Отчет по лабораторной работе №15

Настройка сетевого журналирования

Галацан Николай, НПИбд-01-22

Содержание

# 1 Цель работы

Получение навыков по работе с журналами системных событий.

# 2 Выполнение лабораторной работы

## 2.1 Настройка сервера сетевого журнала

На сервере создаю файл конфигурации сетевого хранения журналов:

cd /etc/rsyslog.d  
touch netlog-server.conf

В данном файле включаю прием записей журнала по TCP-порту 514 (рис. 1).

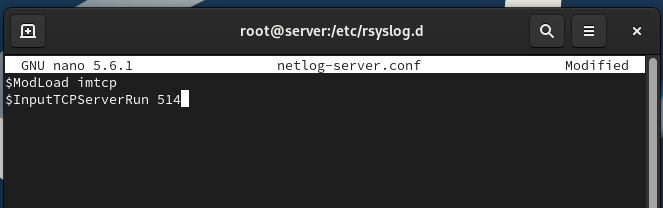


Рис. 1: Редактирование файла конфигурации сетевого хранения журналов /etc/rsyslog.d/netlog-server.conf

Перезапускаю службу rsyslog и просматриваю прослушиваемые порты, которые связаны со службой (рис. 2)

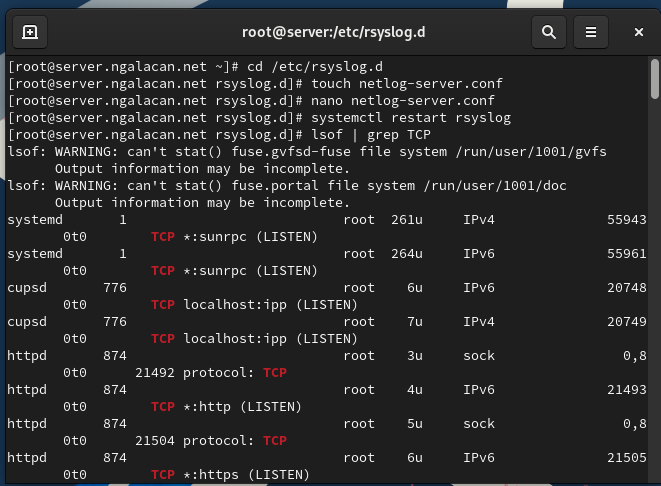


Рис. 2: Перезапуск rsyslog и просмотр прослушиваемых портов

На сервере настраиваю межсетевой экран для работы с TCP-портом 514:

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

## 2.2 Настройка клиента сетевого журнала

На клиенте создаю файл конфигурации сетевого хранения журналов:

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

В данном файле включаю перенаправление сообщений журнала на 514 TCP-порт сервера и перезапускаю службу (рис. 3)

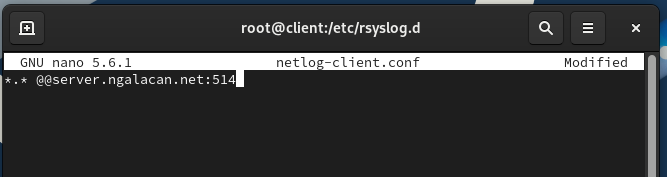


Рис. 3: Редактирование файла конфигурации сетевого хранения журналов на клиенте: включение перенаправления на 514 порт

## 2.3 Просмотр журнала

На сервере просматриваю один из файлов журнала. Обращаю внимание, что выводятся сообщения как с сервера, так и с клиента (рис. 4)

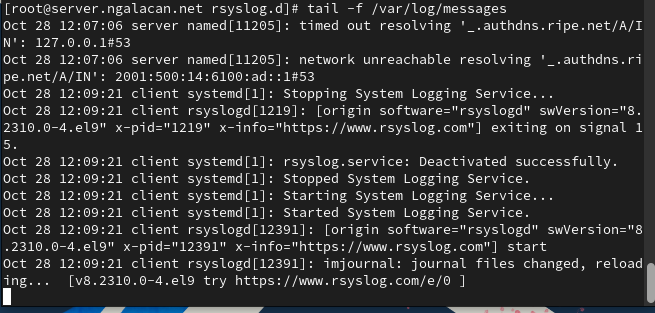


Рис. 4: Просмотр файла журнала на сервере

На сервере под пользователем ngalacan запускаю графическую программу для просмотра журналов (рис. 5).

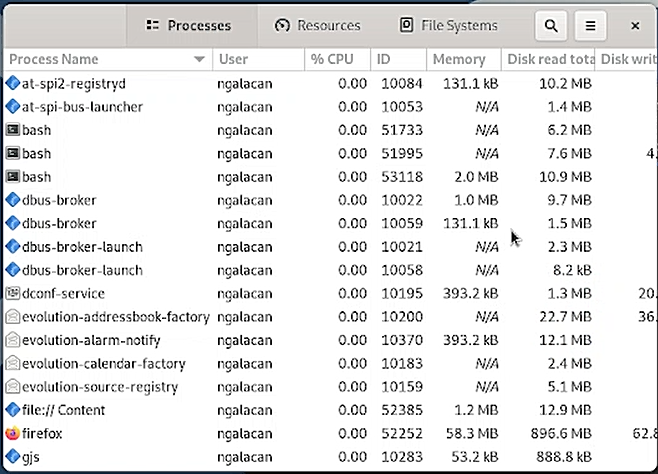


Рис. 5: Запуск графической программы для просмотра журналов

Устанавливаю просмотрщик журналов системных событий lnav:

dnf -y install lnav

Использую lnav для просмотра логов (рис. 6).

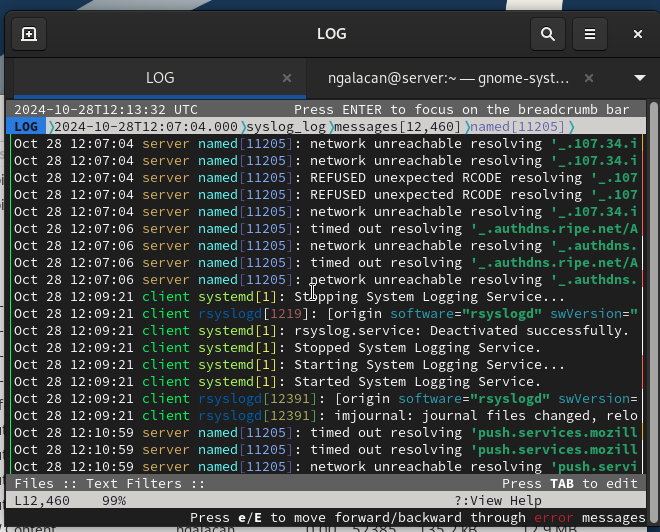


Рис. 6: Использование lnav для просмотра логов

## 2.4 Внесение изменений в настройки внутреннего окружения виртуальной машины

На ВМ server перехожу в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/ и копирую 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

Вношу изменения в файл /vagrant/provision/server/netlog.sh (рис. 7).

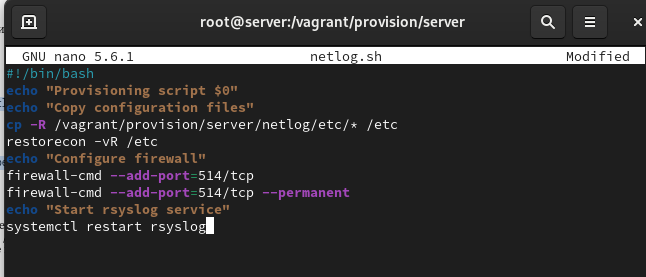


Рис. 7: Редактирование netlog.sh на сервере

На ВМ client перехожу в каталог для внесения изменений в настройки внутреннего окружения и копирую 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/

Создаю и редактирую скрипт /vagrant/provision/client/netlog.sh (рис. 8).

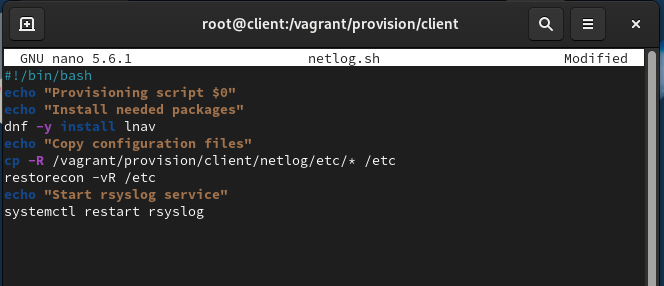


Рис. 8: Редактирование netlog.sh на клиенте

Для отработки созданных скриптов во время загрузки виртуальных машин server и client в конфигурационном файле Vagrantfile добавляю 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 результате выполнения работы были приобретены 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.

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

imklog

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

Cледует использовать параметр “SystemCallFilter[include:omusrmsg.conf?]” в конфигурационном файле rsyslog.conf.

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

Настройки, позволяющие настраивать работу журнала, содержатся в конфигурационном файле rsyslog.conf.

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

Пересылка сообщений из journald в rsyslog управляется параметром “ForwardToSyslog” в файле конфигурации journald.conf.

1. 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.

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

Для пересылки сообщений в базу данных MariaDB следует использовать модуль ommysql.

1. 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

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