Лабораторная работа №15

Настройка сетевого журналирования

Ромицына Анастасия Романовна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

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

2 Выполнение лабораторной работы

На сервере создадим файл конфигурации сетевого хранения журналов(рис. 2.1).

Рис. 2.1: Создание на сервере файла конфигурации сетевого хранения журналов.

В файле конфигурации /etc/rsyslog.d/netlog-server.conf включим приём записей журнала по TCP-порту 514 (рис. 2.2).

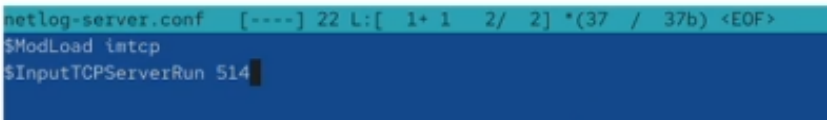


Рис. 2.2: Включение в файле конфигурации /etc/rsyslog.d/netlog-server.conf приёма записей журнала по TCP-порту 514.

Перезапустим службу rsyslog и посмотрим, какие порты, связанные с rsyslog, прослушиваются(рис. 2.3).

Рис. 2.3: Перезапуск службы rsyslog и просмотр прослушиваемых портов, связанных с rsyslog.

На сервере настроим межсетевой экран для приёма сообщений по TCP-порту 514(рис. 2.4).

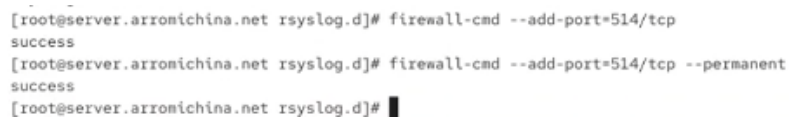


Рис. 2.4: Настройка на сервере межсетевого экрана для приёма сообщений по TCP-порту 514.

На клиенте создадим файл конфигурации сетевого хранения журналов (рис. 2.5).

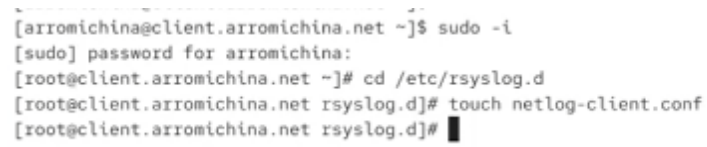


Рис. 2.5: Создание на клиенте файла конфигурации сетевого хранения журналов.

Далее в файле конфигурации /etc/rsyslog.d/netlog-client.conf включим перенаправление сообщений журнала на 514 TCP-порт сервера (рис. 2.6).

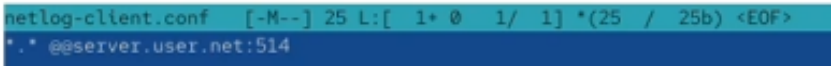


Рис. 2.6: Включение в файле конфигурации /etc/rsyslog.d/netlog-client.conf перенаправления сообщений журнала на 514 TCP-порт сервера.

Перезапустим службу rsyslog (рис. 2.7).

Рис. 2.7: Перезапуск службы rsyslog.

На сервере просмотрим один из файлов журнала(рис. 2.8).

Рис. 2.8: Просмотр на сервере одного из файлов журнала.

На сервере под пользователем arromichina запустим графическую программу для просмотра журналов (рис. 2.9).

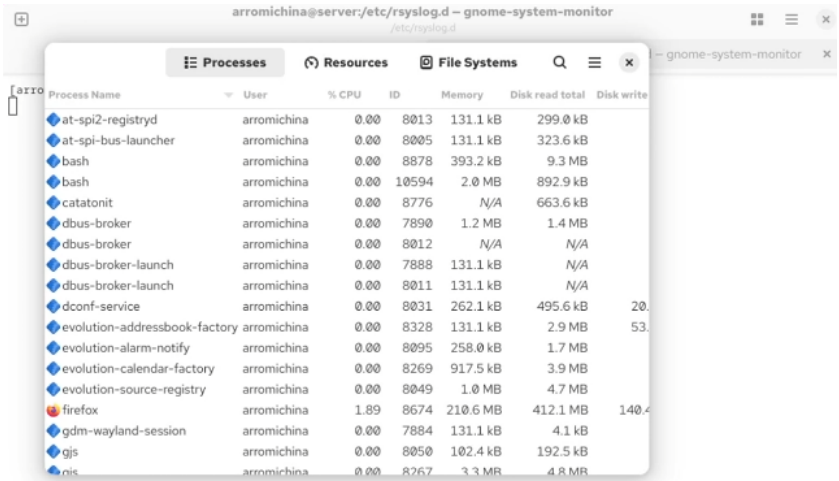
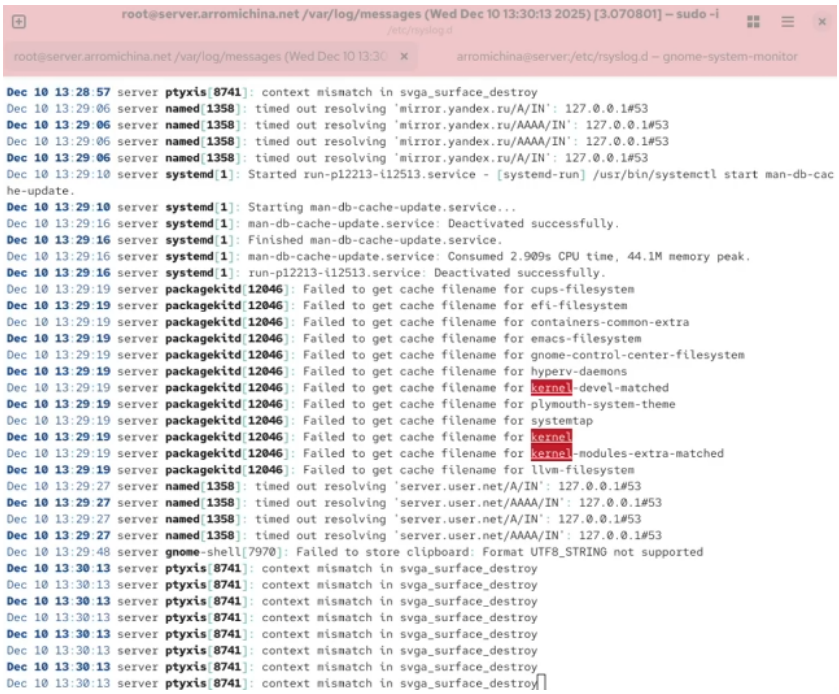


Рис. 2.9: Запуск на сервере под пользователем arromichina графической программы для просмотра журналов.

На сервере установим просмотрщик журналов системных сообщений(рис. 2.10).



```
[root@server.arromichina.net rsyslog.d]# sudo dnf install -y multitail
Last metadata expiration check: 0:50:41 ago on Wed 10 Dec 2025 12:38:23 PM UTC.
Dependencies resolved.
==========================================================================================================
 Package                     Architecture               Version                            Repository
==========================================================================================================
Installing:
 multitail                   x86_64                     7.1.3-2.el10_0                     epel

Transaction Summary
==========================================================================================================
Install  1 Package

Total download size: 148 k
Installed size: 326 k
Downloading Packages:
multitail-7.1.3-2.el10_0.x86_64.rpm                                                   108 kB/s | 148 kB
----------------------------------------------------------------------------------------------------------
Total                                                                                  73 kB/s | 148 kB
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :
  Installing       : multitail-7.1.3-2.el10_0.x86_64
  Running scriptlet: multitail-7.1.3-2.el10_0.x86_64
```

Рис. 2.10: Установка на сервере просмотрщика журналов системных сообщений.

Просмотрим логи(рис. 2.11).

```
Dec 10 13:28:57 server ptyxis[8741]: context mismatch in svga_surface_destroy
Dec 10 13:29:06 server named[1358]: timed out resolving 'mirror.yandex.ru/A/IN': 127.0.0.1#53
Dec 10 13:29:06 server named[1358]: timed out resolving 'mirror.yandex.ru/AAAA/IN': 127.0.0.1#53
Dec 10 13:29:06 server named[1358]: timed out resolving 'mirror.yandex.ru/AAAA/IN': 127.0.0.1#53
Dec 10 13:29:06 server named[1358]: timed out resolving 'mirror.yandex.ru/A/IN': 127.0.0.1#53
Dec 10 13:29:10 server systemd[1]: Started run-p12213-i12513.service - [systemd-run] /usr/bin/systemctl start man-db-cac
he-update.
Dec 10 13:29:10 server systemd[1]: Starting man-db-cache-update.service...
Dec 10 13:29:16 server systemd[1]: man-db-cache-update.service: Deactivated successfully.
Dec 10 13:29:16 server systemd[1]: Finished man-db-cache-update.service.
Dec 10 13:29:16 server systemd[1]: man-db-cache-update.service: Consumed 2.909s CPU time, 44.1M memory peak.
Dec 10 13:29:16 server systemd[1]: run-p12213-i12513.service: Deactivated successfully.
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for cups-filesystem
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for efi-filesystem
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for containers-common-extra
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for emacs-filesystem
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for gnome-control-center-filesystem
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for hyperv-daemons
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for kernel-devel-matched
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for plymouth-system-theme
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for systemtap
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for kernel
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for kernel-modules-extra-matched
Dec 10 13:29:19 server packagekitd[12046]: Failed to get cache filename for llvm-filesystem
Dec 10 13:29:27 server named[1358]: timed out resolving 'server.user.net/A/IN': 127.0.0.1#53
Dec 10 13:29:27 server named[1358]: timed out resolving 'server.user.net/AAAA/IN': 127.0.0.1#53
Dec 10 13:29:27 server named[1358]: timed out resolving 'server.user.net/A/IN': 127.0.0.1#53
Dec 10 13:29:27 server named[1358]: timed out resolving 'server.user.net/AAAA/IN': 127.0.0.1#53
Dec 10 13:29:48 server gnome-shell[7970]: Failed to store clipboard: Format UTF8_STRING not supported
Dec 10 13:30:13 server ptyxis[8741]: context mismatch in svga_surface_destroy
Dec 10 13:30:13 server ptyxis[8741]: context mismatch in svga_surface_destroy
Dec 10 13:30:13 server ptyxis[8741]: context mismatch in svga_surface_destroy
Dec 10 13:30:13 server ptyxis[8741]: context mismatch in svga_surface_destroy
Dec 10 13:30:13 server ptyxis[8741]: context mismatch in svga_surface_destroy
Dec 10 13:30:13 server ptyxis[8741]: context mismatch in svga_surface_destroy
Dec 10 13:30:13 server ptyxis[8741]: context mismatch in svga_surface_destroy
Dec 10 13:30:13 server ptyxis[8741]: context mismatch in svga_surface_destroy
```

Рис. 2.11: Просмотр логов.

На виртуальной машине server перейдём 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. В каталоге /vagrant/provision/server создадим исполняемый файл netlog.sh(рис. 2.12).

Рис. 2.12: Переход на виртуальной машине server в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога netlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге /vagrant/provision/server исполняемого файла netlog.sh.

Открыв его на редактирование, пропишем в нём скрипт (рис. 2.13).

Рис. 2.13: Открытие файла на редактирование и добавление в него скрипта.

На виртуальной машине client перейдём в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создадим в нём каталог nentlog, в который поместим в соответствующие подкаталоги конфигурационные файлы. В каталоге /vagrant/provision/client создадим исполняемый файл netlog.sh(рис. 2.14).

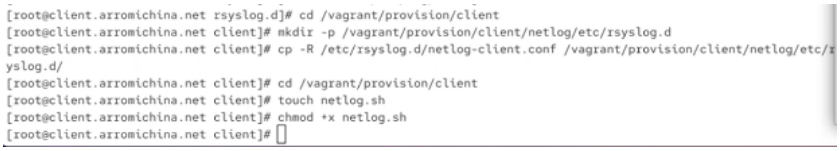


Рис. 2.14: Переход на виртуальной машине client в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создание в нём каталога nentlog, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге /vagrant/provision/client исполняемого файла netlog.sh.

Открыв его на редактирование, пропишем в нём скрипт (рис. 2.15).

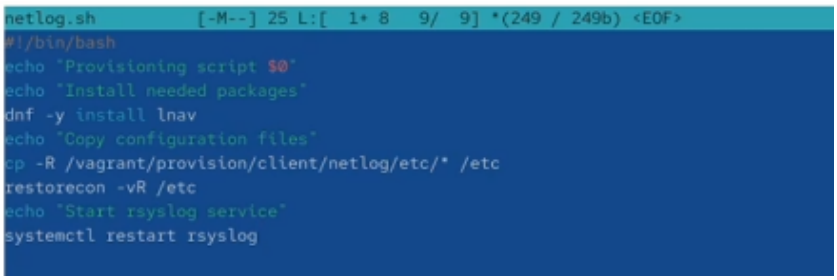


Рис. 2.15: Открытие файла на редактирование и добавление в него скрипта.

Для отработки созданных скриптов во время загрузки виртуальных машин server и client в конфигурационном файле Vagrantfile добавим в соответствующих разделах конфигураций для сервера и клиента (рис. 2.16).

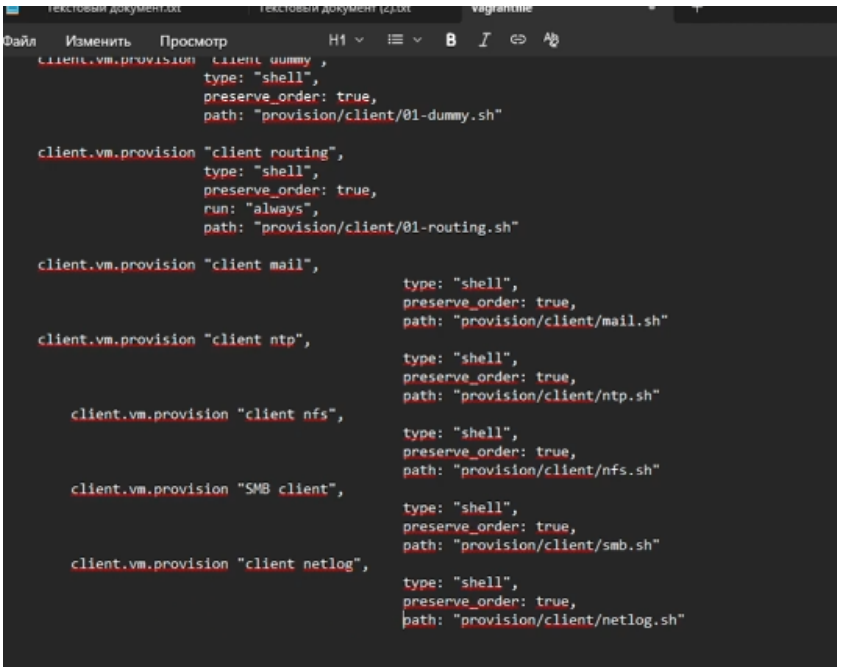


Рис. 2.16: Добавление конфигураций в конфигурационном файле Vagrantfile для сервера и клиента.

3 Выводы

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

4 Ответы на контрольные вопросы:

1. Какой модуль rsyslog вы должны использовать для приёма сообщений от journald? - Для приёма сообщений от journald в rsyslog используется модуль imjournal.

2. Как называется устаревший модуль, который можно использовать для включения приёма сообщений журнала в rsyslog? - Устаревший модуль для приема сообщений журнала в rsyslog - imuxsock (или imuxsock_legacy).

3. Чтобы убедиться, что устаревший метод приёма сообщений из journald в rsyslog не используется, какой дополнительный параметр следует использовать? - Для предотвращения использования устаревшего метода можно использовать параметр SystemMaxUseForward=no в файле /etc/systemd/journald.conf.

4. В каком конфигурационном файле содержатся настройки, которые позволяют вам настраивать работу журнала? - Настройки, позволяющие настроить работу журнала, содержатся в файле /etc/systemd/journald.conf.

5. Каким параметром управляется пересылка сообщений из journald в rsyslog? - Для управления пересылкой сообщений из journald в rsyslog используется параметр ForwardToSyslog=yes в файле /etc/systemd/journald.conf.

6. Какой модуль rsyslog вы можете использовать для включения сообщений из файла журнала, не созданного rsyslog? - Для включения сообщений из файла журнала, не созданного rsyslog, используется модуль imfile.

7. Какой модуль rsyslog вам нужно использовать для пересылки сообщений в базу данных MariaDB? - Для пересылки сообщений в базу данных MariaDB используется модуль ommysql или ommysqlps.

8. Какие две строки вам нужно включить в rsyslog.conf, чтобы позволить текущему журнальному серверу получать сообщения через TCP? - Добавьте следующие строки в rsyslog.conf: $ModLoad imtcp $InputTCPServerRun 514

9. Как настроить локальный брандмауэр, чтобы разрешить приём сообщений журнала через порт TCP 514? – Используйте команды для открытия порта: sudo firewall-cmd –permanent –add-port=514/tcp sudo firewall-cmd –reload Или: sudo iptables -A INPUT -p tcp –dport 514 -j ACCEPT sudo service iptables save sudo service iptables restart

Список литературы