РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

ОТЧЕТ

по лабораторной работе № 15

**«Настройка сетевого журналирования»**

Дисциплина: Администрирование сетевых подсистем

Студент: Карташова А.С.

Группа: НФИбд-03-18

**МОСКВА**

2020 г.

**Оглавление**

[Цель работы 2](#_Toc61024000)

[Задачи 2](#_Toc61024001)

[Ход работы 2](#_Toc61024002)

[Настройка сервера сетевого журнала 2](#_Toc61024003)

[Настройка клиента сетевого журнала 4](#_Toc61024004)

[Просмотр журнала 4](#_Toc61024005)

[Внесение изменений в настройки внутреннего окружения виртуальных машин 6](#_Toc61024006)

[Заключение 8](#_Toc61024007)

[Контрольные вопросы 8](#_Toc61024008)

# Цель работы

Получение навыков по работе с журналами системных событий.

# Задачи

1. Настроить сервер сетевого журналирования событий

2. Настроить клиент для передачи системных сообщений в сетевой журнал насервере

3. Просмотреть журналы системных событий с помощью нескольких программ

4. Написать скрипты для Vagrant, фиксирующие действия по установке и настройке сетевого сервера журналирования

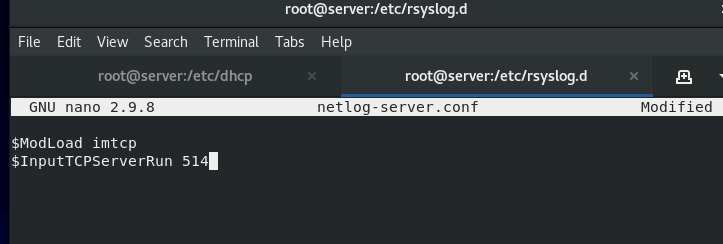
# Ход работы

## Настройка сервера сетевого журнала

На сервере создадим файл конфигурации сетевого хранения журналов:

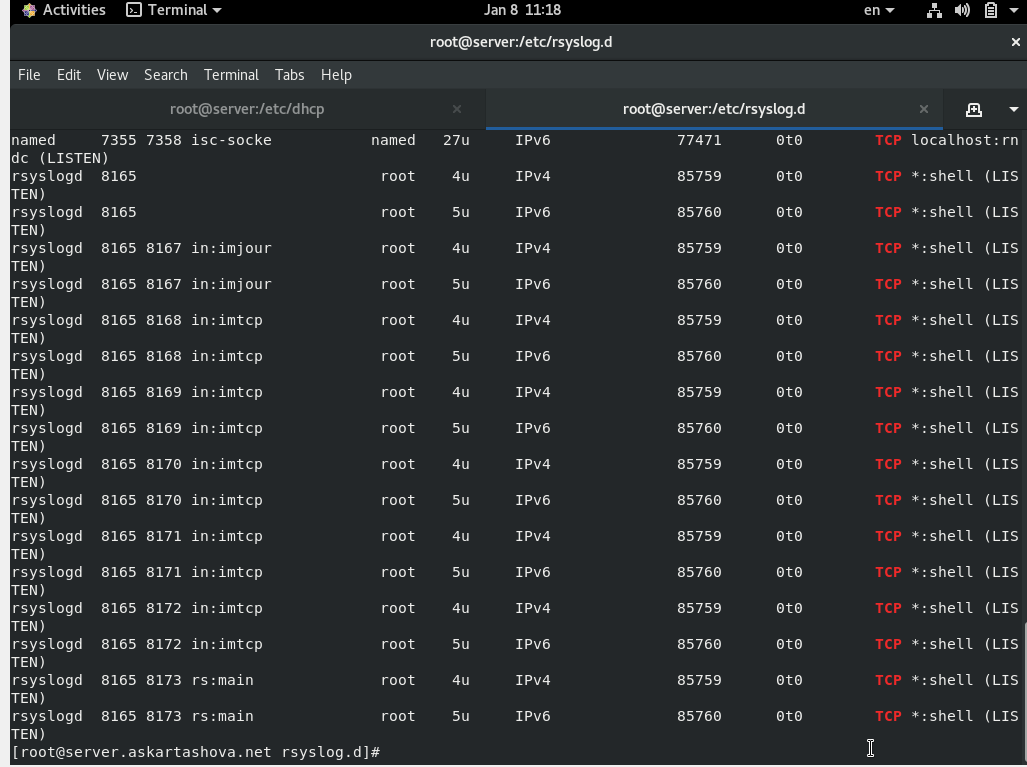
В файле конфигурации /etc/rsyslog.d/netlog-server.conf включим приём за-

писей журнала по TCP-порту 514:

****

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

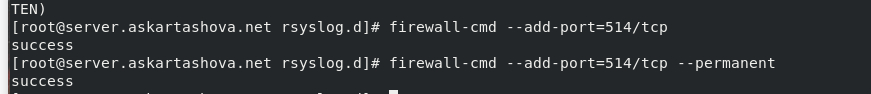
**Команды**: *systemctl restart rsyslog*

*lsof | grep TCP*

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

**Команды:** *firewall-cmd --add-port=514/tcp*

*firewall-cmd --add-port=514/tcp –permanent*

**

## Настройка клиента сетевого журнала

На клиенте создадим файл конфигурации сетевого хранения журналов:

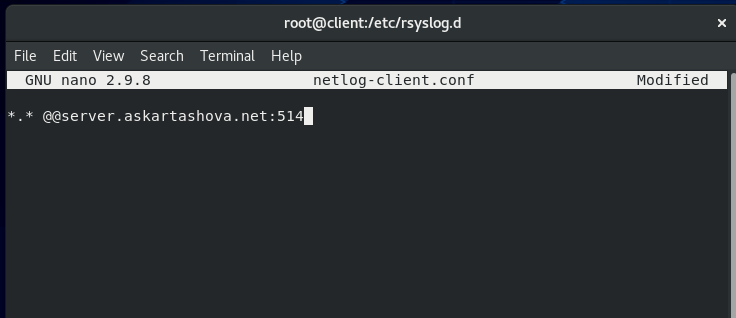
**Команды:** *cd /etc/rsyslog.d*

*touch netlog-client.conf*

**

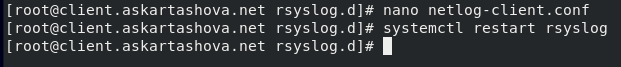
На клиенте в файле конфигурации /etc/rsyslog.d/netlog-client.conf включим перенаправление сообщение журнала на 514 TCP-порт

*\*.\* @@server.user.net:514*

**

Перезапустим службу rsyslog:

**Команда:** *systemctl restart rsyslog*

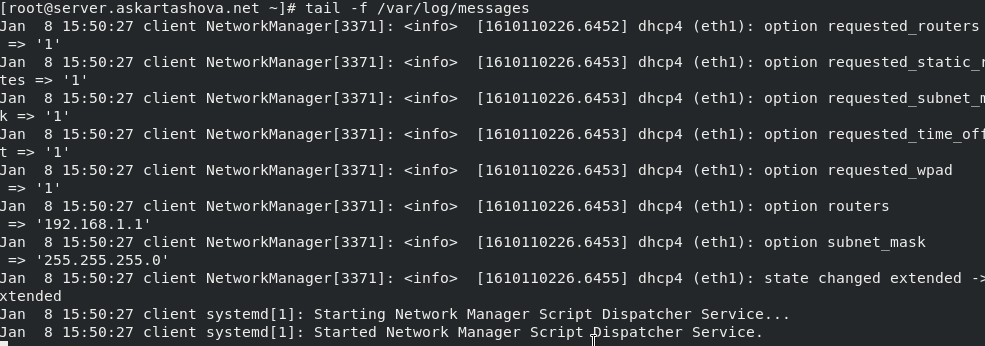


## Просмотр журнала

На сервере откроем еще одно окно терминала и просмотрим один из файлов журнала

**Команда:**  *tail -f /var/log/messages*

Обратим внимание, чо имя хоста client.



На сервере запустим графическую программу для просмотра журналов:

**Команда:**  *gnome-system-log (не получилось установить)*

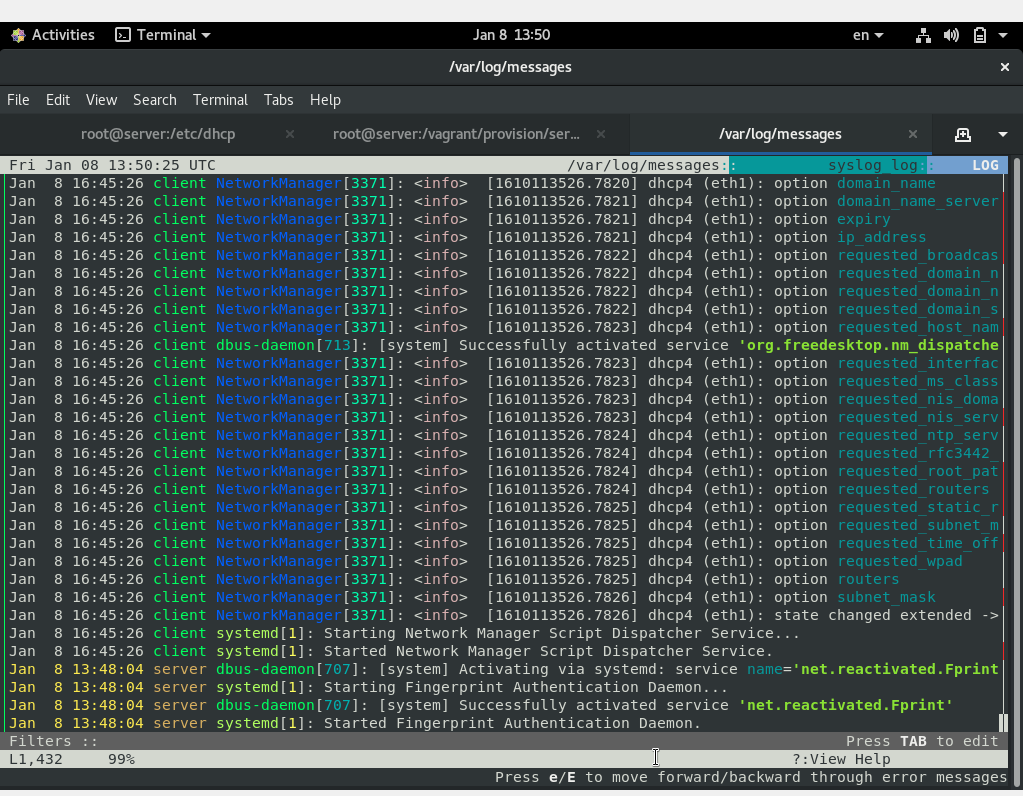
На сервере установим просмотрщик журналов системных сообщений lnav:

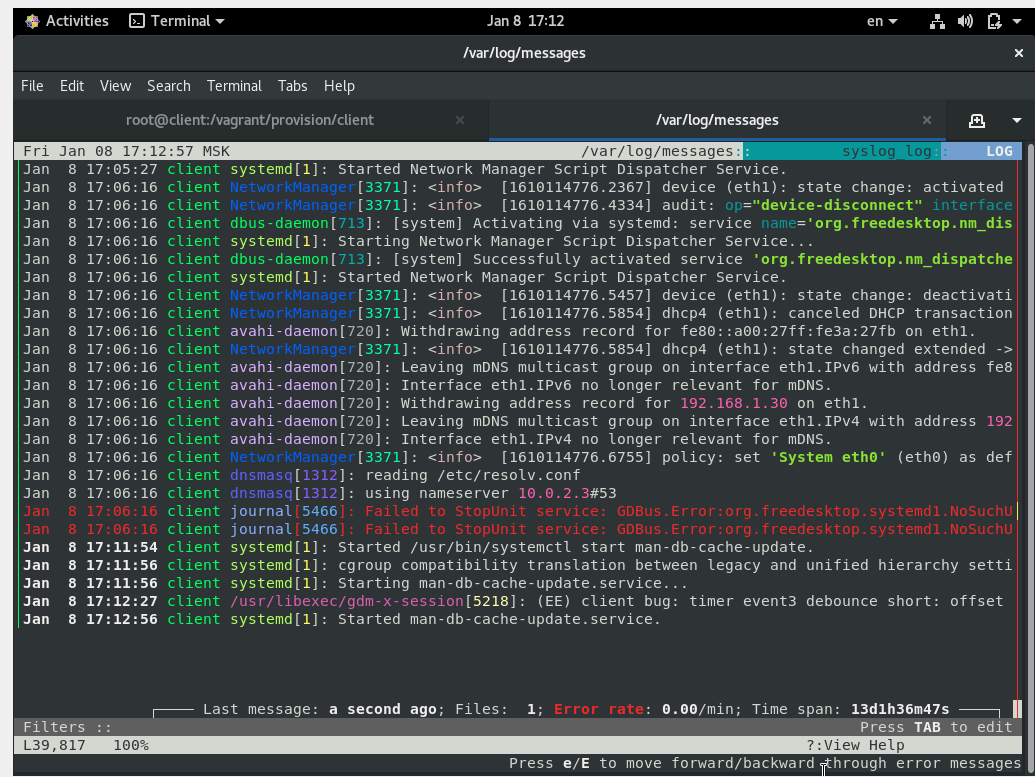
**Команда:** *dnf -y install lnav*

Просмотрим логи с помощью lnav:

**Команда:** *lnav*

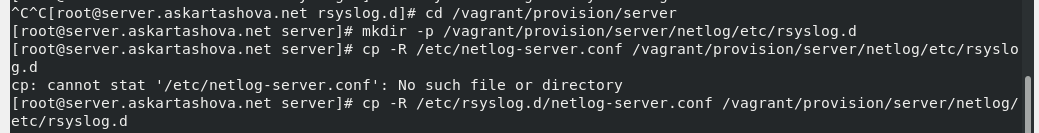
Просмотрим записи с сервера и клиента.





## Внесение изменений в настройки внутреннего окружения виртуальных машин

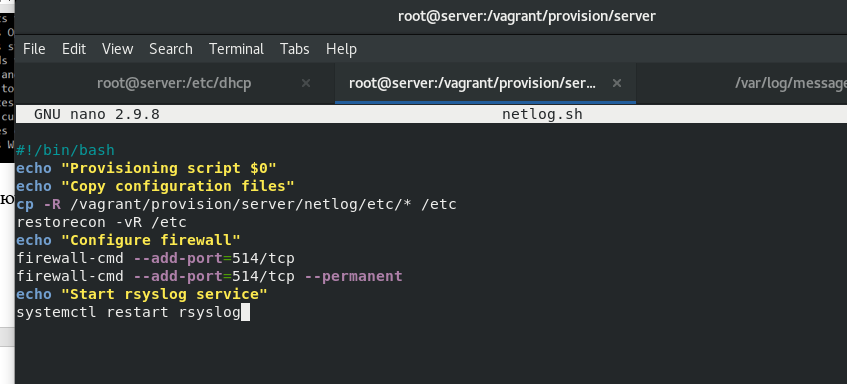
На виртуальной машине server перейдем в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создадим в нём каталог netlog, в который поместите в соответствующие подкаталоги конфигурационные файлы:



В каталоге /vagrant/provision/server создадим исполняемый файл netlog.sh,

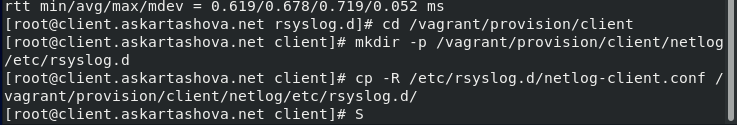
открыв его на редактирование, пропишем в нём следующий скрипт





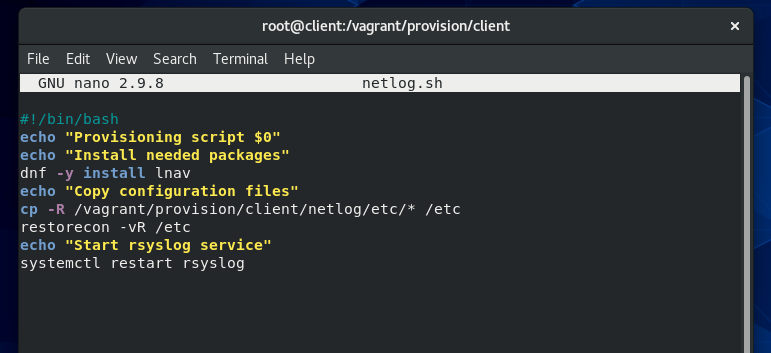
На виртуальной машине client перейдитем в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создадим в нём

каталог nentlog, в который поместим в соответствующие подкаталоги конфигурационные файлы

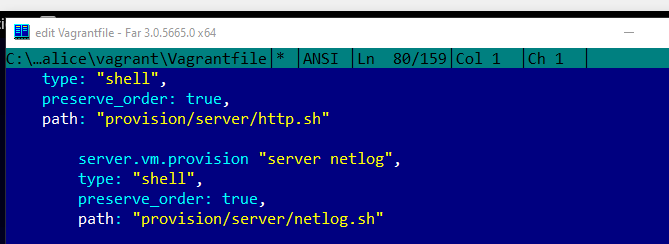


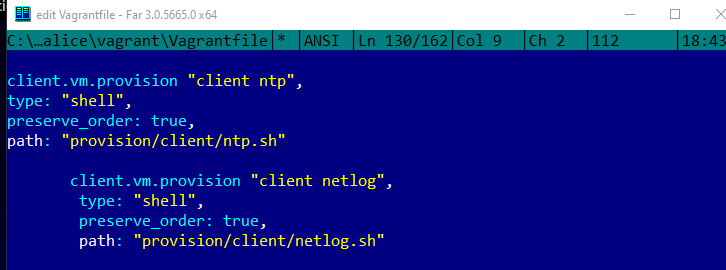
В каталоге /vagrant/provision/client создадим исполняемый файл netlog.sh:





Для отработки созданных скриптов во время загрузки виртуальных машин server и client в конфигурационном файле Vagrantfile необходимо добавим в соответствующих разделах конфигураций для сервера и клиента:





# Заключение

Мы приобрели навыки нпо работе с журналами системных событий

# Контрольные вопросы

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

Модулm imjournal был специально разработан для интеграции rsyslogd и journald.

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

Модуль imuxsock

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

В rsyslog.conf для правильной обработки приема журнала необходимы две строки: В rsyslog.conf для правильной обработки приема журнала необходимы две строки:

*$OmitLocalLogging on*

*$IMJournalStateFile imjournal.state*

Первая отключает прием логов через модуль imuxsocks. Вторая строка определяет имя файла состояния, который rsyslogd использует для отслеживания состояния синхронизации между rsyslogd и journald.

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

Файл /etc/rsyslog.conf.

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

файл /etc/systemd/journald.conf должен содержать строку ForwardToSyslog= yes

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

**Модуль:** *imjournal.*

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

**Модуль:** *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?

*firewall-cmd --add-port=514/tcp*

*firewall-cmd --add-port=514/tcp --permanen*