Отчёт по лабораторной работе 15

Настройка сетевого журналирования

Метвалли Ахмед Фарг Набеех

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получение навыков по работе с журналами системных событий.

2 Выполнение

2.1 Настройка сервера сетевого журнала

2.1.1 Создание конфигурации сервера

1. На сервере создан файл конфигурации сетевого приёма журналов: переходим в каталог `/etc/rsyslog.d` и создаём файл `netlog-server.conf`.

2. В файл `/etc/rsyslog.d/netlog-server.conf` добавлены строки для включения TCP-приёма сообщений:
загрузка модуля imtcp и запуск TCP-сервера на порту 514.

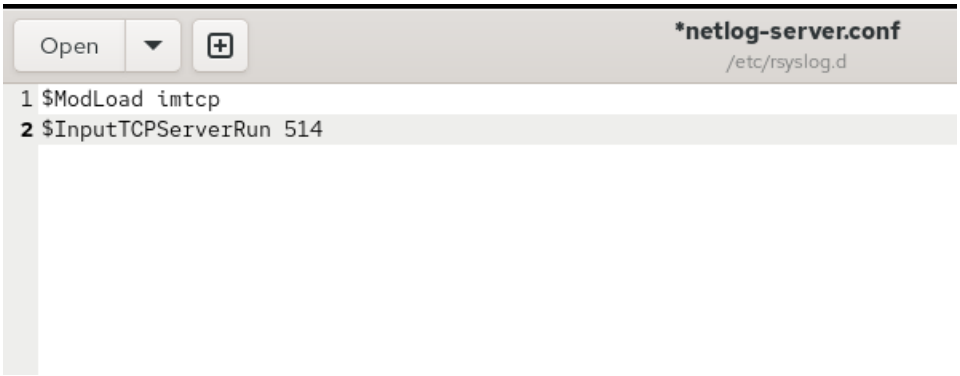


Рис. 2.1: Конфигурация netlog-server.conf

2.1.2 Перезапуск службы и проверка портов

1. Служба rsyslog перезапущена.

2. Выполнена проверка прослушиваемых портов, связанных с rsyslog. Видно, что процесс слушает TCP-порт 514.

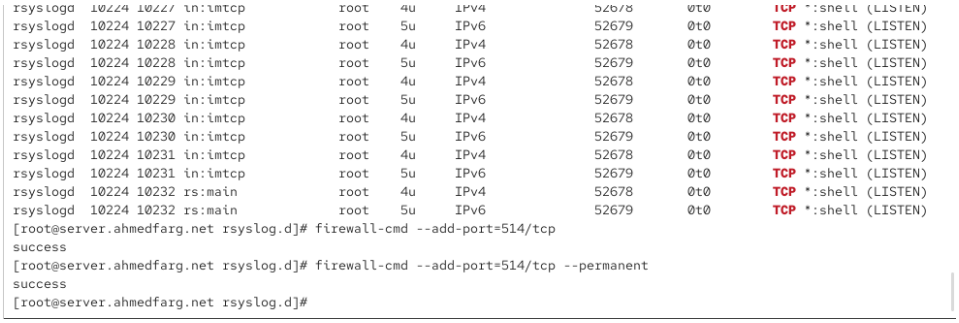


Рис. 2.2: Порты rsyslog и вывод команд firewall-cmd

2.1.3 Настройка межсетевого экрана

3. На сервере открыт TCP-порт 514 для приёма сообщений.

2.2 Настройка клиента сетевого журнала

1. На клиенте создан файл `/etc/rsyslog.d/netlog-client.conf`.

2. В конфигурацию добавлена строка перенаправления всех сообщений на сервер по TCP-порту 514:
   `*.* @@server.ahmedfarg.net:514`

Рис. 2.3: Конфигурация клиента netlog-client.conf

3. Служба rsyslog перезапущена.

2.3 Просмотр журнала

1. На сервере просмотрен файл `/var/log/messages`.

   В логах появляются сообщения от клиента.

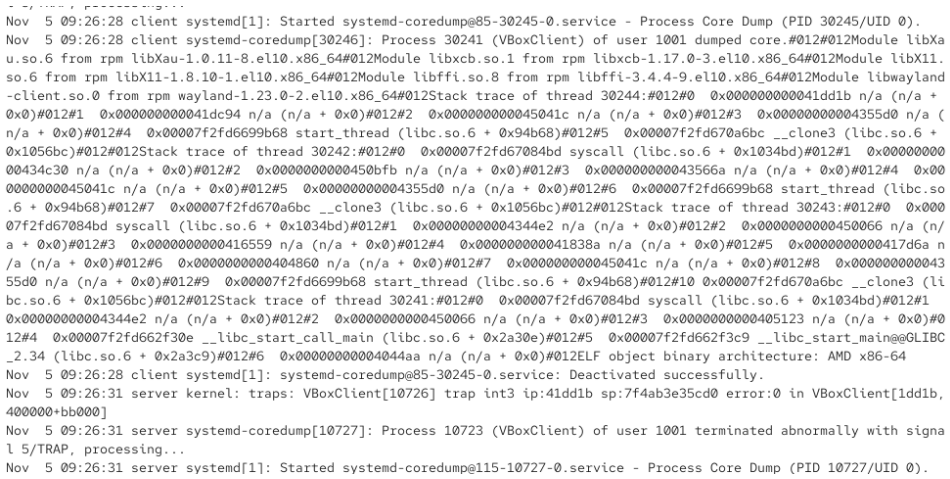


Рис. 2.4: Вывод системных сообщений

2. Запущена графическая программа для просмотра системных журналов.

   Показаны загрузка CPU, память и сетевые показатели.

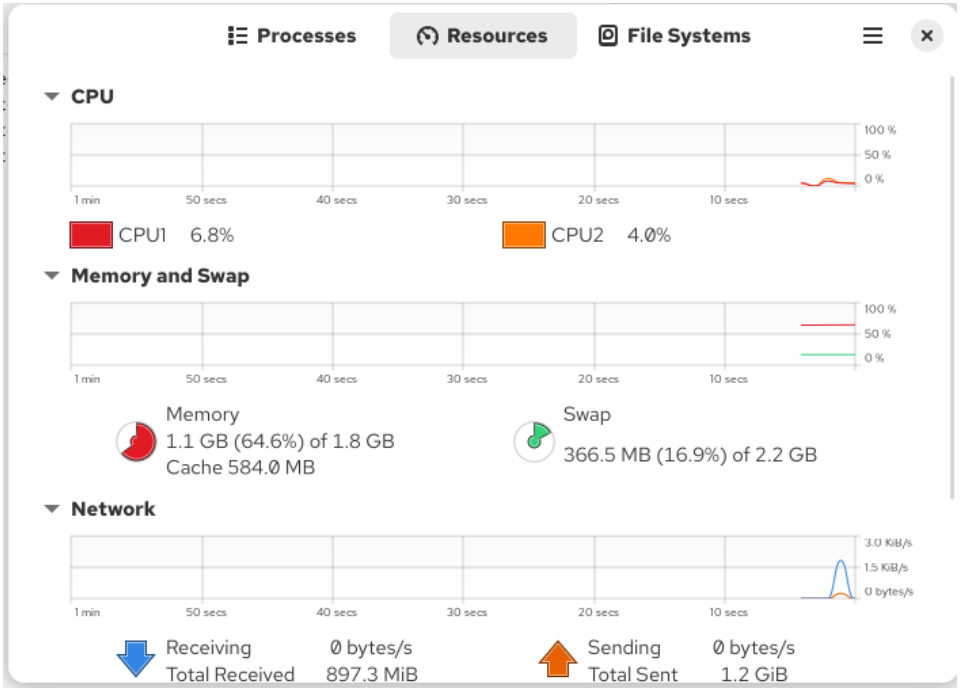


Рис. 2.5: Графическая утилита мониторинга

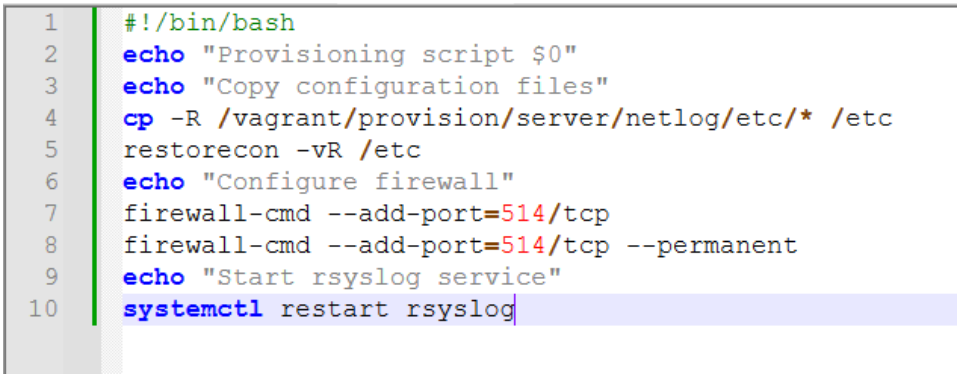
3. На сервер установлен просмотрщик системных логов lnav.

2.4 Внесение изменений в Vagrant provisioning

2.4.1 Настройка provisioning для сервера

1. В каталоге `/vagrant/provision/server` создан каталог `netlog`, содержащий подкаталог
   `etc/rsyslog.d`, куда помещён конфигурационный файл netlog-server.conf.

2. Создан исполняемый файл `netlog.sh`, содержащий:
   копирование конфигурации, восстановление контекстов SELinux, настройку firewall и перезапуск rsyslog.



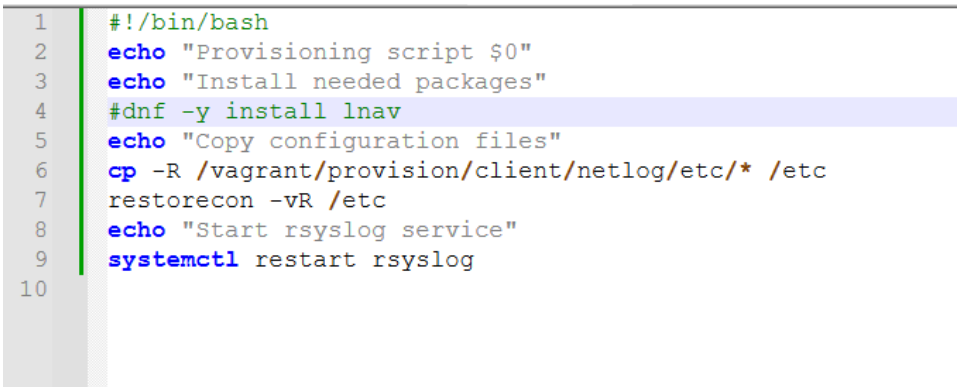
```
#!/bin/bash
echo "Provisioning script $0"
echo "Copy configuration files"
cp -R /vagrant/provision/server/netlog/etc/* /etc
restorecon -vR /etc
echo "Configure firewall"
firewall-cmd --add-port=514/tcp
firewall-cmd --add-port=514/tcp --permanent
echo "Start rsyslog service"
systemctl restart rsyslog
```

Рис. 2.6: Скрипт provisioning на сервере

2.4.2 Настройка provisioning для клиента

1. В каталоге `/vagrant/provision/client` создан каталог `netlog`, куда помещён файл
   netlog-client.conf.

2. Создан исполняемый файл `netlog.sh`, обеспечивающий копирование конфигураций,
   восстановление контекстов и перезапуск rsyslog.



```
#!/bin/bash
echo "Provisioning script $0"
echo "Install needed packages"
#dnf -y install lnav
echo "Copy configuration files"
cp -R /vagrant/provision/client/netlog/etc/* /etc
restorecon -vR /etc
echo "Start rsyslog service"
systemctl restart rsyslog
```

Рис. 2.7: Скрипт provisioning на клиенте

3 Заключение

Сетевой журнал был успешно настроен: сервер принял конфигурацию для получения сообщений по TCP, клиент корректно перенаправляет логи, взаимодействие проверено просмотром системных сообщений. Дополнительно подготовлены provisioning-скрипты для автоматизации развёртывания обеих виртуальных машин.

4 Контрольные вопросы

1. **Какой модуль rsyslog вы должны использовать для приёма сообщений от journald?** Для интеграции journald с rsyslog используется модуль **imjournal**.

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

3. **Чтобы убедиться, что устаревший метод приёма сообщений из journald в rsyslog не используется, какой дополнительный параметр следует применить?** Нужно добавить параметр: **`UseUxSock off`**

4. **В каком конфигурационном файле содержатся настройки, которые позволяют настраивать работу журнала?** Основные параметры работы journald находятся в файле **`/etc/systemd/journald.conf`**.

5. **Каким параметром управляется пересылка сообщений из journald в rsyslog?** За пересылку отвечает параметр journald: **`ForwardToSyslog=`**

6. **Какой модуль rsyslog можно использовать для включения сообщений из файла журнала, не созданного rsyslog?** Для чтения любых лог-файлов используется модуль **imfile**.

7. **Какой модуль rsyslog нужно использовать для пересылки сообщений в базу данных MariaDB?** Для записи сообщений в MariaDB применяют модуль **ommysql**.

8. **Какие две строки нужно включить в rsyslog.conf, чтобы позволить текущему журнальному серверу принимать сообщения через TCP?**

```
$ModLoad imtcp
$InputTCPServerRun 514
```

9. **Как настроить локальный брандмауэр, чтобы разрешить приём сообщений журнала через порт TCP 514?** Нужно открыть порт командой firewall-cmd:

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