

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 15

дисциплина: Администрирование сетевых подсистем

Студент: Бакулин Никита 1032201747

Группа: НПИбд-01-20

МОСКВА

2022 г.

Постановка задачи

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 работы

1.

1.1. На сервере создайте файл конфигурации сетевого хранения журналов

1.2. В файле конфигурации `/etc/rsyslog.d/netlog-server.conf` включите приём записей журнала по TCP-порту 514

```
$ModLoad imtcp
$InputTCPServerRun 514
~
"netlog-server.conf" 2L, 38B
```

Рисунок 1

1.3. Перезапустите службу `rsyslog` и посмотрите, какие порты, связанные с `rsyslog`, прослушиваются

1.4. На сервере настройте межсетевой экран для приёма сообщений по TCP-порту 514

```
rsyslogd 6097 root 4u IPv4 39187 0t0 TCP *:shell (LISTEN)
rsyslogd 6097 root 5u IPv6 39188 0t0 TCP *:shell (LISTEN)
rsyslogd 6097 6098 in:imtcp root 4u IPv4 39187 0t0 TCP *:shell (LISTEN)
rsyslogd 6097 6098 in:imtcp root 5u IPv6 39188 0t0 TCP *:shell (LISTEN)
rsyslogd 6097 6100 in:imjour root 4u IPv4 39187 0t0 TCP *:shell (LISTEN)
rsyslogd 6097 6100 in:imjour root 5u IPv6 39188 0t0 TCP *:shell (LISTEN)
rsyslogd 6097 6101 rs:main root 4u IPv4 39187 0t0 TCP *:shell (LISTEN)
rsyslogd 6097 6101 rs:main root 5u IPv6 39188 0t0 TCP *:shell (LISTEN)
rsyslogd 6097 6102 in:imtcp root 4u IPv4 39187 0t0 TCP *:shell (LISTEN)
rsyslogd 6097 6102 in:imtcp root 5u IPv6 39188 0t0 TCP *:shell (LISTEN)
rsyslogd 6097 6103 in:imtcp root 4u IPv4 39187 0t0 TCP *:shell (LISTEN)
rsyslogd 6097 6103 in:imtcp root 5u IPv6 39188 0t0 TCP *:shell (LISTEN)
rsyslogd 6097 6104 in:imtcp root 4u IPv4 39187 0t0 TCP *:shell (LISTEN)
rsyslogd 6097 6104 in:imtcp root 5u IPv6 39188 0t0 TCP *:shell (LISTEN)
rsyslogd 6097 6105 in:imtcp root 4u IPv4 39187 0t0 TCP *:shell (LISTEN)
rsyslogd 6097 6105 in:imtcp root 5u IPv6 39188 0t0 TCP *:shell (LISTEN)
[root@server.nabakulin.net rsyslog.d]# firewall-cmd --add-port=514/tcp
success
[root@server.nabakulin.net rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent
success
```

Рисунок 2

2.

- 2.1. На клиенте создайте файл конфигурации сетевого хранения журналов
- 2.2. На клиенте в файле конфигурации /etc/rsyslog.d/netlog-client.conf включите перенаправление сообщений журнала на 514 TCP-порт сервера

```

*. * @@server.nabakulin.net:514
~
"netlog-client.conf" 1L, 31B

```

Рисунок 3

- 2.3. Перезапустите службу rsyslog

```

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

```

Рисунок 4

3.

- 3.1. На сервере просмотрите один из файлов журнала

```

[root@server.nabakulin.net rsyslog.d]# tail -f /var/log/messages
Jan 7 18:24:05 client rsyslogd[600]: [origin software="rsyslogd" swVersion="8.2102.0-105.el9" x-pid="600" x-info="https://www.rsyslog.com"] exiting on signal 15.
Jan 7 18:24:05 client systemd[1]: rsyslog.service: Deactivated successfully.
Jan 7 18:24:05 client systemd[1]: Stopped System Logging Service.
Jan 7 18:24:05 client systemd[1]: Starting System Logging Service...
Jan 7 18:24:05 client systemd[1]: Started System Logging Service.
Jan 7 18:24:05 client rsyslogd[6533]: [origin software="rsyslogd" swVersion="8.2102.0-105.el9" x-pid="6533" x-info="https://www.rsyslog.com"] start
Jan 7 18:24:05 client rsyslogd[6533]: imjournal: journal files changed, reloading... [v8.2102.0-105.el9 try https://www.rsyslog.com/e/0 ]
Jan 7 18:24:07 client NetworkManager[5214]: <info> [1673115847.2042] dhcp4 (eth1): state changed new lease, address=192.168.1.30
Jan 7 18:24:07 server dhcpd[1153]: DHCPREQUEST for 192.168.1.30 from 08:00:27:0b:b0:57 (client) via eth1
Jan 7 18:24:07 server dhcpd[1153]: DHCPACK on 192.168.1.30 to 08:00:27:0b:b0:57 (client) via eth1

```

Рисунок 5

- 3.2. На сервере под пользователем user запустите графическую программу для просмотра журналов

Processes							
Process Name	User	% CPU	ID	Memory	Disk read tota	Disk writ	
at-spi2-registryd	nabakulin	0.00	5138	442.4 kB	274.4 kB		
at-spi-bus-launcher	nabakulin	0.00	5107	N/A	16.4 kB		
bash	nabakulin	0.00	6014	1.2 MB	31.8 MB	69	
dbus-broker	nabakulin	0.00	5050	1.2 MB	65.5 kB		
dbus-broker	nabakulin	0.00	5113	192.5 kB	N/A		
dbus-broker-launch	nabakulin	0.00	5049	221.2 kB	544.8 kB		
dbus-broker-launch	nabakulin	0.00	5112	N/A	N/A		
dconf-service	nabakulin	0.00	5242	364.5 kB	245.8 kB	20	
evolution-addressbook-factory	nabakulin	0.00	5299	N/A	4.9 MB	36	
evolution-alarm-notify	nabakulin	0.00	5427	5.3 MB	30.5 MB		
evolution-calendar-factory	nabakulin	0.00	5284	376.8 kB	2.9 MB		
evolution-source-registry	nabakulin	0.00	5230	794.6 kB	4.2 MB		
gjs	nabakulin	0.00	5342	2.5 MB	1.4 MB		
gjs	nabakulin	0.00	5430	2.4 MB	28.7 kB		
gnome-keyring-daemon	nabakulin	0.00	5038	331.8 kB	N/A		
gnome-session-binary	nabakulin	0.00	5041	753.7 kB	11.6 MB	4	
gnome-session-binary	nabakulin	0.00	5159	565.2 kB	12.5 MB	4	

Рисунок 6

3.3. На сервере установите просмотрщик журналов системных сообщений `lnav` или его аналог

3.4. Просмотрите логи с помощью `lnav` или его аналога

```
Jan 07 18:14:07 server.nabakulin.net dhcpcd[1153]: DHCPACK on 192.168.1.30 to 08:00:27:0b:b0:57 (client) via eth1
Jan 07 18:15:41 server.nabakulin.net systemd[1]: Starting Cleanup of Temporary Directories...
Jan 07 18:15:42 server.nabakulin.net systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
Jan 07 18:15:42 server.nabakulin.net systemd[1]: Finished Cleanup of Temporary Directories.
Jan 07 18:17:32 server.nabakulin.net systemd[5024]: Started Application launched by gnome-shell.
Jan 07 18:17:32 server.nabakulin.net systemd[5024]: Started Application launched by gnome-shell.
Jan 07 18:17:36 server.nabakulin.net systemd[5024]: Created slice Slice /app/org.gnome.Terminal.
Jan 07 18:17:36 server.nabakulin.net systemd[5024]: Starting GNOME Terminal Server...
Jan 07 18:17:38 server.nabakulin.net systemd[5024]: Started GNOME Terminal Server.
Jan 07 18:17:39 server.nabakulin.net systemd[5024]: Started VTE child process 6014 launched by gnome-terminal-server process
Jan 07 18:17:53 server.nabakulin.net sudo[6039]: nabakulin : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/bash
Jan 07 18:17:53 server.nabakulin.net sudo[6039]: pam_unix(sudo-i:session): session opened for user root(uid=0) by (uid=1001)
Jan 07 18:17:54 server.nabakulin.net systemd[1]: Starting Hostname Service...
Jan 07 18:17:54 server.nabakulin.net systemd[1]: Started Hostname Service.
Jan 07 18:18:24 server.nabakulin.net systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Jan 07 18:19:07 server.nabakulin.net dhcpcd[1153]: DHCPREQUEST for 192.168.1.30 from 08:00:27:0b:b0:57 (client) via eth1
Jan 07 18:19:07 server.nabakulin.net dhcpcd[1153]: DHCPACK on 192.168.1.30 to 08:00:27:0b:b0:57 (client) via eth1
Jan 07 18:19:41 server.nabakulin.net systemd[1]: Stopping System Logging Service...
Jan 07 18:19:42 server.nabakulin.net rsyslogd[616]: [origin software="rsyslogd" swVersion="8.2102.0-101.el9_0.1" x-pid="616"
Jan 07 18:19:42 server.nabakulin.net systemd[1]: rsyslog.service: Deactivated successfully.
Jan 07 18:19:42 server.nabakulin.net systemd[1]: Stopped System Logging Service.
Jan 07 18:19:42 server.nabakulin.net systemd[1]: Starting System Logging Service...
Jan 07 18:19:42 server.nabakulin.net systemd[1]: Started System Logging Service.
Jan 07 18:19:42 server.nabakulin.net rsyslogd[6097]: [origin software="rsyslogd" swVersion="8.2102.0-101.el9_0.1" x-pid="6097"
Jan 07 18:19:42 server.nabakulin.net rsyslogd[6097]: imjournal: journal files changed, reloading... [v8.2102.0-101.el9_0.1 t
Jan 07 18:24:07 server.nabakulin.net dhcpcd[1153]: DHCPREQUEST for 192.168.1.30 from 08:00:27:0b:b0:57 (client) via eth1
Jan 07 18:24:07 server.nabakulin.net dhcpcd[1153]: DHCPACK on 192.168.1.30 to 08:00:27:0b:b0:57 (client) via eth1
Jan 07 18:25:39 server.nabakulin.net sudo[6039]: pam_unix(sudo-i:session): session closed for user root
Jan 07 18:26:51 server.nabakulin.net systemd[5024]: Started Application launched by gnome-shell.
Jan 07 18:26:51 server.nabakulin.net systemd[5024]: Started Application launched by gnome-shell.
Jan 07 18:27:19 server.nabakulin.net sudo[6246]: nabakulin : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/bash
Jan 07 18:27:19 server.nabakulin.net sudo[6246]: pam_unix(sudo-i:session): session opened for user root(uid=0) by (uid=1001)
Jan 07 18:27:19 server.nabakulin.net systemd[1]: Starting Hostname Service...
Jan 07 18:27:19 server.nabakulin.net systemd[1]: Started Hostname Service.
Jan 07 18:27:50 server.nabakulin.net systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Jan 07 18:29:07 server.nabakulin.net dhcpcd[1153]: DHCPREQUEST for 192.168.1.30 from 08:00:27:0b:b0:57 (client) via eth1
Jan 07 18:29:07 server.nabakulin.net dhcpcd[1153]: DHCPACK on 192.168.1.30 to 08:00:27:0b:b0:57 (client) via eth1
```

Рисунок 7

```
Jan 07 18:14:07 client.nabakulin.net NetworkManager[5214]: <info> [1673115247.3436] dhcp4 (eth1): state changed new lease, a
Jan 07 18:18:13 client.nabakulin.net systemd[1]: Starting Cleanup of Temporary Directories...
Jan 07 18:18:14 client.nabakulin.net systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
Jan 07 18:18:14 client.nabakulin.net systemd[1]: Finished Cleanup of Temporary Directories.
Jan 07 18:19:07 client.nabakulin.net NetworkManager[5214]: <info> [1673115547.2159] dhcp4 (eth1): state changed new lease, a
Jan 07 18:22:17 client.nabakulin.net systemd[5446]: Started Application launched by gnome-shell.
Jan 07 18:22:18 client.nabakulin.net systemd[5446]: Started Application launched by gnome-shell.
Jan 07 18:22:24 client.nabakulin.net systemd[5446]: Created slice Slice /app/org.gnome.Terminal.
Jan 07 18:22:24 client.nabakulin.net systemd[5446]: Starting GNOME Terminal Server...
Jan 07 18:22:24 client.nabakulin.net systemd[5446]: Started GNOME Terminal Server.
Jan 07 18:22:26 client.nabakulin.net systemd[5446]: Started VTE child process 6442 launched by gnome-terminal-server process
Jan 07 18:22:42 client.nabakulin.net sudo[6472]: nabakulin : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/bash
Jan 07 18:22:42 client.nabakulin.net sudo[6472]: pam_unix(sudo-i:session): session opened for user root(uid=0) by (uid=1001)
Jan 07 18:22:42 client.nabakulin.net systemd[1]: Starting Hostname Service...
Jan 07 18:22:43 client.nabakulin.net systemd[1]: Started Hostname Service.
Jan 07 18:23:13 client.nabakulin.net systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Jan 07 18:24:04 client.nabakulin.net systemd[1]: Stopping System Logging Service...
Jan 07 18:24:05 client.nabakulin.net rsyslogd[600]: [origin software="rsyslogd" swVersion="8.2102.0-105.el9" x-pid="600" x-in
Jan 07 18:24:05 client.nabakulin.net systemd[1]: rsyslog.service: Deactivated successfully.
Jan 07 18:24:05 client.nabakulin.net systemd[1]: Stopped System Logging Service.
Jan 07 18:24:05 client.nabakulin.net systemd[1]: Starting System Logging Service...
Jan 07 18:24:05 client.nabakulin.net systemd[1]: Started System Logging Service.
Jan 07 18:24:05 client.nabakulin.net rsyslogd[6533]: [origin software="rsyslogd" swVersion="8.2102.0-105.el9" x-pid="6533" x-
Jan 07 18:24:05 client.nabakulin.net rsyslogd[6533]: imjournal: journal files changed, reloading... [v8.2102.0-105.el9 try h
Jan 07 18:24:07 client.nabakulin.net NetworkManager[5214]: <info> [1673115847.2042] dhcp4 (eth1): state changed new lease, a
Jan 07 18:29:07 client.nabakulin.net NetworkManager[5214]: <info> [1673116147.6020] dhcp4 (eth1): state changed new lease, a
Jan 07 18:33:52 client.nabakulin.net gnome-shell[5611]: Can't update stage views actor MetaWindowGroup is on because it nee
Jan 07 18:33:52 client.nabakulin.net gnome-shell[5611]: Can't update stage views actor MetaWindowActorX11 is on because it ne
Jan 07 18:33:52 client.nabakulin.net gnome-shell[5611]: Can't update stage views actor MetaSurfaceActorX11 is on because it ne
```

Рисунок 8

4.

4.1.1. На виртуальной машине `server` перейдите в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создайте в нём каталог `netlog`, в который поместите в соответствующие

подкаталоги конфигурационные файлы

```
[root@server.nabakulin.net server]# cd /vagrant/provision/server
[root@server.nabakulin.net server]# mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.nabakulin.net server]# cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.nabakulin.net server]# touch netlog.sh
[root@server.nabakulin.net server]# chmod +x netlog.sh
```

Рисунок 9

4.2. В каталоге /vagrant/provision/server создайте исполняемый файл netlog.sh

```
#!/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
```

Рисунок 10

4.3. На виртуальной машине client перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создайте в нём каталог netlog, в который поместите в соответствующие подкаталоги конфигурационные файлы

```
[root@client.nabakulin.net ~]# cd /vagrant/provision/client
[root@client.nabakulin.net client]# mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d
[root@client.nabakulin.net client]# cp -R /etc/rsyslog.d/netlog-client.conf /vagrant/provision/client/netlog/etc/rsyslog.d/
[root@client.nabakulin.net client]# touch netlog.sh
[root@client.nabakulin.net client]# chmod +x netlog.sh
```

Рисунок 11

4.4. В каталоге /vagrant/provision/client создайте исполняемый файл netlog.sh

```
#!/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
```

Рисунок 12

4.5. Для отработки созданных скриптов во время загрузки виртуальных машин server и client в конфигурационном файле Vagrantfile необходимо добавить в соответствующих разделах конфигураций для сервера и клиента

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

Рисунок 13

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

Рисунок 14

Контрольные вопросы

1. Какой модуль rsyslog вы должны использовать для приёма сообщений от journald?
imjournal
2. Как называется устаревший модуль, который можно использовать для включения приёма сообщений журнала в rsyslog?
imuxsock
3. В каком конфигурационном файле содержатся настройки, которые позволяют вам настраивать работу журнала?
/etc/rsyslog.conf

4. Какой модуль rsyslog вам нужно использовать для пересылки сообщений в базу данных MariaDB?
ommysql
5. Какие две строки вам нужно включить в rsyslog.conf, чтобы позволить текущему журнальному серверу получать сообщения через TCP?
\$ModLoad imtcp
\$InputTCPServerRun 514
6. 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