Лабораторная работа №15

Администрирование сетевых подсистем

Иванов Сергей Владимирович, НПИбд-01-23

03 декабря 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Цель работы

Получение навыков по работе с журналами системных событий.

Задание

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

Выполнение лабораторной работы

Настройка сервера сетевого журнала

Запускаю виртуальную машину Server. (рис. 1)

```
C:\work_asp\svivanov\vagrant>vagrant halt server

C:\work_asp\svivanov\vagrant>vagrant up server
Bringing machine 'server' up with 'virtualbox' provider...
==> server: You assigned a static IP ending in ".1" or ":1" to this machine.
==> server: This is very often used by the router and can cause the
==> server: network to not work properly. If the network doesn't work
==> server: properly, try changing this IP.
==> server: You assigned a static IP ending in ".1" or ":1" to this machine.
==> server: This is very often used by the router and can cause the
```

Рис. 1: Запуск Server

Настройка сервера сетевого журнала

На сервере создадим файл конфигурации сетевого хранения журналов:

```
[root@server.svivanov.net ~]# cd /etc/rsyslog.d
[root@server.svivanov.net rsyslog.d]# touch netlog-server.conf
```

Рис. 2: Создание конф. файла

Настройка сервера сетевого журнала

В файле конфигурации включим приём записей журнала по TCP-порту 514:

Рис. 3: Редактирование конф. файла

Настройка сервера сетевого журнала

Перезапустим службу rsyslog и посмотрим, какие порты, связанные с rsyslog, прослушиваются:

```
rsyslogd  13438                        root    4u     IPv4              45592       0t0       TCP *:shell (LISTEN)
rsyslogd  13438                        root    5u     IPv6              45593       0t0       TCP *:shell (LISTEN)
rsyslogd  13438 13440 in:imjour        root    4u     IPv4              45592       0t0       TCP *:shell (LISTEN)
rsyslogd  13438 13440 in:imjour        root    5u     IPv6              45593       0t0       TCP *:shell (LISTEN)
rsyslogd  13438 13441 in:imtcp         root    4u     IPv4              45592       0t0       TCP *:shell (LISTEN)
rsyslogd  13438 13441 in:imtcp         root    5u     IPv6              45593       0t0       TCP *:shell (LISTEN)
rsyslogd  13438 13442 in:imtcp         root    4u     IPv4              45592       0t0       TCP *:shell (LISTEN)
rsyslogd  13438 13442 in:imtcp         root    5u     IPv6              45593       0t0       TCP *:shell (LISTEN)
rsyslogd  13438 13443 in:imtcp         root    4u     IPv4              45592       0t0       TCP *:shell (LISTEN)
rsyslogd  13438 13443 in:imtcp         root    5u     IPv6              45593       0t0       TCP *:shell (LISTEN)
rsyslogd  13438 13444 rs:main          root    4u     IPv4              45592       0t0       TCP *:shell (LISTEN)
rsyslogd  13438 13444 rs:main          root    5u     IPv6              45593       0t0       TCP *:shell (LISTEN)
rsyslogd  13438 13445 in:imtcp         root    4u     IPv4              45592       0t0       TCP *:shell (LISTEN)
rsyslogd  13438 13445 in:imtcp         root    5u     IPv6              45593       0t0       TCP *:shell (LISTEN)
rsyslogd  13438 13446 in:imtcp         root    4u     IPv4              45592       0t0       TCP *:shell (LISTEN)
rsyslogd  13438 13446 in:imtcp         root    5u     IPv6              45593       0t0       TCP *:shell (LISTEN)
[root@server.svivanov.net rsyslog.d]#
```

Рис. 4: Просмотр портов связанных с rsyslog

Настройка сервера сетевого журнала

```
[root@server.svivanov.net rsyslog.d]# firewall-cmd --add-port=514/tcp
success
[root@server.svivanov.net rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent
success
[root@server.svivanov.net rsyslog.d]#
```

Рис. 5: Настройка firewall

Настройка клиента сетевого журнала

Запускаю виртуальную машину Client. (рис. 6)

```
C:\work_asp\svivanov\vagrant>vagrant up client
Bringing machine 'client' up with 'virtualbox' provider...
==> client: Clearing any previously set forwarded ports...
==> client: Fixed port collision for 22 => 2222. Now on port 2200.
==> client: Clearing any previously set network interfaces...
==> client: Preparing network interfaces based on configuration...
    client: Adapter 1: nat
    client: Adapter 2: intnet
==> client: Forwarding ports...
```

Рис. 6: Запуск Client

Настройка клиента сетевого журнала

```
[root@client.svivanov.net ~]# cd /etc/rsyslog.d
[root@client.svivanov.net rsyslog.d]# touch netlog-client.conf
[root@client.svivanov.net rsyslog.d]#
```

Рис. 7: Создание конф.файла

Настройка клиента сетевого журнала

На клиенте в файле конфигурации включим перенаправление сообщений на 514 сервера:

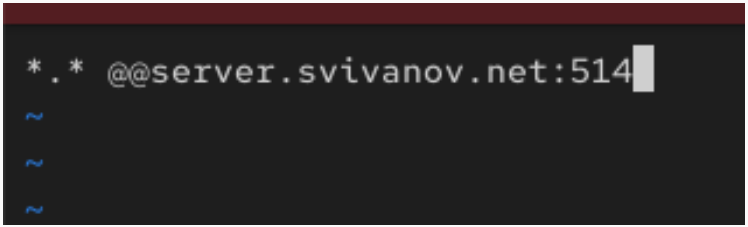

Рис. 8: Редактирование конф. файла

Настройка клиента сетевого журнала

```
[root@client.svivanov.net rsyslog.d]# systemctl restart rsyslog
[root@client.svivanov.net rsyslog.d]#
```

Рис. 9: Перезапуск службы

Просмотр журнала

На сервере просмотрим один из файлов журнала

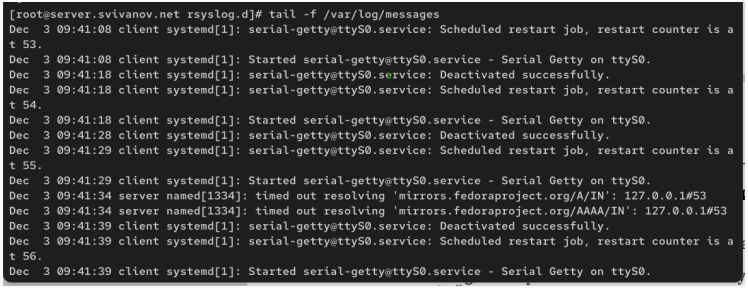

Рис. 10: Просмотр файла журнала

Просмотр журнала

На сервере под запустим графическую программу для просмотра журналов

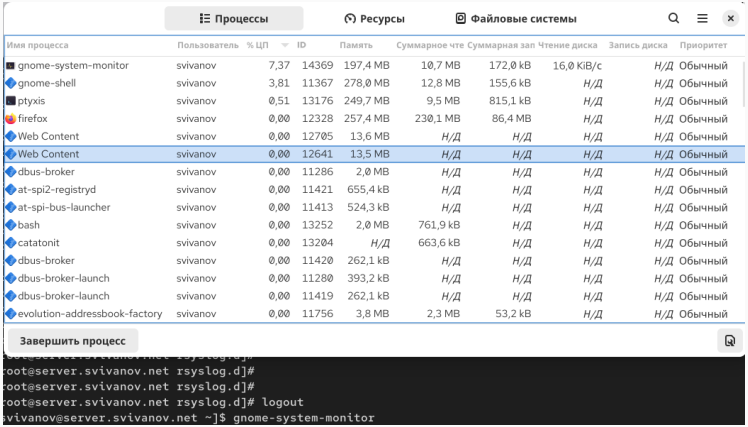

Рис. 11: Запуск программы для просмотра журналов

Просмотр журнала

На сервере установим просмотрщик журналов системных сообщений lnav:

```
[svivanov@server.svivanov.net ~]$ sudo dnf -y install lnav
Last metadata expiration check: 0:00:06 ago on Ср 03 дек 2025 10:09:10.
Dependencies resolved.
================================================================================
 Package              Architecture          Version                 Repository          Size
================================================================================
Installing:
 lnav                 x86_64                0.11.1-1.el9            epel               2.4 M

Transaction Summary
================================================================================
Install  1 Package

Total download size: 2.4 M
Installed size: 6.1 M
Downloading Packages:
lnav-0.11.1-1.el9.x86_64.rpm                                 5.7 MB/s | 2.4 MB     00:00
--------------------------------------------------------------------------------
Total                                                        2.4 MB/s | 2.4 MB     00:00
Extra Packages for Enterprise Linux 9 - x86_64               1.6 MB/s | 1.6 kB     00:00
Importing GPG key 0x3228467C:
 Userid     : "Fedora (epel9) <epel@fedoraproject.org>"
```

Рис. 12: Установка lnav

Просмотр журнала

Просмотр логов с помощью lnav на сервере:

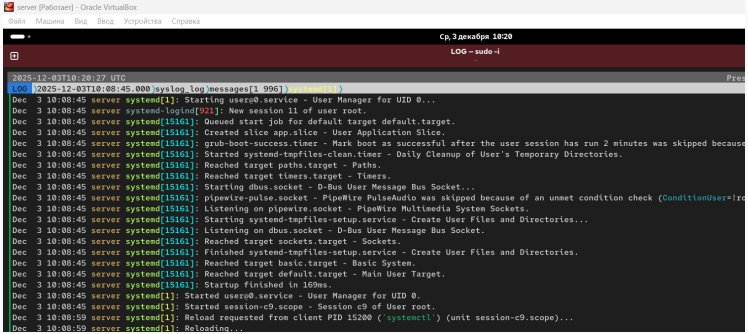

Рис. 13: Просмотр логов

Просмотр журнала

На клиенте установим просмотрщик журналов системных сообщений lnav:

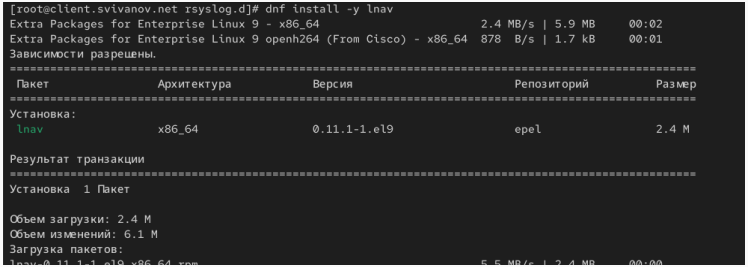

Рис. 14: Установка lnav

Просмотр журнала

Просмотр логов с помощью lnav на клиенте: (рис. 15)

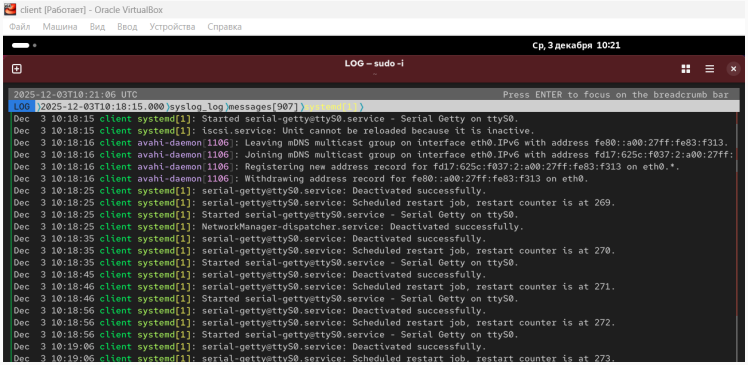

Рис. 15: Просмотр логов

Внесение изменений в настройки внутреннего окружения виртуальных машин

На машине server перейдем в каталог для внесения изменений, в который поместим конфигурационные файлы:

```
[root@server.svivanov.net ~]# cd /vagrant/provision/server
[root@server.svivanov.net server]# mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.svivanov.net server]# cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlo
g/etc/rsyslog.d
[root@server.svivanov.net server]#
```

Рис. 16: Создание каталогов и копирование конф.файлов

Внесение изменений в настройки внутреннего окружения виртуальных машин

Создадм скрипт

```
#!/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. 17: Создание скрипта

Внесение изменений в настройки внутреннего окружения виртуальных машин

На машине client перейдем в каталог для внесения изменений, в который поместим конфигурационные файлы:

```
[root@client.svivanov.net rsyslog.d]# cd /vagrant/provision/client
[root@client.svivanov.net client]# mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d
[root@client.svivanov.net client]# cp -R /etc/rsyslog.d/netlog-client.conf /vagrant/provision/client/netlog/etc/rsyslog.d/
[root@client.svivanov.net client]#
```

Рис. 18: Создание каталогов и копирование конф.файлов

Внесение изменений в настройки внутреннего окружения виртуальных машин

Создадм скрипт

```
#!/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. 19: Создание скрипта

Внесение изменений в настройки внутреннего окружения виртуальных машин

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

Рис. 20: Редактирование Vagrantfile

Внесение изменений в настройки внутреннего окружения виртуальных машин

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

Рис. 21: Редактирование Vagrantfile

Вывод

В ходе выполнения лабораторной работы мы получили навыки по работе с журналами системных событий.