gkr-pam_unlocked_login_keyring
Nov 10 17:30:25 client gdm-passwordd[14381]: gkr-pam_unlocked_login_keyring
Nov 10 17:43:29 client sudo[14405]: root : TTY-pts/0 ; PWD=/etc/rsyslog.d ; USER=root ; COMMAND=/bin/tee /etc/rsyslog.d/reboot-client.log
Nov 10 17:43:29 client sudo[14405]: pam_unix(sudo-session): session opened for user root(uid=0) by sashubina(uid=0)
Nov 10 17:43:29 client sudo[14405]: pam_unix(sudo-session): session closed for user root
Nov 10 17:44:12 client sudo[14404]: root : TTY-pts/0 ; PWD=/etc/rsyslog.d ; USER=root ; COMMAND=/bin/systemctl restart rsyslog
Nov 10 17:44:12 client sudo[14404]: pam_unix(sudo-session): session opened for user root(uid=0) by sashubina(uid=0)
Nov 10 17:44:12 client sudo[14404]: pam_unix(sudo-session): session closed for user root
Nov 10 17:50:13 client gdm-passwordd[14615]: gkr-pam_unlocked_login_keyring
Nov 10 18:07:12 client sudo[14748]: root : TTY-pts/0 ; PWD=/etc/rsyslog.d ; USER=root ; COMMAND=/bin/systemctl restart rsyslog
Nov 10 18:07:13 client sudo[14748]: pam_unix(sudo-session): session closed for user root
Nov 10 18:07:13 client sudo[14748]: pam_unix(sudo-session): session closed for user root
```

Рис. 15: Просмотр логов с клиента

Внесение изменений в настройки внутреннего окружения виртуальных машины

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 поместим в соответствующие подкаталоги конфигурационные файлы, а также создадим исполняемый файл netlog.sh:

```
[root@server.sashubina.net ~]# sudo systemctl restart rsyslog
[root@server.sashubina.net ~]# multitail
[root@server.sashubina.net ~]# cd /vagrant/provision/server
[root@server.sashubina.net server]# mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.sashubina.net server]# cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.sashubina.net server]# cd /vagrant/provision/server
[root@server.sashubina.net server]# touch netlog.sh
[root@server.sashubina.net server]# chmod +x netlog.sh
[root@server.sashubina.net server]# nano netlog.sh
[root@server.sashubina.net server]#
```

Рис. 16: создание файла

В каталоге `/vagrant/provision/server` создадим исполняемый файл `netlog.sh` и внесем скрипт:

```
GNU nano 8.1
#!/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. 17: Скрипта файла `/vagrant/provision/server/netlog.sh`

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, а также создадим исполняемый файл `netlog.sh`:

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

Рис. 18: создание файла

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

```
GNU nano 8.1                               netlog.sh
#!/bin/bash
echo "Provisioning script $0"
echo "Install needed packages"
dnf -y install multitail
echo "Copy configuration files"
cp -R /vagrant/provision/client/netlog/etc/* /etc
restorecon -vR /etc
echo "Start rsyslog service"
systemctl restart rsyslog
```

Рис. 19: Скрипта файла /vagrant/provision/client/ netlog.sh

Затем для отработки созданных скриптов в конфигурационном файле Vagrantfile необходимо добавить в соответствующих разделах конфигураций для сервера и клиента:

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

end
```

Рис. 20: Vagrantfile

Затем для отработки созданных скриптов в конфигурационном файле Vagrantfile необходимо добавить в соответствующих разделах конфигураций для сервера и клиента:

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

Рис. 21: Vagrantfile

Контрольные вопросы

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

Для приёма сообщений от journald вам следует использовать модуль imjournal.

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

Устаревший модуль, который можно использовать для включения приёма сообщений журнала в rsyslog, называется imklog.

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

Чтобы убедиться, что устаревший метод приёма сообщений из `journald` не используется, следует использовать параметр “`SystemCallFilter (include:omusrmmsg.conf?)`” в конфигурационном файле `rsyslog.conf`.

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

Настройки, позволяющие настраивать работу журнала, содержатся в конфигурационном файле rsyslog.conf.

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

Пересылка сообщений из journald в rsyslog управляется параметром “ForwardToSyslog” в файле конфигурации journald.conf.

6. Какой модуль rsyslog вы можете использовать для включения сообщений из файла журнала, не созданного rsyslog?

Модуль rsyslog, который можно использовать для включения сообщений из файла журнала, не созданного rsyslog, называется imfile.

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

Для пересылки сообщений в базу данных MariaDB вам следует использовать модуль `ommysql`.

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

Для позволения текущему журналному серверу получать сообщения через TCP, вам нужно включить две строки в rsyslog.conf:

```
$ModLoad imtcp  
$InputTCPServerRun 514
```

9. Как настроить локальный брандмауэр, чтобы разрешить приём сообщений журнала через порт TCP 514?

Чтобы разрешить приём сообщений журнала через порт TCP 514 можно использовать следующую команду:

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

Выводы

В результате выполнения данной работы были приобретены практические навыки по работе с журналами системных событий.