**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.

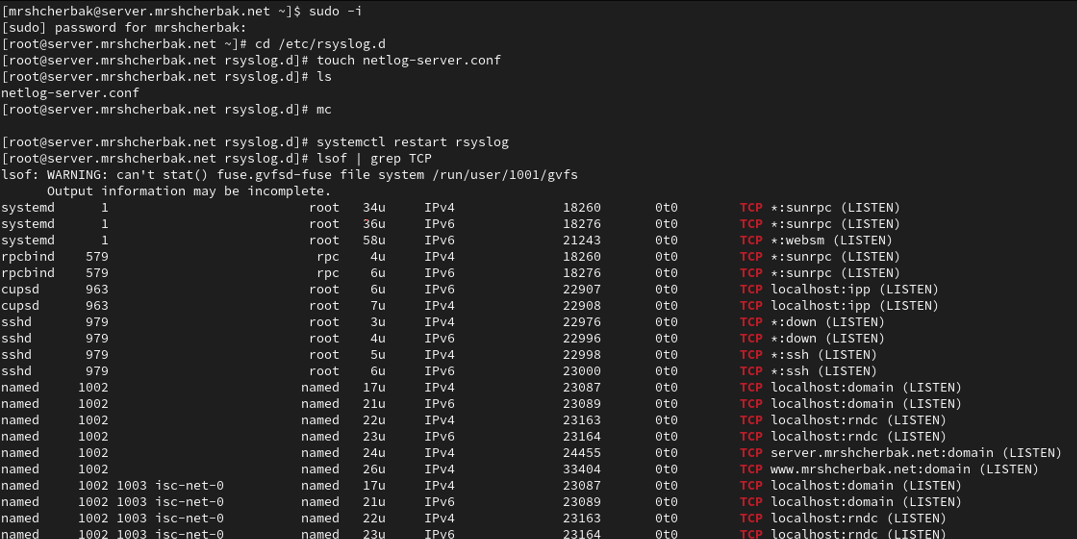


Рис.1.1. Выполнение команд

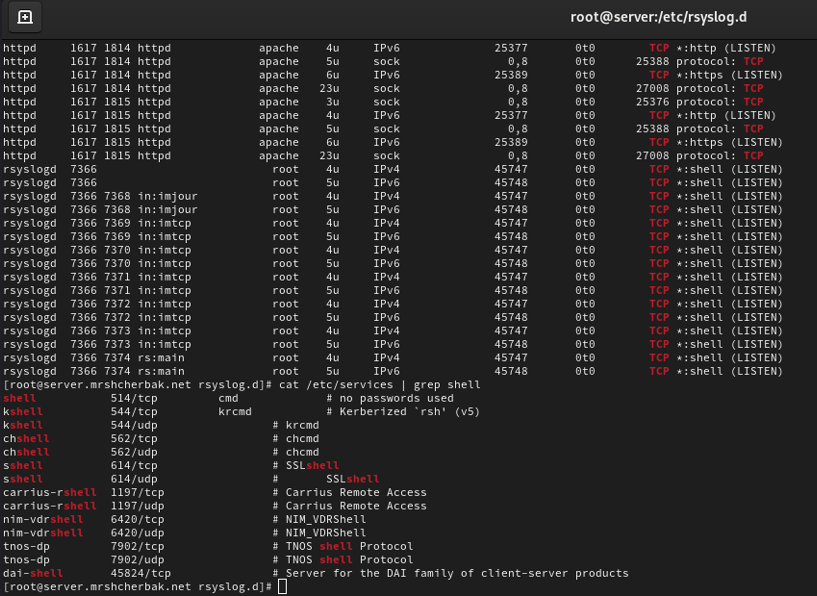


Рис.1.2. Просмотр портов, связанных с rsyslog

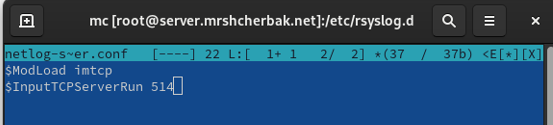


Рис.1.3. Содержимое файла /etc/rsyslog.d/netlog-server.conf

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

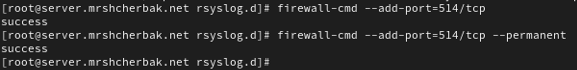


Рис.1.4. Настройка межсетевого экрана для приёма сообщений по TCP-порту 514

**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.

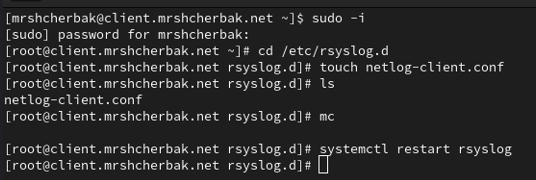


Рис.2.1. Выполнение команд

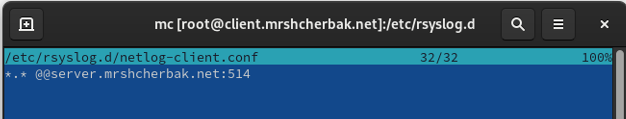


Рис.2.2. Содержимое файла /etc/rsyslog.d/netlog-client.conf

**3. Просмотр журнала**

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

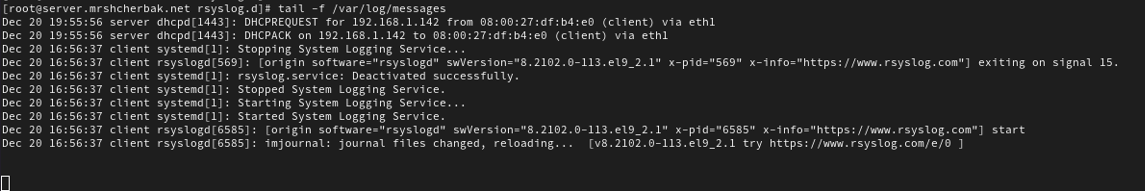


Рис.3.1. Просмотр одного из файлов журнала

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

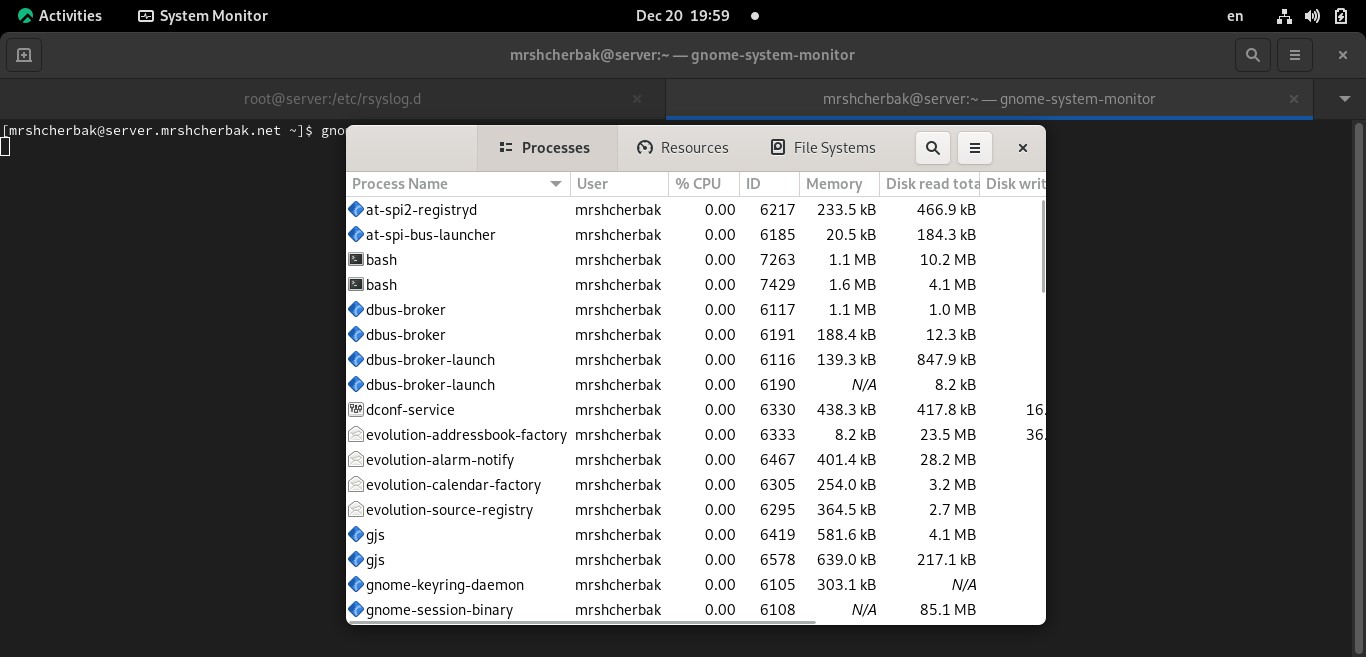


Рис.3.2. Запуск графической программы для просмотра журналов

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

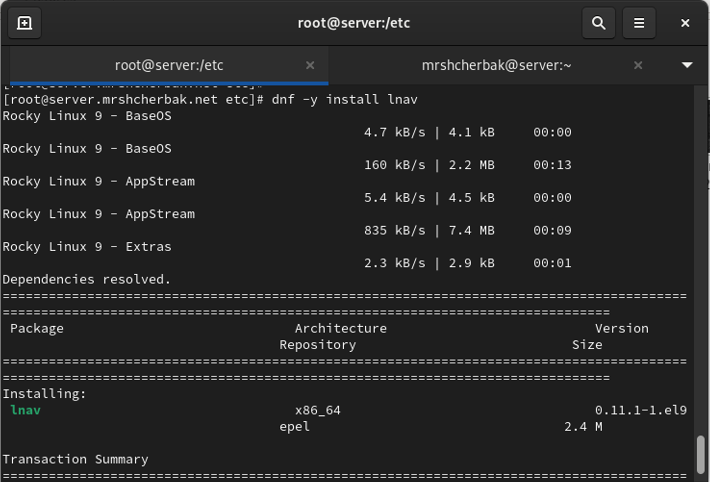


Рис.3.3. Установка просмотрщика журналов системных сообщений

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

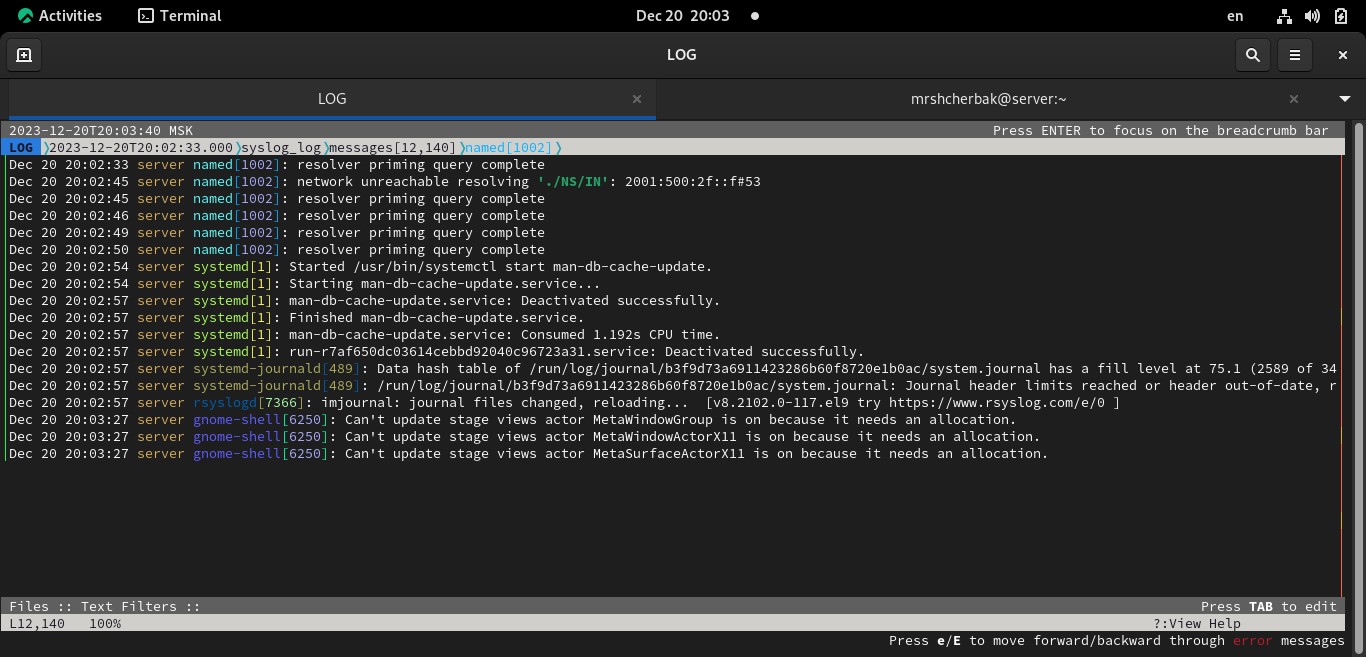


Рис.3.4. Просмотр логов

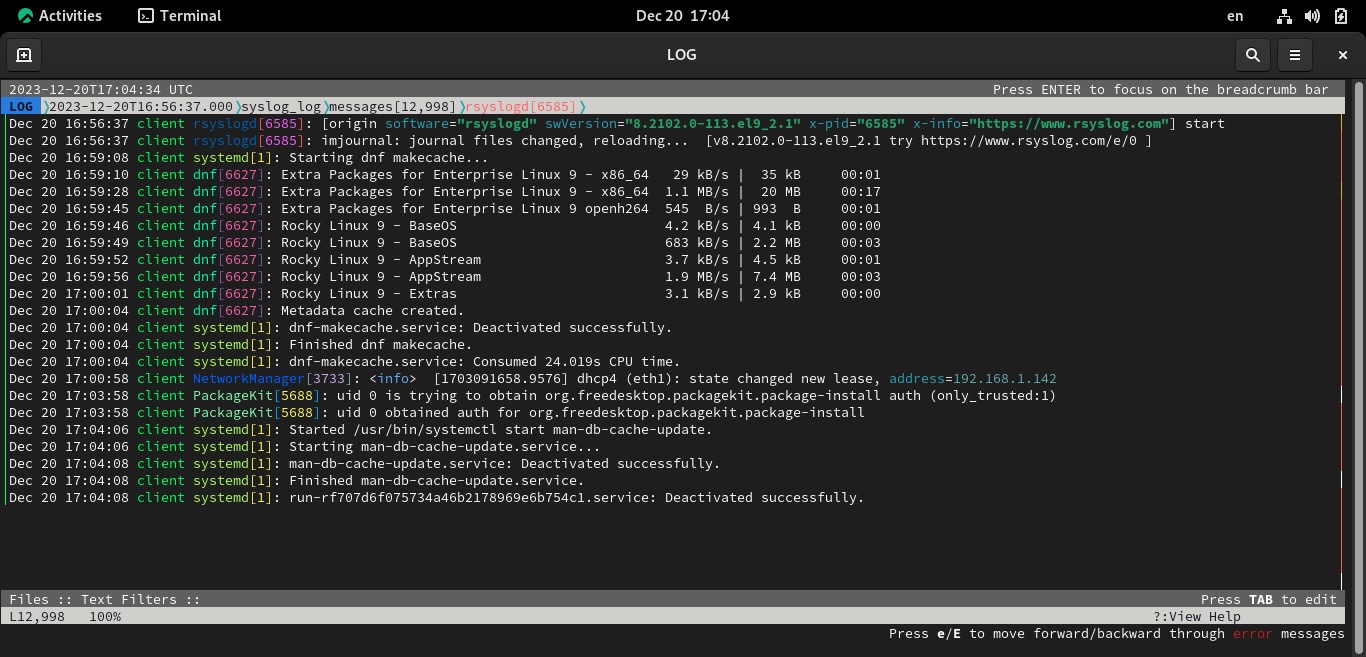


Рис.3.5. Просмотр логов

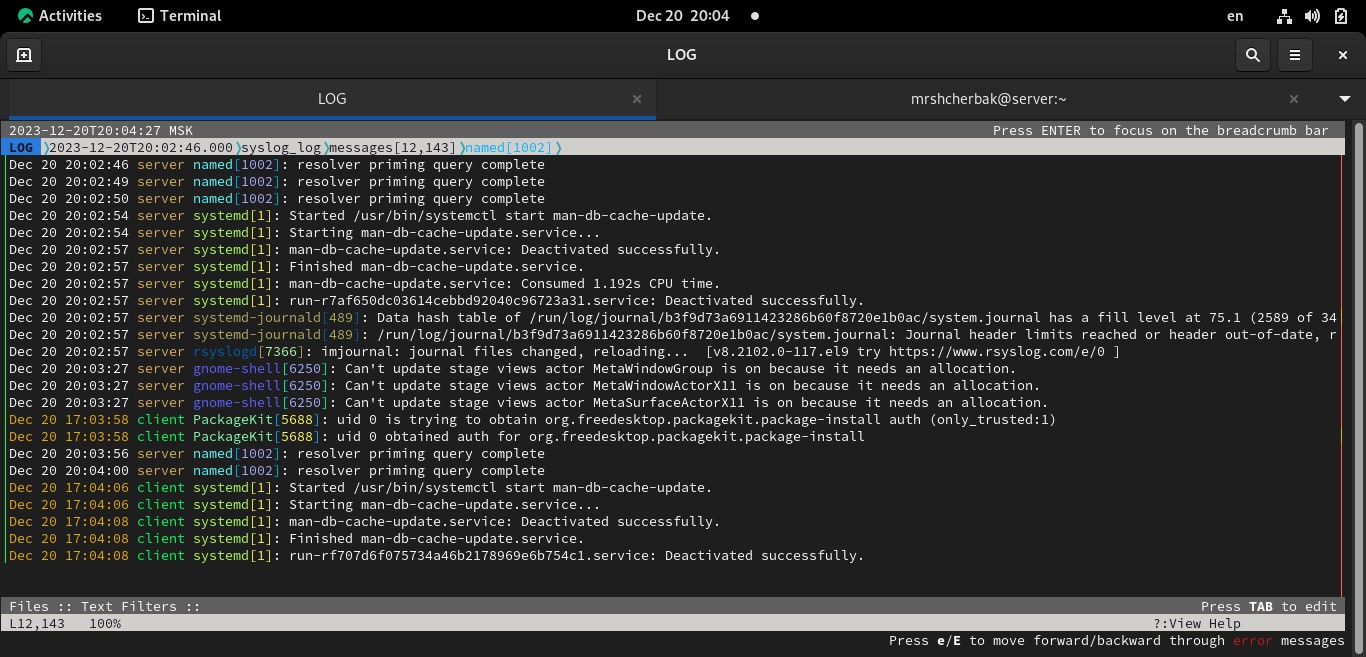


Рис.3.6. Просмотр логов

**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.

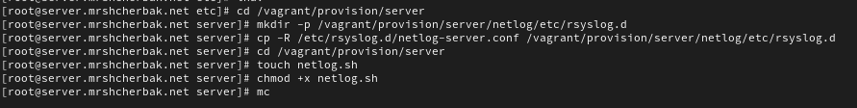


Рис.4.1. Выполнение команд

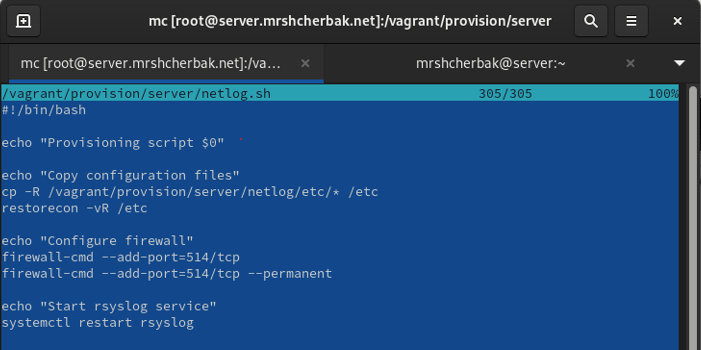


Рис.4.2. Содержимое файла netlog.sh на сервере

2. На виртуальной машине client перешла в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создала в нём каталог nentlog, 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.

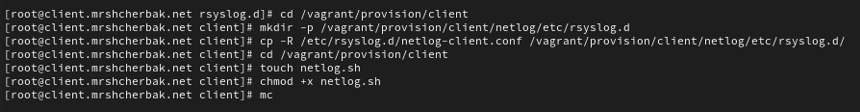


Рис.4.3. Выполнение команд

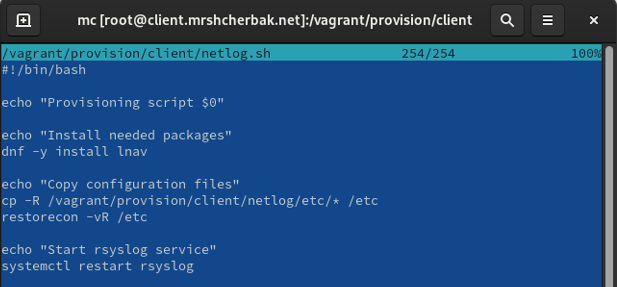


Рис.4.4. Содержимое файла netlog.sh на клиенте

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).

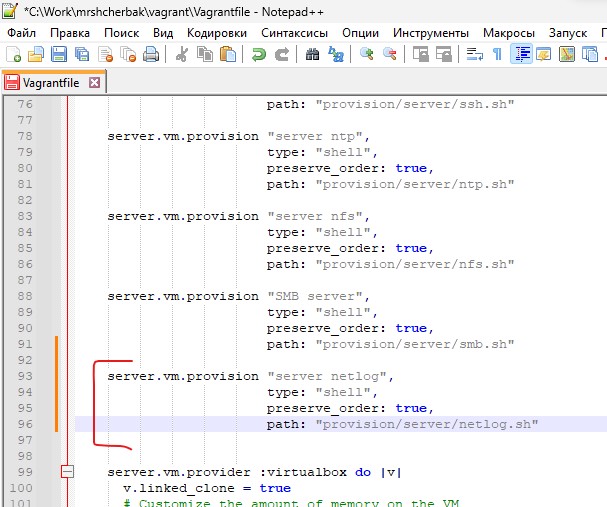


Рис.4.5. Содержимое файла Vagrantfile

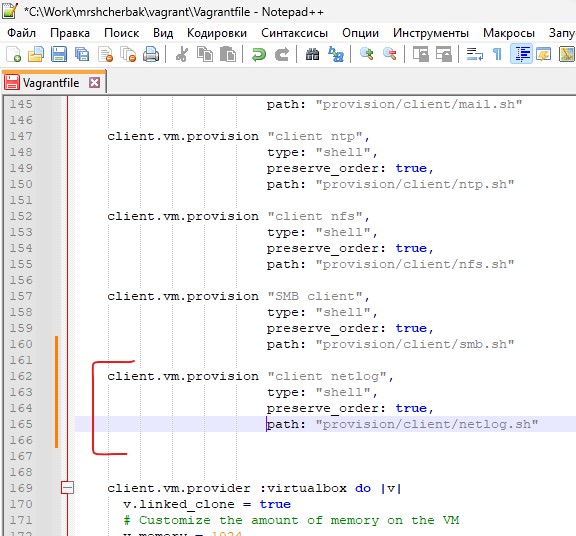


Рис.4.6. Содержимое файла Vagrantfile

**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.

1. 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.

1. 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.

1. 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.

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

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

/etc/systemd/journald.conf

ForwardToSyslog=yes

1. 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

1. 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

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

$ModLoad imtcp

$InputTCPServerRun 514

1. 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.

