Отчёт по лабораторной работе 15

Настройка сетевого журналирования

Сейдалиев Тагиетдин Ровшенович

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получение навыков по работе с журналами системных событий.

2 Выполнение

2.1 Настройка сервера сетевого журнала

В каталоге `/etc/rsyslog.d` был создан конфигурационный файл `netlog-server.conf`, содержащий строки для загрузки модуля `imtcp` и запуска TCP-сервера на порту 514. Это позволяет серверу принимать входящие сообщения журналов от клиентов по TCP.

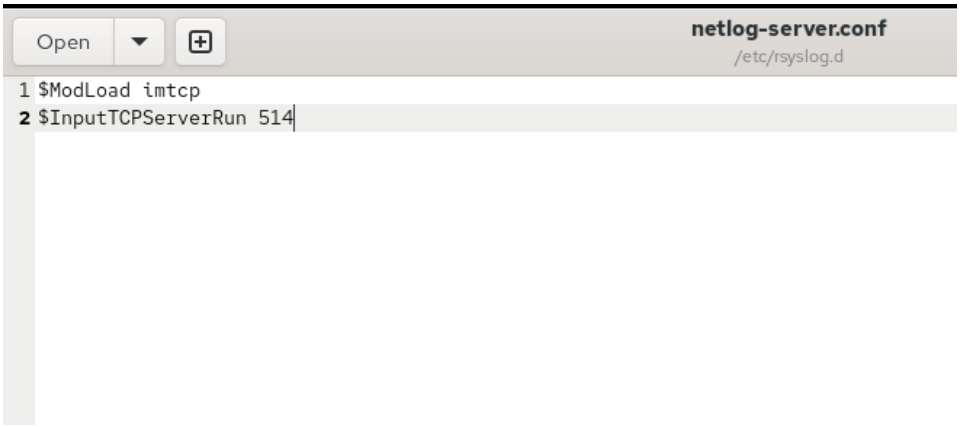

Рис. 2.1: Файл netlog-server.conf с включённым приёмом сообщений по TCP 514

После внесения настроек служба `rsyslog` была перезапущена, а затем просмотрены открытые TCP-порты, связанные с `rsyslogd`. В выводе отображены прослушиваемые порты и работающие процессы. Также через межсетевой экран был открыт порт 514/tcp, временно и на постоянной основе.

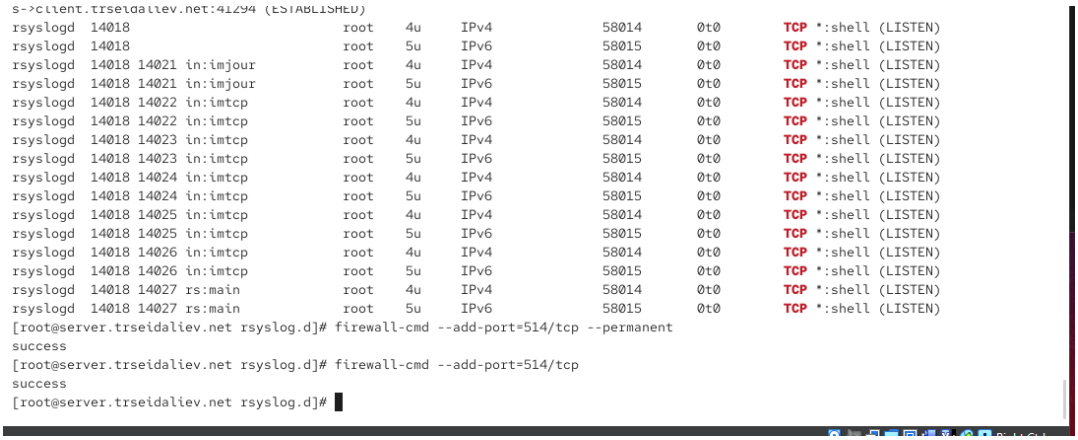

Рис. 2.2: Вывод lsof с TCP-портами rsyslog и команды настройки firewall-cmd

2.2 Настройка клиента сетевого журнала

На клиенте был создан конфигурационный файл `netlog-client.conf`, в котором включена пересылка всех сообщений журнала на сервер по TCP-порту 514. Для перенаправления используется запись `*.* @@server.trseidaliev.net:514`.

Рис. 2.3: Файл netlog-client.conf с перенаправлением логов на сервер по TCP 514

Служба `rsyslog` была перезапущена для применения настроек.

2.3 Просмотр журнала

Для проверки корректности работы логирования на сервере просматривался файл `/var/log/messages` в реальном времени. В выводе присутствуют как локаль-

ные сообщения сервера, так и записи, пришедшие от клиента, что указывает на успешную передачу данных.

```
Dec 11 10:52:50 server systemd[1]: systemd-coredump@113-14434-0.service: Deactivated successfully.
Dec 11 10:52:51 client kernel: traps: VBoxClient[14264] trap int3 ip:41dd1b sp:7f49912cfcd0 error:0 in VBoxClient[1dd1b,400000+bb000]
Dec 11 10:52:51 client systemd-coredump[14265]: Process 14261 (VBoxClient) of user 1001 terminated abnormally with signal 5/TRAP, pro
cessing...
Dec 11 10:52:51 client systemd[1]: Started systemd-coredump@103-14265-0.service - Process Core Dump (PID 14265/UID 0).
Dec 11 10:52:51 client systemd-coredump[14266]: Process 14261 (VBoxClient) of user 1001 dumped core.#012#012Module libXau.so.6 from r
pm 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 libX11-1.8.1
0-1.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 14264:#012#0  0x00000000041dd1b n/a (n/a + 0x0)#012#1  0x00000000041dc94 n/a (n/a + 0x0)#012#2
  0x000000000045041c n/a (n/a + 0x0)#012#3  0x00000000004355d0 n/a (n/a + 0x0)#012#4  0x00007f499f98bb68 start_thread (libc.so.6 + 0x
```

Рис. 2.4: Журнал /var/log/messages с сообщениями от client и server

На сервере под пользователем `trseidaliev` был запущен графический просмотрщик системных ресурсов и процессов `gnome-system-monitor`, что позволяет анализировать состояние системы и активность процессов.

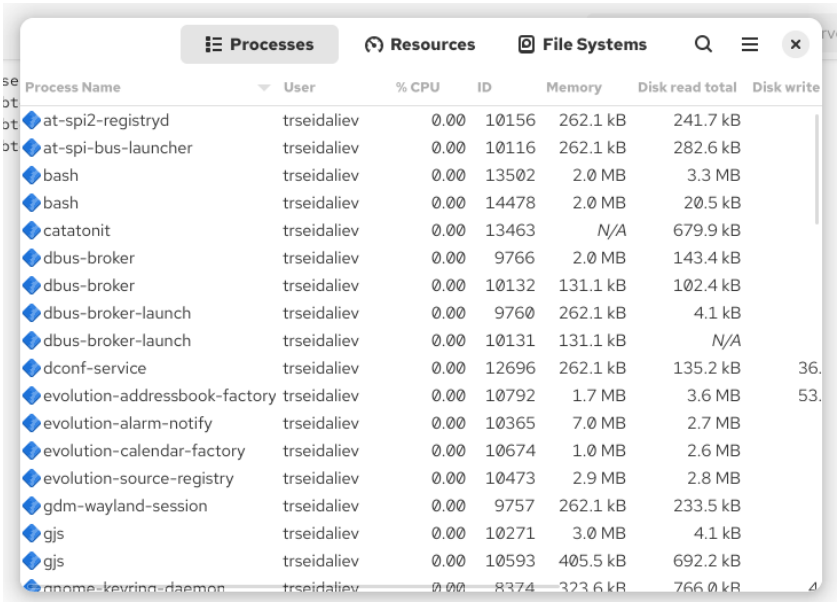

Рис. 2.5: Запущенная графическая утилита gnome-system-monitor под пользователем trseidaliev

Также предпринималась попытка установки просмотрщика логов `lnav`. Однако пакет отсутствует в репозиториях, о чём сообщает вывод менеджера пакетов.

```
[root@server.trseidaliev.net rsyslog.d]#
[root@server.trseidaliev.net rsyslog.d]# dnf -y install lnav
Extra Packages for Enterprise Linux 10 - x86_64                  46 kB/s |  16 kB     00:00
Extra Packages for Enterprise Linux 10 - x86_64                  14 MB/s | 5.6 MB     00:00
Rocky Linux 10 - BaseOS                                         5.8 kB/s | 4.3 kB     00:00
Rocky Linux 10 - AppStream                                       18 kB/s | 4.3 kB     00:00
Rocky Linux 10 - CRB                                             14 kB/s | 4.3 kB     00:00
Rocky Linux 10 - Extras                                          13 kB/s | 3.1 kB     00:00
No match for argument: lnav
Error: Unable to find a match: lnav
[root@server.trseidaliev.net rsyslog.d]#
```

Рис. 2.6: Попытка установки lnav с ошибкой «No match for argument»

2.4 Внесение изменений в настройки внутреннего окружения виртуальных машин

В каталоге `/vagrant/provision/server/` была создана структура `netlog/etc/rsyslog.d`, в которую помещён файл конфигурации `netlog-server.conf`. Далее был создан файл `netlog.sh`, выполняющий копирование файлов, восстановление контекстов SELinux, настройку firewall и перезапуск `rsyslog`.

Vagrantfile | netlog.sh

```
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
11
```

Рис. 2.7: Скрипт провижининга netlog.sh для серверной ВМ

В каталоге `/vagrant/provision/client/` была создана аналогичная структура `netlog/etc/rsyslog.d`, куда был помещён файл `netlog-client.conf`. Затем был создан файл `netlog.sh`, выполняющий установку необходимых пакетов, копирование конфигураций и перезапуск службы `rsyslog`.

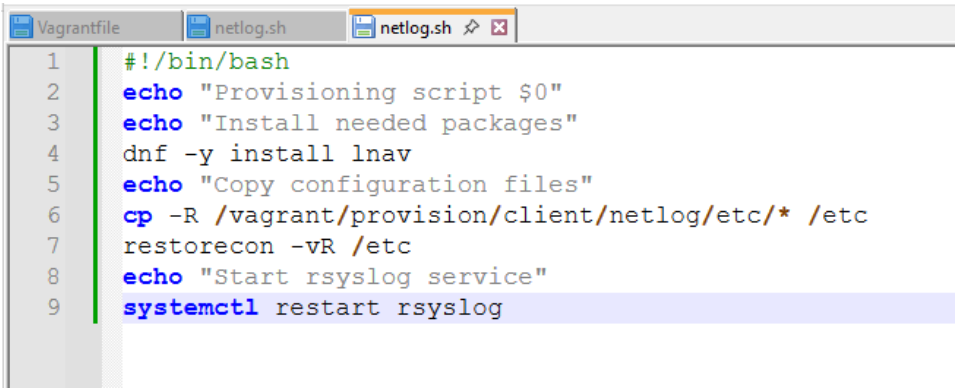

Рис. 2.8: Скрипт провижининга netlog.sh для клиентской ВМ

3 Заключение

В ходе выполнения работы:

- настроен сервер сетевого журналирования с использованием rsyslog и включён приём сообщений по TCP-порту 514;
- создан файл `netlog-server.conf`, активирующий модуль imtcp и работу TCP-сервера журнала;
- проверена работа службы rsyslog и прослушиваемые ею порты, а также открыты необходимые правила в локальном межсетевом экране;
- на клиентской машине создан и настроен файл `netlog-client.conf` для пересылки всех сообщений журнала на сервер;
- выполнена проверка доставки сообщений — в системном журнале сервера отображаются записи как локального хоста, так и клиентской машины;
- произведён просмотр логов с использованием `tail`, `gnome-system-monitor` и попытка установки инструмента lnav;
- подготовлены каталоги, конфигурационные файлы и скрипты провижининга Vagrant для автоматизации настройки сетевого журналирования на сервере и клиенте;
- обеспечено автоматическое копирование конфигураций, настройка SELinux-контекстов, открытие порта 514 и перезапуск rsyslog при развёртывании виртуальных машин.

4 Контрольные вопросы

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

Для приёма сообщений от `journald` используется модуль **imjournal**.
Он обеспечивает интеграцию rsyslog с системным журналом systemd.

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

Устаревшим модулем является **imuxsock**.
Он использовался для чтения сокета `/dev/log`, но в современных системах заменён `imjournal`.

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

Следует использовать параметр:

```
SystemLogSocketName=""
```

Его добавляют в конфигурацию journald, чтобы исключить создание сокета `/run/systemd/journal/syslog` и предотвратить передачу сообщений через старый механизм.

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

Настройки journald находятся в файле:

```
/etc/systemd/journald.conf
```

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

За пересылку отвечает параметр:

```
ForwardToSyslog=
```

Если значение `yes`, journald отправляет сообщения в rsyslog.

4.6 6. Какой модуль rsyslog вы можете использовать для включения сообщений из файла журнала, не созданного rsyslog?

Для этого применяется модуль **imfile**.
Он позволяет rsyslog отслеживать любые текстовые файлы и импортировать их содержимое в систему журналирования.

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

Для работы с MariaDB используется модуль **ommysql**.
Он позволяет rsyslog записывать сообщения в таблицы SQL-базы.

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

Необходимы строки:

```
$ModLoad imtcp
$InputTCPServerRun 514
```

Они включают TCP-модуль и запускают сервер на порту 514.

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

Следует открыть порт 514/tcp:

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

После этого необходимо выполнить перезагрузку правил:

```
firewall-cmd --reload
```