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:

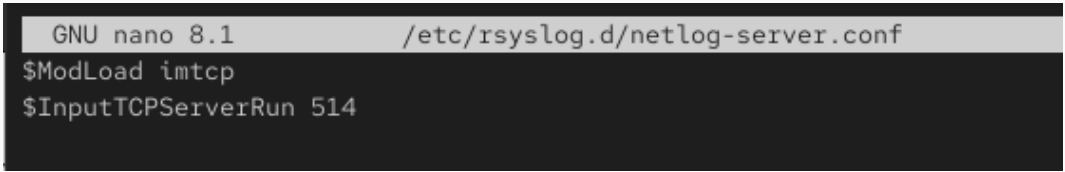

Рис. 2: Включение журналирования по TCP-порту 514

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)
[root@server.sashubina.net rsyslog.d]#
```

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

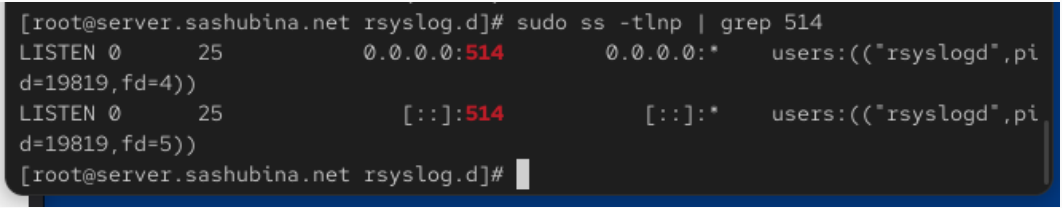

Рис. 5: Проверка 514 порта

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:

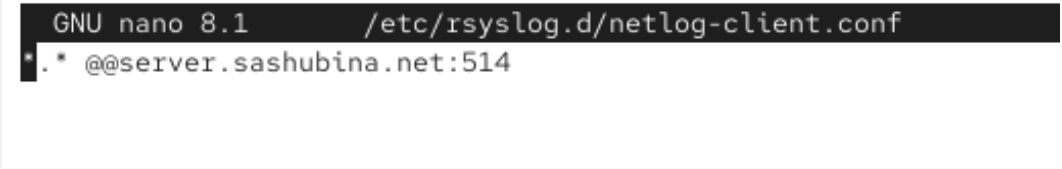

Рис. 7: Включение перенаправления сообщений журнала на 514 TCP-порт сервера

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`:

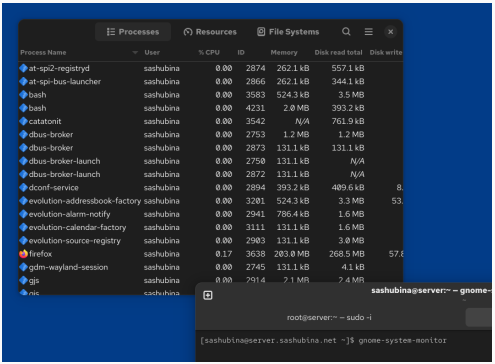

Рис. 10: Запуск графической программы для просмотра журналов

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

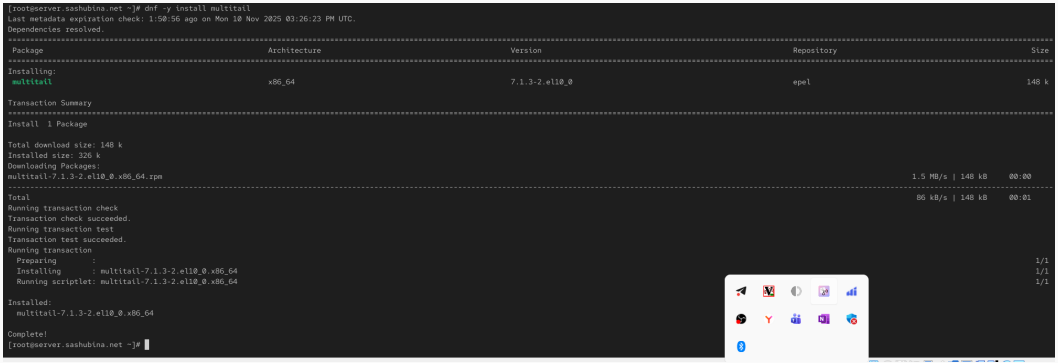

Рис. 11: загрузка

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

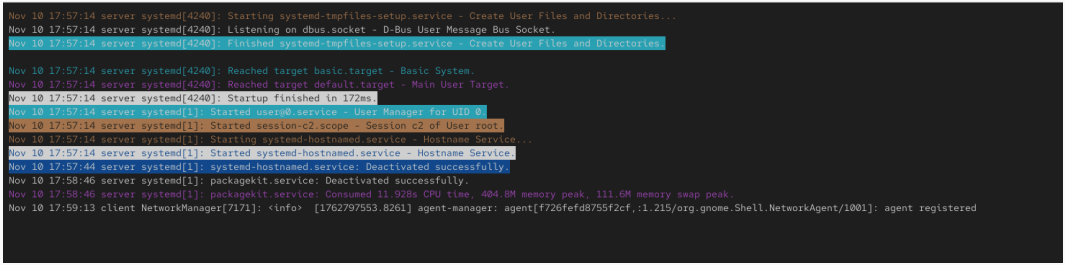

Рис. 12: Просмотр логов с сервера

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

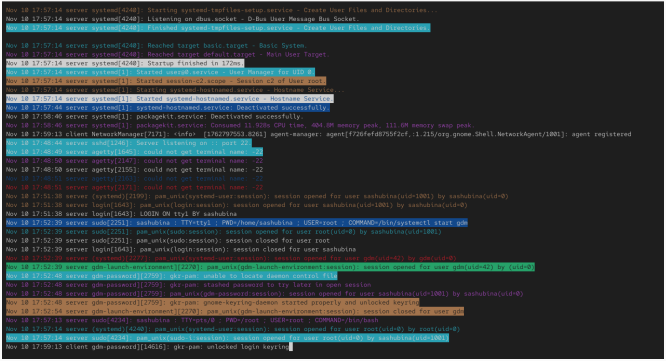

Рис. 13: Просмотр логов с сервера

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

Рис. 14: Просмотр логов с клиента

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

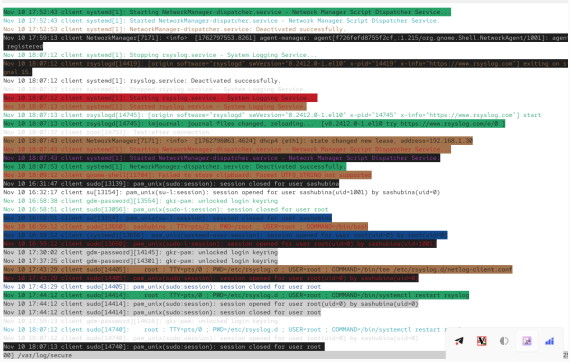

Рис. 15: Просмотр логов с клиента

Внесение изменений в настройки внутреннего окружения виртуальных машины

Внесение изменений в настройки внутреннего окружения виртуальных машины

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/n
etlog/etc/rsyslog.d
[root@client.sashubina.net client]# cp -R /etc/rsyslog.d/netlog-client.c
onf /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:omusrmsg.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 журнальному 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.