Лабораторная работа
Номер 15

Кобзев Д. К.
Российский университет дружбы народов, Москва, Россия
7 декабря 2025

Информация

Докладчик

- Кобзев Дмитрий Константинович
- Студент
- Российский университет дружбы народов
- НПИбд-01-23

Цель работы

Целью данной работы является получение навыков по работе с журналами системных событий.

Настройка сервера сетевого журнала

На сервере создаем файл конфигурации сетевого хранения журналов (Рис. 12.1).

```
[dkkobzev@server.dkkobzev.net ~]$ cd /etc/rsyslog.d
[dkkobzev@server.dkkobzev.net rsyslog.d]$ touch netlog-server.conf
touch: cannot touch 'netlog-server.conf': Permission denied
[dkkobzev@server.dkkobzev.net rsyslog.d]$ sudo -i
[sudo] password for dkkobzev:
[root@server.dkkobzev.net ~]# touch netlog-server.conf
```

Рис. 1: Создание файла конфигурации сетевого хранения журналов

Настройка сервера сетевого журнала

В файле конфигурации /etc/rsyslog.d/netlog-server.conf включаем приём записей журнала по TCP-порту 514 (Рис. 12.2).

Рис. 2: Файл конфигурации /etc/rsyslog.d/netlog-server.conf

Настройка сервера сетевого журнала

Перезапускаем службу rsyslog и смотрим, какие порты, связанные с rsyslog, прослушиваются. На сервере настраиваем межсетевой экран для приёма сообщений по TCP-порту 514 (Рис. 12.3).

```
rsyslogd  13129                        root    4u     IPv4              44519       0t0       TCP *:shell (LISTEN)
rsyslogd  13129                        root    5u     IPv6              44520       0t0       TCP *:shell (LISTEN)
rsyslogd  13129 13131 in:imjour        root    4u     IPv4              44519       0t0       TCP *:shell (LISTEN)
rsyslogd  13129 13131 in:imjour        root    5u     IPv6              44520       0t0       TCP *:shell (LISTEN)
rsyslogd  13129 13132 in:imtcp         root    4u     IPv4              44519       0t0       TCP *:shell (LISTEN)
rsyslogd  13129 13132 in:imtcp         root    5u     IPv6              44520       0t0       TCP *:shell (LISTEN)
rsyslogd  13129 13133 in:imtcp         root    4u     IPv4              44519       0t0       TCP *:shell (LISTEN)
rsyslogd  13129 13133 in:imtcp         root    5u     IPv6              44520       0t0       TCP *:shell (LISTEN)
rsyslogd  13129 13134 in:imtcp         root    4u     IPv4              44519       0t0       TCP *:shell (LISTEN)
rsyslogd  13129 13134 in:imtcp         root    5u     IPv6              44520       0t0       TCP *:shell (LISTEN)
rsyslogd  13129 13135 in:imtcp         root    4u     IPv4              44519       0t0       TCP *:shell (LISTEN)
rsyslogd  13129 13135 in:imtcp         root    5u     IPv6              44520       0t0       TCP *:shell (LISTEN)
rsyslogd  13129 13136 in:imtcp         root    4u     IPv4              44519       0t0       TCP *:shell (LISTEN)
rsyslogd  13129 13136 in:imtcp         root    5u     IPv6              44520       0t0       TCP *:shell (LISTEN)
rsyslogd  13129 13137 rs:main          root    4u     IPv4              44519       0t0       TCP *:shell (LISTEN)
rsyslogd  13129 13137 rs:main          root    5u     IPv6              44520       0t0       TCP *:shell (LISTEN)
[root@server.dkkobzev.net ~]# firewall-cmd --add-port=514/tcp
success
[root@server.dkkobzev.net ~]# firewall-cmd --add-port=514/tcp --permanent
success
```

Рис. 3: Настройка сервера сетевого журнала

Настройка клиента сетевого журнала

На клиенте создаем файл конфигурации сетевого хранения журналов (Рис. 12.4).

```
[dkkobzev@client.dkkobzev.net ~]$ sudo -i
[sudo] password for dkkobzev:
[root@client.dkkobzev.net ~]# cd /etc/rsyslog.d
[root@client.dkkobzev.net rsyslog.d]# touch netlog-client.conf
```

Рис. 4: Создание файла конфигурации сетевого хранения журналов

Настройка клиента сетевого журнала

На клиенте в файле конфигурации /etc/rsyslog.d/netlog-client.conf включаем перенаправление сообщений журнала на 514 TCP-порт сервера (Рис. 12.5).

Рис. 5: Файл конфигурации /etc/rsyslog.d/netlog-client.conf

Настройка клиента сетевого журнала

Перезапускаем службу rsyslog (Рис. 12.6).

Рис. 6: Перезапуск службы rsyslog

Просмотр журнала

На сервере смотрим один из файлов журнала (Рис. 12.7).

```
[root@server.dkkobzev.net ~]# tail -f /var/log/messages
Dec  7 16:56:08 server systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
Dec  7 16:56:08 server systemd[1]: Finished systemd-tmpfiles-clean.service - Cleanup of Temporary Directories.
Dec  7 16:56:57 client systemd[1]: Stopping rsyslog.service - System Logging Service...
Dec  7 16:56:57 client rsyslogd[1447]: [origin software="rsyslogd" swVersion="8.2412.0-1.el10" x-pid="1447" x-info="https://www.
rsyslog.com"] exiting on signal 15.
Dec  7 16:56:57 client systemd[1]: rsyslog.service: Deactivated successfully.
Dec  7 16:56:57 client systemd[1]: Stopped rsyslog.service - System Logging Service.
Dec  7 16:56:57 client systemd[1]: Starting rsyslog.service - System Logging Service...
Dec  7 16:56:57 client rsyslogd[9941]: [origin software="rsyslogd" swVersion="8.2412.0-1.el10" x-pid="9941" x-info="https://www.
rsyslog.com"] start
Dec  7 16:56:57 client systemd[1]: Started rsyslog.service - System Logging Service.
Dec  7 16:56:57 client rsyslogd[9941]: imjournal: journal files changed, reloading...  [v8.2412.0-1.el10 try https://www.rsyslog
.com/e/0 ]
Dec  7 16:57:41 server systemd[6406]: Started run-p13552-i13852.scope - [systemd-run] /usr/bin/bash.
Dec  7 16:58:10 client systemd[8440]: Created slice background.slice - User Background Tasks Slice.
Dec  7 16:58:10 client systemd[8440]: Starting systemd-tmpfiles-clean.service - Cleanup of User's Temporary Files and Directorie
s...
Dec  7 16:58:10 client systemd[8440]: Finished systemd-tmpfiles-clean.service - Cleanup of User's Temporary Files and Directorie
s.
```

Рис. 7: Один из файлов журнала

Просмотр журнала

На сервере под пользователем user запускаем графическую программу для просмотра журналов (Рис. 12.8).

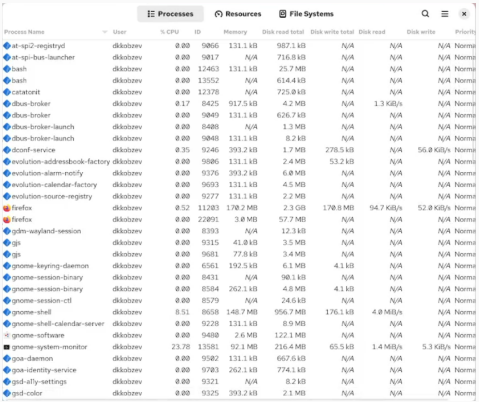

Рис. 8: Графическая программа для просмотра журналов

Просмотр журнала

Просмотрите логи с сервера с помощью lnav (Рис. 12.9).

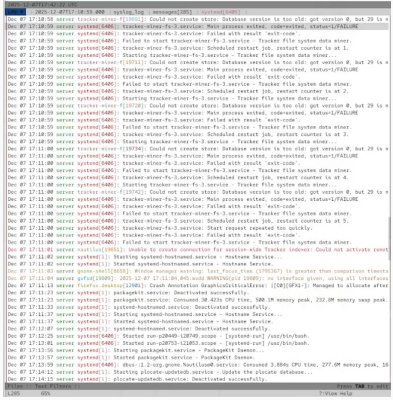

Рис. 9: Логи с сервера

Просмотр журнала

Просмотрите логи с клиента с помощью lnav (Рис. 12.10).

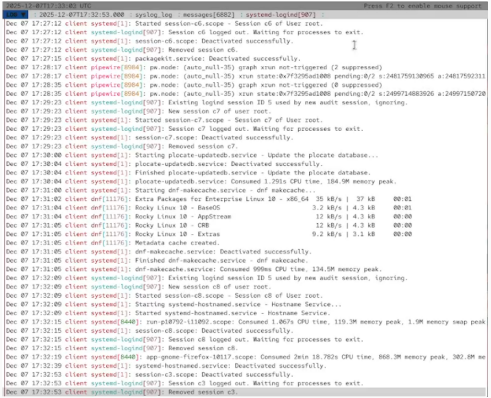

Рис. 10: Логи с клиента

Внесение изменений в настройки внутреннего окружения виртуальных машин

На виртуальной машине server переходим в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создаем в нём каталог netlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. В каталоге /vagrant/provision/server создаем файл netlog.sh (Рис. 12.11).

```
[root@server.dkkobzev.net ~]# cd /vagrant/provision/server
[root@server.dkkobzev.net server]# mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.dkkobzev.net server]# cp -R /etc/rsyslog.d/netlog-server.conf
cp: missing destination file operand after '/etc/rsyslog.d/netlog-server.conf'
Try 'cp --help' for more information.
[root@server.dkkobzev.net server]# cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog.d
[root@server.dkkobzev.net server]# cd /vagrant/provision/server
[root@server.dkkobzev.net server]# touch netlog.sh
[root@server.dkkobzev.net server]# chmod +x netlog.sh
```

Рис. 11: Внесение изменений в настройки внутреннего окружения виртуальной машины

Прописываем скрипт в netlog.sh (Рис. 12.12).

```
 GNU nano 8.1                                                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
```

Рис. 12: Файл netlog.sh

Внесение изменений в настройки внутреннего окружения виртуальных машин

На виртуальной машине client переходим в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создаем в нём каталог netlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. В каталоге /vagrant/provision/client создаем файл netlog.sh (Рис. 12.13).

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

Рис. 13: Внесение изменений в настройки внутреннего окружения виртуальной машины

Прописываем скрипт в netlog.sh (Рис. 12.14).

```
  GNU nano 8.1                                                  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
```

Рис. 14: Файл netlog.sh

Внесение изменений в настройки внутреннего окружения виртуальных машин

Для отработки созданного скрипта во время загрузки виртуальных машин server и client в конфигурационном файле Vagrantfile добавляем в разделе конфигурации для сервера и клиент (Рис. 12.15), (Рис. 12.16).

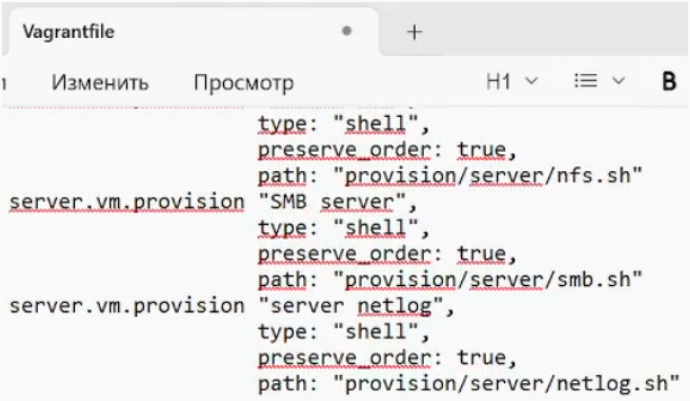

Рис. 15: Vagrantfile

Внесение изменений в настройки внутреннего окружения виртуальных машин

Vagrantfile

Изменить Просмотр H1 B

```
client.vm.network :private_network,
                  ip: "192.168.1.2",
                  virtualbox__intnet: true

client.vm.provider :virtualbox do |virtualbox|
  virtualbox.customize ["modifyvm", :id, "--vrde", "on"
  virtualbox.customize ["modifyvm", :id, "--vrdeport",
end

client.vm.provision "client dummy",
                    type: "shell",
                    preserve_order: true,
                    path: "provision/client/01-dummy.sh
client.vm.provision "client routing",
                    type: "shell",
                    preserve_order: true,
                    run: "always",
                    path: "provision/client/01-routing.
client.vm.provision "client mail",
                    type: "shell",
                    preserve_order: true,
                    run: "always",
                    path: "provision/client/mail.sh"
client.vm.provision "client ntp",
                    type: "shell",
                    preserve_order: true,
                    path: "provision/client/ntp.sh"
client.vm.provision "client nfs",
                    type: "shell",
                    preserve_order: true,
                    path: "provision/client/nfs.sh"
client.vm.provision "SMB client",
                    type: "shell",
                    preserve_order: true,
                    path: "provision/client/smb.sh"
client.vm.provision "client netlog",
                    type: "shell",
                    preserve_order: true,
                    path: "provision/client/netlog.sh"
```

Рис. 16: Vagrantfile

Выводы

В результате выполнения лабораторной работы мною были получены навыки по работе с журналами системных событий.