

Отчёт по лабораторной работе 15

Настройка сетевого журналирования

Заур Мустафеев

Содержание

1	Цель работы	5
2	Выполнение работы	6
2.1	Настройка сервера сетевого журнала	6
2.2	Настройка клиента сетевого журнала	7
2.3	Проверка приёма и просмотра журналов	8
2.4	Автоматизация настройки с помощью provisioning-скриптов . . .	10
3	Вывод	12
4	Контрольные вопросы	13

Список иллюстраций

2.1	Конфигурация netlog-server.conf	6
2.2	Проверка прослушиваемых портов rsyslog	7
2.3	Настройка firewall для порта 514	7
2.4	Конфигурация netlog-client.conf	8
2.5	Просмотр сообщений журнала на сервере	9
2.6	Мониторинг ресурсов системы	9
2.7	Попытка установки lnav	10
2.8	Provisioning-скрипт сервера	11

Список таблиц

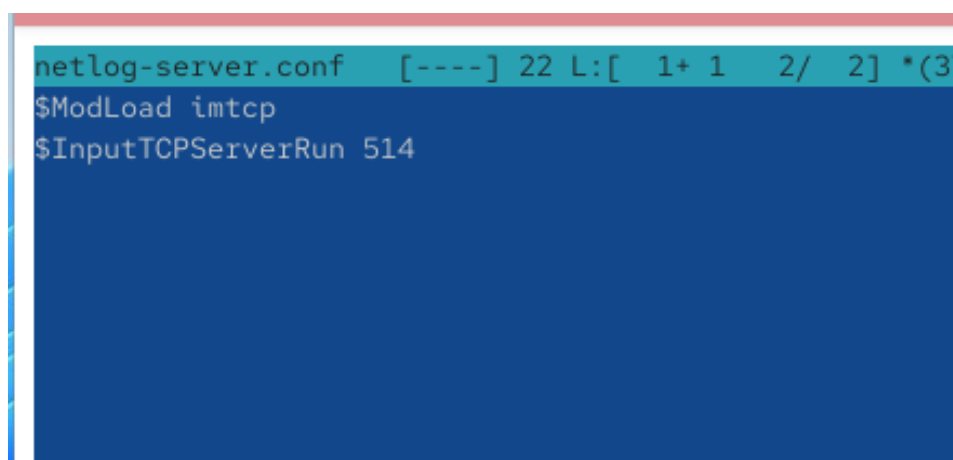
1 Цель работы

Получение навыков по работе с журналами системных событий.

2 Выполнение работы

2.1 Настройка сервера сетевого журнала

1. На виртуальной машине **server** был создан файл конфигурации сетевого хранения журналов. Для этого выполнен переход в каталог `/etc/rsyslog.d`, после чего создан файл `netlog-server.conf`.
2. В файле `/etc/rsyslog.d/netlog-server.conf` включён приём сообщений журнала по протоколу TCP на порту **514**. Для этого были добавлены директивы загрузки модуля TCP и запуска TCP-сервера rsyslog.



```
netlog-server.conf [-----] 22 L:[ 1+ 1 2/ 2] *(37
$ModLoad imtcp
$InputTCPServerRun 514
```

Рис. 2.1: Конфигурация netlog-server.conf

3. После внесения изменений служба **rsyslog** была перезапущена. С помощью утилиты **lsof** проверено, что служба прослушивает TCP-порт 514 и готова принимать входящие соединения.

```
rsyslogd 11220 root 4u IPv4 58857 0t0 TCP *:shell (LISTEN)
rsyslogd 11220 root 5u IPv6 58858 0t0 TCP *:shell (LISTEN)
rsyslogd 11220 11222 in:imjour root 4u IPv4 58857 0t0 TCP *:shell (LISTEN)
rsyslogd 11220 11222 in:imjour root 5u IPv6 58858 0t0 TCP *:shell (LISTEN)
rsyslogd 11220 11223 in:imtcp root 4u IPv4 58857 0t0 TCP *:shell (LISTEN)
rsyslogd 11220 11223 in:imtcp root 5u IPv6 58858 0t0 TCP *:shell (LISTEN)
rsyslogd 11220 11224 in:imtcp root 4u IPv4 58857 0t0 TCP *:shell (LISTEN)
rsyslogd 11220 11224 in:imtcp root 5u IPv6 58858 0t0 TCP *:shell (LISTEN)
rsyslogd 11220 11225 in:imtcp root 4u IPv4 58857 0t0 TCP *:shell (LISTEN)
rsyslogd 11220 11225 in:imtcp root 5u IPv6 58858 0t0 TCP *:shell (LISTEN)
rsyslogd 11220 11226 in:imtcp root 4u IPv4 58857 0t0 TCP *:shell (LISTEN)
rsyslogd 11220 11226 in:imtcp root 5u IPv6 58858 0t0 TCP *:shell (LISTEN)
rsyslogd 11220 11227 in:imtcp root 4u IPv4 58857 0t0 TCP *:shell (LISTEN)
rsyslogd 11220 11227 in:imtcp root 5u IPv6 58858 0t0 TCP *:shell (LISTEN)
rsyslogd 11220 11228 rs:main root 4u IPv4 58857 0t0 TCP *:shell (LISTEN)
rsyslogd 11220 11228 rs:main root 5u IPv6 58858 0t0 TCP *:shell (LISTEN)
[root@server.zmustafaev.net rsyslog.d]# firewall-cmd --add-port=514/tcp
success
[root@server.zmustafaev.net rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent
success
[root@server.zmustafaev.net rsyslog.d]#
```

Рис. 2.2: Проверка прослушиваемых портов rsyslog

4. Для обеспечения сетевого доступа к серверу журналов были добавлены правила межсетевого экрана, разрешающие входящие подключения к TCP-порту 514. Изменения применены как временно, так и на постоянной основе.

```
root@client:/etc/rsyslog.d -- sudo -i
netlog-client.conf [----] 31 L:[ 1+ 0 1/ 1] *(31 / 31b) <
.* @server.zmustafaev.net:514
```

Рис. 2.3: Настройка firewall для порта 514

2.2 Настройка клиента сетевого журнала

1. На виртуальной машине **client** в каталоге `/etc/rsyslog.d` создан файл конфигурации `netlog-client.conf`, предназначенный для настройки пересыл-

ки журналов на удалённый сервер.

2. В файле `/etc/rsyslog.d/netlog-client.conf` включено перенаправление всех сообщений журнала на сервер по TCP-протоколу на порт 514 с использованием синтаксиса `@@`, что указывает на надёжную TCP-передачу.

```
Dec 12 14:05:56 server systemd[1]: systemd-coredump@105-11594-0.service: Deactivated successfully.
Dec 12 14:05:54 client kernel: traps: VBoxClient[14015] trap int3 ip:41dd1b sp:7f5a61a35cd0 error:0 in VBoxClient[1dd1b,400000+bb000]
Dec 12 14:05:54 client systemd-coredump[14016]: Process 14012 (VBoxClient) of user 1001 terminated abnormally with signal 5/TRAP, processing...
Dec 12 14:05:54 client systemd[1]: Started systemd-coredump@86-14016-0.service - Process Core Dump (PID 14016/UID 0).
Dec 12 14:05:54 client systemd-coredump[14017]: Process 14012 (VBoxClient) of user 1001 dumped core.#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 14015:#012#0 0x000000000041dd1b n/a (n/a + 0x0)#012#1 0x000000000041dc94 n/a (n/a + 0x0)#012#2 0x000000000045041c n/a (n/a + 0x0)#012#3 0x00000000000043
```

Рис. 2.4: Конфигурация `netlog-client.conf`

3. После изменения конфигурации служба **rsyslog** на клиенте была перезапущена для применения новых настроек.

2.3 Проверка приёма и просмотра журналов

1. На сервере выполнен просмотр системного журнала `/var/log/messages` в режиме реального времени с помощью команды `tail -f`. Установлено, что в журнале отображаются сообщения как от локальной системы, так и от удалённого клиента.



Рис. 2.5: Просмотр сообщений журнала на сервере

2. Под пользовательской сессией на сервере была запущена графическая утилита **gnome-system-monitor**, с помощью которой выполнен анализ нагрузки на ресурсы системы и сетевой активности.

```
[root@server.zmustafaev.net rsyslog.d]#
[root@server.zmustafaev.net rsyslog.d]# dnf -y install lnav
Extra Packages for Enterprise Linux 10 - x86_64
Extra Packages for Enterprise Linux 10 - x86_64
Rocky Linux 10 - BaseOS
Rocky Linux 10 - BaseOS
Rocky Linux 10 - AppStream
Rocky Linux 10 - AppStream
Rocky Linux 10 - CRB
Rocky Linux 10 - CRB
Rocky Linux 10 - Extras
Rocky Linux 10 - Extras
No match for argument: lnav
Error: Unable to find a match: lnav
[root@server.zmustafaev.net rsyslog.d]#
```

70 kB/s	28 kB	00:00
15 MB/s	5.6 MB	00:00
9.6 kB/s	4.3 kB	00:00
14 MB/s	4.1 MB	00:00
3.5 kB/s	4.3 kB	00:01
4.7 MB/s	2.0 MB	00:00
9.5 kB/s	4.3 kB	00:00
1.0 MB/s	484 kB	00:00
4.9 kB/s	3.1 kB	00:00
5.2 kB/s	4.8 kB	00:00

Рис. 2.6: Мониторинг ресурсов системы

3. Выполнена попытка установки консольного просмотрщика журналов **lnav**. В процессе установки получено сообщение об отсутствии пакета в доступ-

ных репозиториях, что свидетельствует о необходимости дополнительной настройки источников пакетов либо использования альтернативных средств.

```
1  #!/bin/bash
2  echo "Provisioning script $0"
3  echo "Copy configuration files"
4  cp -R /vagrant/provision/server/netlog/etc/* /etc
5  restorecon -vR /etc
6  echo "Configure firewall"
7  firewall-cmd --add-port=514/tcp
8  firewall-cmd --add-port=514/tcp --permanent
9  echo "Start rsyslog service"
10 systemctl restart rsyslog
```

Рис. 2.7: Попытка установки lnav

2.4 Автоматизация настройки с помощью provisioning-скриптов

1. На виртуальной машине **server** в каталоге `/vagrant/provision/server` создана структура каталогов для хранения конфигурационных файлов сетевого журнала. В неё был скопирован файл `netlog-server.conf` с сохранением структуры каталогов.
2. В каталоге `/vagrant/provision/server` создан исполняемый скрипт `netlog.sh`, предназначенный для автоматической настройки сервера сетевого журнала. Скрипт выполняет копирование конфигурационных файлов, настройку межсетевого экрана и перезапуск службы `rsyslog`.

```
1  #!/bin/bash
2  echo "Provisioning script $0"
3  echo "Install needed packages"
4  dnf -y install lnav
5  echo "Copy configuration files"
6  cp -R /vagrant/provision/client/netlog/etc/* /etc
7  restorecon -vR /etc
8  echo "Start rsyslog service"
9  systemctl restart rsyslog
```

Рис. 2.8: Provisioning-скрипт сервера

3. Аналогичный provisioning-скрипт был подготовлен для клиентской виртуальной машины и включает установку необходимых пакетов, копирование конфигурации и перезапуск службы rsyslog, что обеспечивает автоматическую настройку клиента сетевого журнала.

3 Вывод

В ходе работы был настроен сервер сетевого журнала на основе rsyslog. Реализован приём журналов по TCP-протоколу на порту 514, а также настроена пересылка сообщений с клиентской виртуальной машины на сервер. Проверена корректность приёма и отображения журналов, выполнена настройка межсетевого экрана и подготовлены provisioning-скрипты для автоматизации развёртывания, что упрощает повторную настройку среды и снижает вероятность ошибок.

4 Контрольные вопросы

1. **Какой модуль rsyslog вы должны использовать для приёма сообщений от journald?**

Для приёма сообщений от journald используется модуль imjournal.

2. **Как называется устаревший модуль, который можно использовать для включения приёма сообщений журнала в rsyslog?**

Устаревшим модулем является imuxsock, который получает сообщения через сокет /dev/log.

3. **Чтобы убедиться, что устаревший метод приёма сообщений из journald в rsyslog не используется, какой дополнительный параметр следует использовать?**

Необходимо использовать параметр UseJournal="on" в настройках модуля imjournal, чтобы rsyslog работал напрямую с journald.

4. **В каком конфигурационном файле содержатся настройки, которые позволяют вам настраивать работу журнала?**

Основные настройки журнала systemd находятся в файле /etc/systemd/journald.conf.

5. **Каким параметром управляется пересылка сообщений из journald в rsyslog?**

Пересылка сообщений управляется параметром ForwardToSyslog в файле journald.conf.

6. **Какой модуль rsyslog вы можете использовать для включения сообще-**

ний из файла журнала, не созданного rsyslog?

Для чтения сообщений из произвольных файлов используется модуль `imfile`.

- 7. Какой модуль rsyslog вам нужно использовать для пересылки сообщений в базу данных MariaDB?**

Для пересылки сообщений в MariaDB используется модуль `ommysql`.

- 8. Какие две строки вам нужно включить в rsyslog.conf, чтобы позволить текущему журнальному серверу получать сообщения через TCP?**

Необходимо добавить следующие строки:

```
$ModLoad imtcp
```

```
$InputTCPServerRun 514
```

- 9. Как настроить локальный брандмауэр, чтобы разрешить приём сообщений журнала через порт TCP 514?**

Для этого используются команды:

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

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