Лабораторная работа №15

Администрирование сетевых подсистем

Машков Илья Евгеньевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получение навыков по работе с журналами системных событий.

2 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.

3 Выполнение лабораторной работы

3.1 Настройка сервера сетевого журнала

На сервере создаю файл конфигурации сетевого журнала. В конфигурационном файле включаю приём записей журнала по TCP-порту 514 (рис. [3.1]).

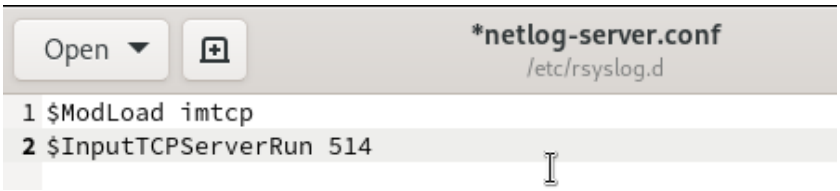

Рис. 3.1: Настройка приёма записей журнала по tcp:514

Перезапускаю службу rsyslog и смотрю, что прослушиваются нужные нам порты (рис. [3.2]).

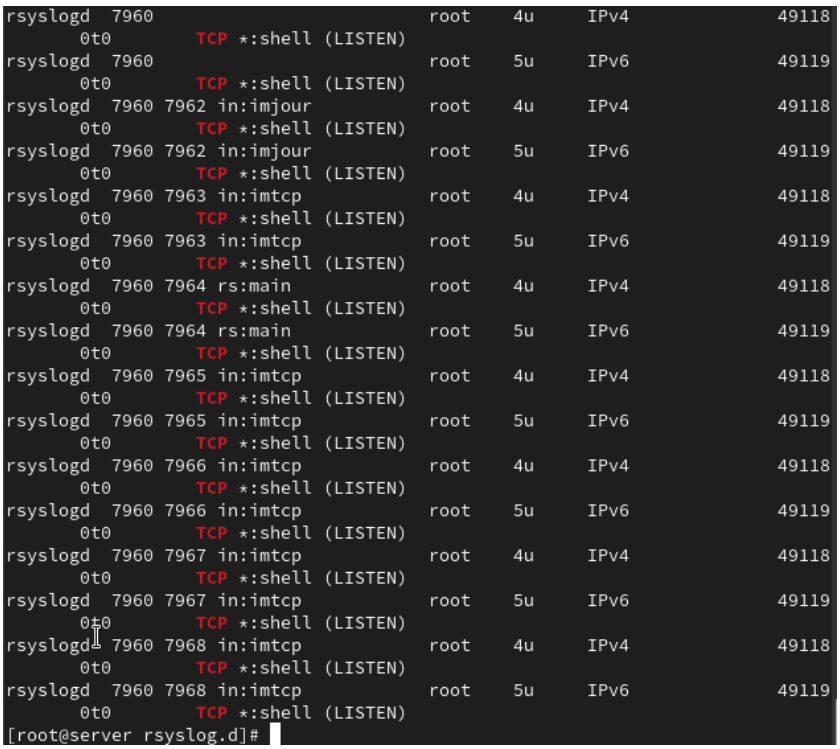

Рис. 3.2: Проверка прослушиваемых tcp портов

Настраиваю межсетевой экран на работу с приёмом записей по tcp-порту 514 (рис. [3.3]).

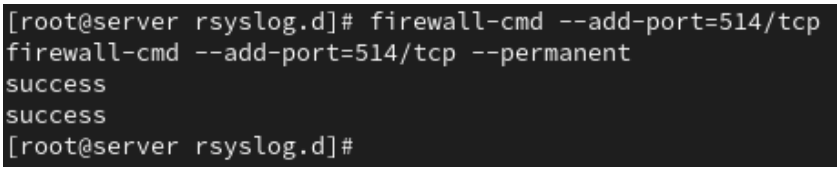

Рис. 3.3: Настройка межсетевого экрана на сервере

3.2 Настройка клиента сетевого журнала

Создаю файл netlog-client.conf на клиенте и включаю перенаправление сообщений журнала на tcp-порт 514, т.е. на порт сервера (рис. [3.4]). После этого перезагружаю службу rsyslog.

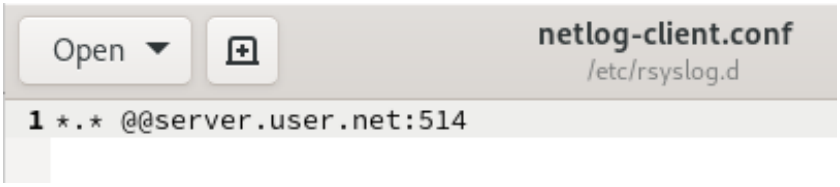

Рис. 3.4: netlog-client.conf на клиенте

3.3 Просмотр журнала

Запускаю лог файлов журнала и просматриваю его(рис. [3.5]).

Рис. 3.5: Лог файлов журнала

Запускаю программу для просмотра журналов под пользователем user (рис. [3.6]).

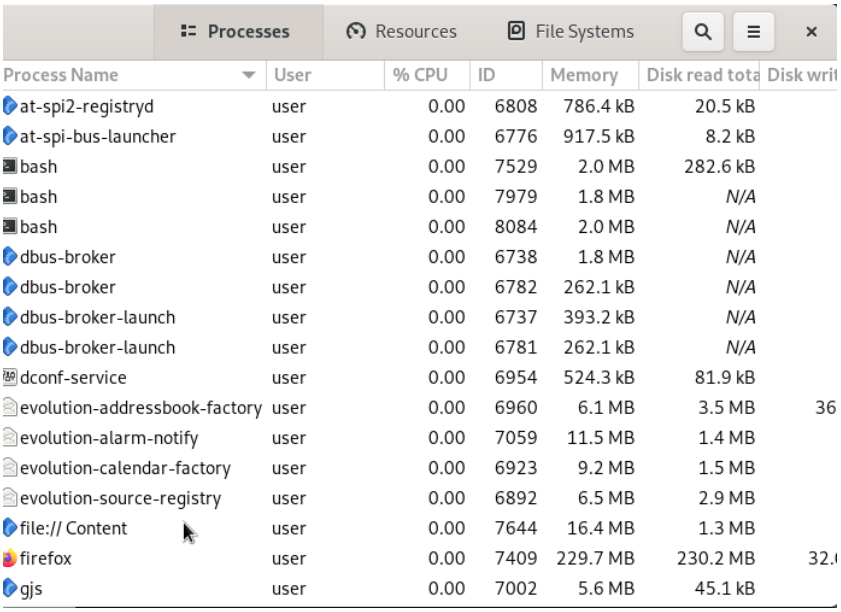

Рис. 3.6: Просмотр журналов пользователя user

Устанавливаю lnav на сервер (рис. [3.7]).

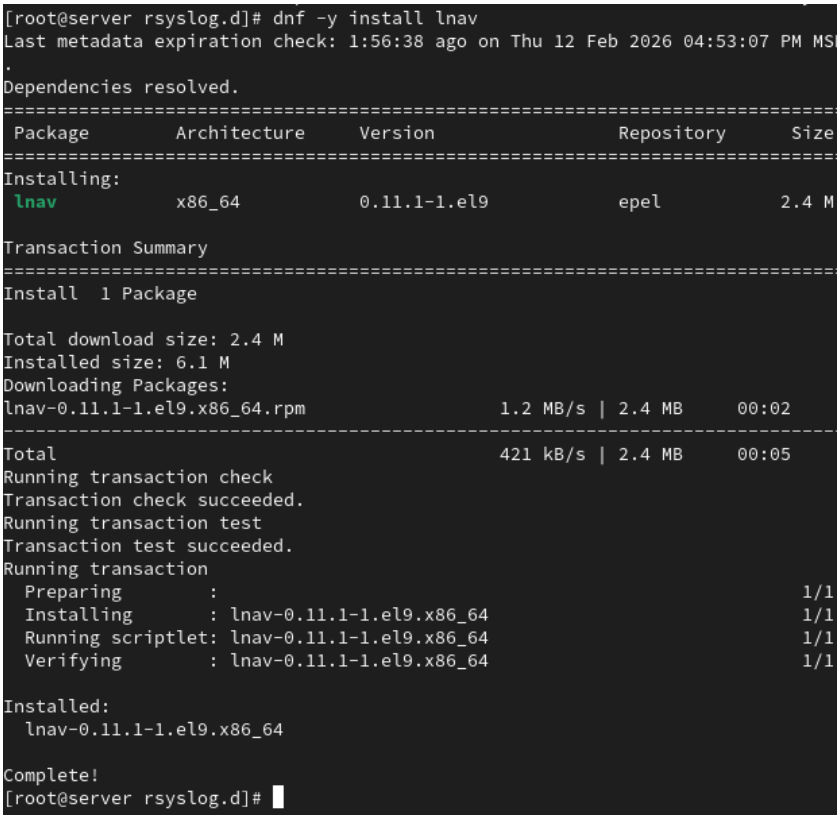

Рис. 3.7: Установка lnav на сервер

С помощью lnav просматриваю логи (рис. [3.8]).

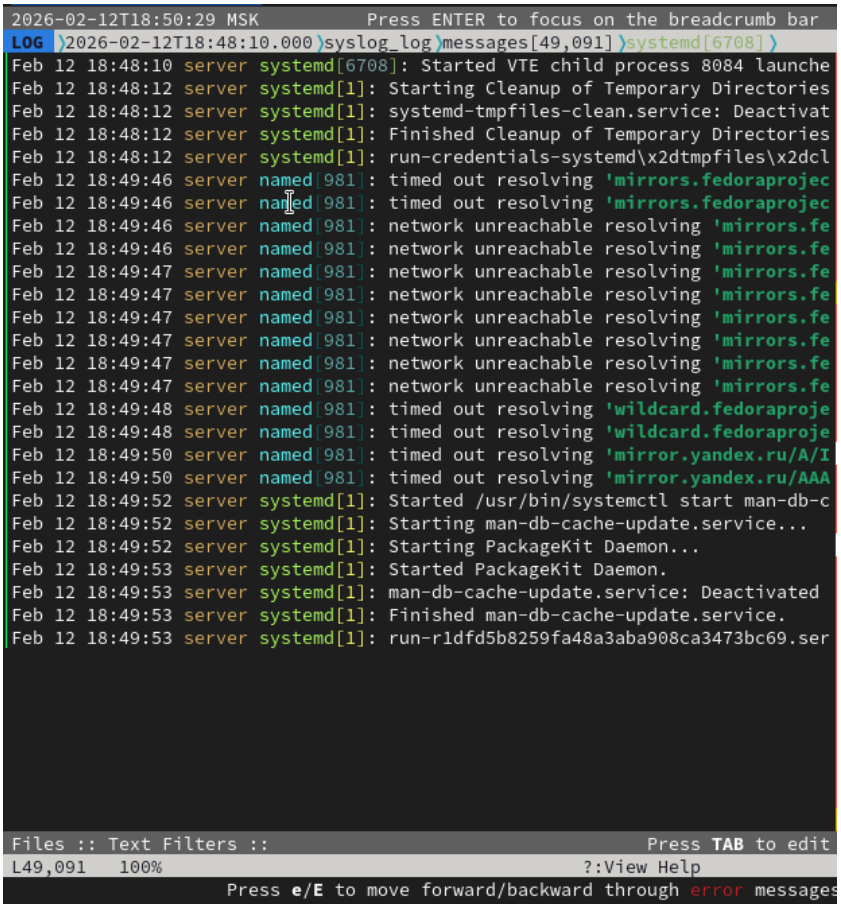

Рис. 3.8: Просмотр лого с помощью lnav

3.4 Внесение изменений в настройки внутреннего окружения виртуальных машин

Вношу копии изменённых конфигов в файлы настройки внутреннего окружения машины server(рис. [3.9]) и client (рис. [3.10]).

Рис. 3.9: Настройки внутреннего окружения машины server

```
[root@client rsyslog.d]# 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/r
syslog.d/
[root@client client]#
```

Рис. 3.10: Настройки внутреннего окружения машины client

Затем создаю скрипт netlog.sh, который повторяет ключевые действия, совершённые на машине server (рис. [3.11]) и client (рис. [3.12]), при каждом запуске этих систем.

Open

netlog.sh
/vagrant/provision/server

```
1  #!/bin/bash
2
3  echo "Provisioning script $0"
4
5  echo "Copy configuration files"
6  cp -R /vagrant/provision/server/netlog/etc/* /etc
7  restorecon -vR /etc
8
9  echo "Configure firewall"
10 firewall-cmd --add-port=514/tcp
11 firewall-cmd --add-port=514/tcp --permanent
12
13 echo "Start rsyslog service"
14 systemctl restart rsyslog
```

Рис. 3.11: netlog.sh на server

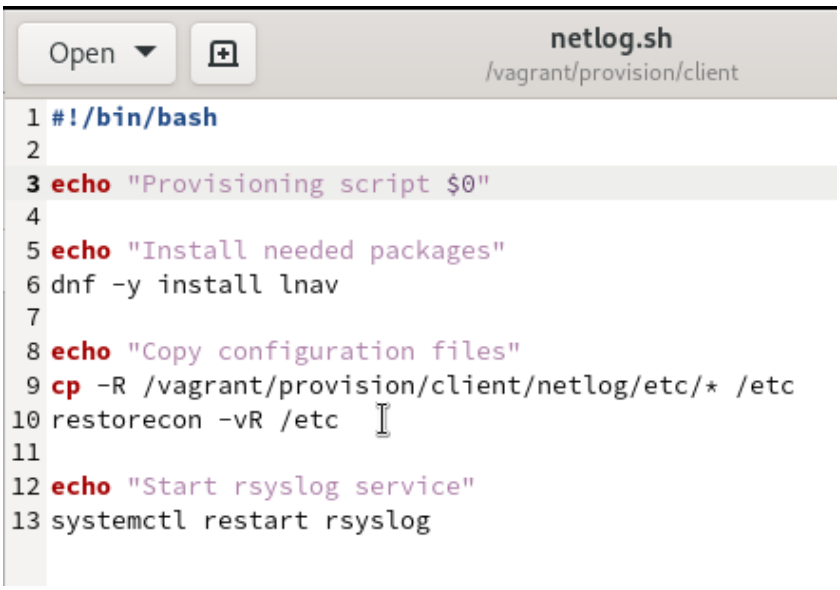

Рис. 3.12: netlog.sh на client

Для отработки скрипта вношу соответствующие изменения в Vagrantfile для server (рис. [3.13]) и client (рис. [3.14]).

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

Рис. 3.13: Правки в Vagrantfile для server

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

Рис. 3.14: Правки в Vagrantfile для client

4 Выводы

В процессе выполнения данной лабораторной работы я освоил навыки по работе с журналами системных событий.

Список литературы

Администрирование сетевых подсисем