Отчёт по лабораторной работе №15

Администрирование сетевых подсистем

Ищенко Ирина НПИбд-02-22

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получение навыков по работе с журналами системных событий.

2 Выполнение лабораторной работы

2.1 Настройка сервера сетевого журнала

На сервере создаем файл конфигурации сетевого хранения журналов: cd /etc/rsyslog.d и touch netlog-server.conf.

В данном файле включаем прием записей журнала по TCP-порту 514 (рис. 2.1).

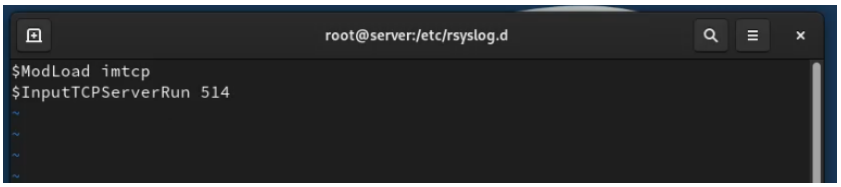

Рис. 2.1: Редактирование файла конфигурации сетевого хранения журналов `/etc/rsyslog.d/netlog-server.conf`

Перезапускаем службу `rsyslog` - systemctl restart rsyslog и просматриваем прослушиваемые порты, которые связаны со службой - lsof | grep TCP (рис. 2.2).

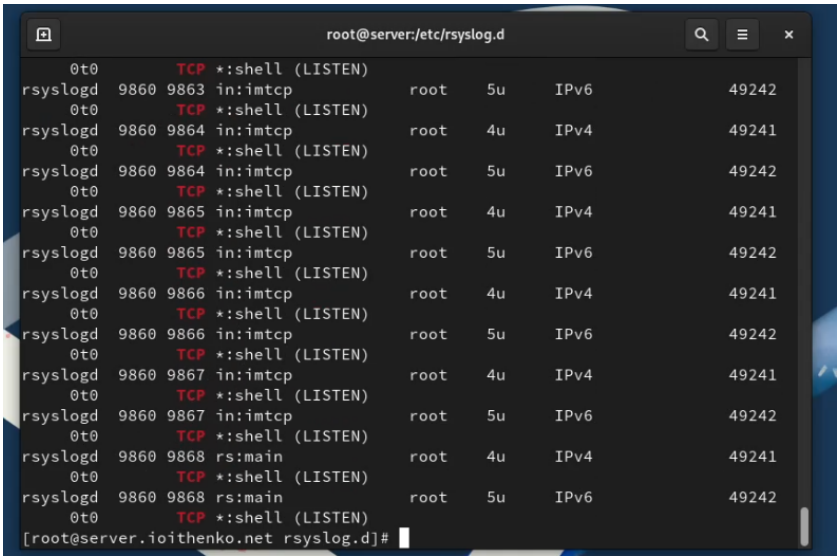

Рис. 2.2: Перезапуск `rsyslog` и просмотр прослушиваемых портов

На сервере настраиваем межсетевой экран для работы с TCP-портом 514 (рис. 2.3).

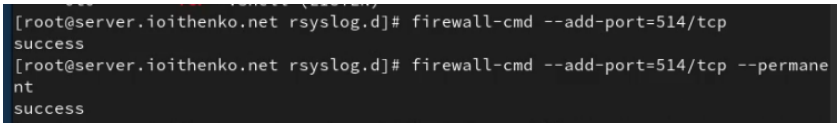

Рис. 2.3: Настройка межсетевого экрана для работы с TCP-портом 514

2.2 Настройка клиента сетевого журнала

На клиенте создаем файл конфигурации сетевого хранения журналов:

```
cd /etc/rsyslog.d
touch netlog-client.conf
```

В данном файле включаем перенаправление сообщений журнала на 514 TCP-порт сервера и перезапускаем службу (рис. 2.4).

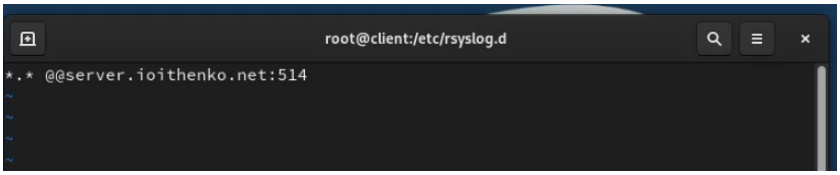

Рис. 2.4: Редактирование файла конфигурации сетевого хранения журналов на клиенте: включение перенаправления на 514 порт

2.3 Просмотр журнала

На сервере просматриваем один из файлов журнала. Обращаем внимание, что выводятся сообщения как с сервера, так и с клиента (рис. 2.5).

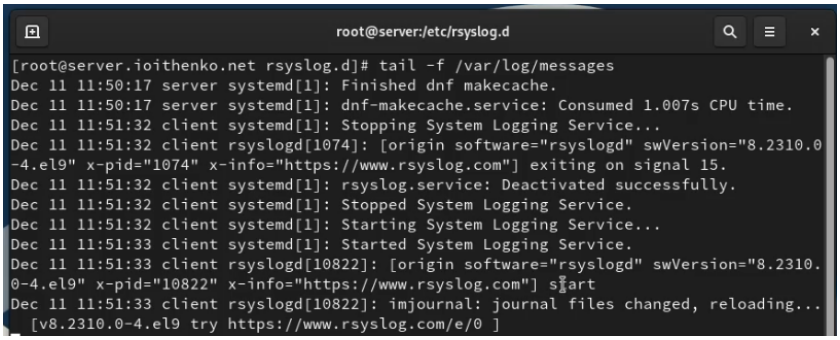

Рис. 2.5: Просмотр файла журнала на сервере

На сервере под пользователем `ioithenko` запускаем графическую программу для просмотра журналов (рис. 2.6).

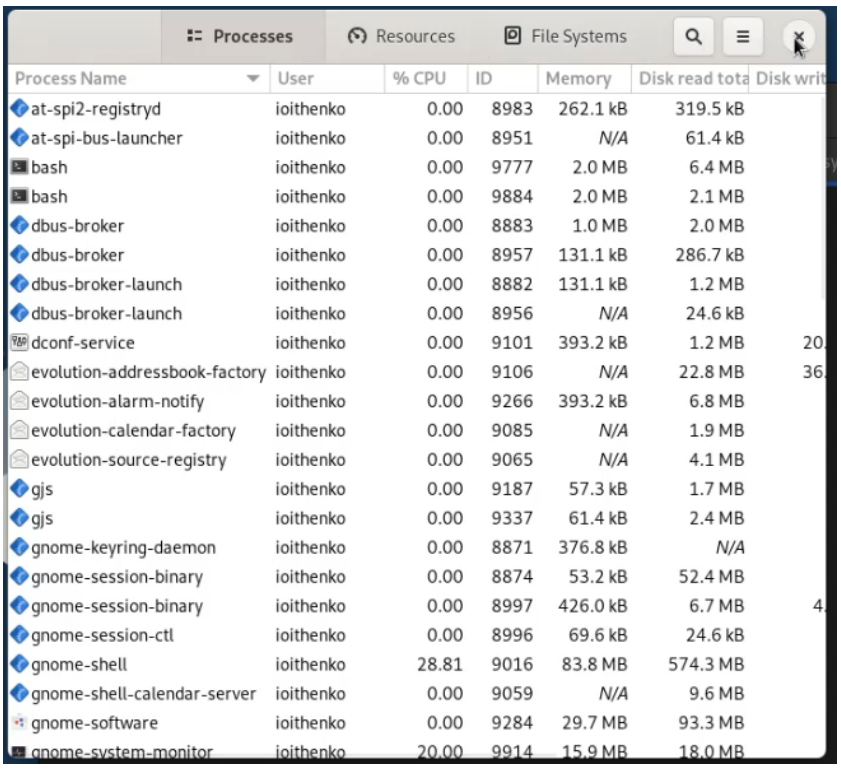

Рис. 2.6: Запуск графической программы для просмотра журналов

Устанавливаем просмотрщик журналов системных событий `lnav`: dnf -y install lnav.

Используем `lnav` для просмотра логов (рис. 2.7).

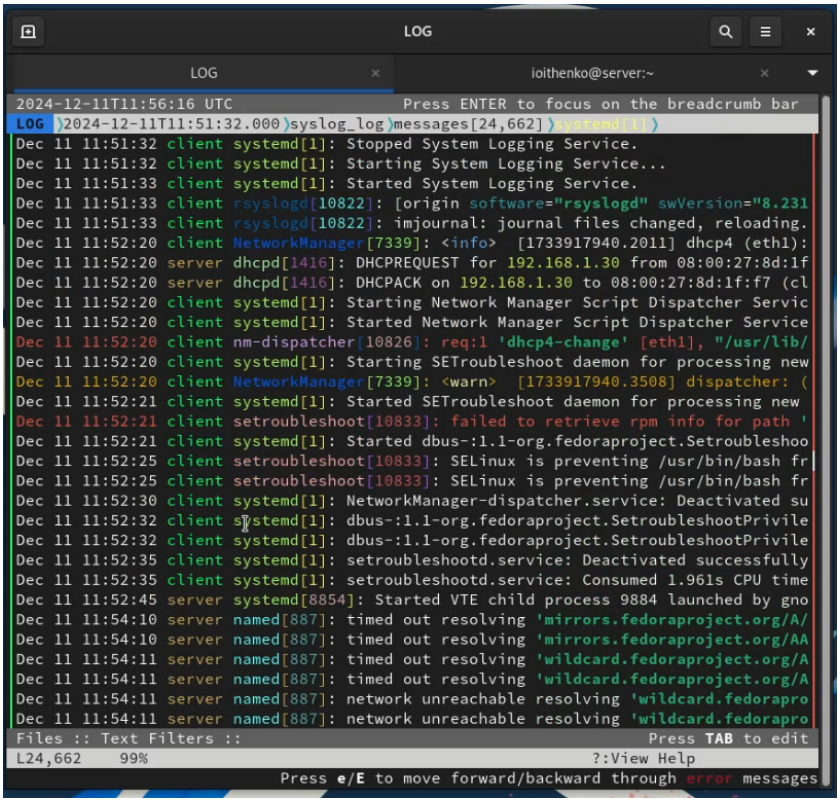

Рис. 2.7: Использование lnav для просмотра логов

2.4 Внесение изменений в настройки внутреннего окружения виртуальной машины

На ВМ server переходим в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/ и копируем в соответствующие каталоги конфигурационные файлы:

```
cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog.d
```

Вносим изменения в файл /vagrant/provision/server/netlog.sh.

На ВМ client переходим в каталог для внесения изменений в настройки внутреннего окружения и копируем в соответствующие каталоги конфигурационные

файлы:

```
cd /vagrant/provision/client
mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d
cp -R /etc/rsyslog.d/netlog-client.conf /vagrant/provision/client/netlog/etc/rsyslog.d
```

Создаем и редактируем скрипт /vagrant/provision/client/netlog.sh.

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

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

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

3 Выводы

В ходе выполнения лабораторной работы я приобрела навыки по работе с журналами системных событий.

4 Ответы на контрольные вопросы

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

Для приёма сообщений от journald следует использовать модуль imjournal.

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

imklog

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

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 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 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?

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