

Управление журналами событий в системе

Майоров Дмитрий Андреевич

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

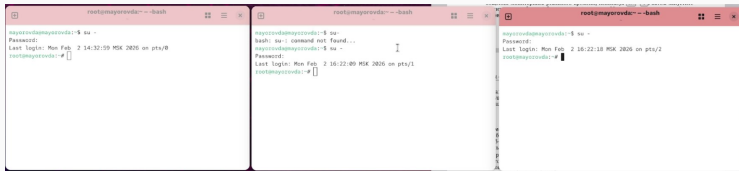


Рисунок 1

3. Выполнение лабораторной работы

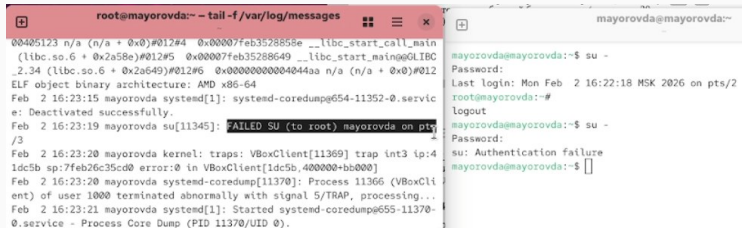
На второй вкладке терминала запускаем мониторинг системных событий в реальном времени

```
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

4. Выполнение лабораторной работы

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



The image shows two terminal windows side-by-side. The left window, titled 'root@mayorovda:~ - tail -f /var/log/messages', displays system logs. The right window, titled 'mayorovda@mayorovda:~', shows the execution of the 'su' command to switch to root, which fails due to an authentication error.

```
root@mayorovda:~ - tail -f /var/log/messages
00405123 n/a (n/a + 0x0)#012#4 0x00007feb3528858e __libc_start_call_main
(libc.so.6 + 0x2a58e)#012#5 0x00007feb35288649 __libc_start_main@GLIBC
_2.34 (libc.so.6 + 0x2a649)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012
ELF object binary architecture: AMD x86-64
Feb  2 16:23:15 mayorovda systemd[1]: systemd-coredump@654-11352-0.servic
e: Deactivated successfully.
Feb  2 16:23:19 mayorovda su[11345]: FAILED SU (to root) mayorovda on pts
/3
Feb  2 16:23:20 mayorovda kernel: traps: VBoxClient[11369] trap int3 ip:4
1dc5b sp:7feb26c35cd0 error:0 in VBoxClient[1dc5b,400000+bb000]
Feb  2 16:23:20 mayorovda systemd-coredump[11370]: Process 11366 (VBoxCli
ent) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Feb  2 16:23:21 mayorovda systemd[1]: Started systemd-coredump@655-11370-
0.service - Process Core Dump (PID 11370/UID 0).

mayorovda@mayorovda:~$ su -
Password:
Last login: Mon Feb  2 16:22:18 MSK 2026 on pts/2
root@mayorovda:~#
logout
mayorovda@mayorovda:~$ su -
Password:
su: Authentication failure
mayorovda@mayorovda:~$
```

Рисунок 3

5. Выполнение лабораторной работы

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

```
0x0000000004507e6 n/a (n/a + 0x0)#012#3 0x000000000405123 n/a (n/a + 0
x0)#012#4 0x00007feb3528858e __libc_start_call_main (libc.so.6 + 0x2a58e
)#012#5 0x00007feb35288649 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x
2a649)#012#6 0x0000000004044aa n/a (n/a + 0x0)#012ELF object binary arc
hitecture: AMD x86-64
Feb  2 16:23:36 mayorovda systemd[1]: systemd-coredump@658-11401-0.servic
e: Deactivated successfully.
Feb  2 16:23:41 mayorovda mayorovda[11409]: hello
Feb  2 16:23:41 mayorovda kernel: traps: VBoxClient[11414] trap int3 ip:4
1dc5b sp:7feb26c35cd0 error:0 in VBoxClient[1dc5b,400000+bb000]
Feb  2 16:23:41 mayorovda systemd-coredump[11415]: Process 11411 (VBoxCli
ent) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Feb  2 16:23:41 mayorovda systemd[1]: Started systemd-coredump@659-11415-
0.service - Process Core Dump (PID 11415/UID 0).
```

```
mayorovda@mayorovda:~$ su -
Password:
Last login: Mon Feb  2 16:22:18 MSK 2026 on pts/2
root@mayorovda:~#
logout
mayorovda@mayorovda:~$ su -
Password:
su: Authentication failure
mayorovda@mayorovda:~$ logger hello
mayorovda@mayorovda:~$
```

Рисунок 4

6. Выполнение лабораторной работы

Во второй вкладке терминала запускаем мониторинг сообщений безопасности

```
root@mayorovda:~# tail -n 20 /var/log/secure  
Feb  2 14:32:21 mayorovda gdm-launch-environment][1418]: pam_unix(gdm  
nch-environment:session): session closed for user gdm
```

Рисунок 5

7. Выполнение лабораторной работы

В первой вкладке терминала устанавливаем Apache

```
root@mayorovda:~# dnf -y install httpd
```

Рисунок 6

8. Выполнение лабораторной работы

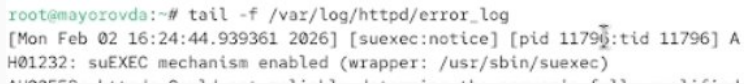
Запускаем веб-службу

```
root@mayorovda:~# systemctl start httpd  
root@mayorovda:~# systemctl enable httpd  
Created symlink '/etc/systemd/system/multi-user.target.wants/httpd.service'  
→ '/usr/lib/systemd/system/httpd.service'.
```

Рисунок 7

9. Выполнение лабораторной работы

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



```
root@mayorovda:~# tail -f /var/log/httpd/error_log
[Mon Feb 02 16:24:44.939361 2026] [suexec:notice] [pid 11796:tid 11796] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
```

Рисунок 8

10. Выполнение лабораторной работы

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

```
# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
ErrorLog syslog:local
```

Рисунок 9

11. Выполнение лабораторной работы

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

```
root@mayorovda:~# cd /etc/rsyslog.d  
root@mayorovda:/etc/rsyslog.d# touch httpd.conf
```

Рисунок 10

12. Выполнение лабораторной работы

Открываем его для редактирования и прописываем там следующую строку



```
GNU nano 8.1 httpd.conf
local1.* -/var/log/httpd-error.log
```

Рисунок 11

13. Выполнение лабораторной работы

В первой вкладке терминала перезагружаем конфигурацию rsyslogd и веб-службу

```
root@mayorovda:~# systemctl restart rsyslog.service  
root@mayorovda:~# systemctl restart httpd
```

Рисунок 12

14. Выполнение лабораторной работы

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

```
root@mayorovda:/etc/rsyslog.d# touch debug.conf  
root@mayorovda:/etc/rsyslog.d# echo "*.debug /var/log/messages-debug  
/etc/rsyslog.d/debug.conf"
```

Рисунок 13

15. Выполнение лабораторной работы

первой вкладке терминала снова перезапускаем rsyslogd

A terminal window showing a root user at a machine named mayorovda. The user enters the command 'systemctl restart rsyslog.service' and the prompt returns.

```
root@mayorovda:~# systemctl restart rsyslog.service
root@mayorovda:~#
```

Рисунок 14

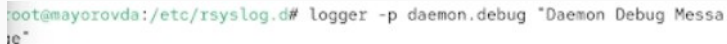
16. Выполнение лабораторной работы

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



```
root@mayorovda:~# tail -f /var/log/messages-debug
```

Рисунок 15



```
root@mayorovda:/etc/rsyslog.d# logger -p daemon.debug "Daemon Debug Message"
```

Рисунок 16

17. Выполнение лабораторной работы

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

```
root@mayorovda:~# journalctl
Feb 02 14:31:57 mayorovda.localdomain kernel: Linux version 6.12.0-124.8
Feb 02 14:31:57 mayorovda.localdomain kernel: Command line: BOOT_IMAGE=(>
Feb 02 14:31:57 mayorovda.localdomain kernel: BIOS-provided physical RAM
```

Рисунок 17

18. Выполнение лабораторной работы

Смотрим содержимое журнала без пейджера

A terminal window screenshot showing a command being entered. The prompt is 'root@mayorovda:~#'. The command 'journalctl --no-pager' is being typed, with a cursor positioned after the first 'l' in 'journalctl'.

```
root@mayorovda:~# journalctl --no-pager
```

Рисунок 18

19. Выполнение лабораторной работы

Смотрим журнал в реальном времени

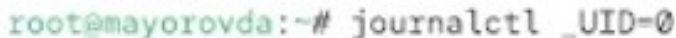
A terminal window screenshot showing a command being entered. The prompt is root@mayorovda:~#. The command journalctl -f is entered, with the cursor at the end of the line. The terminal has a dark background and light-colored text.

```
root@mayorovda:~# journalctl -f
```

Рисунок 19

20. Выполнение лабораторной работы

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



```
root@mayorovda:~# journalctl _UID=0
```

Рисунок 20

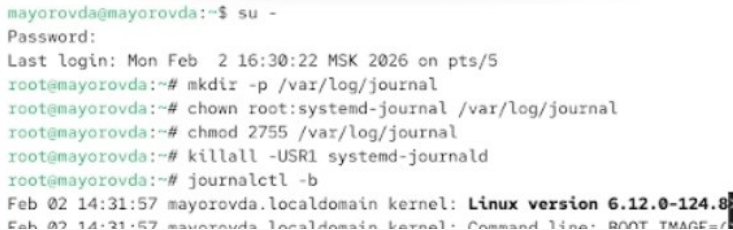


```
root@mayorovda:~# journalctl -p err
Feb 02 14:31:57 mayorovda.localdomain kernel: RETBleed: WARNING: Spectre
Feb 02 14:31:57 mayorovda.localdomain kernel: Warning: Unmaintained driv
Feb 02 14:31:57 mayorovda.localdomain kernel: Warning: Unmaintained driv
```

Рисунок 21

21. Выполнение лабораторной работы

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  
Feb 02 14:31:57 mayorovda.localdomain kernel: Command line: BOOT_IMAGE=/
```

Рисунок 22

22. Выводы

Получены навыки работы с журналами мониторинга различных событий в системе