Управление журналами событий в системе

Майоров Дмитрий Андреевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе

2 Выполнение лабораторной работы

Открываем три терминала и в каждом получаем полномочия администратора

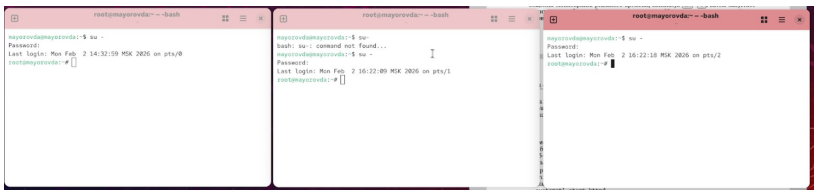

Рисунок 2.1

На второй вкладке терминала запусткаем мониторинг системных событий в реальном времени

```
root@mayorovda:~# tail -f /var/log/messages
Feb  2 16:22:28 mayorovda kernel: traps: VBoxClient[11237] trap int3 ip:4
1dc5b sp:7feb26c35cd0 error:0 in VBoxClient[1dc5b,400000+bb000]
Feb  2 16:22:28 mayorovda systemd-coredump[11238]: Process 11234 (VBoxCli
ent) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Feb  2 16:22:28 mayorovda systemd[1]: Started systemd-coredump@645-11238-
0.service - Process Core Dump (PID 11238/UID 0).
Feb  2 16:22:29 mayorovda systemd-coredump[11239]: Process 11234 (VBoxCli
```

Рисунок 2.2

В третьей вкладке терминала возвращаемся к учётной записи своего пользователя и пробуем получить полномочия администратора, но вводим неправильный пароль. Во второй вкладке терминала с мониторингом событий или ничего не отображается сообщение об ошибке

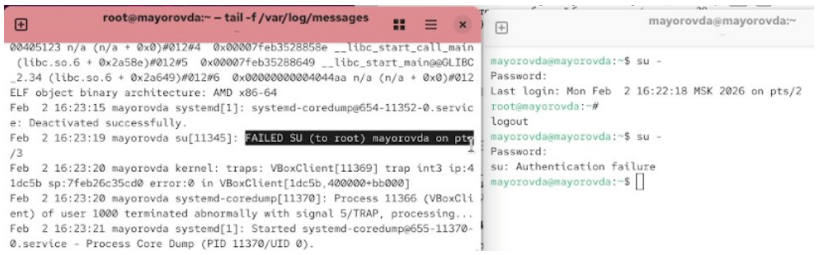

Рисунок 2.3

В третьей вкладке терминала из оболочки пользователя вводим logger hello. Во второй вкладке терминала с мониторингом событий видим это же сообщение

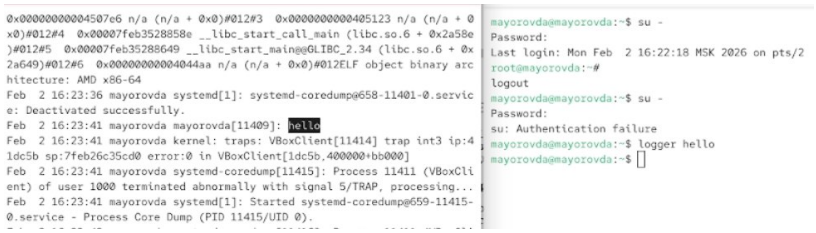

Рисунок 2.4

Во второй вкладке терминала запускаем мониторинг сообщений безопасности

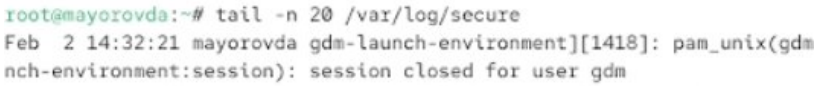

Рисунок 2.5

В первой вкладке терминала устанавливаем Apache

Рисунок 2.6

Запускаем веб-службу

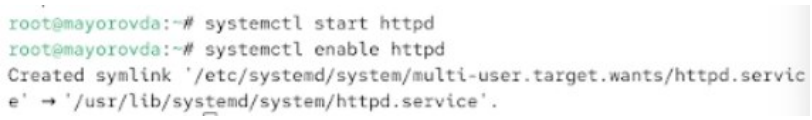

Рисунок 2.7

Во второй вкладке терминала смотрим журнал сообщений об ошибках веб-службы

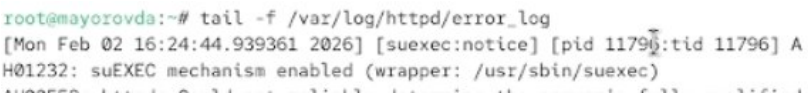

Рисунок 2.8

Открываем файл /etc/httpd/conf/httpd.conf для редактирования и вводим в конце следующую строку

Рисунок 2.9

В каталоге /etc/rsyslog.d создаем файл мониторинга событий веб-службы

Рисунок 2.10

Открываем его для редактирования и прописываем там следующую строку

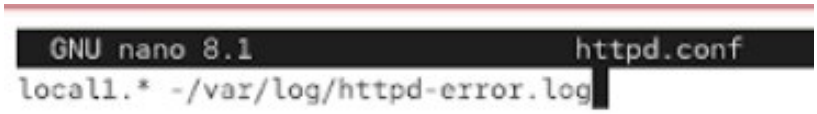

Рисунок 2.11

В первой вкладке терминала перезагрузжаем конфигурацию rsyslogd и веб-службу

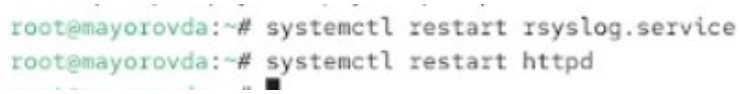

Рисунок 2.12

В третьей вкладке терминала создаем отдельный файл конфигурации для мониторинга отладочной информации и вводим туда нужную команду

Рисунок 2.13

первой вкладке терминала снова перезапускаем rsyslogd

Рисунок 2.14

Во второй вкладке терминала запускаем мониторинг отладочной информации, а в третьей вкладке терминала вводим следующую команду. В терминале с мониторингом смотрим сообщение отладки

Рисунок 2.15

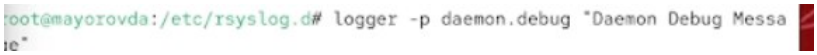

Рисунок 2.16

Во второй вкладке терминала смотрим содержимое журнала с событиями с момента последнего запуска системы

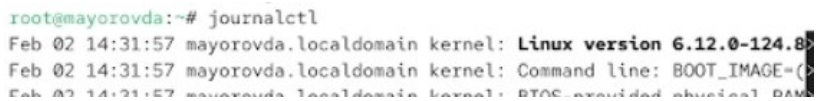

Рисунок 2.17

Смотрим содержимое журнала без пейджера

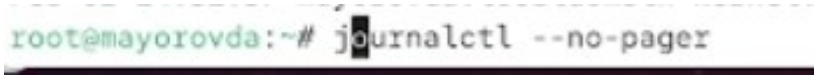

Рисунок 2.18

Смотрим журнал в реальном времени

Рисунок 2.19

Смотрим последние 20 строк журнала, сообщения об ошибках, все сообщения со вчерашнего дня, детальную информацию и доп. информацию о модуле sshd

Рисунок 2.20

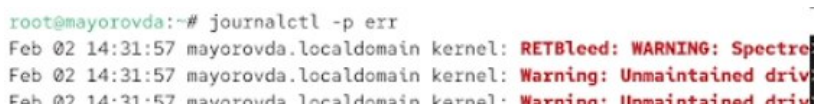

Рисунок 2.21

Создаем каталог для хранения записей журнала. Корректируем права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию. Используем команду для принятия изменений. Смотрим сообщения журнала с момента перезагрузки

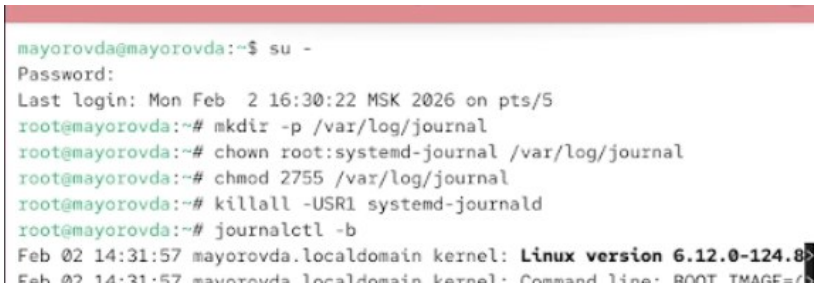
mayorovda@mayorovda:~$ su -
Password:
Last login: Mon Feb 2 16:30:22 MSK 2026 on pts/5
root@mayorovda:~# mkdir -p /var/log/journal
root@mayorovda:~# chown root:systemd-journal /var/log/journal
root@mayorovda:~# chmod 2755 /var/log/journal
root@mayorovda:~# killall -USR1 systemd-journald
root@mayorovda:~# journalctl -b
Feb 02 14:31:57 mayorovda.localdomain kernel: Linux version 6.12.0-124.8

Рисунок 2.22

3 Выводы

Получены навыки работы с журналами мониторинга различных событий в системе