

# **Отчёт по лабораторной работе №7**

**Управление журналами событий в системе**

Анна Саенко

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Ход выполнения работы</b>	<b>6</b>
2.1	Мониторинг журнала системных событий в реальном времени . .	6
2.2	Изменение правил rsyslog.conf . . . . .	8
2.3	Использование journalctl . . . . .	11
2.4	Постоянный журнал journald . . . . .	16
<b>3</b>	<b>Контрольные вопросы</b>	<b>18</b>
<b>4</b>	<b>Заключение</b>	<b>20</b>

# Список иллюстраций

2.1	Мониторинг системных сообщений в реальном времени . . . . .	6
2.2	Ошибка при вводе неверного пароля . . . . .	7
2.3	Регистрируемое сообщение hello . . . . .	7
2.4	Просмотр файла secure . . . . .	8
2.5	Установка и запуск httpd . . . . .	8
2.6	Мониторинг журнала ошибок Apache . . . . .	9
2.7	Добавление параметра ErrorLog в конфигурацию Apache . . . . .	9
2.8	Создание правила для перенаправления логов Apache . . . . .	10
2.9	Создание правил для отладочного логирования . . . . .	10
2.10	Мониторинг и регистрация отладочного сообщения . . . . .	11
2.11	Просмотр журнала событий . . . . .	11
2.12	Вывод журнала без пейджера . . . . .	12
2.13	Режим реального времени в journalctl . . . . .	12
2.14	Просмотр доступных параметров фильтрации . . . . .	13
2.15	Фильтрация журнала по UID . . . . .	13
2.16	Просмотр последних 20 строк журнала . . . . .	14
2.17	Фильтрация по сообщениям с приоритетом “ошибка” . . . . .	14
2.18	Журнал со вчерашнего дня . . . . .	15
2.19	Сообщения об ошибках со вчерашнего дня . . . . .	15
2.20	Детализированный вывод журнала . . . . .	16
2.21	Просмотр журнала для sshd . . . . .	16
2.22	Просмотр системного журнала с момента загрузки . . . . .	17

## **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

Сначала я открыла три вкладки терминала и в каждой получила полномочия администратора, выполнив команду `su -`.

Во второй вкладке я запустила мониторинг системных сообщений в реальном времени при помощи команды `tail -f /var/log/messages`.

На скриншоте показаны примеры сообщений, которые были зафиксированы в логе.

```
-----
root@aasaenko:/home/aasaenko# tail -f /var/log/messages
Sep 30 18:46:59 aasaenko kernel: traps: VBoxClient[3750] trap int3 ip:41ddb sp:7f8584afbcd0 error:0 in VBoxClient[1ddb,400000+bb000]
Sep 30 18:46:59 aasaenko systemd-coredump[3751]: Process 3747 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Sep 30 18:46:59 aasaenko systemd[1]: Started systemd-coredump@40-3751-0.service - Process Core Dump (PID 3751/UID 0).
Sep 30 18:46:59 aasaenko systemd-coredump[3752]: Process 3747 (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 3750:#012#0 0x00000000041ddb n/a (n/a + 0x0)#012#1 0x00000000041dc94 n/a (n/a + 0x0)#012#2 0x000000000045041c n/a (n/a + 0x0)#012#3 0x0000000004355d0 n/a (n/a + 0x0)#012#4 0x00007f85931a211a start_thread (libc.so.6 + 0x9511a)#012#5 0x00007f8593212c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 3747:#012#0 0x00007f8593210a3d syscall (libc.so.6 + 0x103a3d)#012#1 0x0000000004344e2 n/a (n/a + 0x0)#012#2 0x000000000450066 n/a (n/a + 0x0)#012#3 0x000000000405123 n/a (n/a + 0x0)#012#4 0x00007f859313730e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x00007f85931373c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x0000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Sep 30 18:46:59 aasaenko systemd[1]: systemd-coredump@40-3751-0.service: Deactivated successfully.
Sep 30 18:47:04 aasaenko kernel: traps: VBoxClient[3763] trap int3 ip:41ddb sp:7f8584afbcd0 error:0 in VBoxClient[1ddb,400000+bb000]
Sep 30 18:47:04 aasaenko systemd-coredump[3764]: Process 3760 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Sep 30 18:47:04 aasaenko systemd[1]: Started systemd-coredump@41-3764-0.service - Process Core Dump (PID 3764/UID 0).
Sep 30 18:47:04 aasaenko systemd-coredump[3765]: Process 3760 (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 3763:#012#0 0x00000000041ddb n/a (n/a + 0x0)#012#1 0x00000000041dc94 n/a (n/a + 0x0)#012#2 0x0000000000
```

Рис. 2.1: Мониторинг системных сообщений в реальном времени

Затем в третьей вкладке я вернулась к своей учётной записи, нажав **Ctrl + d**, и попыталась получить права суперпользователя, но специально ввела неправильный пароль.

В результате во второй вкладке появилось сообщение о неудачной попытке входа.

```
00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Sep 30 18:47:30 aasaenko systemd[1]: systemd-coredump@46-3831-0.service: Deactivated successfully.
Sep 30 18:47:30 aasaenko su[3817]: FAILED SU (to root) aasaenko on pts/2
Sep 30 18:47:35 aasaenko kernel: traps: VBoxClient[3841] trap int3 ip:41ddb1 sp:7f8584afbcd0 error:0 in VBoxC
lient[1ddb1,400000+bb000]
Sep 30 18:47:35 aasaenko systemd-coredump[3842]: Process 3838 (VBoxClient) of user 1000 terminated abnormally
with signal 5/TRAP, processing...
Sep 30 18:47:35 aasaenko systemd[1]: Started systemd-coredump@47-3842-0.service - Process Core Dump (PID 3842
/UID 0).
```

Рис. 2.2: Ошибка при вводе неверного пароля

После этого я ввела команду `logger hello`.

Сообщение «hello» сразу отобразилось в окне мониторинга системных сообщений.

```
-----
tart_call_main (libc.so.6 + 0x2a30e)#012#5 0x00007f85931373c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2
a3c9)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Sep 30 18:47:50 aasaenko systemd[1]: systemd-coredump@50-3872-0.service: Deactivated successfully.
Sep 30 18:47:54 aasaenko aasaenko[3878]: hello
Sep 30 18:47:55 aasaenko kernel: traps: VBoxClient[3886] trap int3 ip:41ddb1 sp:7f8584afbcd0 error:0 in VBoxC
lient[1ddb1,400000+bb000]
Sep 30 18:47:55 aasaenko systemd-coredump[3887]: Process 3883 (VBoxClient) of user 1000 terminated abnormally
with signal 5/TRAP, processing...
Sep 30 18:47:55 aasaenko systemd[1]: Started systemd-coredump@51-3887-0.service - Process Core Dump (PID 3887
/UID 0).
```

Рис. 2.3: Регистрируемое сообщение hello

Затем я остановила мониторинг файла `/var/log/messages` сочетанием клавиш **Ctrl + C** и просмотрела последние 20 строк журнала безопасности командой `tail -n 20 /var/log/secure`.

В журнале сохранились записи о неудачных попытках авторизации при использовании команды `su`.

```
root@aasaenko:/home/aasaenko# tail -n 20 /var/log/secure
Sep 25 11:07:51 aasaenko su[4426]: pam_unix(su:session): session opened for user root(uid=0) by aasaenko(uid=1000)
Sep 25 11:12:32 aasaenko su[4426]: pam_unix(su:session): session closed for user root
Sep 25 11:12:39 aasaenko su[5190]: pam_unix(su:session): session opened for user root(uid=0) by aasaenko(uid=1000)
Sep 30 18:42:46 aasaenko sshd[1184]: Server listening on 0.0.0.0 port 22.
Sep 30 18:42:46 aasaenko sshd[1184]: Server listening on :: port 22.
Sep 30 18:42:46 aasaenko (systemd)[1249]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)
Sep 30 18:42:46 aasaenko gdm-launch-environment[1228]: pam_unix(gdm-launch-environment:session): session opened for user r gdm(uid=42) by (uid=0)
Sep 30 18:43:30 aasaenko gdm-password[1990]: gkr-pam: unable to locate daemon control file
Sep 30 18:43:30 aasaenko gdm-password[1990]: gkr-pam: stashed password to try later in open session
Sep 30 18:43:30 aasaenko (systemd)[2001]: pam_unix(systemd-user:session): session opened for user aasaenko(uid=1000) by aasaenko(uid=0)
Sep 30 18:43:30 aasaenko gdm-password[1990]: pam_unix(gdm-password:session): session opened for user aasaenko(uid=1000) by aasaenko(uid=0)
Sep 30 18:43:30 aasaenko gdm-password[1990]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Sep 30 18:43:35 aasaenko gdm-launch-environment[1228]: pam_unix(gdm-launch-environment:session): session closed for user r gdm
Sep 30 18:46:13 aasaenko (systemd)[3509]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)
Sep 30 18:46:13 aasaenko su[3484]: pam_unix(su:session): session opened for user root(uid=0) by aasaenko(uid=1000)
Sep 30 18:46:18 aasaenko su[3582]: pam_unix(su:session): session opened for user root(uid=0) by aasaenko(uid=1000)
Sep 30 18:46:23 aasaenko su[3643]: pam_unix(su:session): session opened for user root(uid=0) by aasaenko(uid=1000)
Sep 30 18:47:25 aasaenko su[3643]: pam_unix(su:session): session closed for user root
Sep 30 18:47:28 aasaenko unix_chkpwd[3826]: password check failed for user (root)
Sep 30 18:47:28 aasaenko su[3817]: pam_unix(su:auth): authentication failure; logname=aasaenko uid=1000 euid=0 tty=/dev/pts/2 ruser=aasaenko rhost= user=root
root@aasaenko:/home/aasaenko#
```

Рис. 2.4: Просмотр файла secure

## 2.2 Изменение правил rsyslog.conf

Сначала я установила веб-сервер Apache при помощи пакетного менеджера `dnf`.

После завершения установки я запустила веб-службу и добавила её в автозагрузку.

```
Installed:
apr-1.7.5-2.el10.x86_64          apr-util-1.6.3-21.el10.x86_64          apr-util-ldap-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

Complete!
root@aasaenko:/home/aasaenko# systemctl start httpd
root@aasaenko:/home/aasaenko# systemctl enable httpd
Created symlink '/etc/systemd/system/multi-user.target.wants/httpd.service' -> '/usr/lib/systemd/system/httpd.service'.
root@aasaenko:/home/aasaenko#
```

Рис. 2.5: Установка и запуск httpd

Во второй вкладке терминала я открыла журнал ошибок веб-сервера командой `tail -f /var/log/httpd/error_log`.

На скриншоте видно, что служба `httpd` успешно запущена и функционирует.



```

root@aasaenko:/home/aasaenko#
root@aasaenko:/home/aasaenko# tail -f /var/log/httpd/error_log
[Tue Sep 30 18:52:57.720801 2025] [suexec:notice] [pid 4869:tid 4869] AH01232: suEXEC mechanism enabled (wrapper: /usr/s
bin/suexec)
[Tue Sep 30 18:52:57.770333 2025] [lbmethod_heartbeat:notice] [pid 4869:tid 4869] AH02282: No slotmem from mod_heartmoni
tor
[Tue Sep 30 18:52:57.771160 2025] [systemd:notice] [pid 4869:tid 4869] SELinux policy enabled; httpd running as context
system_u:system_r:httpd_t:s0
[Tue Sep 30 18:52:57.773504 2025] [mpm_event:notice] [pid 4869:tid 4869] AH00489: Apache/2.4.63 (Rocky Linux) configured
-- resuming normal operations
[Tue Sep 30 18:52:57.773518 2025] [core:notice] [pid 4869:tid 4869] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUN
D'

```

Рис. 2.6: Мониторинг журнала ошибок Apache

Затем я отредактировала файл конфигурации `/etc/httpd/conf/httpd.conf`.  
В конец файла я добавила строку `ErrorLog syslog:local1`, чтобы сообщения об  
ошибках веб-службы перенаправлялись в системный журнал через объект **local1**.

```

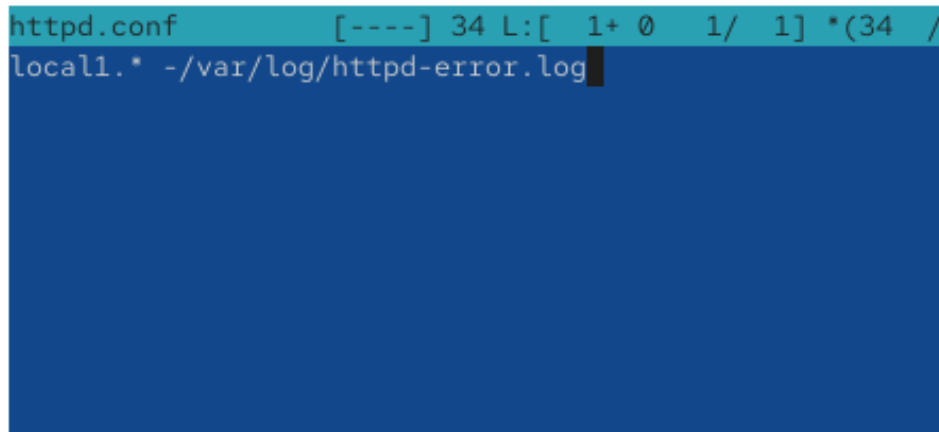
#
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall may be used to deliver
# files. This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# 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

```

Рис. 2.7: Добавление параметра ErrorLog в конфигурацию Apache

После этого в каталоге `/etc/rsyslog.d` я создала новый файл `httpd.conf`.  
Эта настройка позволила перенаправлять все сообщения от объекта **local1** в  
отдельный лог-файл `/var/log/httpd-error.log`.



```
httpd.conf [----] 34 L:[ 1+ 0 1/ 1] *(34 /
local1.* -/var/log/httpd-error.log
```

Рис. 2.8: Создание правила для перенаправления логов Apache

Затем я перезапустила службы rsyslog и httpd, чтобы изменения вступили в силу.

После этого я создала дополнительный файл debug.conf с правилом записи отладочных сообщений в файл /var/log/messages-debug.

```
root@aasaenko:/home/aasaenko# mcedit /etc/httpd/conf/httpd.conf

root@aasaenko:/home/aasaenko# cd /etc/rsyslog.d/
root@aasaenko:/etc/rsyslog.d# touch httpd.conf
root@aasaenko:/etc/rsyslog.d# mcedit httpd.conf

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

Рис. 2.9: Создание правил для отладочного логирования

Во второй вкладке терминала я запустила мониторинг отладочных сообщений с помощью `tail -f /var/log/messages-debug`.

Затем в третьей вкладке я сгенерировала сообщение отладки с помощью команды `logger -p daemon.debug "Daemon Debug Message"`.

Сообщение успешно отобразилось в файле /var/log/messages-debug.

```

0x0)#012#3 0x0000000000040b123 n/a (n/a + 0x0)#012#4 0x0000000000000000 __libc_start_call_main (__libc.so.6 + 0x2a30e)#0
12#5 0x0000000000000000 __libc_start_main@GLIBC_2.34 (__libc.so.6 + 0x2a3c9)#012#6 0x0000000000000000 n/a (n/a + 0x0)#0
12ELF object binary architecture: AMD x86-64
Sep 30 18:58:48 aasaenko systemd[1]: systemd-coredump@179-6544-0.service: Deactivated successfully.
Sep 30 18:58:52 aasaenko root[6550]: Daemon Debug Message
Sep 30 18:58:53 aasaenko kernel: traps: VBoxClient[6555] trap int3 ip:41ddb sp:7f8584afbcd0 error:0 in VBoxClient[1ddb
,400000+bb000]
Sep 30 18:58:53 aasaenko systemd-coredump[6556]: Process 6552 (VBoxClient) of user 1000 terminated abnormally with signa
l 5/TRAP, processing...
Sep 30 18:58:53 aasaenko systemd[1]: Started systemd-coredump@180-6556-0.service - Process Core Dump (PID 6556/UID 0).
Sep 30 18:58:53 aasaenko systemd-coredump[6557]: Process 6552 (VBoxClient) of user 1000 dumped core.#012#012Module libXa

```

Рис. 2.10: Мониторинг и регистрация отладочного сообщения

## 2.3 Использование journalctl

Сначала я просмотрела содержимое системного журнала с момента последнего запуска системы, используя команду `journalctl`.

Для пролистывания журнала я применяла клавиши Enter и Space, а для выхода — q.

```

root@aasaenko:/home/aasaenko# journalctl
Sep 30 18:42:41 aasaenko.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.b
Sep 30 18:42:41 aasaenko.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_64 r
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-provided physical RAM map:
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000009fbff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x00000000000009fc00-0x00000000000009ffff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000000f0000-0x0000000000000fffff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000000fffff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000000ffff0000-0x0000000000000fffff] ACPI data
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffffff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: NX (Execute Disable) protection: active
Sep 30 18:42:41 aasaenko.localdomain kernel: APIC: Static calls initialized
Sep 30 18:42:41 aasaenko.localdomain kernel: SMBIOS 2.5 present.
Sep 30 18:42:41 aasaenko.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 30 18:42:41 aasaenko.localdomain kernel: DMI: Memory slots populated: 0/0
Sep 30 18:42:41 aasaenko.localdomain kernel: Hypervisor detected: KVM
Sep 30 18:42:41 aasaenko.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Sep 30 18:42:41 aasaenko.localdomain kernel: kvm-clock: using sched offset of 4068452678 cycles
Sep 30 18:42:41 aasaenko.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb
Sep 30 18:42:41 aasaenko.localdomain kernel: tsc: Detected 3187.204 MHz processor
Sep 30 18:42:41 aasaenko.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: e820: remove [mem 0x000a0000-0x0000ffff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x40000000
Sep 30 18:42:41 aasaenko.localdomain kernel: total RAM covered: 4096M
Sep 30 18:42:41 aasaenko.localdomain kernel: Found optimal setting for mtrr clean up
Sep 30 18:42:41 aasaenko.localdomain kernel: gran_size: 64K chunk_size: 1G num_reg: 3 lose co
Sep 30 18:42:41 aasaenko.localdomain kernel: MTRR map: 6 entries (3 fixed + 3 variable; max 35), built from 16 variables
Sep 30 18:42:41 aasaenko.localdomain kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT

```

Рис. 2.11: Просмотр журнала событий

Далее я вывела журнал без использования пейджера при помощи ключа `--no-pager`.

```
0x2a30e)                                     ## 0x00007f85931373c9 __libc_start_main (@GLIBC_2.34 + 0x0)
so.6 + 0x2a3c9)                             #6 0x0000000004044aa n/a (n/a + 0x0)
                                             ELF object binary architecture: AMD x86-64
Sep 30 19:00:40 aasaenko.localdomain systemd[1]: systemd-coredump@201-6820-0.service: Deactivated successfully.
Sep 30 19:00:45 aasaenko.localdomain kernel: traps: VBoxClient[6844] trap int3 ip:41dd1b sp:7f8584afbcd0 error:0 in VBox
Client[1dd1b.400000+bb000]
Sep 30 19:00:45 aasaenko.localdomain systemd-coredump[6845]: Process 6841 (VBoxClient) of user 1000 terminated abnormall
y with signal 5/TRAP, processing...
Sep 30 19:00:45 aasaenko.localdomain systemd[1]: Started systemd-coredump@202-6845-0.service - Process Core Dump (PID 68
45/UID 0).
Sep 30 19:00:45 aasaenko.localdomain systemd-coredump[6846]: [?] Process 6841 (VBoxClient) of user 1000 dumped core.

                                         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-1.23.0-2.el1
0.x86_64

                                         Stack trace of thread 6844:
                                         #0 0x00000000041dd1b n/a (n/a + 0x0)
                                         #1 0x00000000041dc94 n/a (n/a + 0x0)
                                         #2 0x00000000045041c n/a (n/a + 0x0)
                                         #3 0x0000000004355d0 n/a (n/a + 0x0)
                                         #4 0x00007f85931a211a start_thread (libc.so.6 + 0x9511a)
```

Рис. 2.12: Вывод журнала без пейджера

Затем я перешла в режим просмотра журнала в реальном времени, выполнив команду `journalctl -f`.

Для завершения мониторинга я использовала сочетание клавиш `Ctrl + C`.

```
root@aasaenko:/home/aasaenko#
root@aasaenko:/home/aasaenko# journalctl -f
Sep 30 19:01:00 aasaenko.localdomain systemd[1]: systemd-coredump@205-6883-0.service: Deactivated successfully.
Sep 30 19:01:01 aasaenko.localdomain CROND[6890]: (root) CMD (run-parts /etc/cron.hourly)
Sep 30 19:01:01 aasaenko.localdomain run-parts[6893]: (/etc/cron.hourly) starting 0anacron
Sep 30 19:01:01 aasaenko.localdomain anacron[6903]: Anacron started on 2025-09-30
Sep 30 19:01:01 aasaenko.localdomain anacron[6903]: Will run job `cron.daily' in 26 min.
Sep 30 19:01:01 aasaenko.localdomain anacron[6903]: Will run job `cron.weekly' in 46 min.
Sep 30 19:01:01 aasaenko.localdomain anacron[6903]: Will run job `cron.monthly' in 66 min.
Sep 30 19:01:01 aasaenko.localdomain anacron[6903]: Jobs will be executed sequentially
Sep 30 19:01:01 aasaenko.localdomain run-parts[6905]: (/etc/cron.hourly) finished 0anacron
Sep 30 19:01:01 aasaenko.localdomain CROND[6889]: (root) CMDEND (run-parts /etc/cron.hourly)
```

Рис. 2.13: Режим реального времени в `journalctl`

Чтобы ознакомиться с параметрами фильтрации, я ввела команду `journalctl` и дважды нажала клавишу `Tab`.

В терминале появился список доступных опций.

```

root@aasaenko:/home/aasaenko# 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=
AVAILABLE_PRETTY=        DBUS_BROKER_METRICS_DISPATCH_COUNT=  REALMD_OPERATION=
_BOOT_ID=               DBUS_BROKER_METRICS_DISPATCH_MAX=    _RUNTIME_SCOPE=
_CAP_EFFECTIVE=          DBUS_BROKER_METRICS_DISPATCH_MIN=    SEAT_ID=
_CMDLINE=               DBUS_BROKER_METRICS_DISPATCH_STDDEV= _SELINUX_CONTEXT=
CODE_FILE=              DISK_AVAILABLE=              SESSION_ID=
CODE_FUNC=              DISK_AVAILABLE_PRETTY=        _SOURCE_BOOTTIME_TIMESTAMP=
CODE_LINE=              DISK_KEEP_FREE=              _SOURCE_MONOTONIC_TIMESTAMP=
_COMM=                  DISK_KEEP_FREE_PRETTY=        _SOURCE_REALTIME_TIMESTAMP=
CONFIG_FILE=            ERRNO=                        SSSD_DOMAIN=
CONFIG_LINE=            _EXE=                        SSSD_PRG_NAME=
COREDUMP_CGROUP=        _GID=                        _STREAM_ID=
COREDUMP_CMDLINE=       GLIB_DOMAIN=                 SYSLOG_FACILITY=
COREDUMP_COMM=          GLIB_OLD_LOG_API=            SYSLOG_IDENTIFIER=
COREDUMP_CWD=           _HOSTNAME=                   SYSLOG_PID=
COREDUMP_ENVIRON=       INITRD_USEC=                  SYSLOG_RAW=
COREDUMP_EXE=           INVOCATION_ID=                SYSLOG_TIMESTAMP=
COREDUMP_FILENAME=      JOB_ID=                       _SYSTEMD_CGROUP=
COREDUMP_GID=           JOB_RESULT=                   _SYSTEMD_INVOCATION_ID=
COREDUMP_HOSTNAME=      JOB_TYPE=                     _SYSTEMD_OWNER_UID=
COREDUMP_OPEN_FDS=      JOURNAL_NAME=                 _SYSTEMD_SESSION=
COREDUMP_OWNER_UID=     JOURNAL_PATH=                 _SYSTEMD_SLICE=
COREDUMP_PACKAGE_JSON=  _KERNEL_DEVICE=              _SYSTEMD_UNIT=
COREDUMP_PID=           _KERNEL_SUBSYSTEM=           _SYSTEMD_USER_SLICE=

```

Рис. 2.14: Просмотр доступных параметров фильтрации

После этого я просмотрела события, относящиеся к пользователю с UID 0, выполнив команду `journalctl _UID=0`.

```

root@aasaenko:/home/aasaenko# journalctl _UID=0
Sep 30 18:42:41 aasaenko.localdomain systemd-journald[283]: Collecting audit messages is disabled.
Sep 30 18:42:41 aasaenko.localdomain systemd-journald[283]: Journal started
Sep 30 18:42:41 aasaenko.localdomain systemd-journald[283]: Runtime Journal (/run/log/journal/4d1da01cd6b0424689deafc9e
Sep 30 18:42:41 aasaenko.localdomain systemd-modules-load[284]: Module 'msr' is built in
Sep 30 18:42:41 aasaenko.localdomain systemd-modules-load[284]: Inserted module 'fuse'
Sep 30 18:42:41 aasaenko.localdomain systemd-modules-load[284]: Module 'scsi_dh_alua' is built in
Sep 30 18:42:41 aasaenko.localdomain systemd-modules-load[284]: Module 'scsi_dh_emc' is built in
Sep 30 18:42:41 aasaenko.localdomain systemd-modules-load[284]: Module 'scsi_dh_rdac' is built in
Sep 30 18:42:41 aasaenko.localdomain systemd-sysusers[295]: Creating group 'nobody' with GID 65534.
Sep 30 18:42:41 aasaenko.localdomain systemd-sysusers[295]: Creating group 'users' with GID 100.
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variables.
Sep 30 18:42:41 aasaenko.localdomain systemd-sysusers[295]: Creating group 'systemd-journal' with GID 190.
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Finished systemd-sysusers.service - Create System Users.
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create Static Device Nodes and
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Finished systemd-vconsole-setup.service - Virtual Console Setup.
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: dracut-cmdline-ask.service - dracut ask for additional cmdline parameters
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Starting dracut-cmdline.service - dracut cmdline hook...
Sep 30 18:42:41 aasaenko.localdomain dracut-cmdline[308]: dracut-105-4.el10_0
Sep 30 18:42:41 aasaenko.localdomain dracut-cmdline[308]: Using kernel command line parameters: BOOT_IMAGE=(hd0,gpt2)/vmlinuz
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev.service - Create Static Device Nodes and
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Finished dracut-cmdline.service - dracut cmdline hook.
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Starting dracut-pre-udev.service - dracut pre-udev hook...
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Finished dracut-pre-udev.service - dracut pre-udev hook.
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Starting systemd-udev.service - Rule-based Manager for Device Events and
Sep 30 18:42:41 aasaenko.localdomain systemd-udev[408]: Using default interface naming scheme 'rhel-10.0'.
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Started systemd-udev.service - Rule-based Manager for Device Events and

```

Рис. 2.15: Фильтрация журнала по UID

Для отображения последних 20 строк журнала я использовала команду `journalctl -n 20`.

```

root@asaenko:/home/asaenko# journalctl -n 20
Sep 30 19:02:43 asaenko.localdomain kernel: traps: VBoxClient[7122] trap int3 ip:41ddb sp:7f8584afbcd0 error:0 in VBox
Sep 30 19:02:43 asaenko.localdomain systemd-coredump[7123]: Process 7119 (VBoxClient) of user 1000 terminated abnormally
Sep 30 19:02:43 asaenko.localdomain systemd[1]: Started systemd-coredump[225-7123-0.service - Process Core Dump (PID 71
Sep 30 19:02:43 asaenko.localdomain systemd-coredump[7124]: [P] Process 7119 (VBoxClient) of user 1000 dumped core.

                               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-1.23.0-2.el10.x86_64
                               Stack trace of thread 7122:
                               #0 0x00000000041ddb 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 0x00007f85931a211a start_thread (libc.so.6 + 0x9511a)
                               #5 0x00007f8593212c3c __clone3 (libc.so.6 + 0x105c3c)

                               Stack trace of thread 7120:
                               #0 0x00007f8593210a3d syscall (libc.so.6 + 0x103a3d)
                               #1 0x0000000000434c30 n/a (n/a + 0x0)
                               #2 0x0000000000450bfb 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 0x00007f85931a211a start_thread (libc.so.6 + 0x9511a)

```

Рис. 2.16: Просмотр последних 20 строк журнала

Затем я вывела только сообщения об ошибках при помощи команды `journalctl -p err`.

```

root@asaenko:/home/asaenko# journalctl -p err
Sep 30 18:42:42 asaenko.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an unsupported
Sep 30 18:42:42 asaenko.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken.
Sep 30 18:42:42 asaenko.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graphics device
Sep 30 18:42:45 asaenko.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Sep 30 18:42:46 asaenko.localdomain alsactl[957]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import
Sep 30 18:42:46 asaenko.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Sep 30 18:43:30 asaenko.localdomain gdm-password[1990]: gkr-pam: unable to locate daemon control file
Sep 30 18:43:33 asaenko.localdomain systemd[2001]: Failed to start app-gnome-gnome\x2dkeyring\x2dsecrets-2108.scope - Process
Sep 30 18:43:33 asaenko.localdomain systemd[2001]: Failed to start app-gnome-xdg\x2duser\x2ddirs-2126.scope - Application
Sep 30 18:43:35 asaenko.localdomain systemd-coredump[2800]: [P] Process 2788 (VBoxClient) of user 1000 dumped core.

                               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-1.23.0-2.el10.x86_64
                               Stack trace of thread 2793:
                               #0 0x00000000041ddb 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 0x00007f85931a211a start_thread (libc.so.6 + 0x9511a)
                               #5 0x00007f8593212c3c __clone3 (libc.so.6 + 0x105c3c)

                               Stack trace of thread 2788:
                               #0 0x00007f8593210a3d syscall (libc.so.6 + 0x103a3d)

```

Рис. 2.17: Фильтрация по сообщениям с приоритетом “ошибка”

После этого я применила фильтрацию по времени и просмотрела все сообщения со вчерашнего дня с помощью команды `journalctl --since yesterday`.

```

root@asaenko:/home/asaenko# journalctl --since yesterday
Sep 30 18:42:41 asaenko.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.b
Sep 30 18:42:41 asaenko.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_64 r
Sep 30 18:42:41 asaenko.localdomain kernel: BIOS-provided physical RAM map:
Sep 30 18:42:41 asaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Sep 30 18:42:41 asaenko.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Sep 30 18:42:41 asaenko.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Sep 30 18:42:41 asaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000000fffff] usable
Sep 30 18:42:41 asaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000dfff0000-0x0000000000dfffff] ACPI data
Sep 30 18:42:41 asaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000fec00000-0x0000000000fec0ffff] reserved
Sep 30 18:42:41 asaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000fee00000-0x0000000000fee0ffff] reserved
Sep 30 18:42:41 asaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000ffc00000-0x0000000000fffff] reserved
Sep 30 18:42:41 asaenko.localdomain kernel: BIOS-e820: [mem 0x0000000010000000-0x0000000011fffff] usable
Sep 30 18:42:41 asaenko.localdomain kernel: NX (Execute Disable) protection: active
Sep 30 18:42:41 asaenko.localdomain kernel: APIC: Static calls initialized
Sep 30 18:42:41 asaenko.localdomain kernel: SMBIOS 2.5 present.
Sep 30 18:42:41 asaenko.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 30 18:42:41 asaenko.localdomain kernel: DMI: Memory slots populated: 0/0
Sep 30 18:42:41 asaenko.localdomain kernel: Hypervisor detected: KVM
Sep 30 18:42:41 asaenko.localdomain kernel: kvm-clock: Using msrc 4b564d01 and 4b564d00
Sep 30 18:42:41 asaenko.localdomain kernel: kvm-clock: using sched offset of 4068452678 cycles
Sep 30 18:42:41 asaenko.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffff max_cycles: 0x1cd42e4dffb
Sep 30 18:42:41 asaenko.localdomain kernel: tsc: Detected 3187.204 MHz processor
Sep 30 18:42:41 asaenko.localdomain kernel: e820: update [mem 0x00000000-0x000000ff] usable ==> reserved
Sep 30 18:42:41 asaenko.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Sep 30 18:42:41 asaenko.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Sep 30 18:42:41 asaenko.localdomain kernel: total RAM covered: 4096M
Sep 30 18:42:41 asaenko.localdomain kernel: Found optimal setting for mtrr clean up
Sep 30 18:42:41 asaenko.localdomain kernel: gran_size: 64K chunk_size: 1G num_reg: 3 lose co
Sep 30 18:42:41 asaenko.localdomain kernel: MTRR map: 6 entries (3 fixed + 3 variable; max 35), built from 16 variable
Sep 30 18:42:41 asaenko.localdomain kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT

```

Рис. 2.18: Журнал со вчерашнего дня

Для просмотра только сообщений с уровнем ошибок, зафиксированных со вчерашнего дня, я выполнила команду `journalctl --since yesterday -p err`.

```

root@asaenko:/home/asaenko# journalctl --since yesterday -p err
Sep 30 18:42:42 asaenko.localdomain kernel: vmwgfx 0000:00:02.0: [drm] "ERROR" vmwgfx seems to be running on an unsupported
Sep 30 18:42:42 asaenko.localdomain kernel: vmwgfx 0000:00:02.0: [drm] "ERROR" This configuration is likely broken.
Sep 30 18:42:42 asaenko.localdomain kernel: vmwgfx 0000:00:02.0: [drm] "ERROR" Please switch to a supported graphics device
Sep 30 18:42:42 asaenko.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Sep 30 18:42:46 asaenko.localdomain alsactl[957]: alsalib main.c:1554:(snd_use_case_mgr_open) error: failed to import
Sep 30 18:42:46 asaenko.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Sep 30 18:43:30 asaenko.localdomain gdm-password[1990]: gkr-pam: unable to locate daemon control file
Sep 30 18:43:33 asaenko.localdomain systemd[2001]: Failed to start app-gnome-gnome-x2dkeyring[x2dsecrets-2108.scope -
Sep 30 18:43:33 asaenko.localdomain systemd[2001]: Failed to start app-gnome-xdg-x2duser[x2ddirs-2126.scope - Applicat
Sep 30 18:43:35 asaenko.localdomain systemd-coredump[2800]: [Process 2788 (VBoxClient) of user 1000 dumped core.

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-1.23.0-2.el10.x86_64

Stack trace of thread 2793:
#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 0x00007f85931a211a start_thread (libc.so.6 + 0x9511a)
#5 0x00007f8593212c3c __clone3 (libc.so.6 + 0x105c3c)

Stack trace of thread 2788:
#0 0x00007f8593210a3d syscall (libc.so.6 + 0x103a3d)
#1 0x00000000004344e2 n/a (n/a + 0x0)
#2 0x0000000000450066 n/a (n/a + 0x0)
#3 0x0000000000405123 n/a (n/a + 0x0)
#4 0x00007f859313730e __libc_start_call_main (libc.so.6 + 0x103730e)

```

Рис. 2.19: Сообщения об ошибках со вчерашнего дня

Наконец, я использовала режим детализированного вывода журнала с помощью опции `-o verbose`.

На скриншоте видно, что каждая запись содержит расширенную информацию о



параметрах события.

```

...
Tue 2025-09-30 18:42:41.807213 MSK [s=dfffc86b5ea7d44adbe60453ec325c33a;i=2;b=3fecebe220d5492c8996ede67293d253;m=eda4a;t
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
_SYSLOG_FACILITY=0
_SYSLOG_IDENTIFIER=kernel
_BOOT_ID=3fecebe220d5492c8996ede67293d253
_MACHINE_ID=4d1da01cd6b0424689deafc9e229859b
_HOSTNAME=aasaenko.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 r
Tue 2025-09-30 18:42:41.807218 MSK [s=dfffc86b5ea7d44adbe60453ec325c33a;i=3;b=3fecebe220d5492c8996ede67293d253;m=eda4a;t
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
_SYSLOG_FACILITY=0
_SYSLOG_IDENTIFIER=kernel
_BOOT_ID=3fecebe220d5492c8996ede67293d253
_MACHINE_ID=4d1da01cd6b0424689deafc9e229859b
root@aasaenko:/home/aasaenko#
```

Рис. 2.20: Детализированный вывод журнала

Для получения сведений о работе службы sshd я применила команду `journalctl _SYSTEMD_UNIT=sshd.service`.  
В результате были отображены сообщения, относящиеся к запуску сервиса.

```

root@aasaenko:/home/aasaenko# journalctl _SYSTEMD_UNIT=sshd.service
root@aasaenko:/home/aasaenko# journalctl _SYSTEMD_UNIT=sshd.service
Sep 30 18:42:46 aasaenko.localdomain (sshd)[1184]: sshd.service: Referenced but unset environment variable evaluates to
Sep 30 18:42:46 aasaenko.localdomain sshd[1184]: Server listening on 0.0.0.0 port 22.
Sep 30 18:42:46 aasaenko.localdomain sshd[1184]: Server listening on :: port 22.
root@aasaenko:/home/aasaenko#
```

Рис. 2.21: Просмотр журнала для sshd

## 2.4 Постоянный журнал journald

По умолчанию система хранит логи journald во временном каталоге `/run/log/journal`, и они доступны только до перезагрузки.

Чтобы сделать журнал постоянным, я выполнила следующие действия:

1. Создала каталог `/var/log/journal`.
2. Назначила владельца `root:systemd-journal`.
3. Установила права доступа 2755.



4. Применяла изменения без перезагрузки, отправив сигнал службе командой `killall -USR1 systemd-journald`.

После этого журнал `journald` стал постоянным.

Для просмотра сообщений с момента последней перезагрузки я воспользовалась командой `journalctl -b`.

```
root@aasaenko:/home/aasaenko# mkdir -p /var/log/journal
root@aasaenko:/home/aasaenko# chown root:systemd-journal /var/log/journal/
root@aasaenko:/home/aasaenko# chmod 2755 /var/log/journal/
root@aasaenko:/home/aasaenko# killall -USR1 systemd-journald
root@aasaenko:/home/aasaenko# journalctl -b
Sep 30 18:42:41 aasaenko.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.b
Sep 30 18:42:41 aasaenko.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_64 r
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-provided physical RAM map:
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x00000000dffff000-0x00000000dfffffff] ACPI data
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee0ffff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffffff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: NX (Execute Disable) protection: active
Sep 30 18:42:41 aasaenko.localdomain kernel: APIC: Static calls initialized
Sep 30 18:42:41 aasaenko.localdomain kernel: SMBIOS 2.5 present.
Sep 30 18:42:41 aasaenko.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 30 18:42:41 aasaenko.localdomain kernel: DMI: Memory slots populated: 0/0
Sep 30 18:42:41 aasaenko.localdomain kernel: Hypervisor detected: KVM
Sep 30 18:42:41 aasaenko.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Sep 30 18:42:41 aasaenko.localdomain kernel: kvm-clock: using sched offset of 4068452678 cycles
Sep 30 18:42:41 aasaenko.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb
Sep 30 18:42:41 aasaenko.localdomain kernel: tsc: Detected 3187.204 MHz processor
Sep 30 18:42:41 aasaenko.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Sep 30 18:42:41 aasaenko.localdomain kernel: total RAM covered: 4096M
```

Рис. 2.22: Просмотр системного журнала с момента загрузки

## 3 Контрольные вопросы

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

Основной конфигурационный файл находится по пути `/etc/rsyslog.conf`.  
Дополнительные настройки могут храниться в каталоге `/etc/rsyslog.d/`.

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

Сообщения, связанные с авторизацией и аутентификацией, сохраняются в файле `/var/log/secure`.

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

По умолчанию ротация файлов журналов выполняется один раз в неделю.  
Эти параметры определяются в конфигурации logrotate, файл `/etc/logrotate.conf`.

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

В файл конфигурации rsyslog нужно добавить строку: `*.info /var/log/messages.info`

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

Для мониторинга сообщений в реальном времени можно использовать:

- `tail -f /var/log/messages` (или другой файл журнала),

- либо `journalctl -f` для просмотра через `systemd-journald`.

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

Для этого используется фильтрация по PID и времени: `journalctl _PID=1 --since "09:00" --until "15:00"`

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

Для этого применяется команда: `journalctl -b`

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

Нужно создать каталог `/var/log/journal`, назначить ему владельца и права:

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

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

- `chmod 2755 /var/log/journal`

После этого отправить сигнал службе `journald`:

- `killall -USR1 systemd-journald`

Теперь логи будут храниться постоянно и сохраняться после перезагрузки.

## 4 Заключение

В ходе выполнения лабораторной работы я научилась использовать средства администрирования журналов в Linux.

Были выполнены следующие действия:

- настройка и мониторинг системных событий в реальном времени с помощью `tail` и `logger`;
- организация перенаправления логов веб-службы Apache через `rsyslog` и создание отдельных файлов для отладочной информации;
- работа с системным журналом с использованием `journalctl`: просмотр, фильтрация по UID, PID, времени и приоритетам сообщений;
- настройка постоянного хранения журналов `journal` и проверка их сохранности после перезагрузки.

В процессе работы я закрепила знания о конфигурационных файлах `/etc/rsyslog.conf`, `/etc/rsyslog.d/*.conf`, а также о возможностях `systemd-journald`. Полученный опыт показал, как можно гибко управлять логированием в системе, обеспечивать сохранность журналов и эффективно анализировать события для администрирования и диагностики.