

Отчёт по лабораторной работе №7

Управление журналами событий в системе

Тукаев Тимур

Содержание

1 Цель работы	5
2 Выполнение	6
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	15
3 Контрольные вопросы	16
4 Заключение	18

Список иллюстраций

2.1	Ошибка при вводе пароля root	7
2.2	Регистрация пользовательского сообщения в журнале	7
2.3	Анализ лога безопасности /var/log/secure	8
2.4	Установка и запуск службы Apache	8
2.5	Проверка журнала ошибок Apache	8
2.6	Редактирование конфигурационного файла httpd.conf	9
2.7	Создание правила для регистрации сообщений Apache в rsyslog	10
2.8	Создание файла конфигурации для отладочных сообщений	10
2.9	Регистрация отладочного сообщения в системном журнале	10
2.10	Просмотр системного журнала после запуска системы	11
2.11	Просмотр журнала без пейджера	12
2.12	Мониторинг журнала в реальном времени и фиксация ошибок VBoxClient	12
2.13	Просмотр параметров фильтрации журнала	13
2.14	Фильтрация сообщений журнала по UID 0	13
2.15	Просмотр последних строк журнала	14
2.16	Просмотр сообщений о работе службы SSHD	14
2.17	Создание каталога для постоянного хранения журнала	15

Список таблиц

1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

2 Выполнение

2.1 Мониторинг журнала системных событий в реальном времени

1. Запущено три окна терминала.

В каждом окне получены права администратора с использованием команды `SU -`.

2. Во втором окне терминала запущен мониторинг системных событий в реальном времени.

Команда позволяет отслеживать поступающие сообщения ядра и системных служб.

3. В третьем окне выполнен выход из режима суперпользователя с помощью `Ctrl + D`.

Затем произведена попытка повторного входа с неверным паролем.

В результате во втором окне отобразилось сообщение об ошибке аутентификации `FAILED SU (to root) titukaev on pts/1`, которое также зафиксировано в журнале `/var/log/messages`.

```

6 + 0x105c3c) #012#012Stack trace of thread 7576:#012#0 0x000007b487b0ba3d syscall (libc.so.6 + 0x103a3d) #012
0x0) #012#2 0x0000000000450066 n/a (n/a + 0x0) #012#3 0x0000000000405123 n/a (n/a + 0x0) #012#4 0x00007fb487a
.so.6 + 0x2a30e) #012#5 0x00007fb487a323c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9) #012#6 0x00000
object binary architecture: AMD x86-64
Oct 9 14:18:38 titukaev systemd[1]: systemd-coredump@347-7580-0.service: Deactivated successfully.
Oct 9 14:18:38 titukaev systemd[1]: fprintd.service: Deactivated successfully.
Oct 9 14:18:41 titukaev su[7574]: FAILED SU (to root) titukaev on pts/1
Oct 9 14:18:43 titukaev kernel: traps: VBoxClient[7594] trap int3 ip:41dd1b sp:7fb4793b4cd0 error:0 in VBoxC
Oct 9 14:18:43 titukaev systemd-coredump[7595]: Process 7591 (VBoxClient) of user 1000 terminated abnormally
Oct 9 14:18:43 titukaev systemd[1]: Started systemd-coredump@348-7595-0.service - Process Core Dump (PID 759
Oct 9 14:18:43 titukaev systemd-coredump[7596]: Process 7591 (VBoxClient) of user 1000 dumped core. #012#012M
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 rp
odule libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.

```

Рис. 2.1: Ошибка при вводе пароля root

4. В третьем окне введена команда logger hello.

Во втором окне с активным мониторингом отобразилось сообщение, подтверждающее регистрацию записи в журнале /var/log/messages.

```

thread /b//:#012#0 0x000000000041dd1b n/a (n/a + 0x0) #012#1 0x000000000041dc94 n/a (n/a + 0x0) #012#2 0x000
3 0x00000000004355d0 n/a (n/a + 0x0) #012#4 0x00007fb487a9d1a start_thread (libc.so.6 + 0x9511a) #012#5 0x1
6 + 0x105c3c) #012#012Stack trace of thread 7674:#012#0 0x00007fb487b0ba3d syscall (libc.so.6 + 0x103a3d) #01
0x0) #012#2 0x0000000000450066 n/a (n/a + 0x0) #012#3 0x0000000000405123 n/a (n/a + 0x0) #012#4 0x00007fb487
.so.6 + 0x2a30e) #012#5 0x00007fb487a323c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9) #012#6 0x00000
object binary architecture: AMD x86-64
Oct 9 14:19:23 titukaev systemd[1]: systemd-coredump@356-7678-0.service: Deactivated successfully.
Oct 9 14:19:27 titukaev titukaev[7684]: hello
Oct 9 14:19:28 titukaev kernel: traps: VBoxClient[7691] trap int3 ip:41dd1b sp:7fb4793b4cd0 error:0 in VBoxC
Oct 9 14:19:28 titukaev systemd-coredump[7692]: Process 7688 (VBoxClient) of user 1000 terminated abnormally
Oct 9 14:19:28 titukaev systemd[1]: Started systemd-coredump@357-7692-0.service - Process Core Dump (PID 76
Oct 9 14:19:28 titukaev systemd-coredump[7693]: Process 7688 (VBoxClient) of user 1000 dumped core. #012#012M
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 rp
odule libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.

```

Рис. 2.2: Регистрация пользовательского сообщения в журнале

5. Мониторинг системных сообщений остановлен сочетанием клавиш Ctrl + C.

Затем выполнен просмотр последних 20 строк журнала безопасности.

В выводе зафиксированы события успешных и неуспешных попыток получения прав суперпользователя, а также операции открытия и закрытия сессий.

```

root@titukaev:/home/titukaev#
root@titukaev:/home/titukaev# tail -n 20 /var/log/secure
Oct 9 13:49:03 titukaev gdm-password[1994]: gkr-pam: stashed password to try later in open session
Oct 9 13:49:03 titukaev (systemd)[2005]: pam_unix(systemd-user:session): session opened for user titukaev(uid=1000) by titukaev(uid=0)
Oct 9 13:49:03 titukaev gdm-password[1994]: pam_unix(gdm-password:session): session opened for user titukaev(uid=1000) by titukaev(uid=0)
Oct 9 13:49:03 titukaev gdm-password[1994]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct 9 13:49:09 titukaev gdm-launch-environment[1247]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Oct 9 13:49:41 titukaev (systemd)[3216]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)
Oct 9 13:49:41 titukaev su[3183]: pam_unix(su:session): session opened for user root(uid=0) by titukaev(uid=1000)
Oct 9 13:57:30 titukaev su[3183]: pam_unix(su:session): session closed for user root
Oct 9 13:58:10 titukaev (systemd)[4644]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)
Oct 9 13:58:10 titukaev su[4619]: pam_unix(su:session): session opened for user root(uid=0) by titukaev(uid=1000)
Oct 9 14:05:19 titukaev su[4619]: pam_unix(su:session): session closed for user root
Oct 9 14:05:25 titukaev su[5649]: pam_unix(su:session): session opened for user root(uid=0) by titukaev(uid=1000)
Oct 9 14:10:14 titukaev su[5649]: pam_unix(su:session): session closed for user root
Oct 9 14:15:22 titukaev su[5649]: pam_unix(su:session): session closed for user root
Oct 9 14:18:10 titukaev su[7376]: pam_unix(su:session): session opened for user root(uid=0) by titukaev(uid=1000)
Oct 9 14:18:17 titukaev su[7443]: pam_unix(su:session): session opened for user root(uid=0) by titukaev(uid=1000)
Oct 9 14:18:22 titukaev su[7503]: pam_unix(su:session): session opened for user root(uid=0) by titukaev(uid=1000)
Oct 9 14:18:30 titukaev su[7503]: pam_unix(su:session): session closed for user root
Oct 9 14:18:40 titukaev unix_chkpwd[7589]: password check failed for user (root)
Oct 9 14:18:40 titukaev su[7574]: pam_unix(su:auth): authentication failure; logname=titukaev uid=1000 euid=0 tty=/dev/pts/1 ruser=titukaev rh
ost* user=root
root@titukaev:/home/titukaev#

```

Рис. 2.3: Анализ лога безопасности /var/log/secure

2.2 Изменение правил rsyslog.conf

1. Установлен веб-сервер Apache.

После завершения установки служба была запущена и добавлена в автозагрузку.

```

=====
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

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

```

Рис. 2.4: Установка и запуск службы Apache

2. Выполнен просмотр журнала ошибок веб-службы для проверки её работы.

В логе отображены уведомления о запуске и настройке Apache, а также о корректном применении контекста SELinux.

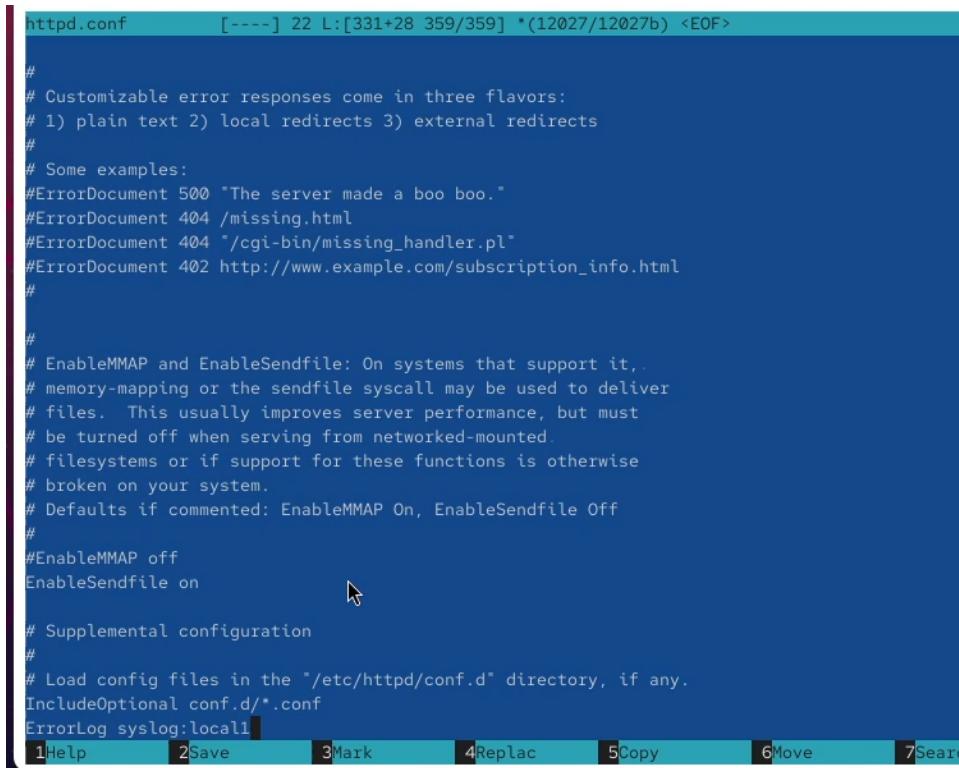
```

titukaev@titukaev:~$ su
Password:
root@titukaev:/home/titukaev# tail -f /var/log/httpd/error_log
[Thu Oct 09 14:20:32.679626 2025] [suexec:notice] [pid 8057:tid 8057] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Thu Oct 09 14:20:32.711112 2025] [lbmethod_heartbeat:notice] [pid 8057:tid 8057] AH02282: No slotmem from mod_heartbeat
[Thu Oct 09 14:20:32.711595 2025] [systemd:notice] [pid 8057:tid 8057] SELinux policy enabled; httpd running as context system_u:system_r:httpd
_t:s0
[Thu Oct 09 14:20:32.712671 2025] [mpm_event:notice] [pid 8057:tid 8057] AH00489: Apache/2.4.63 (Rocky Linux) configured -- resuming normal operations
[Thu Oct 09 14:20:32.712680 2025] [core:notice] [pid 8057:tid 8057] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'

```

Рис. 2.5: Проверка журнала ошибок Apache

3. В конфигурационном файле /etc/httpd/conf/httpd.conf добавлена строка
`ErrorLog syslog:local1,`
обеспечивающая передачу сообщений об ошибках веб-службы через систему журналирования rsyslog.

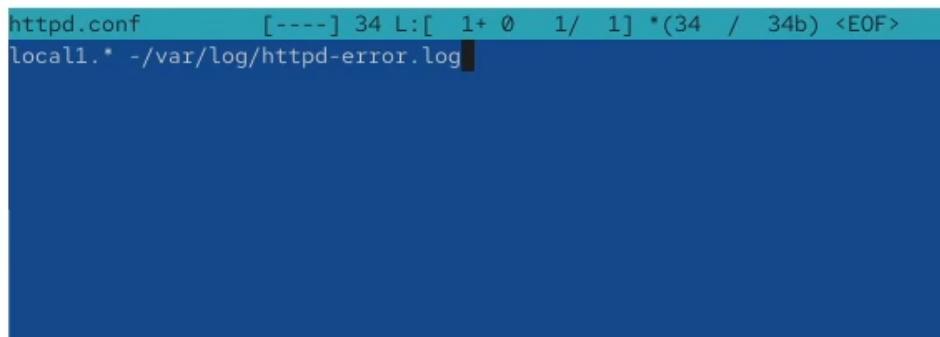


```
httpd.conf      [---] 22 L:[331+28 359/359] *(12027/12027b) <EOF>

#
# 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
```

Рис. 2.6: Редактирование конфигурационного файла httpd.conf

4. В каталоге /etc/rsyslog.d создан файл httpd.conf, в котором прописано правило local1.* -/var/log/httpd-error.log, направляющее сообщения категории local1 в отдельный файл журнала /var/log/httpd-error.log.



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

Рис. 2.7: Создание правила для регистрации сообщений Apache в rsyslog

5. Создан отдельный файл конфигурации `debug.conf` для регистрации отладочных сообщений.

В него добавлено правило `*.debug /var/log/messages-debug`, позволяющее сохранять сообщения уровня отладки в отдельный лог-файл.



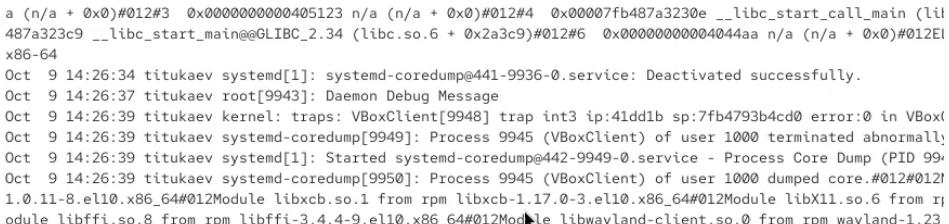
```
root@titukaev:/home/titukaev#
root@titukaev:/home/titukaev# cd /etc/rsyslog.d/
root@titukaev:/etc/rsyslog.d# touch httpd.conf
root@titukaev:/etc/rsyslog.d# mcedit httpd.conf

root@titukaev:/etc/rsyslog.d#
root@titukaev:/etc/rsyslog.d# touc debug.conf
bash: touc: command not found...
root@titukaev:/etc/rsyslog.d# touch debug.conf
root@titukaev:/etc/rsyslog.d# echo "*.*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
root@titukaev:/etc/rsyslog.d#
```

Рис. 2.8: Создание файла конфигурации для отладочных сообщений

6. После внесённых изменений службы `rsyslog` и `httpd` были перезапущены.

При генерации отладочного сообщения с помощью `logger -p daemon.debug "Daemon Debug Message"` запись появилась в файле `/var/log/messages-debug`, что подтвердило корректность настроек.



```
a (n/a + 0x0)#012#3 0x0000000000405123 n/a (n/a + 0x0)#012#4 0x00007fb487a3230e __libc_start_main (lil
487a323c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x0000000004044aa n/a (n/a + 0x0)#012#1
x86-64
Oct 9 14:26:34 titukaev systemd[1]: systemd-coredump@441-9936-0.service: Deactivated successfully.
Oct 9 14:26:37 titukaev root[9943]: Daemon Debug Message
Oct 9 14:26:39 titukaev kernel: traps: VBoxClient[9948] trap int3 ip:41dd1b sp:7fb4793b4cd0 error:0 in VBox(
Oct 9 14:26:39 titukaev systemd-coredump[9949]: Process 9945 (VBoxClient) of user 1000 terminated abnormally;
Oct 9 14:26:39 titukaev systemd[1]: Started systemd-coredump@442-9949-0.service - Process Core Dump (PID 99
Oct 9 14:26:39 titukaev systemd-coredump[9950]: Process 9945 (VBoxClient) of user 1000 dumped core.#012#012#
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 r
odule libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23
```

Рис. 2.9: Регистрация отладочного сообщения в системном журнале

2.3 Использование journalctl

- Просмотрен системный журнал с момента последнего запуска системы.

Отображены сообщения ядра, включая сведения о версии Linux, параметрах BIOS и аппаратной конфигурации.

```
Oct 09 13:48:22 titukaev.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rocky)
Oct 09 13:48:22 titukaev.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_64 root=/dev/map
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-provided physical RAM map:
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000005fbff] usable
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x0000000000091c00-0x000000000009ffff] reserved
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x0000000000f00000-0x0000000000ffff] reserved
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x0000000001000000-0x000000000dfeffff] usable
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x000000000dff0000-0x000000000dffffff] ACPI data
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x000000000fec0000-0x000000000fec00ff] reserved
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x000000000fee0000-0x000000000fee00ff] reserved
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x000000000ffc0000-0x000000000fffffff] reserved
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x0000000010000000-0x0000000011ffffff] usable
Oct 09 13:48:22 titukaev.localdomain kernel: NX (Execute Disable) protection: active
Oct 09 13:48:22 titukaev.localdomain kernel: APIC: Static calls initialized
Oct 09 13:48:22 titukaev.localdomain kernel: SMBIOS 2.5 present.
Oct 09 13:48:22 titukaev.localdomain kernel: DMI: innotech GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 09 13:48:22 titukaev.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 09 13:48:22 titukaev.localdomain kernel: Hypervisor detected: KVM
Oct 09 13:48:22 titukaev.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 09 13:48:22 titukaev.localdomain kernel: kvm-clock: using sched offset of 4612772641 cycles
Oct 09 13:48:22 titukaev.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dff, max_idle_ns: 0xffffffff
Oct 09 13:48:22 titukaev.localdomain kernel: tsc: Detected 3187.202 MHz processor
Oct 09 13:48:22 titukaev.localdomain kernel: e820: update [mem 0x00000000-0x0000ffff] usable ==> reserved
Oct 09 13:48:22 titukaev.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Oct 09 13:48:22 titukaev.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 09 13:48:22 titukaev.localdomain kernel: total RAM covered: 4096M
Oct 09 13:48:22 titukaev.localdomain kernel: Found optimal setting for mtrr clean up
Oct 09 13:48:22 titukaev.localdomain kernel: gran_size: 64K      chunk_size: 1G      num_reg: 3      lose cover RAM: 0G
Oct 09 13:48:22 titukaev.localdomain kernel: MTRR map: 6 entries (3 fixed + 3 variable; max 35), built from 16 variable MTRRs
lines 1-29
```

Рис. 2.10: Просмотр системного журнала после запуска системы

- Произведён просмотр журнала без использования пейджера для вывода всех сообщений в непрерывном виде.

Это позволяет анализировать логи без постраничной навигации.

```

Oct 09 14:30:42 titukaev.localdomain systemd-coredump[10578]: Process 10574 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Oct 09 14:30:42 titukaev.localdomain systemd[1]: Started systemd-coredump@490-10578-0.service - Process Core Dump (PID 10578/UID 0).
Oct 09 14:30:42 titukaev.localdomain systemd-coredump[10579]: [..] Process 10574 (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 10577:
#0 0x000000000041dd1b n/a (n/a + 0x0)
#1 0x000000000041dc94 n/a (n/a + 0x0)
#2 0x000000000045041c n/a (n/a + 0x0)
#3 0x00000000004335d0 n/a (n/a + 0x0)
#4 0x00007fb487a5d11a start_thread (libc.so.6 + 0x9511a)
#5 0x00007fb487b032c3 __clone3 (libc.so.6 + 0x105c3c)

Stack trace of thread 10574:
#0 0x00007fb487b03ba3d 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 0x00007fb487a3230e __libc_start_main (libc.so.6 + 0x2a30e)
#5 0x00007fb487a322e9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a30e)

3c9)
#6 0x00000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x86-64
Oct 09 14:30:42 titukaev.localdomain systemd[1]: systemd-coredump@490-10578-0.service: Deactivated successfully.
root@titukaev:/home/titukaev#

```

Рис. 2.11: Просмотр журнала без пейджера

3. Активирован режим мониторинга журнала в реальном времени.

В ходе наблюдения зафиксированы ошибки, связанные с процессом **VBoxClient**, приведшие к созданию дампа ядра.

_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=
COREDUMP_PROC_AUXV=	KERNEL_USEC=	_SYSTEMD_USER_UNIT=
COREDUMP_PROC_CGROUP=	LEADER=	THREAD_ID=
COREDUMP_PROC_LIMITS=	LIMIT=	TID=
- More -		

Рис. 2.12: Мониторинг журнала в реальном времени и фиксация ошибок **VBoxClient**

4. Выполнен просмотр всех доступных параметров фильтрации с помощью двойного нажатия клавиши Tab после ввода команды `journalctl`.

В списке представлены ключи, позволяющие выполнять выборку по полям системных сообщений.

```
Oct 09 13:48:22 titukaev.localdomain systemd-journald[302]: Collecting audit messages is disabled.
Oct 09 13:48:22 titukaev.localdomain systemd-journald[302]: Journal started
Oct 09 13:48:22 titukaev.localdomain systemd-journald[302]: Runtime Journal (/run/log/journal/8799d6cafd5a4a0788922e3534d8e65e) is active.
Oct 09 13:48:22 titukaev.localdomain systemd-modules-load[303]: Module 'msr' is built in
Oct 09 13:48:22 titukaev.localdomain systemd-modules-load[303]: Inserted module 'fuse'
Oct 09 13:48:22 titukaev.localdomain systemd-modules-load[303]: Module 'scsi_dh_alua' is built in
Oct 09 13:48:22 titukaev.localdomain systemd-modules-load[303]: Module 'scsi_dh_emc' is built in
Oct 09 13:48:22 titukaev.localdomain systemd-modules-load[303]: Module 'scsi_dh_rdac' is built in
Oct 09 13:48:22 titukaev.localdomain systemd[1]: Finished systemd-modules-load.service - Load Kernel Modules.
Oct 09 13:48:22 titukaev.localdomain systemd[1]: Starting systemd-sysctl.service - Apply Kernel Variables...
Oct 09 13:48:22 titukaev.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev-early.service - Create Static Device Nodes in /dev...
Oct 09 13:48:22 titukaev.localdomain systemd[1]: Starting systemd-sysusers.service - Create System Users...
Oct 09 13:48:22 titukaev.localdomain systemd[1]: Finished systemd-vconsole-setup.service - Virtual Console Setup.
Oct 09 13:48:22 titukaev.localdomain systemd[1]: dracut-cmdline-ask.service - dracut ask for additional cmdline parameters was skipped.
Oct 09 13:48:22 titukaev.localdomain systemd[1]: Starting dracut-cmdline.service - dracut cmdline hook...
Oct 09 13:48:22 titukaev.localdomain systemd-sysusers[322]: Creating group 'nobody' with GID 65534.
Oct 09 13:48:22 titukaev.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variables.
Oct 09 13:48:22 titukaev.localdomain systemd-sysusers[322]: Creating group 'users' with GID 100.
Oct 09 13:48:22 titukaev.localdomain systemd-sysusers[322]: Creating group 'systemd-journal' with GID 190.
Oct 09 13:48:22 titukaev.localdomain systemd[1]: Finished systemd-sysusers.service - Create System Users.
Oct 09 13:48:22 titukaev.localdomain systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create Static Device Nodes in /dev...
Oct 09 13:48:22 titukaev.localdomain dracut-cmdline[326]: dracut-105-4.el10_0
Oct 09 13:48:22 titukaev.localdomain dracut-cmdline[326]: Using kernel command line parameters: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.1.14-200.el10_0
Oct 09 13:48:22 titukaev.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev.service - Create Static Device Nodes in /dev.
Oct 09 13:48:22 titukaev.localdomain systemd[1]: Finished dracut-cmdline.service - dracut cmdline hook.
Oct 09 13:48:22 titukaev.localdomain systemd[1]: Starting dracut-pre-udev.service - dracut pre-udev hook...
Oct 09 13:48:22 titukaev.localdomain systemd[1]: Finished dracut-pre-udev.service - dracut pre-udev hook.
Oct 09 13:48:22 titukaev.localdomain systemd[1]: Finished dracut-pre-udev.service - dracut pre-udev hook.
Oct 09 13:48:22 titukaev.localdomain systemd[1]: Starting systemd-udevd.service - Rule-based Manager for Device Events and Files...
Oct 09 13:48:22 titukaev.localdomain systemd-udevd[433]: Using default interface naming scheme 'rhel-10.0'.
lines 1-29
```

Рис. 2.13: Просмотр параметров фильтрации журнала

5. Выполнен фильтр вывода по идентификатору пользователя с UID 0, чтобы отобразить все события, связанные с пользователем root.

```
Oct 09 14:31:33 titukaev.localdomain systemd-coredump[10754]: Process 10750 (VBoxClient) of user 1000 terminated abnormally with signal 11.
Oct 09 14:31:33 titukaev.localdomain systemd[1]: Started systemd-coredump@500-10754-0.service - Process Core Dump (PID 10754/UID 0).
Oct 09 14:31:33 titukaev.localdomain systemd-coredump[10755]: [..] Process 10750 (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 10753:
#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 0x00007fb487a9d11a start_thread (libc.so.6 + 0x9511a)
#5 0x00007fb487b0dc3c __clone3 (libc.so.6 + 0x105c3c)

Stack trace of thread 10750:
#0 0x00007fb487b0ba3d 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 0x00007fb487a3230e __libc_start_main (libc.so.6 + 0x2a30e)
#5 0x00007fb487a323c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a30e)
#6 0x00000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x86-64

Oct 09 14:31:33 titukaev.localdomain systemd[1]: systemd-coredump@500-10754-0.service: Deactivated successfully.
Oct 09 14:31:38 titukaev.localdomain kernel: traps: VBoxClient[10787] trap int3 ip:41dd1b sp:7fb4793b4cd0 error:0 in VBoxClient[10787]
[...]
```

Рис. 2.14: Фильтрация сообщений журнала по UID 0

6. Произведён просмотр последних 20 строк системного журнала для анализа последних записей.

Зафиксированы записи об успешной инициализации служб и завершении процессов.

```
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-provided physical RAM map:  
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000fbfff] usable  
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x00000000000009fc00-0x00000000000fffff] reserved  
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000fffff] reserved  
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x0000000000000001,00000-0x00000000000fffff] usable  
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x0000000000fffe0000-0x0000000000fffff] ACPI data  
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x0000000000fec00000-0x0000000000fec0000] reserved  
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x0000000000fee0000-0x0000000000fee0000] reserved  
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x0000000000fffc0000-0x000000000fffffff] reserved  
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x0000000010000000-0x000000001fffffff] usable  
Oct 09 13:48:22 titukaev.localdomain kernel: NX (Execute Disable) protection: active  
Oct 09 13:48:22 titukaev.localdomain kernel: APIC: Static calls initialized  
Oct 09 13:48:22 titukaev.localdomain kernel: SMBIOS 2.5 present.  
Oct 09 13:48:22 titukaev.localdomain kernel: DME: innotele GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006  
Oct 09 13:48:22 titukaev.localdomain kernel: DME: Memory slots populated: 0/0  
Oct 09 13:48:22 titukaev.localdomain kernel: Hypervisor detected: KVM  
Oct 09 13:48:22 titukaev.localdomain kernel: kvm-clock: Using msr 4b564d01 and 4b564d00  
Oct 09 13:48:22 titukaev.localdomain kernel: kvm-clock: using sched offset 4612772641 cycles  
Oct 09 13:48:22 titukaev.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffff max_cycles: 0x1cd42e4dff, max_idle_ns: 88159059148  
Oct 09 13:48:22 titukaev.localdomain kernel: tsc: Detected 3187.202 MHz processor  
Oct 09 13:48:22 titukaev.localdomain kernel: e820: update [mem 0x00000000-0x0000ffff] usable => reserved  
Oct 09 13:48:22 titukaev.localdomain kernel: e820: remove [mem 0x0000a000-0x000fffff] usable  
Oct 09 13:48:22 titukaev.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000  
Oct 09 13:48:22 titukaev.localdomain kernel: total RAM core'd: 4096M  
Oct 09 13:48:22 titukaev.localdomain kernel: Found optimal setting for mtrr clean up  
Oct 09 13:48:22 titukaev.localdomain kernel: gran_size: 64K chunk_size: 1G num_reg: 3 lose cover RAM: 00  
Oct 09 13:48:22 titukaev.localdomain kernel: MTRR map: 6 entries (3 fixed + 3 variable; max 35), built from 16 variable MTRRs  
Oct 09 13:48:22 titukaev.localdomain kernel: x86/PAT: Configuration [0-7]: WB WC UC-UC WB WP UC-WT  
Oct 09 13:48:22 titukaev.localdomain kernel: e820: update [mem 0xe0000000-0xfffffff] usable => reserved  
Oct 09 13:48:22 titukaev.localdomain kernel: last_pfn = 0xe0000 max_arch_pfn = 0x400000000  
Oct 09 13:48:22 titukaev.localdomain kernel: found SMP MP-table at [mem 0x00009fb0-0x0009fbff]  
Oct 09 13:48:22 titukaev.localdomain kernel: Incomplete global flushes, disabling PCID  
Oct 09 13:48:22 titukaev.localdomain kernel: RAMDISK: [mem 0x34339000-0x36194fff]  
Oct 09 13:48:22 titukaev.localdomain kernel: ACPI: Early table checksum verification disabled  
root@titukaev:/home/titukaev#  
root@titukaev:/home/titukaev#
```

Рис. 2.15: Просмотр последних строк журнала

7. Выполнен фильтр по модулю `sshd.service` для получения сведений о работе SSH-сервера.

В журнале отображены записи о запуске службы и активации прослушивания порта 22.

```
_RUNTIME_SCOPE=initrd  
Thu 2025-10-09 13:48:22.274295 MSK [s=b1fb7e54d3e040859adbf224e7cd47cc6;l=2;b=016ce7c7ef06485daf0402bcec5b3026;m=23975e;t=640b78a3658f7;x=857705b  
_SOURCE_BOOTTIME_TIMESTAMP=0  
_SOURCE_MONOTONIC_TIMESTAMP=0  
_TRANSPORT=kernel  
SYSLOG_FACILITY=0  
SYSLOG_IDENTIFIER=kernel  
_BOOT_ID=016ce7c7ef06485daf0402bcec5b3026  
_MACHINE_ID=8799d9cacf5a4a0789922e3534d8e65e  
_HOSTNAME=titukaev.localdomain  
_RUNTIME_SCOPE=initrd  
PRIORITY=6  
MESSAGE=Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el11_0.x86_64 root=/dev/mapper/vl_vbox-root ro resume=UUID=f51f7d8c-5e1e-4  
Thu 2025-10-09 13:48:22.274512 MSK [s=b1fb7e54d3e040859adbf224e7cd47cc6;l=3;b=016ce7c7ef06485daf0402bcec5b3026;m=239837;t=640b78a3659d0;x=c6100602  
_SOURCE_BOOTTIME_TIMESTAMP=0  
_SOURCE_MONOTONIC_TIMESTAMP=0  
_TRANSPORT=kernel  
SYSLOG_FACILITY=0  
SYSLOG_IDENTIFIER=kernel  
_BOOT_ID=016ce7c7ef06485daf0402bcec5b3026  
_MACHINE_ID=8799d9cacf5a4a0789922e3534d8e65e  
_HOSTNAME=titukaev.localdomain  
_RUNTIME_SCOPE=initrd  
PRIORITY=6  
root@titukaev:/home/titukaev# journalctl _SYSTEMD_UNIT=sshd.service  
Oct 09 13:48:35 titukaev.localdomain (sshd)[1222]: sshd.service: Referenced but unset environment variable evaluates to an empty string: OPTIONS  
Oct 09 13:48:35 titukaev.localdomain sshd[1222]: Server listening on 0.0.0.0 port 22.  
Oct 09 13:48:35 titukaev.localdomain sshd[1222]: Server listening on :: port 22.  
root@titukaev:/home/titukaev#
```

Рис. 2.16: Просмотр сообщений о работе службы SSHD

2.4 Постоянный журнал `journald`

1. Получены права администратора для внесения изменений в конфигурацию службы журналирования.
2. Создан каталог `/var/log/journal`, предназначенный для хранения постоянных записей системного журнала.

Это позволяет сохранять логи между перезагрузками системы.

```
root@titukaev:/home/titukaev#
root@titukaev:/home/titukaev#
root@titukaev:/home/titukaev# mkdir -p /var/log/journal
root@titukaev:/home/titukaev# chown root:systemd-journal /var/log/journal/
root@titukaev:/home/titukaev# chmod 2755 /var/log/journal/
root@titukaev:/home/titukaev# killall -USR1 systemd-journald
root@titukaev:/home/titukaev#
```

Рис. 2.17: Создание каталога для постоянного хранения журнала

3. Установлены необходимые права доступа к каталогу: владельцем назначена группа `systemd-journal`, а права доступа заданы как 2755.
Такая настройка обеспечивает возможность записи службы `journald` в данный каталог.
4. Для применения изменений выполнена команда `killall -USR1 systemd-journald`, сигнализирующая службе `journald` о необходимости перезапуска с учётом новой конфигурации.
5. После выполнения всех шагов система ведёт **постоянный журнал**, записи которого сохраняются в каталоге `/var/log/journal` и доступны после перезагрузки.

3 Контрольные вопросы

1. Для настройки службы системного журналирования используется файл конфигурации `/etc/rsyslog.conf`.
2. Сообщения, связанные с аутентификацией пользователей и доступом, сохраняются в файле `/var/log/secure`.
3. Если не изменять стандартную конфигурацию, ротация файлов журналов выполняется еженедельно.
4. Для записи всех сообщений с приоритетом `info` в отдельный файл необходимо добавить строку:
`*.info /var/log/messages.info`
5. Для просмотра сообщений журнала в режиме реального времени используется команда `tail -f /var/log/messages`
или её системная альтернатива `journalctl -f`.
6. Чтобы вывести все сообщения, записанные для процесса с PID 1 между 9:00 и 15:00, применяют команду:
`journalctl _PID=1 --since "09:00" --until "15:00".`
7. Для просмотра всех сообщений `journald`, зафиксированных после последней перезагрузки системы, используется команда:
`journalctl -b.`
8. Чтобы сделать журнал `journald` постоянным, необходимо создать каталог `/var/log/journal`,

назначить ему владельца `root:systemd-journal`, установить права доступа
`chmod 2755`,

а затем перезапустить службу `journald` с помощью команды
`killall -USR1 systemd-journald` или перезагрузить систему.

4 Заключение

В ходе лабораторной работы были изучены механизмы системного журналирования в Linux.

Рассмотрены принципы работы службы `rsyslogd` и `journald`, методы фильтрации и анализа сообщений,

а также способы настройки постоянного хранения логов.

Полученные навыки позволяют эффективно контролировать состояние системы и выявлять источники ошибок.