

# **Отчёт по лабораторной работе 7**

**Управление журналами событий в системе**

Вишняков Родион Сергеевич

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>3</b>	<b>Вывод</b>	<b>16</b>
<b>4</b>	<b>Контрольные вопросы</b>	<b>17</b>

# Список иллюстраций

2.1	root . . . . .	6
2.2	Мониторинг системных событий . . . . .	6
2.3	Ввод команд . . . . .	7
2.4	Мониторинг системных событий . . . . .	7
2.5	Мониторинг сообщений безопасности . . . . .	7
2.6	Apache . . . . .	7
2.7	Запуск веб-службы . . . . .	7
2.8	Сообщения об ошибках . . . . .	8
2.9	Добавление строки . . . . .	8
2.10	Файл мониторинга . . . . .	8
2.11	Перезагрузка . . . . .	8
2.12	Файл конфигурации . . . . .	9
2.13	Перезапуск rsyslogd . . . . .	9
2.14	Мониторинг отладочной информации . . . . .	9
2.15	Ввод команды . . . . .	9
2.16	Содержимое журнала . . . . .	10
2.17	Содержимое журнала . . . . .	10
2.18	Содержимое журнала . . . . .	11
2.19	Содержимое журнала . . . . .	11
2.20	Просмотр событий для UIDO . . . . .	12
2.21	Содержимое журнала . . . . .	12
2.22	Содержимое журнала . . . . .	13
2.23	Содержимое журнала . . . . .	13
2.24	Содержимое журнала . . . . .	14
2.25	Содержимое журнала . . . . .	14
2.26	Создание каталога . . . . .	14
2.27	Права доступа . . . . .	15
2.28	Принятие изменений . . . . .	15

## Список таблиц

# 1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.



```
root@rodvishh:~# logger hello
root@rodvishh:~#
```

Рис. 2.3: Ввод команд

Получаю сообщение из мониторинга событий

```
Oct 18 18:44:07 rodvishh systemd[1]: systemd-coredump@166-6571-0.service: Deactivated successfully.
Oct 18 18:44:08 rodvishh root[6582]: hello
```

Рис. 2.4: Мониторинг системных событий

Просматриваю последний 20 строк из мониторинга сообщений безопасности

```
root@rodvishh:~# tail -n 20 /var/log/secure
Oct 11 22:47:23 rodvishh gdm-password[4734]: gkr-pam: unlocked login keyring
Oct 18 18:28:09 rodvishh sshd[1154]: Server listening on 0.0.0.0 port 22.
Oct 18 18:28:09 rodvishh sshd[1154]: Server listening on :: port 22.
Oct 18 18:28:10 rodvishh (systemd)[1218]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)
Oct 18 18:28:10 rodvishh gdm-launch-environment[1198]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=42) by (uid=0)
Oct 18 18:29:08 rodvishh gdm-password[2300]: gkr-pam: unable to locate daemon control file
Oct 18 18:29:08 rodvishh gdm-password[2300]: gkr-pam: stashed password to try later in open session
Oct 18 18:29:08 rodvishh (systemd)[2313]: pam_unix(systemd-user:session): session opened for user rodvishh(uid=1000) by rodvishh(uid=0)
Oct 18 18:29:08 rodvishh gdm-password[2300]: pam_unix(gdm-password:session): session opened for user rodvishh(uid=1000) by rodvishh(uid=0)
Oct 18 18:29:08 rodvishh gdm-password[2300]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct 18 18:29:16 rodvishh gdm-launch-environment[1198]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Oct 18 18:39:11 rodvishh sudo[5716]: rodvishh : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/bash
Oct 18 18:39:11 rodvishh (systemd)[5729]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)
Oct 18 18:39:11 rodvishh sudo[5716]: pam_unix(sudo-l:session): session opened for user root(uid=0) by rodvishh(uid=1000)
Oct 18 18:40:06 rodvishh sudo[5946]: rodvishh : TTY=pts/2 ; PWD=/root ; USER=root ; COMMAND=/bin/bash
Oct 18 18:40:06 rodvishh sudo[5946]: pam_unix(sudo-l:session): session opened for user root(uid=0) by rodvishh(uid=1000)
Oct 18 18:41:54 rodvishh unix_chkpwd[6261]: password check failed for user (rodvishh)
Oct 18 18:41:54 rodvishh sudo[6252]: pam_unix(sudo-l:auth): authentication failure; logname=rodvishh uid=1000 euid=0 tty=/dev/pts/4 ruser=rodvishh ih
Oct 18 18:43:37 rodvishh sudo[6252]: rodvishh : TTY=pts/4 ; PWD=/root ; USER=root ; COMMAND=/bin/bash
Oct 18 18:43:37 rodvishh sudo[6252]: pam_unix(sudo-l:session): session opened for user root(uid=0) by rodvishh(uid=1000)
root@rodvishh:~#
```

Рис. 2.5: Мониторинг сообщений безопасности

Устанавливаю Apache

```
root@rodvishh:~# dnf -y install httpd
Rocky Linux 10 - BaseOS [=====
```

Рис. 2.6: Apache

Запускаю веб-службу

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

Рис. 2.7: Запуск веб-службы

Просматриваю журнал сообщений об ошибках веб-службы

```
root@rodvishh:~# tail -f /var/log/httpd/error_log
[Sat Oct 18 18:48:25.446496 2025] [suexec:notice] [pid 7541:tid 7541] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::a00:27ff:fee3:b6fb#03. Set the 'ServerName' directive globally to suppress this message
[Sat Oct 18 18:48:25.489660 2025] [lbmethod:heartbeat:notice] [pid 7541:tid 7541] AH02282: No slotmem from mod_heartbeat
[Sat Oct 18 18:48:25.490960 2025] [systemd:notice] [pid 7541:tid 7541] SELinux policy enabled: httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 18 18:48:25.494954 2025] [mpm_event:notice] [pid 7541:tid 7541] AH00489: Apache/2.4.63 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 18 18:48:25.494975 2025] [core:notice] [pid 7541:tid 7541] AH00054: Command line: /usr/sbin/httpd -D FOREGROUND
```

Рис. 2.8: Сообщения об ошибках

Добавляю предоставленную строку в конец

```
root@rodvishh:/etc/httpd/conf# echo "ErrorLog syslog:local1" >> /etc/httpd/conf/httpd.conf
root@rodvishh:/etc/httpd/conf#
```

Рис. 2.9: Добавление строки

Создаю файл мониторинга событий веб-службы и прописываю в нем следующую команду

```
root@rodvishh:/etc/httpd/conf# cd /etc/rsyslog.d
root@rodvishh:/etc/rsyslog.d# touch httpd.conf
root@rodvishh:/etc/rsyslog.d# local1.* -/var/log/httpd-error.log
bash: local1.*: команда не найдена...
root@rodvishh:/etc/rsyslog.d# nano httpd.conf
root@rodvishh:/etc/rsyslog.d#
```

Рис. 2.10: Файл мониторинга

Перезагружаю конфигурацию rsyslogd и веб-службу

```
root@rodvishh:/etc/rsyslog.d# systemctl restart rsyslog.service
root@rodvishh:/etc/rsyslog.d# systemctl restart httpd
root@rodvishh:/etc/rsyslog.d#
```

Рис. 2.11: Перезагрузка

Создаю файл конфигурации для мониторинга отладочной информации и ввожу следующую команду



```

root@rodvishh:/etc/rsyslog.d# touch debug.conf
root@rodvishh:/etc/rsyslog.d# echo "*.debug /var/log/messages-debug" >
/etc/rsyslog.d/debug.conf
-bash: синтаксическая ошибка рядом с неожиданным маркером «newline»
root@rodvishh:/etc/rsyslog.d# echo "*.debug /var/log/messages-debug" >
-bash: синтаксическая ошибка рядом с неожиданным маркером «newline»
root@rodvishh:/etc/rsyslog.d# echo "*.debug /var/log/messages-debug" >
/etc/rsyslog.d/debug.conf
-bash: синтаксическая ошибка рядом с неожиданным маркером «newline»
-bash: /etc/rsyslog.d/debug.conf: Отказано в доступе
root@rodvishh:/etc/rsyslog.d# echo "*.debug /var/log/messages-debug" >
/etc/rsyslog.d/debug.conf
-bash: синтаксическая ошибка рядом с неожиданным маркером «newline»
-bash: /etc/rsyslog.d/debug.conf: Нет такого файла или каталога
root@rodvishh:/etc/rsyslog.d# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
root@rodvishh:/etc/rsyslog.d#

```

Рис. 2.12: Файл конфигурации

## Перезапускаю rsyslogd

```

root@rodvishh:~# systemctl restart rsyslog.service
root@rodvishh:~#

```

Рис. 2.13: Перезапуск rsyslogd

## Запускаю мониторинг отладочной информации

```

root@rodvishh:~# tail -f /var/log/messages-debug
Oct 18 19:04:41 rodvishh kernel: traps: VBoxClient[10500] trap int3 (ip:41d61b sp:7f48bd1b4cd0 error:0 in VBoxClient[1dd1b:40000000bb000]
Oct 18 19:04:41 rodvishh system-coredump[10510]: Process 10500 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Oct 18 19:04:41 rodvishh systemd[1]: Started system-coredump399-10510-0.service - Process Core Dump (PID 10510/UID 0).
Oct 18 19:04:42 rodvishh system-coredump[10511]: Process 10500 (VBoxClient) of user 1000 dumped core.#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Modu
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-3.4.4-0.el10.x86_64#012Modu
libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 10509:#012#0 0x00000000041dd1b n/a (n/a + 0x0)#012#1 0x00000000041dc94 n/a (n/a + 0x
)#012#2 0x000000000045841c n/a (n/a + 0x0)#012#3 0x00000000004355d0 n/a (n/a + 0x0)#012#4 0x00007f48cb8ce6b8 start_thread (libc.so.6 + 0x94b658)#012#5 0x00007f48cb93f6bc ...
onad (libc.so.6 + 0x10560bc)#012#012Stack trace of thread 10506:#012#0 0x00007f48cb8ce6b8 syscall (libc.so.6 + 0x1034bd)#012#1 0x00000000041e3ba n/a (n/a + 0x0)#012#2 0x00
0000045080fb n/a (n/a + 0x0)#012#3 0x0000000000405123 n/a (n/a + 0x0)#012#4 0x00007f48cb8ce6b8 _libc_start_call_main (libc.so.6 + 0x2a3bc9)#012#5 0x00007f48cb8ce63c9 _libc
start_call_main@libc-2.34 (libc.so.6 + 0x2a3bc9)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Oct 18 19:04:42 rodvishh systemd[1]: system-coredump399-10510-0.service: Deactivated successfully.
Oct 18 19:04:42 rodvishh kernel: traps: VBoxClient[10533] trap int3 (ip:41d61b sp:7f48bd1b4cd0 error:0 in VBoxClient[1dd1b:40000000bb000]
Oct 18 19:04:42 rodvishh system-coredump[10534]: Process 10530 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Oct 18 19:04:42 rodvishh systemd[1]: Started system-coredump400-10534-0.service - Process Core Dump (PID 10534/UID 0).
Oct 18 19:04:47 rodvishh system-coredump[10535]: Process 10530 (VBoxClient) of user 1000 dumped core.#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Modu
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-3.4.4-0.el10.x86_64#012Modu
libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 10533:#012#0 0x00000000041dd1b n/a (n/a + 0x0)#012#1 0x00000000041dc94 n/a (n/a + 0x
)#012#2 0x000000000045841c n/a (n/a + 0x0)#012#3 0x00000000004355d0 n/a (n/a + 0x0)#012#4 0x00007f48cb8ce6b8 start_thread (libc.so.6 + 0x94b658)#012#5 0x00007f48cb93f6bc ...
#03 (libc.so.6 + 0x10560bc)#012#012Stack trace of thread 10531:#012#0 0x00007f48cb8ce6b8 syscall (libc.so.6 + 0x1034bd)#012#1 0x000000000453a30 n/a (n/a + 0x0)#012#2 0x00
0000045080fb n/a (n/a + 0x0)#012#3 0x000000000043566a n/a (n/a + 0x0)#012#4 0x000000000045841c n/a (n/a + 0x0)#012#5 0x00000000004355d0 n/a (n/a + 0x0)#012#6 0x00007f48cb
8ce6b8 start_thread (libc.so.6 + 0x94b658)#012#7 0x00007f48cb93f6bc _clone3 (libc.so.6 + 0x10560bc)#012#012Stack trace of thread 10532:#012#0 0x00007f48cb93d4bd syscall (libc
.so.6 + 0x1034bd)#012#1 0x000000000454a2 n/a (n/a + 0x0)#012#2 0x0000000000450866 n/a (n/a + 0x0)#012#3 0x00000000041e3ba n/a (n/a + 0x0)#012#4 0x00000000041e3ba n/a (n/
+ 0x0)#012#5 0x0000000004179a n/a (n/a + 0x0)#012#6 0x000000000040460a n/a (n/a + 0x0)#012#7 0x000000000045841c n/a (n/a + 0x0)#012#8 0x00000000004355d0 n/a (n/a + 0x
12#9 0x00007f48cb8ce6b8 start_thread (libc.so.6 + 0x94b658)#012#10 0x00007f48cb93f6bc _clone3 (libc.so.6 + 0x10560bc)#012#012Stack trace of thread 10530:#012#0 0x00007f48cb9
4bd syscall (libc.so.6 + 0x1034bd)#012#1 0x000000000434ae2 n/a (n/a + 0x0)#012#2 0x0000000000450866 n/a (n/a + 0x0)#012#3 0x0000000000405123 n/a (n/a + 0x0)#012#4 0x0000
40b06420e _libc_start_call_main (libc.so.6 + 0x2a3bc9)#012#5 0x00007f48cb8ce63c9 _libc_start_call_main@libc-2.34 (libc.so.6 + 0x2a3bc9)#012#6 0x00000000004044aa n/a (n/a + 0x
0)#012ELF object binary architecture: AMD x86-64
Oct 18 19:04:47 rodvishh systemd[1]: system-coredump400-10534-0.service: Deactivated successfully.
Oct 18 19:04:52 rodvishh kernel: traps: VBoxClient[10547] trap int3 (ip:41d61b sp:7f48bd1b4cd0 error:0 in VBoxClient[1dd1b:40000000bb000]
Oct 18 19:04:52 rodvishh system-coredump[10548]: Process 10544 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Oct 18 19:04:52 rodvishh systemd[1]: Started system-coredump401-10548-0.service - Process Core Dump (PID 10548/UID 0).
Oct 18 19:04:52 rodvishh system-coredump[10549]: Process 10544 (VBoxClient) of user 1000 dumped core.#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Modu
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-3.4.4-0.el10.x86_64#012Modu
libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 10547:#012#0 0x00000000041dd1b n/a (n/a + 0x0)#012#1 0x00000000041dc94 n/a (n/a + 0x
)#012#2 0x000000000045841c n/a (n/a + 0x0)#012#3 0x00000000004355d0 n/a (n/a + 0x0)#012#4 0x00007f48cb8ce6b8 start_thread (libc.so.6 + 0x94b658)#012#5 0x00007f48cb93f6bc ...

```

Рис. 2.14: Мониторинг отладочной информации

## Ввожу предоставленную команду

```

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

```

Рис. 2.15: Ввод команды

## Просматриваю содержимое журнала с событиями с момента последнего запуска системы

```

root@rodvishh:~# journalctl
Okt 18 18:27:57 rodvishh kernel: Linux version 6.12.0-55.32.1.el10_0.x86_64 (mockbuild@adadi-prd-build001.bld.eur.rockylinux.org) (gcc (GCC) 14.2.1 20250110 (Red Hat 14.2.1-7)
Okt 18 18:27:57 rodvishh kernel: Command line: BOOT_IMAGE=(hdb,gpt2)/vmlinuz-6.12.0-55.32.1.el10_0.x86_64 root=/dev/mapper/rl_vbox-root ro resume=UUID=fad36b5c-bc75-4fe2-ba2f
Okt 18 18:27:57 rodvishh kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
Okt 18 18:27:57 rodvishh kernel: BIOS-provided physical RAM map:
Okt 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000000fbff] usable
Okt 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x000000000000009fcb0-0x000000000000009ffff] reserved
Okt 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x0000000000000000000-0x0000000000000000ffff] reserved
Okt 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x0000000000000000000-0x0000000000000000ffff] usable
Okt 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x00000000ffff00000-0x00000000000000ffff] ACPI data
Okt 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x000000000fe000000-0x000000000fe000000] reserved
Okt 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x000000000fe000000-0x000000000fe000000] reserved
Okt 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x000000000fffc0000-0x000000000fffc0000] reserved
Okt 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x000000000fffc0000-0x000000000fffc0000] reserved
Okt 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x00000000100000000-0x00000000100000000] reserved
Okt 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x00000000100000000-0x00000000100000000] usable
Okt 18 18:27:57 rodvishh kernel: NX (Execute Disable) protection: active
Okt 18 18:27:57 rodvishh kernel: APIC: Static calls initialized
Okt 18 18:27:57 rodvishh kernel: SMBIOS 2.5 present.
Okt 18 18:27:57 rodvishh kernel: DMI: VMware, Inc. VMware VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Okt 18 18:27:57 rodvishh kernel: DMI: Memory slots populated: 0/8
Okt 18 18:27:57 rodvishh kernel: Hypervisor detected: KVM
Okt 18 18:27:57 rodvishh kernel: kvm-clock: Using msrc 4b564d81 and 4b564d80
Okt 18 18:27:57 rodvishh kernel: kvm-clock: using sched offset of 126426674 cycles
Okt 18 18:27:57 rodvishh kernel: clocksource: kvm-clock: mask: 0xffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 881590591483 ns
Okt 18 18:27:57 rodvishh kernel: tsc: Detected 3293.814 MHz processor
Okt 18 18:27:57 rodvishh kernel: s02: update [mem 0x00000000-0x00000000] usable ==> reserved
Okt 18 18:27:57 rodvishh kernel: s02: remove [mem 0x00000000-0x00000000] usable
Okt 18 18:27:57 rodvishh kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Okt 18 18:27:57 rodvishh kernel: total RAM covered: 4096M
Okt 18 18:27:57 rodvishh kernel: Found optimal setting for mtrr clean up
Okt 18 18:27:57 rodvishh kernel: gran_size: 64K chunk_size: 10 num_reg: 3 lose cover RAM: 00
Okt 18 18:27:57 rodvishh kernel: MTRR map: 6 entries (3 fixed + 3 variable; max 35), built from 16 variable MTRRs
Okt 18 18:27:57 rodvishh kernel: s06/PAT: Configuration [0-7]: WB WC UC- UC WB UC WB UC WT
Okt 18 18:27:57 rodvishh kernel: s02: update [mem 0x00000000-0xffffffff] usable ==> reserved
Okt 18 18:27:57 rodvishh kernel: last_pfn = 0xe0000 max_arch_pfn = 0x400000000
Okt 18 18:27:57 rodvishh kernel: found SMP WP-table at [mem 0x00000000-0x00000000]
Okt 18 18:27:57 rodvishh kernel: RAMDISK: [mem 0x33e23800-0x35f00fff]

```

Рис. 2.16: Содержимое журнала

Просматриваю содержимое журнала без использования пейджера

```

Okt 18 19:20:36 rodvishh systemd[1]: systemd-coredump[581-12711-0.service: Deactivated successfully.
Okt 18 19:20:41 rodvishh kernel: traps: VBoxClient[12726] trap int3 ip:41dd1b sp:7f48bd1b4cd0 error:0 in VBoxClient[1dd1b.400000+bb000]
Okt 18 19:20:41 rodvishh systemd-coredump[12727]: Process 12723 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Okt 18 19:20:41 rodvishh systemd[1]: Started systemd-coredump[582-12727-0.service - Process Core Dump (PID 12727/UID 0)].
Okt 18 19:20:41 rodvishh systemd-coredump[12728]: [^] Process 12723 (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 12726:
#0 0x00000000001dd1b n/a (n/a + 0x0)
#1 0x000000000041dc34 n/a (n/a + 0x0)
#2 0x000000000045041c n/a (n/a + 0x0)
#3 0x0000000000435d00 n/a (n/a + 0x0)
#4 0x00007f48cb86430e __libc_start_call_main (libc.so.6 + 0x2a30e)
#5 0x00007f48cb93f6bc __clone3 (libc.so.6 + 0x1056bc)

Stack trace of thread 12723:
#0 0x00007f48cb93d4bd syscall (libc.so.6 + 0x1034bd)
#1 0x00000000004344e2 n/a (n/a + 0x0)
#2 0x0000000000450006 n/a (n/a + 0x0)
#3 0x0000000000405123 n/a (n/a + 0x0)
#4 0x00007f48cb86430e __libc_start_call_main (libc.so.6 + 0x2a30e)
#5 0x00007f48cb864309 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a309)
ELF object binary architecture: AMD x86-64
Okt 18 19:20:41 rodvishh systemd[1]: systemd-coredump[582-12727-0.service: Deactivated successfully.
Okt 18 19:20:41 rodvishh systemd[2313]: dbus-1.2-org.gnome.Nautilus@.service: Consumed 5.521s CPU time, 232.2M memory peak, 4K memory swap peak.
root@rodvishh:~#

```

Рис. 2.17: Содержимое журнала

Просматриваю содержимое в реальном времени

```

#3 0x000000000405123 n/a (n/a + 0x0)
#4 0x00007f48cb86430e __libc_start_call_main (libc.so.6 + 0x2a30e)
#5 0x00007f48cb8643c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a30e)
#6 0x0000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x86-64
ОКТ 18 19:21:28 rodvishh systemd[1]: systemd-coredump[591-12846-0.service: Deactivated successfully.
ОКТ 18 19:21:33 rodvishh kernel: traps: VBoxClient[12860] trap int3 ip:41dd1b sp:7f48bd1b4cd0 error:0 in VBoxClient[1dd
ОКТ 18 19:21:33 rodvishh systemd-coredump[12861]: Process 12857 (VBoxClient) of user 1000 terminated abnormally with si
ОКТ 18 19:21:33 rodvishh systemd[1]: Started systemd-coredump[592-12861-0.service - Process Core Dump (PID 12861/UID 0)
ОКТ 18 19:21:33 rodvishh systemd-coredump[12862]: [?] Process 12857 (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 12860:
#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 0x00007f48cb8ce68 start_thread (libc.so.6 + 0x94b68)
#5 0x00007f48cb93f6bc __clone3 (libc.so.6 + 0x1056bc)

Stack trace of thread 12857:
#0 0x00007f48cb93d4bd syscall (libc.so.6 + 0x1034bd)
#1 0x0000000004344e2 n/a (n/a + 0x0)
#2 0x000000000450066 n/a (n/a + 0x0)
#3 0x000000000405123 n/a (n/a + 0x0)
#4 0x00007f48cb86430e __libc_start_call_main (libc.so.6 + 0x2a30e)
#5 0x00007f48cb8643c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a30e)
#6 0x0000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x86-64
ОКТ 18 19:21:33 rodvishh systemd[1]: systemd-coredump[592-12861-0.service: Deactivated successfully.

```

Рис. 2.18: Содержимое журнала

Просматриваю конкретные параметры

```

ОКТ 18 18:27:57 rodvishh systemd-journald[256]: Journal started
ОКТ 18 18:27:57 rodvishh systemd-journald[256]: Runtime Journal (/run/log/journal/ee3d489206ca4b58bca2
ОКТ 18 18:27:57 rodvishh systemd-modules-load[257]: Module 'msr' is built in
ОКТ 18 18:27:57 rodvishh systemd-modules-load[257]: Inserted module 'fuse'
ОКТ 18 18:27:57 rodvishh systemd-modules-load[257]: Module 'scsi_dh_alua' is built in
ОКТ 18 18:27:57 rodvishh systemd-modules-load[257]: Module 'scsi_dh_emc' is built in
ОКТ 18 18:27:57 rodvishh systemd-modules-load[257]: Module 'scsi_dh_rdac' is built in
ОКТ 18 18:27:57 rodvishh systemd[1]: Finished systemd-tmpfiles-setup-dev-early.service - Create Static
ОКТ 18 18:27:57 rodvishh systemd[1]: Starting systemd-sysusers.service - Create System Users...
ОКТ 18 18:27:57 rodvishh systemd-sysusers[270]: Creating group 'nobody' with GID 65534.
ОКТ 18 18:27:57 rodvishh systemd-sysctl.service - Apply Kernel Variables.
ОКТ 18 18:27:57 rodvishh systemd-sysusers[270]: Creating group 'users' with GID 100.
ОКТ 18 18:27:57 rodvishh systemd-sysusers[270]: Creating group 'systemd-journal' with GID 190.
ОКТ 18 18:27:57 rodvishh systemd[1]: Finished systemd-sysusers.service - Create System Users.
ОКТ 18 18:27:57 rodvishh systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create Static Device
ОКТ 18 18:27:58 rodvishh systemd[1]: Finished systemd-vconsole-setup.service - Virtual Console Setup.
ОКТ 18 18:27:58 rodvishh systemd[1]: dracut-cmdline-ask.service - dracut ask for additional cmdline pa
ОКТ 18 18:27:58 rodvishh systemd[1]: Starting dracut-cmdline.service - dracut cmdline hook...
ОКТ 18 18:27:58 rodvishh dracut-cmdline[280]: dracut-105-4.el10_0
ОКТ 18 18:27:58 rodvishh dracut-cmdline[280]: Using kernel command line parameters: BOOT_IMAGE=(hd0
ОКТ 18 18:27:58 rodvishh systemd[1]: Finished systemd-tmpfiles-setup-dev.service - Create Static Device
ОКТ 18 18:27:58 rodvishh systemd[1]: Finished dracut-cmdline.service - dracut cmdline hook.
ОКТ 18 18:27:58 rodvishh systemd[1]: Starting dracut-pre-udev.service - dracut pre-udev hook...
ОКТ 18 18:27:58 rodvishh systemd[1]: Finished dracut-pre-udev.service - dracut pre-udev hook.
ОКТ 18 18:27:58 rodvishh systemd[1]: Starting systemd-udev.service - Rule-based Manager for Device Ev
ОКТ 18 18:27:58 rodvishh systemd-udev[379]: Using default interface naming scheme 'rhel-10.0'.
ОКТ 18 18:27:58 rodvishh systemd[1]: Started systemd-udev.service - Rule-based Manager for Device Ev
ОКТ 18 18:27:58 rodvishh systemd[1]: dracut-pre-trigger.service - dracut pre-trigger hook was skipped
ОКТ 18 18:27:58 rodvishh systemd[1]: Starting systemd-udev-trigger.service - Coldplug All udev Devices
ОКТ 18 18:27:58 rodvishh systemd[1]: Created slice system-modprobe.slice - Slice /system/modprobe.
ОКТ 18 18:27:58 rodvishh systemd[1]: Starting modprobe@configfs.service - Load Kernel Module configs.
ОКТ 18 18:27:58 rodvishh systemd[1]: Finished systemd-udev-trigger.service - Coldplug All udev Devices
ОКТ 18 18:27:58 rodvishh systemd[1]: Starting dracut-initqueue.service - dracut initqueue hook...
ОКТ 18 18:27:58 rodvishh systemd[1]: Starting plymouth-start.service - Show Plymouth Boot Screen...
ОКТ 18 18:27:58 rodvishh systemd[1]: modprobe@configfs.service: Deactivated successfully.
ОКТ 18 18:27:58 rodvishh systemd[1]: Finished modprobe@configfs.service - Load Kernel Module configs.
ОКТ 18 18:27:58 rodvishh systemd[1]: Received SIGRTMIN+20 from PID 401 (plymouthd).
lines 1-38

```

Рис. 2.19: Содержимое журнала

Просматриваю события для UID0

```
ОКТ 18 19:23:07 rodvishh systemd-coredump[13082]: Process 13078 (VBoxClient) of user 1000 terminated a
ОКТ 18 19:23:07 rodvishh systemd[1]: Started systemd-coredump@610-13082-0.service - Process Core Dump
ОКТ 18 19:23:07 rodvishh systemd-coredump[13083]: [?] Process 13078 (VBoxClient) of user 1000 dumped c

Module libXau.so.6 from rpm libXau-1.0.11-8.el10.
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.
Module libX11.so.6 from rpm libX11-1.8.10-1.el10.
Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x
Module libwayland-client.so.0 from rpm wayland-1.
Stack trace of thread 13081:
#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 0x00007f48cb8ceb68 start_thread (libc.so.6 +
#5 0x00007f48cb93f6bc __clone3 (libc.so.6 + 0x10

Stack trace of thread 13078:
#0 0x00007f48cb93d4bd syscall (libc.so.6 + 0x103
#1 0x0000000004344e2 n/a (n/a + 0x0)
#2 0x000000000450066 n/a (n/a + 0x0)
#3 0x000000000405123 n/a (n/a + 0x0)
#4 0x00007f48cb86430e __libc_start_call_main (li
#5 0x00007f48cb8643c9 __libc_start_main@@GLIBC.2
#6 0x0000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x86-64
ОКТ 18 19:23:07 rodvishh systemd[1]: systemd-coredump@610-13082-0.service: Deactivated successfully.
ОКТ 18 19:23:12 rodvishh kernel: traps: VBoxClient[13093] trap int3 ip:41dd1b sp:7f48bdlb4cd0 error:0
ОКТ 18 19:23:12 rodvishh systemd-coredump[13094]: Process 13090 (VBoxClient) of user 1000 terminated a
ОКТ 18 19:23:12 rodvishh systemd[1]: Started systemd-coredump@611-13094-0.service - Process Core Dump
ОКТ 18 19:23:12 rodvishh systemd-coredump[13095]: [?] Process 13090 (VBoxClient) of user 1000 dumped c

Module libXau.so.6 from rpm libXau-1.0.11-8.el10.
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.
Module libX11.so.6 from rpm libX11-1.8.10-1.el10.
Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x
Module libwayland-client.so.0 from rpm wayland-1.

lines 1-38
```

Рис. 2.20: Просмотр событий для UID0

Просматриваю последний 20 строк журнала

```
ОКТ 18 18:27:59 rodvishh kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graph
ОКТ 18 18:28:07 rodvishh kernel: Warning: Unmaintained driver is detected: e1000
ОКТ 18 18:28:08 rodvishh alsactl[889]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to f
ОКТ 18 18:28:09 rodvishh kernel: Warning: Unmaintained driver is detected: ip_set
ОКТ 18 18:28:21 rodvishh rsyslogd[1290]: imjournal: fscanf on state file '/var/lib/rsyslog/imjournal.s
ОКТ 18 18:28:21 rodvishh rsyslogd[1290]: imjournal: ignoring invalid state file /var/lib/rsyslog/imjou
ОКТ 18 18:29:08 rodvishh gdm-password[2300]: gkr-pam: unable to locate daemon control file
ОКТ 18 18:29:12 rodvishh systemd[2313]: Failed to start app-gnome-gnome\x2dkeyring\x2dpkcs11-2426.scope
ОКТ 18 18:29:12 rodvishh systemd[2313]: Failed to start app-gnome-gnome\x2dkeyring\x2dssh-2421.scope -
ОКТ 18 18:29:12 rodvishh systemd[2313]: Failed to start app-gnome-xdg\x2duser\x2ddirs-2437.scope - App
ОКТ 18 18:29:24 rodvishh systemd-coredump[3151]: [?] Process 3138 (VBoxClient) of user 1000 dumped cor

Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x
Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x
Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x
Module libwayland-client.so.0 from rpm wayland-1.2
Stack trace of thread 3142:
#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 0x00007f48cb8ceb68 start_thread (libc.so.6 + 0
#5 0x00007f48cb93f6bc __clone3 (libc.so.6 + 0x105

Stack trace of thread 3139:
#0 0x00007f48cb93d4bd syscall (libc.so.6 + 0x1034
#1 0x000000000434c30 n/a (n/a + 0x0)
#2 0x000000000450bfb n/a (n/a + 0x0)
#3 0x00000000043566a n/a (n/a + 0x0)
#4 0x00000000045041c n/a (n/a + 0x0)
#5 0x0000000004355d0 n/a (n/a + 0x0)
#6 0x00007f48cb8ceb68 start_thread (libc.so.6 + 0
#7 0x00007f48cb93f6bc __clone3 (libc.so.6 + 0x105

Stack trace of thread 3140:

lines 1-38
```

Рис. 2.21: Содержимое журнала

Просматриваю только сообщения об ошибках

```
OCT 18 18:27:57 rodvissh kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-0.12.0-3.el10.x86_64
OCT 18 18:27:57 rodvissh kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
OCT 18 18:27:57 rodvissh kernel: BIOS-provided physical RAM map:
OCT 18 18:27:57 rodvissh kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
OCT 18 18:27:57 rodvissh kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
OCT 18 18:27:57 rodvissh kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
OCT 18 18:27:57 rodvissh kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] usable
OCT 18 18:27:57 rodvissh kernel: BIOS-e820: [mem 0x000000000dfff0000-0x000000000dfffffff] ACPI data
OCT 18 18:27:57 rodvissh kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
OCT 18 18:27:57 rodvissh kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
OCT 18 18:27:57 rodvissh kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
OCT 18 18:27:57 rodvissh kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff] usable
OCT 18 18:27:57 rodvissh kernel: NX (Execute Disable) protection: active
OCT 18 18:27:57 rodvissh kernel: APIC: Static calls initialized
OCT 18 18:27:57 rodvissh kernel: SMBIOS 2.5 present.
OCT 18 18:27:57 rodvissh kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
OCT 18 18:27:57 rodvissh kernel: DMI: Memory slots populated: 0/0
OCT 18 18:27:57 rodvissh kernel: Hypervisor detected: KVM
OCT 18 18:27:57 rodvissh kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
OCT 18 18:27:57 rodvissh kernel: kvm-clock: using sched offset of 12642684574 cycles
OCT 18 18:27:57 rodvissh kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e
OCT 18 18:27:57 rodvissh kernel: tsc: Detected 3293.814 MHz processor
OCT 18 18:27:57 rodvissh kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
OCT 18 18:27:57 rodvissh kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
OCT 18 18:27:57 rodvissh kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
OCT 18 18:27:57 rodvissh kernel: total RAM covered: 4096M
OCT 18 18:27:57 rodvissh kernel: Found optimal setting for mtrr clean up
OCT 18 18:27:57 rodvissh kernel: gran_size: 64K chunk_size: 1G num_reg: 3 lc
OCT 18 18:27:57 rodvissh kernel: MTRR map: 6 entries (3 fixed + 3 variable; max 35), built from 16 var
OCT 18 18:27:57 rodvissh kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
OCT 18 18:27:57 rodvissh kernel: e820: update [mem 0x00000000-0xffffffff] usable ==> reserved
OCT 18 18:27:57 rodvissh kernel: last_pfn = 0xe0000 max_arch_pfn = 0x400000000
OCT 18 18:27:57 rodvissh kernel: found SMP MP-table at [mem 0x0009fbf0-0x0009fbff]
OCT 18 18:27:57 rodvissh kernel: RAMDISK: [mem 0x33e23000-0x35f09fff]
OCT 18 18:27:57 rodvissh kernel: ACPI: Early table checksum verification disabled
OCT 18 18:27:57 rodvissh kernel: ACPI: RSDP 0x000000000000E000 000024 (v02 VBOX )
OCT 18 18:27:57 rodvissh kernel: ACPI: XSDT 0x00000000DFFF0030 00003C (v01 VBOX VBOXXSDT 00000001 AS
lines 1-38
```

Рис. 2.22: Содержимое журнала

Просматриваю все сообщения вчерашнего дня

```
OCT 18 18:27:59 rodvissh kernel: vmgfx 0000:00:02:0: [drm] "ERROR" Please switch to a supported graphics device to avoid problems.
OCT 18 18:28:07 rodvissh kernel: Warning: Unmaintained driver is detected: e1000
OCT 18 18:28:08 rodvissh alsactl[889]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import hrt use case configuration -2
OCT 18 18:28:09 rodvissh kernel: Warning: Unmaintained driver is detected: lp_set
OCT 18 18:28:21 rodvissh rsyslogd[1290]: imjournal: fscant on state file '/var/lib/rsyslog/imjournal.state' failed [v8.2412.0-1.el10 try https://ma
OCT 18 18:28:21 rodvissh rsyslogd[1290]: imjournal: ignoring invalid state file '/var/lib/rsyslog/imjournal.state [v8.2412.0-1.el10]
OCT 18 18:29:08 rodvissh gdm-password[2300]: gdm-pam: unable to locate dnmom control file
OCT 18 18:29:12 rodvissh systemd[2313]: Failed to start app-gnome-gnome\x2dkeyring\x2dpcsc11-2426.scope - Application launched by gnome-session-bin
OCT 18 18:29:12 rodvissh systemd[2313]: Failed to start app-gnome-gnome\x2dkeyring\x2dssh-2421.scope - Application launched by gnome-session-binary
OCT 18 18:29:12 rodvissh systemd[2313]: Failed to start app-gnome-xdg\x2duser\x2ddirs-2437.scope - Application launched by gnome-session-binary.
OCT 18 18:29:24 rodvissh systemd-coredump[3151]: [?] Process 3138 (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 3142:
#0 0x000000000041dd1b n/a (n/a + 0x0)
#1 0x000000000041de54 n/a (n/a + 0x0)
#2 0x000000000045041c n/a (n/a + 0x0)
#3 0x00000000004355d8 n/a (n/a + 0x0)
#4 0x00007f48cb0ceb68 start_thread (libc.so.6 + 0x94b68)
#5 0x00007f48cb03f6bc __clone3 (libc.so.6 + 0x1056bc)

Stack trace of thread 3139:
#0 0x00007f48cb03d4bd syscall (libc.so.6 + 0x1034bd)
#1 0x0000000000434c30 n/a (n/a + 0x0)
#2 0x0000000000450fb3 n/a (n/a + 0x0)
#3 0x000000000043566a n/a (n/a + 0x0)
#4 0x000000000045041c n/a (n/a + 0x0)
#5 0x00000000004355d8 n/a (n/a + 0x0)
#6 0x00007f48cb0ceb68 start_thread (libc.so.6 + 0x94b68)
#7 0x00007f48cb03f6bc __clone3 (libc.so.6 + 0x1056bc)

Stack trace of thread 3140:
lines 1-38
```

Рис. 2.23: Содержимое журнала

Просматриваю сообщения с ошибкой приоритета со вчерашнего дня

```

Sat 2025-10-18 18:27:57.91107 MSK [s=f21c5c9c32ec4654a5e004ecce3a77c5; t=1; b=8548b42490354a79a0b0a266beefbe4; m=15ed24; t=641707eb0a043; x=d313ed440b]
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
PRIORITY=5
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
MESSAGE=Linux version 6.12.0-55.32.1.el10_0.x86_64 (mockbuild@ladi-prod-build001.bld.equ.rockylinux.org) (gcc (GCC) 14.2.1 20250110 (Red Hat 14.2.1-7)) #1 SMP Tue Oct 15 16:08:00 EDT 2024
_MACHINE_ID=ee3d489206ca4b85bcaa50f2993d21da
_HOSTNAME=rodvishh
_RUNTIME_SCOPE=initrd
Sat 2025-10-18 18:27:57.91133 MSK [s=f21c5c9c32ec4654a5e004ecce3a77c5; t=2; b=8548b42490354a79a0b0a266beefbe4; m=15ed3d; t=641707eb0a05d; x=5793ab561703c379]
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=8548b42490354a79a0b0a266beefbe4
_MACHINE_ID=ee3d489206ca4b85bcaa50f2993d21da
_HOSTNAME=rodvishh
_RUNTIME_SCOPE=initrd
PRIORITY=6
MESSAGE=Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.32.1.el10_0.x86_64 root=/dev/mapper/zl_vbox-root ro resume=UUID=fad36b5c-0c75-4fe2-ba2f-abd4877c7f72 rd
Sat 2025-10-18 18:27:57.91162 MSK [s=f21c5c9c32ec4654a5e004ecce3a77c5; t=3; b=8548b42490354a79a0b0a266beefbe4; m=15ed5a; t=641707eb0a07a; x=a3475f4e3cc655ae]
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=8548b42490354a79a0b0a266beefbe4
_MACHINE_ID=ee3d489206ca4b85bcaa50f2993d21da
_HOSTNAME=rodvishh
_RUNTIME_SCOPE=initrd
PRIORITY=4
MESSAGE=[Firmware Bug]: TSC doesn't count with P0 frequency!
Sat 2025-10-18 18:27:57.91171 MSK [s=f21c5c9c32ec4654a5e004ecce3a77c5; t=4; b=8548b42490354a79a0b0a266beefbe4; m=15ed63; t=641707eb0a083; x=dec775fad9085e5]
_SOURCE_BOOTTIME_TIMESTAMP=0

```

Рис. 2.24: Содержимое журнала

Просматриваю дополнительную информацию о модуле sshd

```

MESSAGE=Linux version 6.12.0-55.32.1.el10_0.x86_64 (mockbuild@ladi-prod-build001.bld.equ.rockylinux.org) (gcc (GCC) 14.2.1 20250110 (Red Hat 14.2.1-7)) #1 SMP Tue Oct 15 16:08:00 EDT 2024
_MACHINE_ID=ee3d489206ca4b85bcaa50f2993d21da
_HOSTNAME=rodvishh
_RUNTIME_SCOPE=initrd
Sat 2025-10-18 18:27:57.91133 MSK [s=f21c5c9c32ec4654a5e004ecce3a77c5; t=2; b=8548b42490354a79a0b0a266beefbe4; m=15ed3d; t=641707eb0a05d; x=5793ab561703c379]
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=8548b42490354a79a0b0a266beefbe4
_MACHINE_ID=ee3d489206ca4b85bcaa50f2993d21da
_HOSTNAME=rodvishh
_RUNTIME_SCOPE=initrd
PRIORITY=6
MESSAGE=Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.32.1.el10_0.x86_64 root=/dev/mapper/zl_vbox-root ro resume=UUID=fad36b5c-0c75-4fe2-ba2f-abd4877c7f72 rd
Sat 2025-10-18 18:27:57.91162 MSK [s=f21c5c9c32ec4654a5e004ecce3a77c5; t=3; b=8548b42490354a79a0b0a266beefbe4; m=15ed5a; t=641707eb0a07a; x=a3475f4e3cc655ae]
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=8548b42490354a79a0b0a266beefbe4
_MACHINE_ID=ee3d489206ca4b85bcaa50f2993d21da
_HOSTNAME=rodvishh
_RUNTIME_SCOPE=initrd
PRIORITY=4
MESSAGE=[Firmware Bug]: TSC doesn't count with P0 frequency!
Sat 2025-10-18 18:27:57.91171 MSK [s=f21c5c9c32ec4654a5e004ecce3a77c5; t=4; b=8548b42490354a79a0b0a266beefbe4; m=15ed63; t=641707eb0a083; x=dec775fad9085e5]
_SOURCE_BOOTTIME_TIMESTAMP=0

root@rodvishh:~# journalctl -SYSTEMD_UNIT=sshd.service
окт 18 18:28:09 rodvishh (sshd)[1154]: sshd.service: Referenced but unset environment variable evaluates to an empty string: OPTIONS
окт 18 18:28:09 rodvishh sshd[1154]: Server listening on 0.0.0.0 port 22.
окт 18 18:28:09 rodvishh sshd[1154]: Server listening on :: port 22.
root@rodvishh:~#

```

Рис. 2.25: Содержимое журнала

Создаю каталог для хранения записей журнала

```

root@rodvishh:/etc/rsyslog.d# mkdir -p /var/log/journal
root@rodvishh:/etc/rsyslog.d#

```

Рис. 2.26: Создание каталога

Корректирую права доступа

```
root@rodvishh:/etc/rsyslog.d# chown root:systemd-journal /var/log/journal
root@rodvishh:/etc/rsyslog.d# chmod 2755 /var/log/journal
root@rodvishh:/etc/rsyslog.d#
```

Рис. 2.27: Права доступа

Для принятия изменений ввожу следующую команду

```
root@rodvishh:/etc/rsyslog.d# killall -USR1 systemd-journald
root@rodvishh:/etc/rsyslog.d#
```

Рис. 2.28: Принятие изменений

## 3 Вывод

Мы получили навыки работы с журналами мониторинга различных событий в системе.



## 4 Контрольные вопросы

1. Какой файл используется для настройки rsyslogd? `/etc/rsyslog.conf`
2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией? `/var/log/auth.log` (в Red Hat-системах — `/var/log/secure`)
3. Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов? Еженедельно
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? `tail -f` для файлов журналов или `journalctl -f` для systemd
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 вас видеть сообщения journald после последней перезагрузки системы? `journalctl -b`
8. Какая процедура позволяет сделать журнал journald постоянным? Создать директорию `/var/log/journal` и перезапустить `systemd-journald`