

Лабораторная работа № 15

Настройка сетевого журналирования

Демидова Екатерина Алексеевна

Содержание

1	Цель работы	4
2	Задание	5
3	Выполнение лабораторной работы	6
3.1	Настройка сервера сетевого журнала	6
3.2	Настройка клиента сетевого журнала	7
3.3	Просмотр журнала	8
3.4	Внесение изменений в настройки внутреннего окружения виртуальных машины	10
4	Контрольные вопросы	13
5	Выводы	15

Список иллюстраций

3.1	Включение журналирования по TCP-порту 514	6
3.2	Просмотр прослушиваемых портов, связанных с rsyslog	7
3.3	Настройка межсетевого экрана для приёма сообщений по TCP-порту 514	7
3.4	Включение перенаправления сообщений журнала на 514 TCP-порт сервера	8
3.5	Просмотр файла ar/log/messages журнала	8
3.6	Запуск графической программы для просмотра журналов	9
3.7	Просмотр логов с клиента и сервера	10
3.8	Скрипта файла /vagrant/provision/server/netlog.sh	11
3.9	Скрипта файла /vagrant/provision/client/netlog.sh	12

1 Цель работы

Получение навыков по работе с журналами системных событий.

2 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

3 Выполнение лабораторной работы

3.1 Настройка сервера сетевого журнала

Загрузим нашу операционную систему и перейдем в рабочий каталог с проектом:

```
cd /var/tmp/eademidova/vagrant
```

Затем запустим виртуальную машину server:

```
make server-up
```

На сервере создадим файл конфигурации сетевого хранения журналов:

```
cd /etc/rsyslog.d
```

```
touch netlog-server.conf
```

В файле конфигурации /etc/rsyslog.d/netlog-server.conf включим приём записей журнала по TCP-порту 514(рис. 3.1):



Рис. 3.1: Включение журналирования по TCP-порту 514

Перезапустим службу rsyslog и посмотрим, какие порты, связанные с rsyslog, прослушиваются(рис. 3.2):

```

[ameidova@193.174 ~]$ cat /etc/passwd | grep rsyslogd
rsyslogd:x:1938:0:root:::/usr/sbin/rsyslogd:/usr/sbin/rsyslogd
rsyslogd 6981 root 4u IPv4 42991 0t0 TCP *:sshell (LISTEN)
rsyslogd 6981 root 4u IPv6 42992 0t0 TCP *:sshell (LISTEN)
rsyslogd 6981 6982 in:intcp root 4u IPv4 42991 0t0 TCP *:sshell (LISTEN)
rsyslogd 6981 6982 in:intcp root 5u IPv6 42992 0t0 TCP *:sshell (LISTEN)
rsyslogd 6981 6984 in:injour root 4u IPv4 42991 0t0 TCP *:sshell (LISTEN)
rsyslogd 6981 6984 in:injour root 5u IPv6 42992 0t0 TCP *:sshell (LISTEN)
rsyslogd 6981 6985 rs:main root 4u IPv4 42991 0t0 TCP *:sshell (LISTEN)
rsyslogd 6981 6985 rs:main root 5u IPv6 42992 0t0 TCP *:sshell (LISTEN)
rsyslogd 6981 6986 in:intcp root 4u IPv4 42991 0t0 TCP *:sshell (LISTEN)
rsyslogd 6981 6986 in:intcp root 5u IPv6 42992 0t0 TCP *:sshell (LISTEN)
rsyslogd 6981 6987 in:intcp root 4u IPv4 42991 0t0 TCP *:sshell (LISTEN)
rsyslogd 6981 6987 in:intcp root 5u IPv6 42992 0t0 TCP *:sshell (LISTEN)
rsyslogd 6981 6988 in:intcp root 4u IPv4 42991 0t0 TCP *:sshell (LISTEN)
rsyslogd 6981 6988 in:intcp root 5u IPv6 42992 0t0 TCP *:sshell (LISTEN)
rsyslogd 6981 6989 in:intcp root 4u IPv4 42991 0t0 TCP *:sshell (LISTEN)
rsyslogd 6981 6989 in:intcp root 5u IPv6 42992 0t0 TCP *:sshell (LISTEN)
[root@server.eadimidova.net rsyslog.d]# systemctl restart rsyslogd
Failed to restart rsyslogd.service: Unit rsyslogd.service not found.
[root@server.eadimidova.net rsyslog.d]# ls -l -i $14
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
rsyslogd 6981 root 4u IPv4 42991 0t0 TCP *:sshell (LISTEN)
rsyslogd 6981 root 5u IPv6 42992 0t0 TCP *:sshell (LISTEN)
[root@server.eadimidova.net rsyslog.d]# █

```

Рис. 3.2: Просмотр прослушиваемых портов, связанных с rsyslog

На сервере настроим межсетевой экран для приёма сообщений по ТСР-порту 514(3.3):

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

Рис. 3.3: Настройка межсетевого экрана для приёма сообщений по ТСР-порту

3.2 Настройка клиента сетевого журнала

На клиенте создадим файл конфигурации сетевого хранения журналов:

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

На клиенте в файле конфигурации `/etc/rsyslog.d/netlog-client.conf` включим перенаправление сообщений журнала на 514 TCP-порт сервера(3.4):

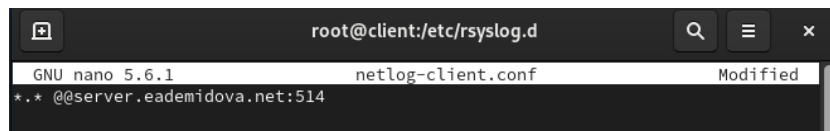


Рис. 3.4: Включение перенаправления сообщений журнала на 514 TCP-порт сервера

Перезапустим службу rsyslog:

```
systemctl restart rsyslog
```

3.3 Просмотр журнала

На сервере посмотрим один из файлов журнала(3.5):

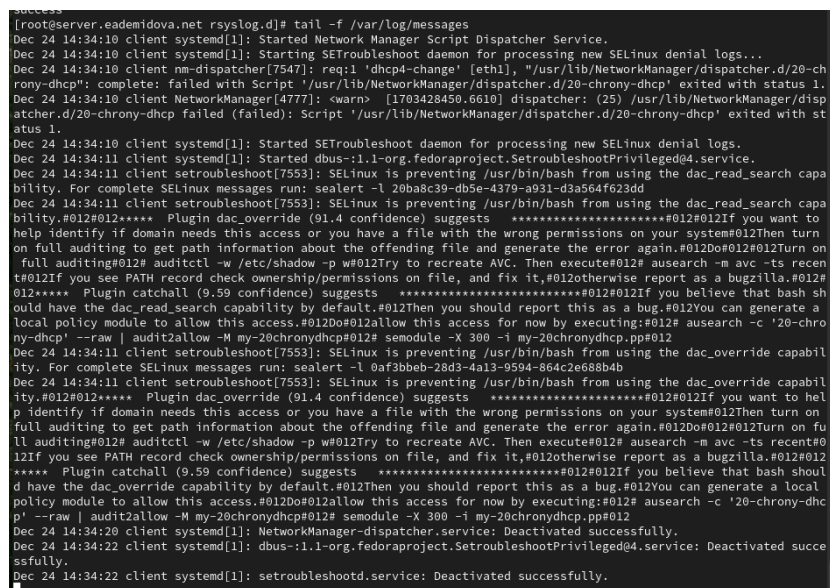


Рис. 3.5: Просмотр файла /var/log/messages журнала

На сервере под пользователем eademidova запустим графическую программу для просмотра журналов с помощью команды gnome-system-monitor(3.6):

Process Name	User	% CPU	ID	Memory	Disk read total	Disk write total
at-spi2-registr	eademidova	0.00	1853	299.0 kB	147.5 kB	
at-spi-bus-launcher	eademidova	0.00	1821	172.0 kB	389.1 kB	
bash	eademidova	0.00	6877	1.0 MB	23.0 MB	8
dbus-broker	eademidova	0.00	1747	1.2 MB	221.2 kB	
dbus-broker	eademidova	0.00	1827	315.4 kB	N/A	
dbus-broker-launch	eademidova	0.00	1746	172.0 kB	102.4 kB	
dbus-broker-launch	eademidova	0.00	1826	184.3 kB	N/A	
dconf-service	eademidova	0.00	2993	499.7 kB	352.3 kB	32
evolution-addressbook-factory	eademidova	0.00	3002	1.4 MB	5.8 MB	36
evolution-alarm-notify	eademidova	0.00	3546	3.7 MB	24.6 MB	
evolution-calendar-factory	eademidova	0.00	2951	1.4 MB	2.7 MB	
evolution-source-registry	eademidova	0.00	2897	1.1 MB	3.3 MB	
gjs	eademidova	0.00	3321	3.1 MB	4.5 MB	
gjs	eademidova	0.00	3551	3.2 MB	1.3 MB	
gnome-keyring-daemon	eademidova	0.00	1735	303.1 kB	N/A	
gnome-session-binary	eademidova	0.00	1738	N/A	12.4 MB	
gnome-session-binary	eademidova	0.00	2610	913.4 kB	7.6 MB	4

```
logout
[eademidova@server.eademidova.net ~]$ gnome-system-monitor
```

Рис. 3.6: Запуск графической программы для просмотра журналов

На сервере установите просмотрщик журналов системных сообщений lnav или его аналог:

```
dnf -y install lnav
```

Просмотрим логи с помощью lnav на клиенте и на сервере(3.7):

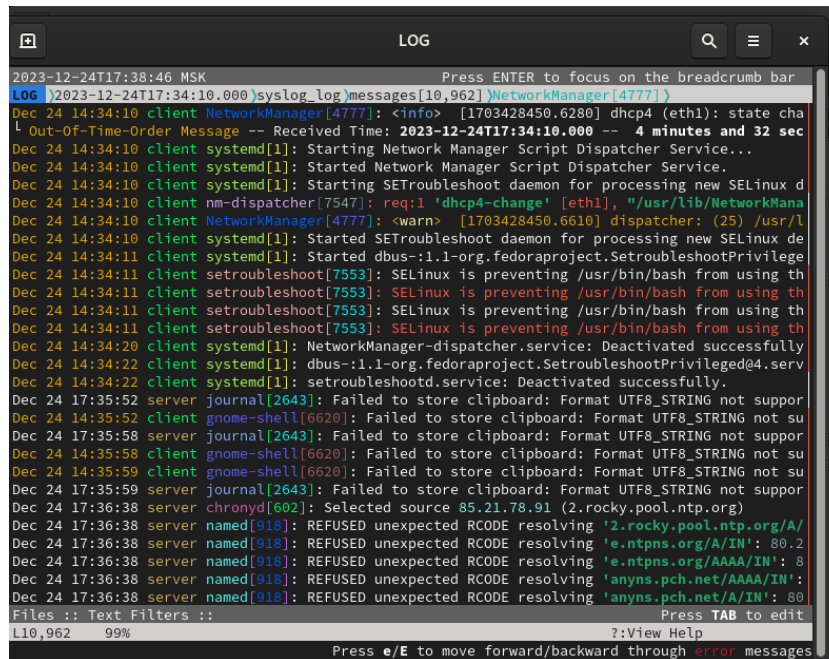


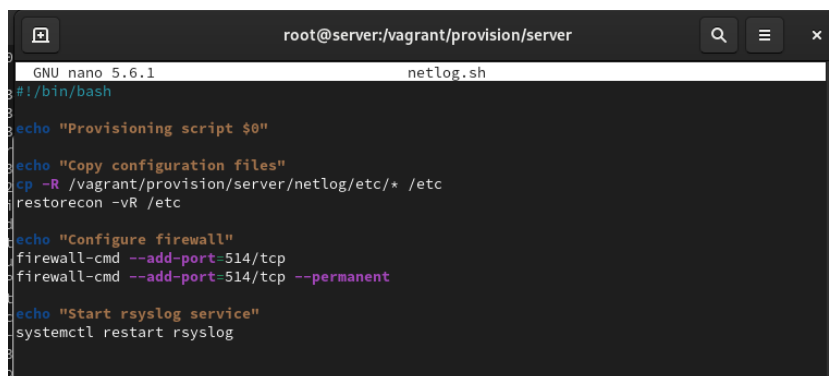
Рис. 3.7: Просмотр логов с клиента и сервера

3.4 Внесение изменений в настройки внутреннего окружения виртуальных машины

На виртуальной машине server перейдем в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создадим в нём каталог `netlog`, в который поместим в соответствующие подкаталоги конфигурационные файлы, а также создадим исполняемый файл `netlog.sh`:

```
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
touch netlog.sh
chmod +x netlog.sh
```

В каталоге `/vagrant/provision/server` создадим исполняемый файл `netlog.sh` и внесем скрипт(3.8):

A screenshot of a terminal window titled 'root@server:/vagrant/provision/server'. The terminal shows the GNU nano 5.6.1 editor editing the file 'netlog.sh'. The script content is as follows:

```
#!/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

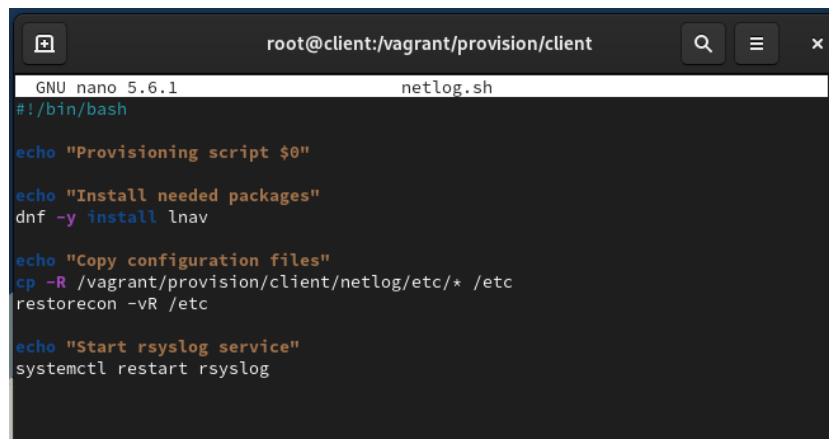
echo "Start rsyslog service"
systemctl restart rsyslog
```

Рис. 3.8: Скрипта файла `/vagrant/provision/server/netlog.sh`

На виртуальной машине `client` перейдем в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/client/`, создадим в нём каталог `netlog`, в который поместим в соответствующие подкаталоги конфигурационные файлы, а также создадим исполняемый файл `netlog.sh`:

```
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/
touch netlog.sh
chmod +x netlog.sh
```

В каталоге `/vagrant/provision/client` создадим исполняемый файл `netlog.sh` и внесем скрипт(3.9):

A screenshot of a terminal window with a dark background. The title bar shows 'root@client:/vagrant/provision/client'. The terminal is running GNU nano 5.6.1 editing a file named 'netlog.sh'. The script content is as follows:

```
#!/bin/bash

echo "Provisioning script $@"

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. 3.9: Скрипта файла /vagrant/provision/client/ netlog.sh

Затем для отработки созданных скриптов 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"
client.vm.provision "client netlog",
  type: "shell",
  preserve_order: true,
  path: "provision/client/netlog.sh"
```

4 Контрольные вопросы

1. Какой модуль rsyslog вы должны использовать для приёма сообщений от journald?
2. Как называется устаревший модуль, который можно использовать для включения приёма сообщений журнала в rsyslog?
3. Чтобы убедиться, что устаревший метод приёма сообщений из journald в rsyslog не используется, какой дополнительный параметр следует использовать?
4. В каком конфигурационном файле содержатся настройки, которые позволяют вам настраивать работу журнала?
5. Каким параметром управляется пересылка сообщений из journald в rsyslog?
6. Какой модуль rsyslog вы можете использовать для включения сообщений из файла журнала, не созданного rsyslog?
7. Какой модуль rsyslog вам нужно использовать для пересылки сообщений в базу данных MariaDB?
8. Какие две строки вам нужно включить в rsyslog.conf, чтобы позволить текущему журнальному серверу получать сообщения через TCP?
9. Как настроить локальный брандмауэр, чтобы разрешить приём сообщений журнала через порт TCP 514?

10. Для приёма сообщений от journald вам следует использовать модуль imjournal.
11. Устаревший модуль, который можно использовать для включения приёма сообщений журнала в rsyslog, называется imklog.
12. Чтобы убедиться, что устаревший метод приёма сообщений из journald не используется, следует использовать параметр “SystemCallFilter [include:omusrmsg.conf?]” в конфигурационном файле rsyslog.conf.
13. Настройки, позволяющие настраивать работу журнала, содержатся в конфигурационном файле rsyslog.conf.
14. Пересылка сообщений из journald в rsyslog управляется параметром “ForwardToSyslog” в файле конфигурации journald.conf.
15. Модуль rsyslog, который можно использовать для включения сообщений из файла журнала, не созданного rsyslog, называется imfile.
16. Для пересылки сообщений в базу данных MariaDB вам следует использовать модуль ommysql.
17. Для позволения текущему журнальному серверу получать сообщения через TCP, вам нужно включить две строки в rsyslog.conf:

\$ModLoad imtcp \$InputTCPServerRun 514
18. Чтобы разрешить приём сообщений журнала через порт TCP 514 можно использовать следующую команду:

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

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

5 Выводы

В результате выполнения данной работы были приобретены практические навыки по работе с журналами системных событий.