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: Ким Реачна

Группа: НПИбд 02-20

Студенческий билет: 1032205204

**МОСКВА**

2022 г.

**Цель работы:**

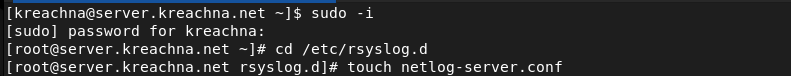
Получение навыков по работе с журналами системных событий.

**Выполнение работы:**

1. **Настройка сервера сетевого журнала**
2. На сервере создайте файл конфигурации сетевого хранения журналов:

cd /etc/rsyslog.d

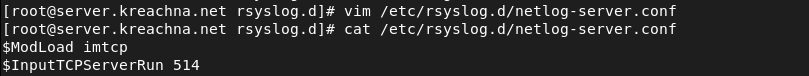
touch netlog-server.conf



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

$ModLoad imtcp

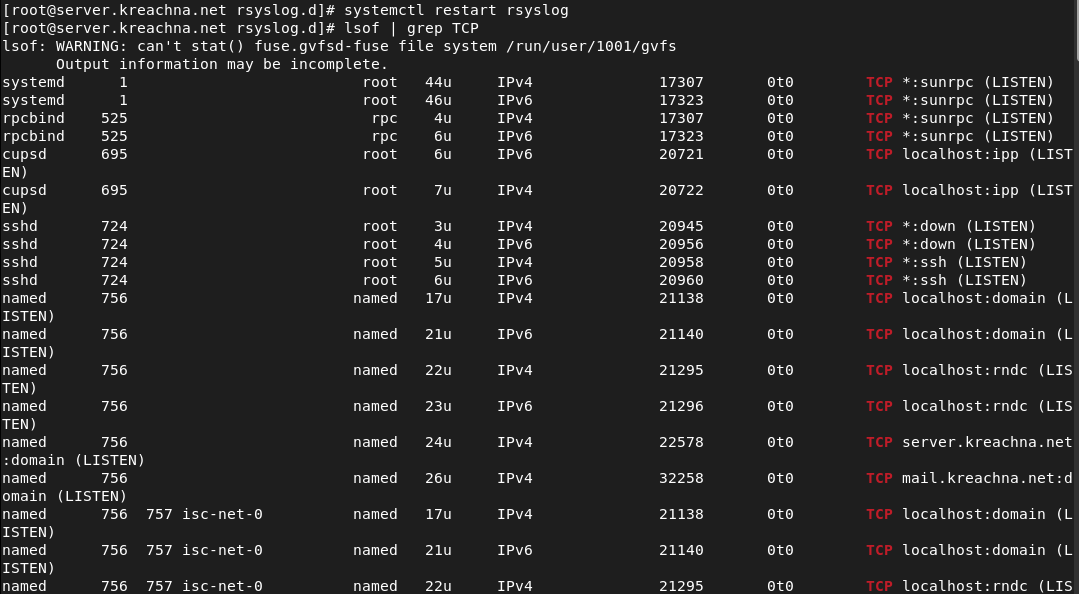
$InputTCPServerRun 514

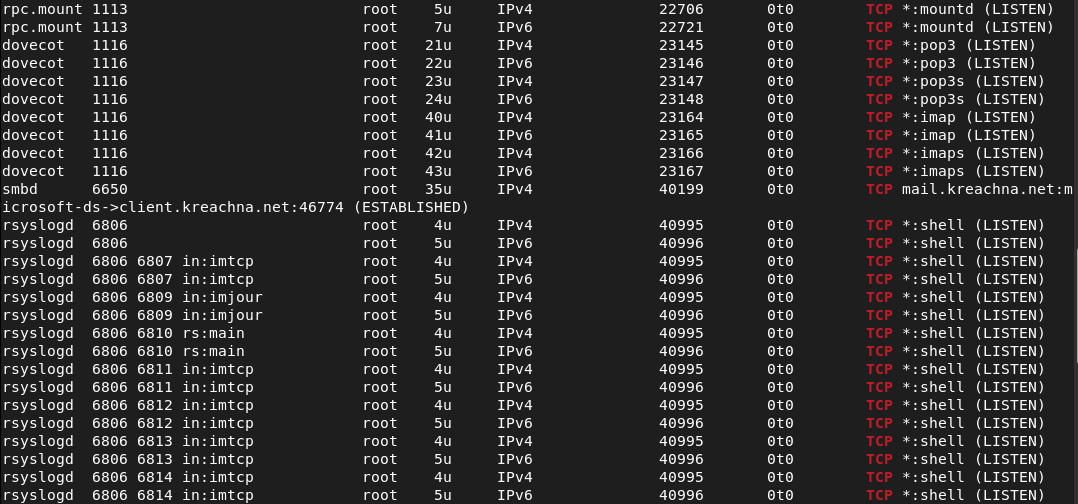


1. Перезапустите службу rsyslog и посмотрите, какие порты, связанные с rsyslog, прослушиваются:

systemctl restart rsyslog

lsof | grep TCP

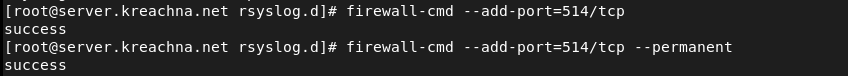




1. На сервере настройте межсетевой экран для приёма сообщений по TCP-порту 514:

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

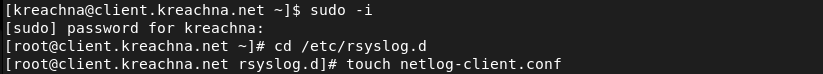
firewall-cmd --add-port=514/tcp –permanent



1. **Настройка клиента сетевого журнала**
2. На клиенте создайте файл конфигурации сетевого хранения журналов:

cd /etc/rsyslog.d

touch netlog-client.conf



1. На клиенте в файле конфигурации /etc/rsyslog.d/netlog-client.conf включите перенаправление сообщений журнала на 514 TCP-порт сервера (вместо user укажите свой логин):

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



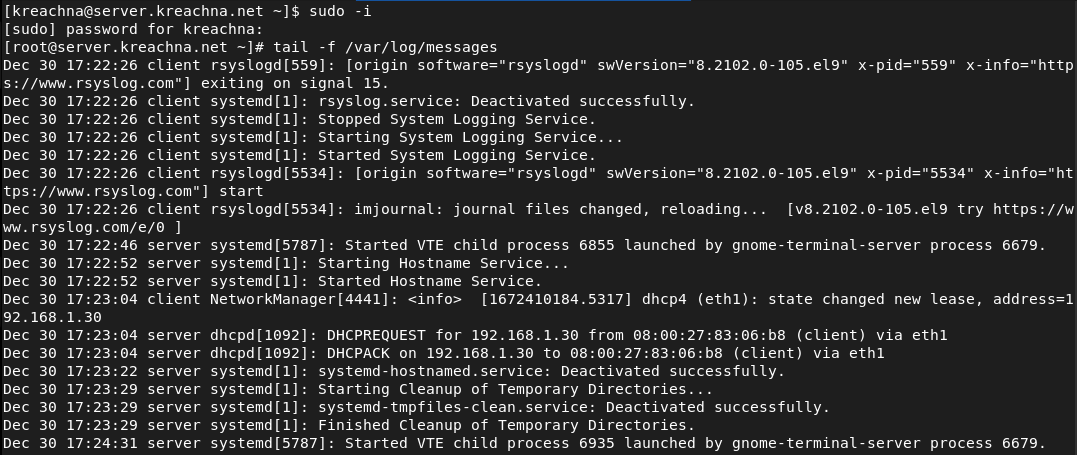
1. Перезапустите службу rsyslog:

systemctl restart rsyslog



1. **Просмотр журнала**
2. На сервере просмотрите один из файлов журнала

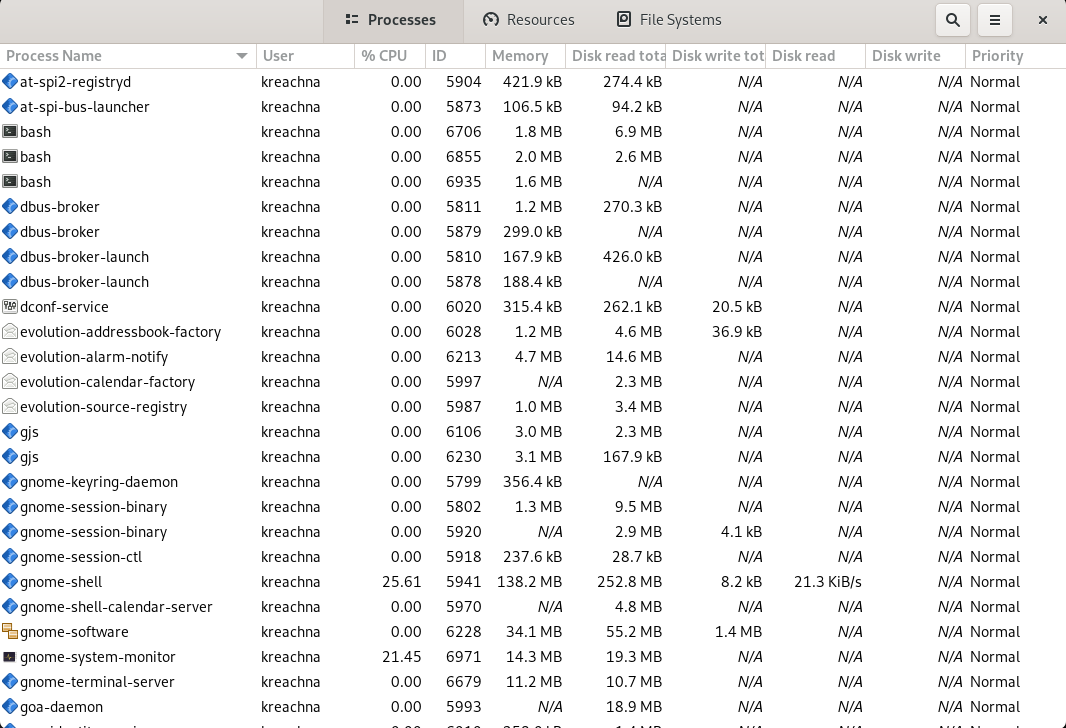
tail -f /var/log/messages



Обратите внимание на имя хоста.

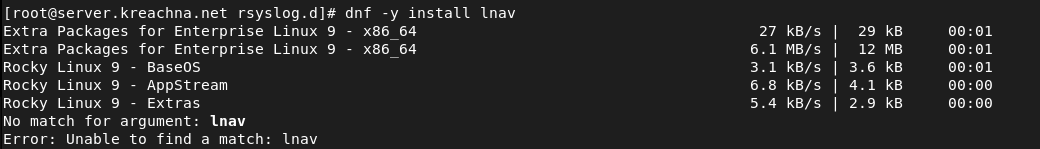
1. На сервере под пользователем user (вместо user укажите свой логин) запустите графическую программу для просмотра журналов:

gnome-system-monitor



1. На сервере установите просмотрщик журналов системных сообщений lnav:

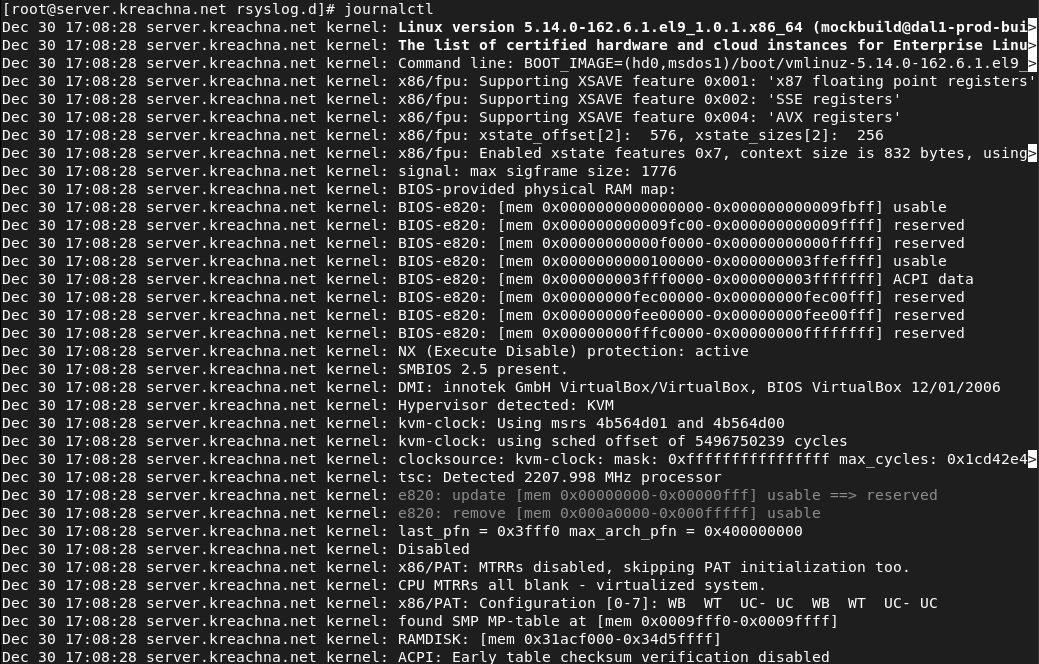
dnf -y install lnav

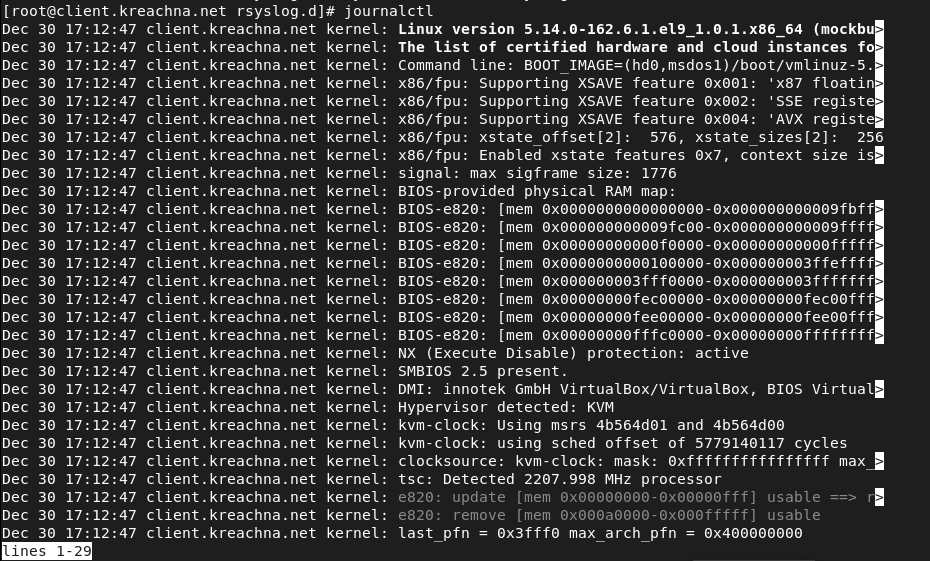


1. Просмотрите логи с помощью lnav:

lnav

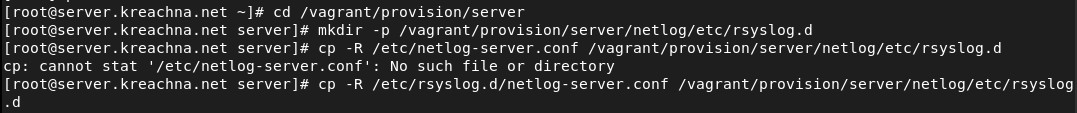






Просмотрите записи с сервера и клиента.

1. **Внесение изменений в настройки внутреннего окружения виртуальных машин**
2. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создайте в нём каталог netlog, в который поместите в соответствующие подкаталоги конфигурационные файлы:

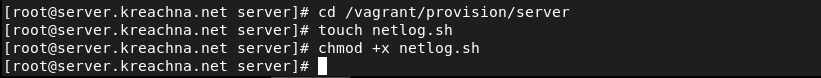


1. В каталоге /vagrant/provision/server создайте исполняемый файл netlog.sh:

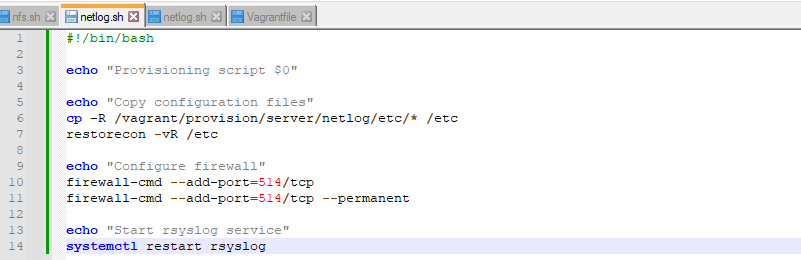
cd /vagrant/provision/server

touch netlog.sh

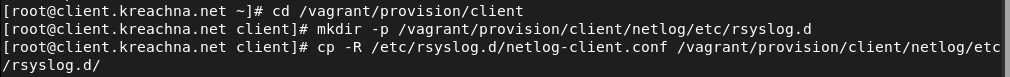
chmod +x netlog.sh



Открыв его на редактирование, пропишите в нём следующий скрипт:



1. На виртуальной машине client перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создайте в нём каталог nentlog, в который поместите в соответствующие подкаталоги конфигурационные файлы:

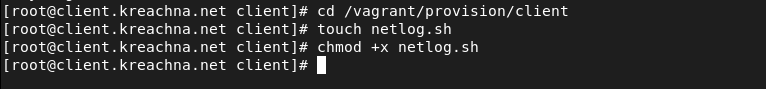


1. В каталоге /vagrant/provision/client создайте исполняемый файл netlog.sh:

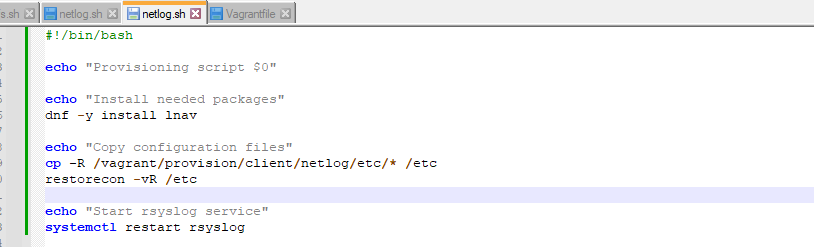
cd /vagrant/provision/client

touch netlog.sh

chmod +x netlog.sh

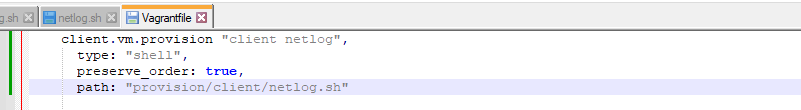


Открыв его на редактирование, пропишите в нём следующий скрипт:



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





**Ответы на контрольные вопросы**

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

imjournal

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

imuxsock

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

$OmitLocalLogging on – данная строка отключает прием логов через модуль imuxsock.

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

Все настройки rsyslog находятся в файле /etc/rsyslog.conf.

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

Journald отправляет сообщения в rsyslog по умолчанию. Об этом заботятся две части конфигурации. Во-первых, файл /etc/systemd/journald.conf содержит строку ForwardToSyslog, которая по умолчанию имеет значение yes. Вовторых rsyslog.conf содержит модуль imjournal, необходимый для получения сообщений из journald.

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

imfile - модуль ввода текстовых файлов

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

ommysql

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

$ModLoad imtcp и $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 --permanent

**Вывод:**

Получила навыков по работе с журналами системных событий.