

# **Отчёт по лабораторной работе №7**

**Управление журналами событий в системе**

Агдjabекова Эся Рустамовна

# **Содержание**

<b>1 Цель работы</b>	<b>5</b>
<b>2 Ход выполнения работы</b>	<b>6</b>
2.1 Мониторинг журнала системных событий в реальном времени . . . . .	6
2.2 Изменение правил rsyslog.conf . . . . .	9
2.3 Использование journalctl . . . . .	12
2.4 Постоянный журнал journald . . . . .	17
<b>3 Контрольные вопросы</b>	<b>19</b>
<b>4 Заключение</b>	<b>21</b>

# Список иллюстраций

2.1	Мониторинг системных событий в реальном времени . . . . .	7
2.2	Ошибка при вводе неправильного пароля . . . . .	7
2.3	Сообщение, записанное с помощью logger . . . . .	8
2.4	Просмотр сообщений безопасности . . . . .	9
2.5	Установка и запуск Apache . . . . .	9
2.6	Просмотр журнала ошибок Apache . . . . .	10
2.7	Добавление правила ErrorLog в httpd.conf . . . . .	10
2.8	Создание файла конфигурации для ошибок Apache . . . . .	11
2.9	Создание конфигурации для отладочных сообщений . . . . .	11
2.10	Вывод отладочного сообщения через logger . . . . .	12
2.11	Просмотр журнала с момента запуска . . . . .	12
2.12	Вывод журнала без пейджера . . . . .	13
2.13	Просмотр журнала в реальном времени . . . . .	13
2.14	Параметры фильтрации journalctl . . . . .	14
2.15	Фильтрация по UID=0 . . . . .	14
2.16	Просмотр последних 20 строк . . . . .	15
2.17	Фильтрация только ошибок . . . . .	15
2.18	Просмотр событий со вчерашнего дня . . . . .	16
2.19	Ошибки со вчерашнего дня . . . . .	16
2.20	Детализированный вывод сообщений . . . . .	17
2.21	Просмотр информации о модуле sshd . . . . .	17
2.22	Включение постоянного журнала journald . . . . .	18

# **Список таблиц**

# **1 Цель работы**

Получить навыки работы с журналами мониторинга различных событий в системе.

## **2 Ход выполнения работы**

### **2.1 Мониторинг журнала системных событий в реальном времени**

1. В трёх вкладках терминала получены полномочия администратора командой `su -`.
2. Во второй вкладке запущен мониторинг системных событий в реальном времени:  
`tail -f /var/log/messages`  
(см. рис. fig. 2.1).

```

Sep 29 10:48:46 eragdzhabekova systemd-coredump[3997]: Process 3993 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Sep 29 10:48:46 eragdzhabekova systemd[1]: Started systemd-coredump@77-3997-.service - Process Core Dump (PID 3997/UID 0).
Sep 29 10:48:46 eragdzhabekova systemd-coredump[3998]: Process 3993 (VBoxClient) of user 1000 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 3996:#012#0 0x00000000000041dd1b n/a (n/a + 0x0)#012#1 0x00000000000041dc94 n/a (n/a + 0x0)#012#2 0x00000000000045041c n/a (n/a + 0x0)#012#3 0x00000000004355d0 n/a (n/a + 0x0)#012#4 0x000007f317484011a start_thread (libc.so.6 + 0x9511a)#012#5 0x000007f31748b0c3c __clone3 (libc.so.6 + 0x105c3c)#012#0 0x000007f31748b0c3d syscall (libc.so.6 + 0x103a3d) #012#1 0x000000000000434c30 n/a (n/a + 0x0)#012#2 0x0000000000004506fb n/a (n/a + 0x0)#012#3 0x00000000000043566 n/a (n/a + 0x0)#012#4 0x00000000000045041c n/a (n/a + 0x0)#012#5 0x0000000000004355d0 n/a (n/a + 0x0)#012#6 0x0000000000004355d0 n/a (n/a + 0x0)#012#7 0x000007f31748b0c3e __clone3 (libc.so.6 + 0x105c3c)#012#0 0x000007f31748b0c3d syscall (libc.so.6 + 0x103a3d) #012#1 0x000007f317484011a start_thread (libc.so.6 + 0x9511a)#012#2 0x000007f31748b0c3e __clone3 (libc.so.6 + 0x105c3c)#012#0 0x000007f31748b0c3d syscall (libc.so.6 + 0x103a3d) #012#1 0x0000000000004344e2 n/a (n/a + 0x0)#012#2 0x000000000000450066 n/a (n/a + 0x0)#012#3 0x000000000000405123 n/a (n/a + 0x0)#012#4 0x000007f31747d530e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x000007f31747d53c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x0000000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Sep 29 10:48:51 eragdzhabekova systemd[1]: systemd-coredump@78-4008-.service: Deactivated successfully.
Sep 29 10:48:51 eragdzhabekova kernel: traps: VBoxClient[4007] trap int3 ip:41dd1b sp:7f3166188cd0 error:0 in VBoxClient[1]lddb1,4000000:bb0000
Sep 29 10:48:51 eragdzhabekova systemd-coredump[4008]: Process 4004 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Sep 29 10:48:51 eragdzhabekova systemd[1]: Started systemd-coredump@78-4008-.service - Process Core Dump (PID 4004/UID 0).
Sep 29 10:48:51 eragdzhabekova systemd-coredump[4009]: Process 4004 (VBoxClient) of user 1000 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 4007:#012#0 0x00000000000041dd1b n/a (n/a + 0x0)#012#1 0x00000000000041dc94 n/a (n/a + 0x0)#012#2 0x00000000000045041c n/a (n/a + 0x0)#012#3 0x00000000004355d0 n/a (n/a + 0x0)#012#4 0x000007f317484011a start_thread (libc.so.6 + 0x9511a)#012#5 0x000007f31748b0c3c __clone3 (libc.so.6 + 0x105c3c)#012#0 0x000007f31748b0c3d syscall (libc.so.6 + 0x103a3d) #012#1 0x000000000000434c30 n/a (n/a + 0x0)#012#2 0x0000000000004506fb n/a (n/a + 0x0)#012#3 0x00000000000043566 n/a (n/a + 0x0)#012#4 0x00000000000045041c n/a (n/a + 0x0)#012#5 0x0000000000004355d0 n/a (n/a + 0x0)#012#6 0x0000000000004355d0 n/a (n/a + 0x0)#012#7 0x000007f31748b0c3e __clone3 (libc.so.6 + 0x105c3c)#012#0 0x000007f31748b0c3d syscall (libc.so.6 + 0x103a3d) #012#1 0x000007f317484011a start_thread (libc.so.6 + 0x9511a)#012#2 0x000007f31748b0c3e __clone3 (libc.so.6 + 0x105c3c)#012#0 0x000007f31748b0c3d syscall (libc.so.6 + 0x103a3d) #012#1 0x0000000000004344e2 n/a (n/a + 0x0)#012#2 0x000000000000450066 n/a (n/a + 0x0)#012#3 0x000000000000405123 n/a (n/a + 0x0)#012#4 0x000007f31747d530e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x000007f31747d53c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x0000000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Sep 29 10:48:51 eragdzhabekova systemd[1]: systemd-coredump@78-4008-.service: Deactivated successfully.

```

Рис. 2.1: Мониторинг системных событий в реальном времени

3. В третьей вкладке выполнена попытка получить права администратора с неверным паролем. В результате в журнале зафиксирована ошибка авторизации FAILED su (to root) (см. рис. fig. 2.2).

```

le 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 4078:#012#0 0x00000000000041dd1b n/a (n/a + 0x0)#012#1 0x00000000000041dc94 n/a (n/a + 0x0)#012#2 0x00000000000045041c n/a (n/a + 0x0)#012#3 0x00000000004355d0 n/a (n/a + 0x0)#012#4 0x000007f317484011a start_thread (libc.so.6 + 0x9511a)#012#5 0x000007f31748b0c3c __clone3 (libc.so.6 + 0x105c3c)#012#0 0x000007f31748b0c3d syscall (libc.so.6 + 0x103a3d) #012#1 0x000000000000434c30 n/a (n/a + 0x0)#012#2 0x0000000000004506fb n/a (n/a + 0x0)#012#3 0x00000000000043566 n/a (n/a + 0x0)#012#4 0x00000000000045041c n/a (n/a + 0x0)#012#5 0x0000000000004355d0 n/a (n/a + 0x0)#012#6 0x0000000000004355d0 n/a (n/a + 0x0)#012#7 0x000007f31748b0c3e __clone3 (libc.so.6 + 0x105c3c)#012#0 0x000007f31748b0c3d syscall (libc.so.6 + 0x103a3d) #012#1 0x000007f317484011a start_thread (libc.so.6 + 0x9511a)#012#2 0x000007f31748b0c3e __clone3 (libc.so.6 + 0x105c3c)#012#0 0x000007f31748b0c3d syscall (libc.so.6 + 0x103a3d) #012#1 0x0000000000004344e2 n/a (n/a + 0x0)#012#2 0x000000000000450066 n/a (n/a + 0x0)#012#3 0x000000000000405123 n/a (n/a + 0x0)#012#4 0x000007f31747d530e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x000007f31747d53c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x0000000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Sep 29 10:49:17 eragdzhabekova systemd[1]: systemd-coredump@63-4079-.service: Deactivated successfully.
Sep 29 10:49:17 eragdzhabekova su[4065]: FAILED SU (to root) eragdzhabekova on pts/2
Sep 29 10:49:22 eragdzhabekova kernel: traps: VBoxClient[4090] trap int3 ip:41dd1b sp:7f3166188cd0 error:0 in VBoxClient[1]lddb1,4000000:bb0000
Sep 29 10:49:22 eragdzhabekova systemd-coredump[4091]: Process 4087 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Sep 29 10:49:22 eragdzhabekova systemd[1]: Started systemd-coredump@84-4091-.service - Process Core Dump (PID 4087/UID 0).
Sep 29 10:49:22 eragdzhabekova systemd-coredump[4092]: Process 4087 (VBoxClient) of user 1000 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 4090:#012#0 0x00000000000041dd1b n/a (n/a + 0x0)#012#1 0x00000000000041dc94 n/a (n/a + 0x0)#012#2 0x00000000000045041c n/a (n/a + 0x0)#012#3 0x00000000004355d0 n/a (n/a + 0x0)#012#4 0x000007f317484011a start_thread (libc.so.6 + 0x9511a)#012#5 0x000007f31748b0c3c __clone3 (libc.so.6 + 0x105c3c)#012#0 0x000007f31748b0c3d syscall (libc.so.6 + 0x103a3d) #012#1 0x000000000000434c30 n/a (n/a + 0x0)#012#2 0x0000000000004506fb n/a (n/a + 0x0)#012#3 0x00000000000043566 n/a (n/a + 0x0)#012#4 0x00000000000045041c n/a (n/a + 0x0)#012#5 0x0000000000004355d0 n/a (n/a + 0x0)#012#6 0x0000000000004355d0 n/a (n/a + 0x0)#012#7 0x000007f31748b0c3e __clone3 (libc.so.6 + 0x105c3c)#012#0 0x000007f31748b0c3d syscall (libc.so.6 + 0x103a3d) #012#1 0x000007f317484011a start_thread (libc.so.6 + 0x9511a)#012#2 0x000007f31748b0c3e __clone3 (libc.so.6 + 0x105c3c)#012#0 0x000007f31748b0c3d syscall (libc.so.6 + 0x103a3d) #012#1 0x0000000000004344e2 n/a (n/a + 0x0)#012#2 0x000000000000450066 n/a (n/a + 0x0)#012#3 0x000000000000405123 n/a (n/a + 0x0)#012#4 0x000007f31747d530e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x000007f31747d53c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x0000000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Sep 29 10:49:22 eragdzhabekova systemd[1]: systemd-coredump@84-4091-.service: Deactivated successfully.

```

Рис. 2.2: Ошибка при вводе неправильного пароля

4. В оболочке пользователя выполнена команда:

```
logger hello
```

Сообщение появилось в окне мониторинга и было сохранено в журнале `/var/log/messages` (см. рис. fig. 2.3).

```
n/a (n/a + 0x0)#012#7 0x000000000045041c n/a (n/a + 0x0)#012#8 0x00000000004355d0 n/a (n/a + 0x0)#012#9 0x000007f317484011a start_thread (_libc.so.6 + 0x9511a)#012#10 0x000007f31748b0c3c __clone3 (_libc.so.6 + 0x105c3c)#012#012Stack trace of thread 4117:#012#0 0x000007f31748ae43d syscall (_libc.so.6 + 0x103a3d)#012#1 0x0000000000004344e2 n/a (n/a + 0x0)#012#2 0x0000000000450066 n/a (n/a + 0x0)#012#3 0x000000000000405123 n/a (n/a + 0x0)#012#4 0x000007f31747d520e __libc_start_main (_libc.so.6 + 0x2a30e)#012#5 0x000007f31747d53c9 __libc_start_main@GLIBC_2.34 (_libc.so.6 + 0x2a3c9)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64 Sep 29 10:49:37 eragdzhabekova systemd[1]: systemd-coredump@87-4121-0.service: Deactivated successfully. Sep 29 10:49:40 eragdzhabekova eragdzhabekova[4127]: hello Sep 29 10:49:42 eragdzhabekova kernel: traps: VBoxClient[4132] trap int3 ip:41dd1b sp:7f3166188cd0 error:0 in VBoxClient[1dd1b,400000+bb000] Sep 29 10:49:42 eragdzhabekova systemd-coredump[4133]: Process 4129 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing... Sep 29 10:49:42 eragdzhabekova systemd[1]: Started systemd-coredump@88-4133-0.service - Process Core Dump (PID 4133/UID 0). Sep 29 10:49:42 eragdzhabekova systemd-coredump[4134]: Process 4129 (VBoxClient) of user 1000 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 4132:#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 0x000000000045041d n/a (n/a + 0x0)#012#4 0x000000000045041e n/a (n/a + 0x0)#012#5 0x000000000045041f n/a (n/a + 0x0)#012#6 0x000000000045041g n/a (n/a + 0x0)#012#7 0x000000000045041h n/a (n/a + 0x0)#012#8 0x000000000045041i n/a (n/a + 0x0)#012#9 0x000000000045041j n/a (n/a + 0x0)#012#10 0x000000000045041k n/a (n/a + 0x0)#012#11 0x000000000045041l n/a (n/a + 0x0)#012#12 0x000000000045041m n/a (n/a + 0x0)#012#13 0x000000000045041n n/a (n/a + 0x0)#012#14 0x000000000045041o n/a (n/a + 0x0)#012#15 0x000000000045041p n/a (n/a + 0x0)#012#16 0x000000000045041q n/a (n/a + 0x0)#012#17 0x000000000045041r n/a (n/a + 0x0)#012#18 0x000000000045041s n/a (n/a + 0x0)#012#19 0x000000000045041t n/a (n/a + 0x0)#012#20 0x000000000045041u n/a (n/a + 0x0)
```

Рис. 2.3: Сообщение, записанное с помощью logger

5. Мониторинг системных сообщений во второй вкладке остановлен комбинацией **Ctrl + C**. Затем просмотрены последние 20 строк файла журнала безопасности командой:

```
tail -n 20 /var/log/secure
```

В нём отобразились записи о неудачной попытке авторизации (см. рис. fig. 2.4).

```
root@eragdzhabekova:/home/eragdzhabekova# tail -n 20 /var/log/messages
Sep 29 10:49:52 eragdzhabekova kernel: traps: VBoxClient[4156] trap int3 ip:41dd1b sp:7f3166188cd0 error:0 in VBoxClient[1][lddlb, 400000+bb000]
Sep 29 10:49:52 eragdzhabekova kernel: traps: VBoxClient[4157] Process 4153 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Sep 29 10:49:52 eragdzhabekova systemd[1]: Started systemd-coredump@0-4157-0.service - Process Core Dump (PID 4157/UID 0).
Sep 29 10:49:52 eragdzhabekova systemd-coredump[4158]: Process 4153 (VBoxClient) of user 1000 dumped core. #012#012Modu
le 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#012Modu
le libX11.so.6 from rpm libX11-8.1.10-9.el10.x86_64#012Module libfftw.so.3 from rpm libfftw-3.4.4-9.el10.x86_64#012Modu
le libwayland-client.so.0 from rpm wayland-1.23-0.2.el10.x86_64#012Stack trace of thread 4156:#012#0 0x000000000041d1
b n/a (n/a + 0x0)#012#1 0x000000000041dc94 n/a (n/a + 0x0)#012#2 0x000000000045041c n/a (n/a + 0x0)#012#3 0x00000000
004355d0 n/a (n/a + 0x0)#012#4 0x0000007f317484011a start_thread (libc.so.6 + 0x9511a)#012#5 0x0000007f31748Bbc3c _clo
se3 (libc.so.6 + 0x105c3c)#012#6 0x0000007f31748ae3d syscall (libc.so.6 + 0x103a3d)
#012#1 0x0000000000434c30 n/a (n/a + 0x0)#012#2 0x0000000000450fb n/a (n/a + 0x0)#012#3 0x000000000043566a n/a (n/a
+ 0x0)#012#4 0x000000000045041c n/a (n/a + 0x0)#012#5 0x00000000004355d0 n/a (n/a + 0x0)#012#6 0x0000007f317484011a
start_thread (libc.so.6 + 0x9511a)#012#7 0x0000007f31748Bbc3c _close3 (libc.so.6 + 0x105c3c)#012#8 0x0000007f31748
read 4155:#012#0 0x0000007f31748ea3d syscall (libc.so.6 + 0x103a3d)#012#1 0x0000000000434e2 n/a (n/a + 0x0)#012#2
0x000000000045066 n/a (n/a + 0x0)#012#3 0x0000000000416559 n/a (n/a + 0x0)#012#4 0x0000000000434e2 n/a (n/a + 0x0)#012#5
0x0000000000417d6a n/a (n/a + 0x0)#012#6 0x0000000000404860 n/a (n/a + 0x0)#012#7 0x000000000045041c n/a (n/a
+ 0x0)#012#8 0x00000000004355d0 n/a (n/a + 0x0)#012#9 0x0000007f317484011a start_thread (libc.so.6 + 0x9511a)#012#10
#012#0 0x0000007f31748Bbc3c _close3 (libc.so.6 + 0x105c3c)#012#11 0x0000007f31748ae3d syscall (libc.so.6 + 0x103a3d)
#012#1 0x0000000000434462 n/a (n/a + 0x0)#012#2 0x0000000000450666 n/a (n/a + 0x0)#012#3 0x0000000000450123 n/a (n/a + 0x0)
#012#4 0x0000007f31747d4000 __libc_start_main (libc.so.6 + 0x2a30e)#012#5 0x0000007f31747d53c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012ELF objec
t binary architecture: AMD x86-64
Sep 29 10:49:52 eragdzhabekova systemd[1]: systemd-coredump@0-4157-0.service: Deactivated successfully.
Sep 29 10:49:52 eragdzhabekova kernel: traps: VBoxClient[4166] trap int3 ip:41dd1b sp:7f3166188cd0 error:0 in VBoxClient[1][lddlb, 400000+bb000]
Sep 29 10:49:52 eragdzhabekova kernel: traps: VBoxClient[4167] Process 4163 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Sep 29 10:49:52 eragdzhabekova systemd[1]: Started systemd-coredump@0-4167-0.service - Process Core Dump (PID 4167/UID 0).
Sep 29 10:49:52 eragdzhabekova systemd-coredump[4168]: Process 4163 (VBoxClient) of user 1000 dumped core. #012#012Modu
le 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#012Modu
```

Рис. 2.4: Просмотр сообщений безопасности

## 2.2 Изменение правил rsyslog.conf

1. Установлен Apache (если ранее не был установлен) и запущена веб-служба:

```
dnf -y install httpd
```

```
systemctl start httpd
```

```
systemctl enable httpd
```

(см. рис. fig. 2.5).

```
Running scriptlet: httpd-2.4.63-1.el10_0.2.x86_64                                         11/11

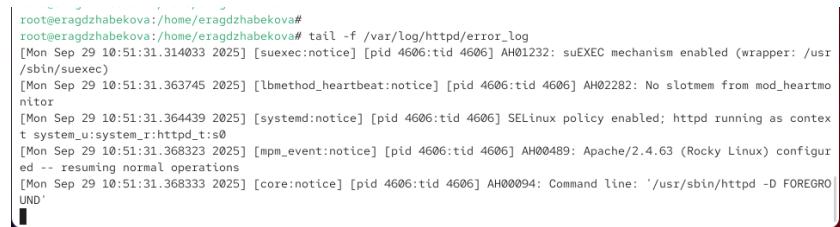
Installed:
  apr-1.7.5-2.el10.x86_64          apr-util-1.6.3-21.el10.x86_64          apr-util-lmdb-1.6.3-21.el10.x86_64
  apr-util-openssl-1.6.3-21.el10.x86_64      httpd-2.4.63-1.el10_0.2.x86_64      httpd-core-2.4.63-1.el10_0.2.x86_64
  httpd-filesystem-2.4.63-1.el10_0.2.noarch  httpd-tools-2.4.63-1.el10_0.2.x86_64  mod_http2-2.0.29-2.el10_0.1.x86_64
  mod_lua-2.4.63-1.el10_0.2.x86_64        rocky-logos-httpd-100.4-7.el10.noarch
```

Рис. 2.5: Установка и запуск Apache

2. Во второй вкладке терминала просмотрен журнал ошибок веб-службы командой

```
tail -f /var/log/httpd/error_log
```

(см. рис. fig. 2.6).



```
root@eragdzhabekova:/home/eragdzhabekova# tail -f /var/log/httpd/error_log
[Mon Sep 29 10:51:31.314033 2025] [suexec:notice] [pid 4606:tid 4606] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Mon Sep 29 10:51:31.363745 2025] [lbbmethod_heartbeat:notice] [pid 4606:tid 4606] AH02282: No slotmem from mod_heartbeat
[Mon Sep 29 10:51:31.364439 2025] [systemd:notice] [pid 4606:tid 4606] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Mon Sep 29 10:51:31.368323 2025] [mpm_event:notice] [pid 4606:tid 4606] AH00489: Apache/2.4.63 (Rocky Linux) configur
ed -- resuming normal operations
[Mon Sep 29 10:51:31.368333 2025] [core:notice] [pid 4606:tid 4606] AH00094: Command line: '/usr/sbin/httpd -D FOREGRO
UND'
```

Рис. 2.6: Просмотр журнала ошибок Apache

3. В файле `/etc/httpd/conf/httpd.conf` добавлена строка перенаправления ошибок в syslog:

```
ErrorLog syslog:local1
```

(см. рис. fig. 2.7).

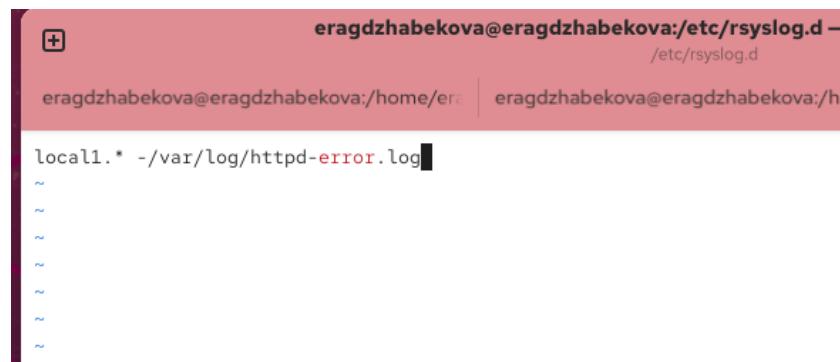


Рис. 2.7: Добавление правила ErrorLog в httpd.conf

4. В каталоге `/etc/rsyslog.d` создан файл `httpd.conf` со строкой:

```
local1.* -/var/log/httpd-error.log
```

(см. рис. fig. 2.8).

```

#
# Customizable error responses come in three flavors:
# 1) plain text 2) local redirects 3) external redirects
#
# Some examples:
#ErrorDocument 500 "The server made a boo boo."
#ErrorDocument 404 /missing.html
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#ErrorDocument 402 http://www.example.com/subscription_info.html
#
#
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall may be used to deliver
# files. This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults if commented: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
EnableSendfile on

# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
ErrorLog syslog:local1
-- INSERT --

```

Рис. 2.8: Создание файла конфигурации для ошибок Apache

5. Перезагружены службы `rsyslog` и `httpd`. Сообщения об ошибках веб-сервера начали записываться в `/var/log/httpd-error.log`.
6. Создан файл `/etc/rsyslog.d/debug.conf` с правилом:  
`*.debug /var/log/messages-debug`  
(см. рис. fig. 2.9).

```

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

```

Рис. 2.9: Создание конфигурации для отладочных сообщений

7. После перезапуска `rsyslog` запущен мониторинг нового файла:  
`tail -f /var/log/messages-debug`
8. С помощью команды  
`logger -p daemon.debug "Daemon Debug Message"`  
в журнал отправлено тестовое сообщение, которое успешно отобразилось в логе (см. рис. fig. 2.10).

```

0004355d0 n/a (n/a + 0x0)#012#4 0x00007f317484011a start_thread (libc.so.6 + 0x9511a)#012#5 0x00007f31748b0c3c
ne3 (libc.so.6 + 0x105c3c)#012#6 Stack trace of thread 6254:#012#0 0x00007f31748aea3d syscall (libc.so.6 + 0x10
#012#1 0x00000000004344e2 n/a (n/a + 0x0)#012#2 0x0000000000450066 n/a (n/a + 0x0)#012#3 0x0000000000405123 n/
a + 0x0)#012#4 0x000007f31747d530e __libc_start_main (libc.so.6 + 0x2a30e)#012#5 0x000007f31747d53c9 __libc_
_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012#ELF object binary architec
MD x86-64
Sep 29 10:58:45 eragdzhabekova systemd[1]: systemd-coredump@195-6258-0.service: Deactivated successfully.
Sep 29 10:58:49 eragdzhabekova root[6264]: Daemon Debug Message
Sep 29 10:58:50 eragdzhabekova kernel: traps: VBoxClient[6269] trap int3 ip:41dd1b sp:7f3166188cd0 error:0 in VBo
nt!l1ddib, 400000+bb000]
Sep 29 10:58:50 eragdzhabekova systemd-coredump[6270]: Process 6266 (VBoxClient) of user 1000 terminated abnormal
th signal 5/TRAP, processing...
Sep 29 10:58:50 eragdzhabekova systemd[1]: Started systemd-coredump@195-6270-0.service - Process Core Dump (PID 6
ID 0).
Sep 29 10:58:50 eragdzhabekova systemd-coredump[6271]: Process 6266 (VBoxClient) of user 1000 dumped core.#012#01

```

Рис. 2.10: Вывод отладочного сообщения через logger

## 2.3 Использование journalctl

- Просмотрен журнал событий с момента последнего запуска системы командой  
**journalctl**  
(см. рис. fig. 2.11).

```

root@eragdzhabekova:/home/eragdzhabekova#
root@eragdzhabekova:/home/eragdzhabekova# journalctl
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-bu
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: Command line: BOOT_IMAGE=/hd0,gpt2/vmlinuz-6.12.0-55.12.1.el10_0
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-provided physical RAM map:
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009bf] usable
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000ffff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000007ffff] usable
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x00000000007ff0000-0x0000000007ffff] ACPI data
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x000000000fec0000-0x000000000fec0fff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x000000000fee0000-0x000000000fee0fff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x000000000ffc0000-0x000000000ffcffff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: NX (Execute Disable) protection: active
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: APIC: Static calls initialized
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: SMBIOS 2.5 present.
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: DMI: innoteck GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: DMI: Memory slots populated: 0/0
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: Hypervisor detected: KVM
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: kvm-clock: Using sched offset of 4050277964 cycles
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: clocksource: kvm-clock: mask: 0xfffffffffffffff max_cycles: 0x1cd8
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: tsc: Detected 3187.202 MHz processor
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: e820: update [mem 0x00000000-0x0000ffff] usable ==> reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: e820: remove [mem 0x00000000-0x0000ffff] usable
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: last_lfn = 0x80000 max_arch_pfn = 0x4000000000
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: MTRR map: 4 entries (3 fixed + 1 variable; max 35), built from 16
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: x86/PAT: Configuration [0-7]: WB WC UC UC WB WP UC- WT
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: found SMP MP-table at [mem 0x0009fb0-0x0009fbff]
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: Incomplete global flushes, disabling PCID
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: RAMDISK: [mem 0x34338000-0x36193fff]
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: ACPI: Early table checksum verification disabled
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: ACPI: RSDP 0x0000000000000000 000024 (v02 VBOX )
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: ACPI: XSDT 0x000000007FFF0030 00003C (v01 VBOX  VBOXXSDT 00000001)
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: ACPI: FACP 0x000000007FFF00F0 0000F4 (v04 VBOX  VBOXFACP 00000001)

```

Рис. 2.11: Просмотр журнала с момента запуска

- Выведено содержимое журнала без использования пейджера:  
**journalctl -no-pager**  
(см. рис. fig. 2.12).

```

Sep 29 11:00:57 eragdzhabekova.localdomain systemd[1]: systemd-coredump@221-6528-0.service: Deactivated successfully.
Sep 29 11:01:01 eragdzhabekova.localdomain CROND[6535]: (root) CMD (run-parts /etc/cron.hourly)
Sep 29 11:01:02 eragdzhabekova.localdomain run-parts[6538]: (/etc/cron.hourly) starting 0anacron
Sep 29 11:01:02 eragdzhabekova.localdomain anacron[6548]: Anacron started on 2025-09-29
Sep 29 11:01:02 eragdzhabekova.localdomain anacron[6548]: Will run job 'cron.daily' in 18 min.
Sep 29 11:01:02 eragdzhabekova.localdomain anacron[6548]: Will run job 'cron.weekly' in 38 min.
Sep 29 11:01:02 eragdzhabekova.localdomain anacron[6548]: Will run job 'cron.monthly' in 58 min.
Sep 29 11:01:02 eragdzhabekova.localdomain anacron[6548]: Jobs will be executed sequentially
Sep 29 11:01:02 eragdzhabekova.localdomain run-parts[6550]: (/etc/cron.hourly) finished 0anacron
Sep 29 11:01:02 eragdzhabekova.localdomain CROND[6534]: (root) CMDEND (run-parts /etc/cron.hourly)
Sep 29 11:01:02 eragdzhabekova.localdomain kernel: traps: VBoxClient[1dd1b,4000000-bb000] error:0
Sep 29 11:01:02 eragdzhabekova.localdomain systemd-coredump[6555]: Process 6551 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Sep 29 11:01:02 eragdzhabekova.localdomain systemd[1]: Started systemd-coredump@222-6555-0.service - Process Core Dump (PID 6555/UID 0).
Sep 29 11:01:02 eragdzhabekova.localdomain systemd-coredump[6556]: [..] Process 6551 (VBoxClient) of user 1000 dumped core.

Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x8
6_64
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x8
6_64
Module libXi11.so.6 from rpm libXi11-1.8.10-1.el10.x8
6_64
Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86
Module libwayland-client.so.0 from rpm wayland-1.23
.0-2.el10.x86_64

Stack trace of thread 6554:
#0 0x000000000041dd1b n/a (n/a + 0x0)
#1 0x000000000041dc94 n/a (n/a + 0x0)
#2 0x000000000041dc94 n/a (n/a + 0x0)

```

Рис. 2.12: Вывод журнала без пейджера

### 3. Включён режим просмотра журнала в реальном времени:

`journalctl -f`

Для выхода использована комбинация `Ctrl + C` (см. рис. fig. 2.13).

```

9511a)
3c)

d)

9511a)
3c)

d)

.so.6 + 0x2a30e)
4 (libc.so.6 + 0x2a3c9)

Stack trace of thread 6604:
#0 0x00007f31748aea3d syscall (libc.so.6 + 0x103a3
#1 0x00000000004344e2 n/a (n/a + 0x0)
#2 0x0000000000450066 n/a (n/a + 0x0)
#3 0x0000000000405123 n/a (n/a + 0x0)
#4 0x000000000045041c n/a (n/a + 0x0)
#5 0x00000000004355d0 n/a (n/a + 0x0)
#6 0x00007f317484011a start_thread (libc.so.6 + 0x

Stack trace of thread 6603:
#0 0x00007f31748aea3d syscall (libc.so.6 + 0x103a3
#1 0x00000000004344e2 n/a (n/a + 0x0)
#2 0x0000000000450066 n/a (n/a + 0x0)
#3 0x0000000000405123 n/a (n/a + 0x0)
#4 0x00007f31747d530e __libc_start_call_main (libc
#5 0x00007f31747d53c9 __libc_start_main@GLIBC_2.3
#6 0x00000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x86-64

Sep 29 11:01:22 eragdzhabekova.localdomain systemd[1]: systemd-coredump@226-6607-0.service: Deactivated successfully.

```

Рис. 2.13: Просмотр журнала в реальном времени

### 4. Для изучения доступных параметров фильтрации к команде `journalctl` была добавлена двойная клавиша `Tab`. Отобразился список поддерживаемых ключей (см. рис. fig. 2.14).

```

root@eragdzhabekova:/home/eragdzhabekova# journalctl
Display all 128 possibilities? (y or n)
_AUDIT_LOGINUID= CURRENT_USE_PRETTY= PODMAN_TIME=
_AUDIT_SESSION= DBUS_BROKER_LOG_DROPPED= PODMAN_TYPE=
AVAILABLE= DBUS_BROKER_METRICS_DISPATCH_AVG= PRIORITY=
_BOOT_ID= DBUS_BROKER_METRICS_DISPATCH_COUNT= REALM_OPERACTION=
_CAP_EFFECTIVE= DBUS_BROKER_METRICS_DISPATCH_MAX= _RUNTIME_SCOPE=
_CMDLINE= DBUS_BROKER_METRICS_DISPATCH_MIN= SEAT_ID=
_CODE_FILE= DBUS_BROKER_METRICS_DISPATCH_STDDEV= _SELINUX_CONTEXT=
_CODE_FUNC= DISK_AVAILABLE= SESSION_ID=
_CODE_LINE= DISK_AVAILABLE_PRETTY= _SOURCE_BOOTTIME_TIMESTAMP=
_CODE_LINE= DISK_KEEP_FREE= _SOURCE_MONOTONIC_TIMESTAMP=
_COMM= DISK_KEEP_FREE_PRETTY= _SOURCE_REALTIME_TIMESTAMP=
CONFIG_FILE= ERNNO= SSSD_DOMAIN=
COREDUMP_CGROUP= _EXE= SSSD_PNG_NAME=
COREDUMP_CMDLINE= _GID= _STREAM_ID=
COREDUMP_COMM= GLIB_DOMAIN= SYSLOG_FACILITY=
COREDUMP_CWD= GLIB_OLD_LOG_API= SYSLOG_IDENTIFIER=
COREDUMP_ENVIRON= _HOSTNAME= SYSLOG_PID=
COREDUMP_EXE= INITRD_USEC= SYSLOG_RAW=
COREDUMP_FILENAME= INVOCATION_ID= SYSLOG_TIMESTAMP=
COREDUMP_GID= JOB_ID= _SYSTEMD_CGROUP=
COREDUMP_HOSTNAME= JOB_RESULT= _SYSTEMD_INVOCATION_ID=
COREDUMP_OPEN_FDS= JOURNAL_NAME= _SYSTEMD_OWNER_UID=
COREDUMP_OWNER_UID= JOURNAL_PATH= _SYSTEMD_SESSION=
COREDUMP_PACKAGE_JSON= _KERNEL_DEVICE= _SYSTEMD_SLICE=
COREDUMP_OFD= _VMLINUX_CRC32= _SYSTEMD_UNIT=

```

Рис. 2.14: Параметры фильтрации journalctl

5. Отображены события, связанные с пользователем UID 0:

`journalctl _UID=0`

(см. рис. fig. 2.15).

```

root@eragdzhabekova:/home/eragdzhabekova# journalctl _UID=0
Sep 29 10:41:55 eragdzhabekova.localdomain systemd-journald[258]: Collecting audit messages is disabled.
Sep 29 10:41:55 eragdzhabekova.localdomain systemd-journald[258]: Journal started
Sep 29 10:41:55 eragdzhabekova.localdomain systemd-journald[258]: Runtime Journal (/run/log/journal/8d3b0805f55e426c8)
Sep 29 10:41:55 eragdzhabekova.localdomain systemd-modules-load[259]: Module 'msr' is built in
Sep 29 10:41:55 eragdzhabekova.localdomain systemd-modules-load[259]: Inserted module 'fuse'
Sep 29 10:41:55 eragdzhabekova.localdomain systemd-modules-load[259]: Module 'scsi_dh_alua' is built in
Sep 29 10:41:55 eragdzhabekova.localdomain systemd-modules-load[259]: Module 'scsi_dh_emc' is built in
Sep 29 10:41:55 eragdzhabekova.localdomain systemd-modules-load[259]: Module 'scsi_dh_rdac' is built in
Sep 29 10:41:55 eragdzhabekova.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev-early.service - Create Sta...
Sep 29 10:41:55 eragdzhabekova.localdomain systemd[1]: Starting systemd-sysusers.service - Create System Users...
Sep 29 10:41:55 eragdzhabekova.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variables.
Sep 29 10:41:55 eragdzhabekova.localdomain systemd-sysusers[276]: Creating group 'nobody' with GID 65534.
Sep 29 10:41:55 eragdzhabekova.localdomain systemd-sysusers[276]: Creating group 'users' with GID 100.
Sep 29 10:41:55 eragdzhabekova.localdomain systemd-sysusers[276]: Creating group 'systemd-journal' with GID 190.
Sep 29 10:41:55 eragdzhabekova.localdomain systemd-sysusers[276]: Finished systemd-sysusers.service - Create System Users.
Sep 29 10:41:55 eragdzhabekova.localdomain systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create Static De...
Sep 29 10:41:55 eragdzhabekova.localdomain systemd[1]: Finished systemd-vconsole-setup.service - Virtual Console Setup
Sep 29 10:41:55 eragdzhabekova.localdomain systemd[1]: dracut-cmdline-ask.service - dracut ask for additional cmdline...
Sep 29 10:41:55 eragdzhabekova.localdomain dracut-cmdline[285]: dracut-105-4.el10_0
Sep 29 10:41:55 eragdzhabekova.localdomain dracut-cmdline[285]: Using kernel command line parameters: BOOT_IMAGE=...
Sep 29 10:41:55 eragdzhabekova.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev.service - Create Static De...

```

Рис. 2.15: Фильтрация по UID=0

6. Выведены последние 20 строк журнала:

`journalctl -n 20`

(см. рис. fig. 2.16).

```

root@eragdzhabekova:/home/eragdzhabekova#
root@eragdzhabekova:/home/eragdzhabekova# journalctl -n 20
Sep 29 11:02:53 eragdzhabekova.localdomain kernel: traps: VBoxClient[6807] trap int3 ip:41dd1b sp:7f3166188cd0 error:0
Sep 29 11:02:53 eragdzhabekova.localdomain systemd[6808]: Process 6804 (VBoxClient) of user 1000 terminated
Sep 29 11:02:53 eragdzhabekova.localdomain systemd[1]: Started systemd-coredump@244-6808-0.service - Process Core Dump
Sep 29 11:02:54 eragdzhabekova.localdomain systemd-coredump[6809]: [?] Process 6804 (VBoxClient) of user 1000 dumped

Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64
Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64
Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64
Module libwayland-client.so.0 from rpm wayland-1.2.x86_64
Stack trace of thread 6807:
#0 0x000000000041dd1b n/a (n/a + 0x0)
#1 0x000000000041dc94 n/a (n/a + 0x0)
#2 0x000000000045041c n/a (n/a + 0x0)
#3 0x00000000004355d0 n/a (n/a + 0x0)
#4 0x00007f317484011a start_thread (libc.so.6 + 0x105)
#5 0x00007f31748b0c3c __clone3 (libc.so.6 + 0x105)

Stack trace of thread 6804:
#0 0x00007f31748aea3d syscall (libc.so.6 + 0x103a)
#1 0x00000000004344e2 n/a (n/a + 0x0)
#2 0x0000000000450066 n/a (n/a + 0x0)
#3 0x0000000000405123 n/a (n/a + 0x0)
#4 0x00007f31747d530e __libc_start_main (libc.so.6 + 0x105)
#5 0x00007f31747d53c9 __libc_start_main@@GLIBC_2.2
#6 0x00000000004044aa n/a (n/a + 0x0)

ELF object binary architecture: AMD x86-64

Sep 29 11:02:54 eragdzhabekova.localdomain systemd[1]: systemd-coredump@244-6808-0.service: Deactivated successfully.
Sep 29 11:02:59 eragdzhabekova.localdomain kernel: traps: VBoxClient[6819] trap int3 ip:41dd1b sp:7f3166188cd0 error:0
Sep 29 11:02:59 eragdzhabekova.localdomain systemd-coredump[6820]: Process 6816 (VBoxClient) of user 1000 terminated

```

Рис. 2.16: Просмотр последних 20 строк

## 7. Получены только сообщения с уровнем «ошибки»:

`journalctl -p err`

(см. рис. fig. 2.17).

```

root@eragoznabekova:/home/eragoznabekova#
root@eragdzhabekova:/home/eragdzhabekova# journalctl -p err
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on a
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely br
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported gr
Sep 29 10:41:58 eragdzhabekova.localdomain alsactl[875]: alsalib main.c:1554:(snd_use_case_mgr_open) error: failed to
Sep 29 10:41:59 eragdzhabekova.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Sep 29 10:42:09 eragdzhabekova.localdomain gdm-password[1896]: gkr-pam: unable to locate daemon control file
Sep 29 10:42:12 eragdzhabekova.localdomain systemd[1908]: Failed to start app-gnome-xdg\x2duser\x2ddirs-2034.scope -
Sep 29 10:42:13 eragdzhabekova.localdomain systemd[1908]: Failed to start app-gnome-vmware\x2duser-2235.scope - Appli
Sep 29 10:42:14 eragdzhabekova.localdomain systemd-coredump[2699]: [?] Process 2693 (VBoxClient) of user 1000 dumped

Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64
Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64
Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64
Module libwayland-client.so.0 from rpm wayland-1.2.x86_64
Stack trace of thread 2697:
#0 0x000000000041dd1b n/a (n/a + 0x0)
#1 0x000000000041dc94 n/a (n/a + 0x0)
#2 0x000000000045041c n/a (n/a + 0x0)
#3 0x00000000004355d0 n/a (n/a + 0x0)
#4 0x00007f317484011a start_thread (libc.so.6 + 0x105)
#5 0x00007f31748b0c3c __clone3 (libc.so.6 + 0x105)

Stack trace of thread 2695:
#0 0x00007f31748aea3d syscall (libc.so.6 + 0x103a)
#1 0x0000000000434c30 n/a (n/a + 0x0)
#2 0x0000000000450fb n/a (n/a + 0x0)
#3 0x000000000043566a n/a (n/a + 0x0)
#4 0x000000000045041c n/a (n/a + 0x0)

```

Рис. 2.17: Фильтрация только ошибок

## 8. Просмотрены все события со вчерашнего дня:

`journalctl --since yesterday`

(см. рис. fig. 2.18).

```

root@eragdzhabekova:/home/eragdzhabekova# journalctl --since yesterday
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build)
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-provided physical RAM map:
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000009fbff] usable
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x00000000009fc00-0x00000000009ffff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x0000000000ffff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000007ffff] usable
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x00000000007ffff000-0x0000000007ffffff] ACPI data
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x0000000000fec0000-0x00000000fec00ff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x0000000000fee0000-0x00000000fee00ff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x0000000000fffc0000-0x000000000fffffff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: NX (Execute Disable) protection: active
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: APIC: Static calls initialized
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: SMBIOS 2.5 present.
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: DMI: innoteck GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: DMI: Memory slots populated: 0/0
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: Hypervisor detected: KVM
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: kvm-clock: Using msr 4b564d01 and 4b564d00
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: kvm-clock: using sched offset of 4050277964 cycles
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: clocksource: kvm-clock: mask: 0xfffffffffffffff max_cycles: 0x1cd8
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: tsc: Detected 3187.202 MHz processor
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: e820: update [mem 0x00000000-0x0000ffff] usable ==> reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: e820: remove [mem 0x00000000-0x0000ffff] usable
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: last_pfn = 0x800000 max_arch_pfn = 0x4000000000
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: MTRR map: 4 entries (3 fixed + 1 variable; max 35), built from 16
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: x86/PAT: Configuration [0-7]: WB WC UC UC WB WP UC- WT
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: found SMP MP-table at [mem 0x0009fbf0-0x0009fbff]
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: Incomplete global flushes, disabling PCID

```

Рис. 2.18: Просмотр событий со вчерашнего дня

## 9. Отображены только ошибки со вчерашнего дня:

`journalctl -since yesterday -p err`  
 (см. рис. fig. 2.19).

```

root@eragdzhabekova:/home/eragdzhabekova# journalctl --since yesterday -p err
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: vwgfx 0000:00:02.0: [drm] *ERROR* vwgfx seems to be running on a
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: vwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely br
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: vwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported gr
Sep 29 10:41:58 eragdzhabekova.localdomain kernel: Warning: Unmaintained driver is detected: el1000
Sep 29 10:41:59 eragdzhabekova.localdomain alsactl[875]: alsalib main.c:1554:(snd_use_case_mixer_open) error: failed to
Sep 29 10:41:59 eragdzhabekova.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Sep 29 10:42:09 eragdzhabekova.localdomain gdm-password[1896]: gkr-pam: unable to locate daemon control file
Sep 29 10:42:12 eragdzhabekova.localdomain systemd[1908]: Failed to start app-gnome-xdg|x2duser|x2ddirs-2034.scope -
Sep 29 10:42:13 eragdzhabekova.localdomain systemd[1908]: Failed to start app-gnome-vmware|x2duser-2235.scope - Appli
Sep 29 10:42:14 eragdzhabekova.localdomain systemd-coredump[2699]: [...] Process 2693 (VBoxClient) of user 1000 dumped
Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64
Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64
Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64
Module libwayland-client.so.0 from rpm wayland-1.2-1.el10.x86_64
Stack trace of thread 2697:
#0 0x000000000041dd1b n/a (n/a + 0x0)
#1 0x000000000041dc94 n/a (n/a + 0x0)
#2 0x000000000045041c n/a (n/a + 0x0)
#3 0x00000000004355d0 n/a (n/a + 0x0)
#4 0x00007f317484011a start_thread (libc.so.6 + 0x105)
#5 0x00007f31748b0c3c __clone3 (libc.so.6 + 0x105)

Stack trace of thread 2695:
#0 0x00007f31748ea3d syscall (libc.so.6 + 0x103a)
#1 0x0000000000434c30 n/a (n/a + 0x0)
#2 0x0000000000450fb n/a (n/a + 0x0)
#3 0x000000000043566a n/a (n/a + 0x0)
#4 0x000000000045041c n/a (n/a + 0x0)
#5 0x00000000004355d0 n/a (n/a + 0x0)
#6 0x00007f317484011a start_thread (libc.so.6 + 0x105)
#7 0x00000000004355d0 n/a (n/a + 0x0)

```

Рис. 2.19: Ошибки со вчерашнего дня

## 10. Использован режим детализированного вывода:

`journalctl -o verbose`  
 (см. рис. fig. 2.20).

```

[...]
Mon 2025-09-29 10:41:55.6666675 MSK [s=b17203d2cf9d4acca6f3e52e30edda96;i=2;b=24c94e4675094dee9d364f8a2d02f85c;m=71942]
    _SOURCE_BOOTTIME_TIMESTAMP=0
    _SOURCE_MONOTONIC_TIMESTAMP=0
    _TRANSPORT=kernel
    SYSLOG_FACILITY=0
    SYSLOG_IDENTIFIER=kernel
    _BOOT_ID=24c94e4675094dee9d364f8a2d02f85c
    _MACHINE_ID=d3db0805f55e426c81d006a05a020583
    _HOSTNAME=eragdzhabekova.localdomain
    _RUNTIME_SCOPE=initrd
    PRIORITY=6
MESSAGE=Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_64 root=/dev/mapper/r1_vbox-root ro
Mon 2025-09-29 10:41:55.6666800 MSK [s=b17203d2cf9d4acca6f3e52e30edda96;i=3;b=24c94e4675094dee9d364f8a2d02f85c;m=71947]
    _SOURCE_BOOTTIME_TIMESTAMP=0
    _SOURCE_MONOTONIC_TIMESTAMP=0
    _TRANSPORT=kernel
    SYSLOG_FACILITY=0
    SYSLOG_IDENTIFIER=kernel
    _BOOT_ID=24c94e4675094dee9d364f8a2d02f85c
    _MACHINE_ID=d3db0805f55e426c81d006a05a020583
    _HOSTNAME=eragdzhabekova.localdomain
    _RUNTIME_SCOPE=initrd
    PRIORITY=6
MESSAGE=BIOS-provided physical RAM map:
Mon 2025-09-29 10:41:55.666685 MSK [s=b17203d2cf9d4acca6f3e52e30edda96;i=4;b=24c94e4675094dee9d364f8a2d02f85c;m=7194c]
lines 1-37

```

Рис. 2.20: Детализированный вывод сообщений

- Для просмотра дополнительной информации о модуле `sshd` использована команда:

```
journalctl _SYSTEMD_UNIT=sshd.service
```

В выводе отобразились записи о запуске службы (см. рис. fig. 2.21).

```

root@eragdzhabekova:/home/eragdzhabekova# journalctl _SYSTEMD_UNIT=sshd.service
Sep 29 10:41:59 eragdzhabekova.localdomain (sshd)[1138]: sshd.service: Referenced but unset environment variable eva...
Sep 29 10:41:59 eragdzhabekova.localdomain sshd[1138]: Server listening on 0.0.0.0 port 22.
Sep 29 10:41:59 eragdzhabekova.localdomain sshd[1138]: Server listening on :: port 22.
lines 1-3/3 (END)

```

Рис. 2.21: Просмотр информации о модуле `sshd`

## 2.4 Постоянный журнал `journald`

- Создан каталог для хранения постоянных записей журнала:

```
mkdir -p /var/log/journal
```

- Для каталога `/var/log/journal` скорректированы права доступа, чтобы служба `systemd-journald` могла вести туда запись:

```
chown root:systemd-journal /var/log/journal
```

```
chmod 2755 /var/log/journal
```

- Чтобы принять изменения без перезагрузки системы, `journald` был принудительно перезапущен сигналом:

```
killall -USR1 systemd-journald
```

- После этого просмотрен журнал с момента последней перезагрузки с помощью команды:

```
journalctl -b
```

(см. рис. fig. 2.22).

```
root@eragdzhabekova:/home/eragdzhabekova# /home/eragdzhabekova# mkdir -p /var/log/journal
root@eragdzhabekova:/home/eragdzhabekova# chown root:systemd-journal /var/log/journal/
root@eragdzhabekova:/home/eragdzhabekova# chmod 2755 /var/log/journal/
root@eragdzhabekova:/home/eragdzhabekova# killall -USR1 systemd-journald
root@eragdzhabekova:/home/eragdzhabekova# journalctl -b
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build)
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-provided physical RAM map:
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000fff] usable
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x00000000000009f0-0x000000000009ffff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x000000000000f000-0x000000000000ffff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x00000000000100000-0x00000000007ffff] usable
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x00000000007ffff-0x00000000007ffff] ACPI data
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x000000000fec0000-0x000000000fec0fff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x000000000fee0000-0x000000000fee0fff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x000000000fffc0000-0x000000000fffcffff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: NX (Execute Disable) protection: active
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: APIC: Static calls initialized
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: SMBIOS 2.5 present.
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: DMI: Memory slots populated: 0/0
```

Рис. 2.22: Включение постоянного журнала journald

## 3 Контрольные вопросы

### 1. Какой файл используется для настройки rsyslogd?

Основной конфигурационный файл – /etc/rsyslog.conf. Дополнительные правила могут храниться в каталоге /etc/rsyslog.d/.

### 2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?

Сообщения об аутентификации и авторизации записываются в файл /var/log/secure.

### 3. Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?

По умолчанию лог-файлы ротируются **еженедельно**, настройки задаются в /etc/logrotate.conf.

### 4. Какую строку следует добавить в конфигурацию для записи всех сообщений с приоритетом info в файл /var/log/messages.info?

\*.info /var/log/messages.info

### 5. Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?

Используются команды:

- tail -f /var/log/имя\_журнала – для файлов rsyslog.

- journalctl -f – для systemd-journald.

**6. Какая команда позволяет вам видеть все сообщения журнала, которые были написаны для PID 1 между 9:00 и 15:00?**

```
journalctl _PID=1 --since "09:00" --until "15:00"
```

**7. Какая команда позволяет вам видеть сообщения journald после последней перезагрузки системы?**

```
journalctl -b
```

**8. Какая процедура позволяет сделать журнал journald постоянным?**

- Создать каталог /var/log/journal.

- Назначить права доступа:

```
chown root:systemd-journal /var/log/journal
```

```
chmod 2755 /var/log/journal
```

- Перезапустить journald командой killall -USR1 systemd-journald или выполнить перезагрузку.

## **4 Заключение**

В ходе лабораторной работы были изучены принципы работы с системными журналами в Linux. Рассмотрена настройка службы rsyslog, включая перенаправление сообщений веб-сервера Apache и регистрацию отладочной информации в отдельные файлы. Освоены приёмы мониторинга логов в реальном времени с помощью `tail` и `journalctl`, выполнена фильтрация событий по различным параметрам. Настроен постоянный журнал `journald`, что позволило сохранять сообщения после перезагрузки системы. Получены практические навыки администрирования, связанные с управлением логами и диагностикой работы служб.