

Презентация лабораторной работы №15

Бакулин Никита 1032201747

Цель работы

- Получение навыков по работе с журналами системных событий.

Задачи

- Настройте сервер сетевого журналирования событий.
- Настройте клиент для передачи системных сообщений в сетевой журнал на сервере.
- Просмотрите журналы системных событий с помощью нескольких программ. При наличии сообщений о некорректной работе сервисов исправьте ошибки в настройках соответствующих служб.
- Напишите скрипты для Vagrant, фиксирующие действия по установке и настройке сетевого сервера журналирования

Результаты выполнения

- Настройте сервер сетевого журналирования событий.

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

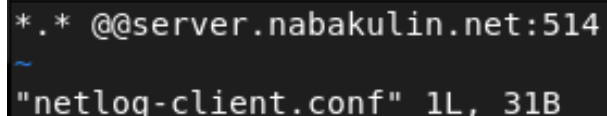
Рис. 1

```
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
```

Рис. 2

Результаты выполнения

- Настройте клиент для передачи системных сообщений в сетевой журнал на сервере.



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

A terminal window with a dark background. The first line shows a command prompt with two asterisks followed by the host and port. The second line shows a tilde character. The third line shows the command output, indicating the file size in lines and bytes.

Рис. 3

Результаты выполнения

- Просмотрите журналы системных событий с помощью нескольких программ. При наличии сообщений о некорректной работе сервисов исправьте ошибки в настройках соответствующих служб.

```
[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
```

Рис. 4

| 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 |

Рис. 5

Результаты выполнения

- Напишите скрипты для Vagrant, фиксирующие действия по установке и настройке сетевого сервера журналирования

```
#!/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. 6

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

Рис. 7

```
#!/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. 8

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

Рис. 9