

Отчёт по лабораторной работе №7

Управление журналами событий в системе

Шаханеоядж Хаоладар

Содержание

1 Цель работы	5
2 Выполнение	6
2.1 Мониторинг журнала системных событий в реальном времени	6
3 Выполнение	9
3.1 Изменение правил rsyslog.conf	9
3.2 Использование journalctl	12
3.3 Постоянный журнал journald	18
4 Контрольные вопросы	20
5 Заключение	22

Список иллюстраций

2.1 Мониторинг системных событий в реальном времени	7
2.2 Ошибка при попытке входа с неверным паролем	7
2.3 Сообщение logger hello в системном журнале	8
2.4 Журнал безопасности /var/log/secure	8
3.1 Установка и запуск службы httpd	9
3.2 Журнал ошибок Apache	10
3.3 Добавление строки ErrorLog syslog:local1 в конфигурацию httpd . .	10
3.4 Создание файла конфигурации rsyslog для httpd	11
3.5 Создание файла debug.conf для регистрации отладочных сообщений	11
3.6 Отображение отладочного сообщения в системном журнале	12
3.7 Просмотр системного журнала с момента последней загрузки . .	12
3.8 Просмотр возможных параметров фильтрации журнала	13
3.9 Просмотр возможных параметров фильтрации журнала	13
3.10 Просмотр возможных параметров фильтрации журнала	14
3.11 Отображение событий, связанных с пользователем root	15
3.12 Просмотр последних 20 строк журнала	15
3.13 Просмотр сообщений уровня ошибок	16
3.14 Просмотр сообщений со вчерашнего дня	16
3.15 Просмотр сообщений об ошибках со вчерашнего дня	17
3.16 Просмотр журнала службы SSH	18
3.17 Настройка постоянного хранения системного журнала journald . .	19

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. В трёх вкладках терминала были получены права администратора с помощью команды **su -**.

Это позволило выполнять команды от имени суперпользователя во всех сессиях.

2. На второй вкладке терминала был запущен мониторинг системных событий в реальном времени с помощью команды **tail -f /var/log/messages**.

В результате на экране стали отображаться новые записи журнала, появляющиеся в процессе работы системы.

```

root@haoladar:/home/haoladar# tail -f /var/log/messages
Oct 1 18:36:33 haoladar kernel: traps: VBoxClient[3482] trap int3 ip:41dd1b sp:7f6f15188cd0 error:0 in VBox
Client[1dd1b,400000+0b000]
Oct 1 18:36:33 haoladar systemd-coredump[3483]: Process 3479 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Oct 1 18:36:33 haoladar systemd[1]: Started systemd-coredump@16-3483-0.service - Process Core Dump (PID 3483/UID 0).
Oct 1 18:36:33 haoladar systemd-coredump[3484]: Process 3479 (VBoxClient) of user 1000 dumped core.#012#012
Module 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 libXi11.so.6 from rpm libXi11-1.8.10-1.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 3482:#012#0 0x000000000041dd1b n/a (n/a + 0x0)#012#1 0x000000000041dc94 n/a (n/a + 0x0)#012#2 0x0000000045041c n/a (n/a + 0x0)#012#3 0x00000000004355d0 n/a (n/a + 0x0)#012#4 0x00007f6f2382911a start_thread
(libc.so.6 + 0x9511a)#012#5 0x00007f6f23899c3e __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 3479:#012#0 0x00007f6f23897a3d syscall (libc.so.6 + 0x103a3d)#012#1 0x00000000004344e2 n/a (n/a + 0x0)#012#2 0x0000000000450066 n/a (n/a + 0x0)#012#3 0x0000000000405123 n/a (n/a + 0x0)#012#4 0x00007f6f237be30e __libc_start_main (libc.so.6 + 0x2a30e)#012#5 0x00007f6f237be3c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Oct 1 18:36:33 haoladar systemd[1]: systemd-coredump@16-3483-0.service: Deactivated successfully.
Oct 1 18:36:38 haoladar kernel: traps: VBoxClient[3496] trap int3 ip:41dd1b sp:7f6f15188cd0 error:0 in VBox
Client[1dd1b,400000+0b000]
Oct 1 18:36:38 haoladar systemd-coredump[3497]: Process 3493 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Oct 1 18:36:38 haoladar systemd[1]: Started systemd-coredump@17-3493-0.service - Process Core Dump (PID 3497/UID 0).
Oct 1 18:36:38 haoladar systemd-coredump[3498]: Process 3493 (VBoxClient) of user 1000 dumped core.#012#012
Module 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.

```

Рис. 2.1: Мониторинг системных событий в реальном времени

3. В третьей вкладке терминала была выполнена попытка получить права администратора с помощью команды **su**, но с введением неверного пароля. В окне мониторинга появилось сообщение об ошибке аутентификации: **FAILED SU (to root) haoladar on pts/2.**

Это событие также было зафиксировано в файле **/var/log/messages**.

```

Oct 1 18:39:17 haoladar su[3831]: FAILED SU (to root) haoladar on pts/2
Oct 1 18:39:22 haoladar kernel: traps: VBoxClient[3855] trap int3 ip:41dd1b sp:7f6f15188cd0 error:0 in VBox
Client[1dd1b,400000+0b000]
Oct 1 18:39:22 haoladar systemd-coredump[3856]: Process 3852 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Oct 1 18:39:22 haoladar systemd[1]: Started systemd-coredump@49-3856-0.service - Process Core Dump (PID 3856/UID 0).
Oct 1 18:39:22 haoladar systemd-coredump[3857]: Process 3852 (VBoxClient) of user 1000 dumped core.#012#012
Module 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.

```

Рис. 2.2: Ошибка при попытке входа с неверным паролем

4. Далее в третьей вкладке от имени пользователя была выполнена команда **logger hello**.

После этого в окне мониторинга появилось сообщение **hello**, подтверждающее запись пользовательского события в системный журнал.

```

4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 3912:#012#0 0x000000000041dd1b n/a (n/a + 0x0)#012#1 0x000000000041dc94 n/a (n/a + 0x0)#012#2 0x000000000045041c n/a (n/a + 0x0)#012#3 0x00000000004355d0 n/a (n/a + 0x0)#012#4 0x00007f6f2382911a start_thread (libc.so.6 + 0x9511a)#012#5 0x00007f6f23899c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 3909:#012#0 0x00007f6f23897a3d syscall (libc.so.6 + 0x103a3d)#012#1 0x00000000004344e2 n/a (n/a + 0x0)#012#2 0x0000000000450066 n/a (n/a + 0x0)#012#3 0x0000000000405123 n/a (n/a + 0x0)#012#4 0x00007f6f237be30e __libc_start_main (libc.so.6 + 0x2a30e)#012#5 0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64 Oct 1 18:39:48 haoladar systemd[1]: systemd-coredump@54-3913-0.service: Deactivated successfully. Oct 1 18:39:49 haoladar haoladar[3919]: hello Oct 1 18:39:50 haoladar haoladar[3924]: hello

```

Рис. 2.3: Сообщение logger hello в системном журнале

5. Мониторинг журнала **/var/log/messages** был завершён с помощью сочетания клавиш **Ctrl + C**.

Затем был запущен просмотр последних 20 строк файла журнала безопасности командой **tail -n 20 /var/log/secure**.

В результате отобразились сообщения о сессиях входа и ошибке аутентификации при вводе неправильного пароля команды **su**.

```

root@haoladar:/home/haoladar#
root@haoladar:/home/haoladar# tail -n 20 /var/log/secure
Sep 27 14:28:37 haoladar su[4295]: pam_unix(su:session): session closed for user root
Sep 27 14:33:00 haoladar su[5235]: pam_unix(su:session): session opened for user root(uid=0) by haoladar(uid=1000)
Sep 27 14:34:59 haoladar su[5235]: pam_unix(su:session): session closed for user root
Oct 1 18:32:28 haoladar sshd[1195]: Server listening on 0.0.0.0 port 22.
Oct 1 18:32:28 haoladar sshd[1195]: Server listening on :: port 22.
Oct 1 18:32:28 haoladar (systemd)[1263]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)
Oct 1 18:32:29 haoladar gdm-launch-environment][1240]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=42) by (uid=0)
Oct 1 18:35:07 haoladar gdm-password][1974]: gkr-pam: unable to locate daemon control file
Oct 1 18:35:07 haoladar gdm-password][1974]: gkr-pam: stashed password to try later in open session
Oct 1 18:35:07 haoladar (systemd)[1986]: pam_unix(systemd-user:session): session opened for user haoladar(uid=1000) by haoladar(uid=0)
Oct 1 18:35:07 haoladar gdm-password][1974]: pam_unix(gdm-password:session): session opened for user haoladar(uid=1000) by haoladar(uid=0)
Oct 1 18:35:07 haoladar gdm-password][1974]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct 1 18:35:11 haoladar gdm-launch-environment][1240]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Oct 1 18:36:21 haoladar (systemd)[3295]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)
Oct 1 18:36:21 haoladar su[2277]: pam_unix(su:session): session opened for user root(uid=0) by haoladar(uid=0)

```

Рис. 2.4: Журнал безопасности **/var/log/secure**

3 Выполнение

3.1 Изменение правил rsyslog.conf

1. В первой вкладке терминала был установлен веб-сервер **Apache (httpd)** с помощью команды **dnf -y install httpd**.

После завершения установки служба была запущена и добавлена в автозагрузку командами **systemctl start httpd** и **systemctl enable httpd**.

```
[[email protected] ~]# dnf -y install httpd
[[email protected] ~]# systemctl start httpd
[[email protected] ~]# systemctl enable httpd
[[email protected] ~]#
```

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

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

Рис. 3.1: Установка и запуск службы httpd

2. Во второй вкладке был открыт журнал ошибок веб-службы с помощью команды **tail -f /var/log/httpd/error_log**.

На экране отобразились сообщения о запуске и настройке Apache, включая строки о включении SELinux, активации suEXEC и конфигурации модуля **mpm_event**.

```

root@haoladar:/home/haoladar#
root@haoladar:/home/haoladar# tail -f /var/log/httpd/error_log
[Wed Oct 01 18:41:42.027397 2025] [suexec:notice] [pid 4405:tid 4405] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Wed Oct 01 18:41:42.078182 2025] [lbbmethod_heartbeat:notice] [pid 4405:tid 4405] AH02282: No slotmem from module _od_heartbeat
[Wed Oct 01 18:41:42.078672 2025] [systemd:notice] [pid 4405:tid 4405] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Wed Oct 01 18:41:42.079793 2025] [mpm_event:notice] [pid 4405:tid 4405] AH00489: Apache/2.4.63 (Rocky Linux) configured -- resuming normal operations
[Wed Oct 01 18:41:42.079803 2025] [core:notice] [pid 4405:tid 4405] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'

```

Рис. 3.2: Журнал ошибок Apache

3. В третьей вкладке был отредактирован конфигурационный файл **/etc/httpd/conf/httpd.conf**, в конец которого добавлена строка **ErrorLog syslog:local1**. Эта настройка перенаправляет сообщения об ошибках веб-сервера 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. 3.3: Добавление строки ErrorLog syslog:local1 в конфигурацию httpd

4. В каталоге **/etc/rsyslog.d** был создан новый файл **httpd.conf** с правилом перенаправления сообщений от объекта **local1** в отдельный лог-файл **/var/log/httpd-error.log**:

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

Это позволяет сохранять ошибки веб-службы в отдельном файле.

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

Рис. 3.4: Создание файла конфигурации rsyslog для httpd

5. После добавления правил конфигурации службы **rsyslog** и **httpd** были перезапущены командами

systemctl restart rsyslog.service и **systemctl restart httpd**.

Теперь все ошибки веб-службы записываются через **rsyslog** в файл **/var/log/httpd-error.log**.

6. В каталоге **/etc/rsyslog.d** был также создан дополнительный файл **debug.conf** для регистрации отладочных сообщений.

В нём добавлена строка ***.debug /var/log/messages-debug**,

что позволяет сохранять все отладочные сообщения в отдельный лог-файл.

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

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

Рис. 3.5: Создание файла debug.conf для регистрации отладочных сообщений

7. После перезапуска службы **rsyslog** в терминале был запущен мониторинг нового журнала с помощью команды **tail -f /var/log/messages-debug**.

Далее от имени суперпользователя было отправлено отладочное сообщение:

logger -p daemon.debug “Daemon Debug Message”.

Сообщение успешно появилось в журнале, что подтверждает корректную настройку регистрации событий.

```
a b300:#01#0 0x0000/0x0000000045006 n/a (n/a + 0x0)#01#1 0x00000000004344e2 n/a (n/a + 0x0)#01#2 0x0000000000405123 n/a (n/a + 0x0)#01#3 0x00007f6f237be30e __libc_start_main_(libc.so.6 + 0x2a30e)#01#4 0x00007f6f237be3c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#01#5 0x000000004044aa n/a (n/a + 0x0)#01#6 object binary architecture: AMD x86-64 Oct 1 18:49:35 haoladar systemd[1]: systemctl-coredump@169-6304-0.service: Deactivated successfully. Oct 1 18:49:39 haoladar root[6310]: Daemon DEbug Message Oct 1 18:49:40 haoladar kernel: traps: VBoxClient[6315] trap int3 ip:41dd1b sp:7f6f15188cd0 error:0 in VBoxClient[1dd1b,40000+bb000] Oct 1 18:49:40 haoladar systemd-coredump[6316]: Process 6312 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing... Oct 1 18:49:40 haoladar systemd[1]: Started systemctl-coredump@170-6316-0.service - Process Core Dump (PID 6316/UID 0). Oct 1 18:49:40 haoladar systemd-coredump[6317]: Process 6312 (VBoxClient) of user 1000 dumped core.#01#012 Module libXau.so.6 from rom libXau-1.0.11-8.el10.x86_64#01#012Module libxcb.so.1 from rom libxcb-1.17.0-3.el10.
```

Рис. 3.6: Отображение отладочного сообщения в системном журнале

3.2 Использование journalctl

1. Во второй вкладке терминала был выполнен просмотр системного журнала с момента последнего запуска системы с помощью команды **journalctl**.

На экране отобразились сообщения ядра и системных служб, включая данные о версии ядра, параметрах загрузки, BIOS и виртуальной среде.

```
root@haoladar:/home/haoladar# journalctl
Oct 01 18:32:23 haoladar.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-pro)
Oct 01 18:32:23 haoladar.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-provided physical RAM map:
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x000000000100000-0x00000000dfffffff] usable
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x00000000dfffe000-0x00000000dfffffff] ACPI data
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] reserved
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x00000000000fee0000-0x000000000fee00ffff] reserved
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff] usable
Oct 01 18:32:23 haoladar.localdomain kernel: NX (Execute Disable) protection: active
Oct 01 18:32:23 haoladar.localdomain kernel: APIC: Static calls initialized
Oct 01 18:32:23 haoladar.localdomain kernel: SMBIOS 2.5 present.
Oct 01 18:32:23 haoladar.localdomain kernel: DMI: innoteck GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01
Oct 01 18:32:23 haoladar.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 01 18:32:23 haoladar.localdomain kernel: Hypervisor detected: KVM
Oct 01 18:32:23 haoladar.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 01 18:32:23 haoladar.localdomain kernel: kvm-clock: using sched offset of 4355093733 cycles
Oct 01 18:32:23 haoladar.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffffff max_cycles: 0xffffffff
Oct 01 18:32:23 haoladar.localdomain kernel: tsc: Detected 3187.196 MHz processor
Oct 01 18:32:23 haoladar.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Oct 01 18:32:23 haoladar.localdomain kernel: e820: remove [mem 0x00000000-0x0000ffff] usable
Oct 01 18:32:23 haoladar.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x4000000000
Oct 01 18:32:23 haoladar.localdomain kernel: total RAM covered: 4096M
```

Рис. 3.7: Просмотр системного журнала с момента последней загрузки

2. Для получения подробных сообщений без использования постраничного

вывода была выполнена команда **journalctl -no-pager**, которая вывела весь журнал в непрерывном виде.



```
+ 0x9511a)
105c3c)

03a3d)

+ 0x9511a)
105c3c)

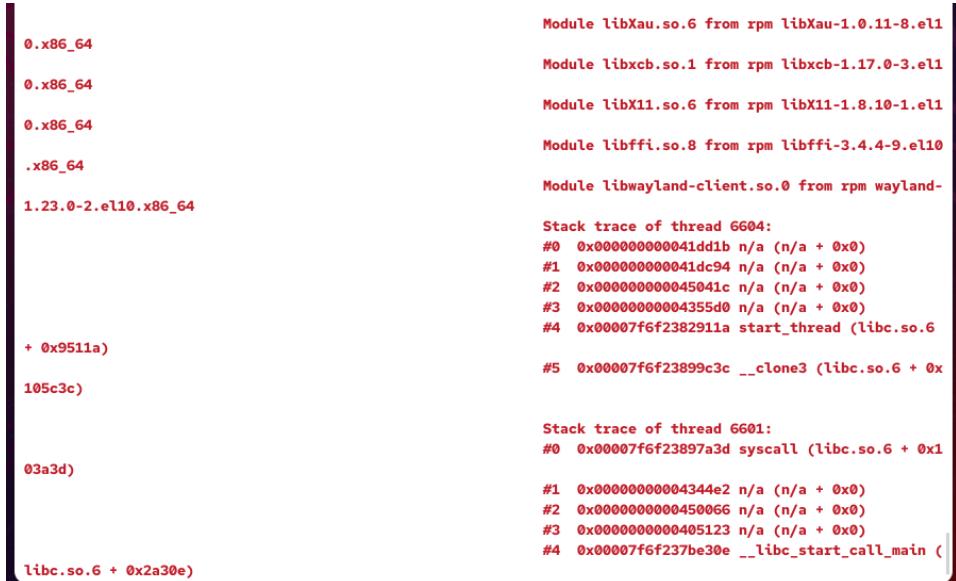
Stack trace of thread 6526:
#0 0x00007f6f23897a3d syscall (libc.so.6 + 0x1
#1 0x00000000004344e2 n/a (n/a + 0x0)
#2 0x0000000000450066 n/a (n/a + 0x0)
#3 0x0000000000416559 n/a (n/a + 0x0)
#4 0x000000000041838a n/a (n/a + 0x0)
#5 0x0000000000417d6a n/a (n/a + 0x0)
#6 0x0000000000404860 n/a (n/a + 0x0)
#7 0x000000000045041c n/a (n/a + 0x0)
#8 0x00000000004355d0 n/a (n/a + 0x0)
#9 0x00007f6f2382911a start_thread (libc.so.6
#10 0x00007f6f23899c3c __clone3 (libc.so.6 + 0x

Stack trace of thread 6524:
#0 0x00007f6f23897a3d syscall (libc.so.6 + 0x1
#1 0x00000000004344e2 n/a (n/a + 0x0)
#2 0x0000000000450066 n/a (n/a + 0x0)
```

Рис. 3.8: Просмотр возможных параметров фильтрации журнала

3. Режим реального времени включался командой **journalctl -f**, что позволило наблюдать новые системные события по мере их появления.

Для выхода использовалось сочетание клавиш **Ctrl + C**.



```
0.x86_64
Module libXau.so.6 from rpm libXau-1.0.11-8.el1
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el1
Module libX11.so.6 from rpm libX11-1.8.10-1.el1
Module libffi.so.8 from rpm libffi-3.4.4-9.el10
Module libwayland-client.so.0 from rpm wayland-
1.23.0-2.el10.x86_64

Stack trace of thread 6604:
#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 0x00007f6f2382911a start_thread (libc.so.6
#5 0x00007f6f23899c3c __clone3 (libc.so.6 + 0x

Stack trace of thread 6601:
#0 0x00007f6f23897a3d syscall (libc.so.6 + 0x1
#1 0x00000000004344e2 n/a (n/a + 0x0)
#2 0x0000000000450066 n/a (n/a + 0x0)
#3 0x0000000000405123 n/a (n/a + 0x0)
#4 0x00007f6f237be30e __libc_start_call_main (libc.so.6 + 0x2a30e)
```

Рис. 3.9: Просмотр возможных параметров фильтрации журнала

4. Для ознакомления с параметрами фильтрации журнала была введена команда **journalctl** с двойным нажатием клавиши **Tab**, после чего на экран был выведен перечень всех доступных полей фильтрации: **_UID**, **_PID**, **_SYSTEMD_UNIT**, **_COMM** и другие.

```
root@haoladar:/home/haoladar# journalctl
Display all 128 possibilities? (y or n)
_AUDIT_LOGINUID=          _JOB_TYPE=
_AUDIT_SESSION=           _JOURNAL_NAME=
AVAILABLE=                _JOURNAL_PATH=
AVAILABLE_PRETTY=         _KERNEL_DEVICE=
_BOOT_ID=                 _KERNEL_SUBSYSTEM=
_CAP_EFFECTIVE=          KERNEL_USEC=
_CMDLINE=                 LEADER=
CODE_FILE=                LIMIT=
CODE_FUNC=                LIMIT_PRETTY=
CODE_LINE=                _LINE_BREAK=
_COMM=                   _MACHINE_ID=
CONFIG_FILE=              MAX_USE=
CONFIG_LINE=              MAX_USE_PRETTY=
COREDUMP_CGROUP=          MEMORY_PEAK=
COREDUMP_CMDLINE=         MEMORY_SWAP_PEAK=
COREDUMP_COMM=            MESSAGE=
COREDUMP_CWD=              MESSAGE_ID=
COREDUMP_ENVIRON=          NM_DEVICE=
COREDUMP_EXE=              NM_LOG_DOMAINS=
COREDUMP_FILENAME=         NM_LOG_LEVEL=
COREDUMP_GID=              _PID=
COREDUMP_HOSTNAME=        PODMAN_EVENT=
```

Рис. 3.10: Просмотр возможных параметров фильтрации журнала

5. С помощью команды ****journalctl _UID=0**** были отображены события, относящиеся к пользователю с идентификатором **UID 0 (root)**.

```

JOB_RESULT=                               USER_UNIT=
root@haoladar:/home/haoladar# journalctl _UID=0
Oct 01 18:32:23 haoladar.localdomain systemd-journald[282]: Collecting audit messages is disabled.
Oct 01 18:32:23 haoladar.localdomain systemd-journald[282]: Journal started
Oct 01 18:32:23 haoladar.localdomain systemd-journald[282]: Runtime Journal (/run/log/journal/680b0151ac144)
Oct 01 18:32:23 haoladar.localdomain systemd-modules-load[283]: Module 'msr' is built in
Oct 01 18:32:23 haoladar.localdomain systemd-modules-load[283]: Inserted module 'fuse'
Oct 01 18:32:23 haoladar.localdomain systemd-modules-load[283]: Module 'scsi_dh_ahua' is built in
Oct 01 18:32:23 haoladar.localdomain systemd-modules-load[283]: Module 'scsi_dh_emc' is built in
Oct 01 18:32:23 haoladar.localdomain systemd-modules-load[283]: Module 'scsi_dh_rdac' is built in
Oct 01 18:32:23 haoladar.localdomain systemd[1]: Finished systemd-modules-load.service - Load Kernel Modules
Oct 01 18:32:23 haoladar.localdomain systemd[1]: Starting systemd-sysctl.service - Apply Kernel Variables...
Oct 01 18:32:23 haoladar.localdomain systemd[1]: Starting systemd-sysusers.service - Create System Users...
Oct 01 18:32:23 haoladar.localdomain systemd[299]: Creating group 'nobody' with GID 65534.
Oct 01 18:32:23 haoladar.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variables.
Oct 01 18:32:23 haoladar.localdomain systemd-sysusers[299]: Creating group 'users' with GID 100.
Oct 01 18:32:23 haoladar.localdomain systemd-sysusers[299]: Creating group 'systemd-journal' with GID 190.
Oct 01 18:32:23 haoladar.localdomain systemd[1]: Finished systemd-sysusers.service - Create System Users.
Oct 01 18:32:23 haoladar.localdomain systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create Static...
Oct 01 18:32:24 haoladar.localdomain systemd[1]: Finished systemd-vconsole-setup.service - Virtual Console...
Oct 01 18:32:24 haoladar.localdomain systemd[1]: dracut-cmdline-ask.service - dracut ask for additional cmd...
Oct 01 18:32:24 haoladar.localdomain dracut-cmdline[310]: dracut-105.4.el10_0
Oct 01 18:32:24 haoladar.localdomain dracut-cmdline[310]: Using kernel command line parameters:   BOOT_IMA

```

Рис. 3.11: Отображение событий, связанных с пользователем root

- Для просмотра последних двадцати строк системного журнала использовалась команда **journalctl -n 20**, которая вывела актуальные системные события, включая сообщения о работе ядра и процессах.

```

root@haoladar:/home/haoladar# journalctl -n 20
Oct 01 18:54:37 haoladar.localdomain kernel: traps: VBoxClient[7000] trap int3 ip:41dd1b sp:7f6f15188cd0 err:0
Oct 01 18:54:37 haoladar.localdomain systemd-coredump[7001]: Process 6997 (VBoxClient) of user 1000 terminated
Oct 01 18:54:37 haoladar.localdomain systemd[1]: Started systemd-coredump@228-7001-0.service - Process Core...
Oct 01 18:54:38 haoladar.localdomain systemd-coredump[7002]: [!] Process 6997 (VBoxClient) of user 1000 dumped core

Module libXau.so.6 from rpm libXau-1.0.11-8.el7
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el7
Module libXi.so.6 from rpm libXi-1.8.10-1.el7
Module libffi.so.8 from rpm libffi-3.4.4-9.el7
Module libwayland-client.so.0 from rpm wayland-client-1.15.0-1.el7
Stack trace of thread 7000:
#0 0x00000000041dd1b 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 0x00007fcf2382911a start_thread (libc.so.6 + 0x7f6f15188cd0)
#5 0x00007fcf23899c3c __clone3 (libc.so.6 + 0x7f6f15188cd0)

Stack trace of thread 6997:
#0 0x00007fcf23897a3d syscall (libc.so.6 + 0x7f6f15188cd0)
#1 0x00000000004344e2 n/a (n/a + 0x0)
#2 0x0000000000450066 n/a (n/a + 0x0)

```

Рис. 3.12: Просмотр последних 20 строк журнала

- Для отображения только сообщений об ошибках была введена команда **journalctl -p err**, которая вывела ошибки, зарегистрированные различными службами, включая **vmwgfx**, **alsa**, **gdm-password** и **systemd**.

```

root@haoladar:/home/haoladar# journalctl -p err
Oct 01 18:32:24 haoladar.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running
Oct 01 18:32:24 haoladar.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely to cause problems
Oct 01 18:32:24 haoladar.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported configuration
Oct 01 18:32:27 haoladar.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Oct 01 18:32:28 haoladar.localdomain alsactl[931]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to open file
Oct 01 18:32:28 haoladar.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Oct 01 18:35:07 haoladar.localdomain gdm-password[1974]: gkr-pam: unable to locate daemon control file
Oct 01 18:35:10 haoladar.localdomain systemd[1986]: Failed to start app-gnome-gnome\x2dkeyring\x2dpkcs11-20
Oct 01 18:35:10 haoladar.localdomain systemd[1986]: Failed to start app-gnome-gnome\x2dkeyring\x2dsecrets-2
Oct 01 18:35:10 haoladar.localdomain systemd[1986]: Failed to start app-gnome-xdg\x2duser\x2ddirs-2111.scop
Oct 01 18:35:11 haoladar.localdomain systemd-coredump[2819]: [.] Process 2796 (VBoxClient) of user 1000 dumped core
                                                Module libXau.so.6 from rpm libXau-1.0.11-8.el7
                                                Module libxcb.so.1 from rpm libxcb-1.17.0-3.el7
                                                Module libXi.so.6 from rpm libXi-1.8.10-1.el7
                                                Module libffi.so.8 from rpm libffi-3.4.4-9.el7
                                                Module libwayland-client.so.0 from rpm wayland-1.18.0-1.el7
                                                Stack trace of thread 2800:
                                                #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 0x000007f6f2382911a start_thread (libc.so.6)
                                                #5 0x000007f6f23899c3c __clone3 (libc.so.6 + 0)

                                                Stack trace of thread 2799:

```

Рис. 3.13: Просмотр сообщений уровня ошибок

8. Для вывода всех сообщений со вчерашнего дня использовалась команда **journalctl –since yesterday**.

В журнале отобразились все события, начиная с момента последней загрузки системы.

```

root@haoladar:/home/haoladar#
root@haoladar:/home/haoladar# journalctl --since yesterday
Oct 01 18:32:23 haoladar.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod)
Oct 01 18:32:23 haoladar.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el7
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-provided physical RAM map:
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000009fbff] usable
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff] reserved
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x000000000000ffff] reserved
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x000000000100000-0x0000000000ffff] usable
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x000000000dff0000-0x000000000dffffff] ACPI data
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] reserved
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee0ffff] reserved
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x0000000010000000-0x0000000011fffffff] usable
Oct 01 18:32:23 haoladar.localdomain kernel: NX (Execute Disable) protection: active
Oct 01 18:32:23 haoladar.localdomain kernel: APIC: Static calls initialized
Oct 01 18:32:23 haoladar.localdomain kernel: SMBIOS 2.5 present.
Oct 01 18:32:23 haoladar.localdomain kernel: DMI: innotech GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01
Oct 01 18:32:23 haoladar.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 01 18:32:23 haoladar.localdomain kernel: Hypervisor detected: KVM
Oct 01 18:32:23 haoladar.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 01 18:32:23 haoladar.localdomain kernel: kvm-clock: using sched offset of 4355093733 cycles
Oct 01 18:32:23 haoladar.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffff max_cycles: 0xffffffff
Oct 01 18:32:23 haoladar.localdomain kernel: tsc: Detected 3187.196 MHz processor
Oct 01 18:32:23 haoladar.localdomain kernel: e820: update [mem 0x00000000-0x000fffff] usable ==> reserved
Oct 01 18:32:23 haoladar.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Oct 01 18:32:23 haoladar.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 01 18:32:23 haoladar.localdomain kernel: total RAM covered= 400GM

```

Рис. 3.14: Просмотр сообщений со вчерашнего дня

9. Для фильтрации сообщений уровня ошибок, зафиксированных со вчераш-

него дня, применена команда **journalctl -since yesterday -p err**.

На экране появились только сообщения с приоритетом «error» за заданный период.

Рис. 3.15: Просмотр сообщений об ошибках со вчерашнего дня

10. Для детализированного вывода информации о записях журнала была использована команда **journalctl -o verbose**, которая показала дополнительные поля: идентификаторы процессов, время загрузки, имена модулей и приоритет сообщений.
 11. Для анализа работы службы **sshd** была введена команда ****journalctl _SYSTEMD_UNIT=sshd.service****. В результате отобразились сообщения о запуске службы SSH и активации прослушивания порта 22 на всех интерфейсах.

```

_HOSTNAME=haoladar.localdomain
_RUNTIME_SCOPE=initrd
Wed 2025-10-01 18:32:23.769044 MSK [s=e4b896883f2e432dbf118504c42f13fb; i=2; b=0d27ca7ce57e47c8855449e2347256]
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=0d27ca7ce57e47c8855449e23472568
_MACHINE_ID=680b0151ac144c679386de82018881d0
_HOSTNAME=haoladar.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_vb
Wed 2025-10-01 18:32:23.769054 MSK [s=e4b896883f2e432dbf118504c42f13fb; i=3; b=0d27ca7ce57e47c8855449e2347256]
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
root@haoladar:/home/haoladar# journalctl _SYSTEMD_UNIT=sshd.service
Oct 01 18:32:28 haoladar.localdomain (sshd)[1195]: sshd.service: Referenced but unset environment variable
Oct 01 18:32:28 haoladar.localdomain sshd[1195]: Server listening on 0.0.0.0 port 22.
Oct 01 18:32:28 haoladar.localdomain sshd[1195]: Server listening on :: port 22.
root@haoladar:/home/haoladar#

```

Рис. 3.16: Просмотр журнала службы SSH

3.3 Постоянный журнал **journald**

1. По умолчанию служба **systemd-journald** хранит свои журналы во временном каталоге **/run/log/journal**,
поэтому записи теряются после перезагрузки системы.
Для обеспечения постоянного хранения логов был создан каталог
/var/log/journal командой
mkdir -p /var/log/journal.
2. Далее были установлены корректные права доступа, позволяющие службе journald записывать данные в данный каталог:
 - **chown root:systemd-journal /var/log/journal** – назначает владельцем каталог root и группу systemd-journal;
 - **chmod 2755 /var/log/journal** – задаёт права доступа, обеспечивающие корректную работу службы при записи логов.
3. После изменения параметров доступа служба journald была уведомлена о необходимости обновить конфигурацию

без полной перезагрузки системы с помощью команды **killall -USR1 systemd-journald**.

4. Для проверки работоспособности постоянного хранения логов была выполнена команда **journalctl -b**, которая вывела сообщения системного журнала, начиная с момента последней загрузки.
- В выводе отображается информация о версии ядра, загрузочных параметрах и аппаратной конфигурации.

```
root@haoladar:/home/haoladar# 
root@haoladar:/home/haoladar# mkdir -p /var/log/journal
root@haoladar:/home/haoladar# chown root:systemd-journal /var/log/journal/
root@haoladar:/home/haoladar# chmod 2755 /var/log/journal/
root@haoladar:/home/haoladar# killall -USR1 systemd-journald
root@haoladar:/home/haoladar# journalctl -b
Oct 01 18:32:23 haoladar.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-pro)
Oct 01 18:32:23 haoladar.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-provided physical RAM map:
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x00000000009ffff] reserved
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x0000000000f0000-0x0000000000ffff] reserved
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x000000000100000-0x00000000dfffeffff] usable
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x000000000fff0000-0x000000000fffffeffff] ACPI data
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000fffffc0000] reserved
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x0000000010000000-0x0000000011fffffc0000] usable
Oct 01 18:32:23 haoladar.localdomain kernel: NX (Execute Disable) protection: active
Oct 01 18:32:23 haoladar.localdomain kernel: APIC: Static calls initialized
Oct 01 18:32:23 haoladar.localdomain kernel: SMBIOS 2.5 present.
Oct 01 18:32:23 haoladar.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01
Oct 01 18:32:23 haoladar.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 01 18:32:23 haoladar.localdomain kernel: Hypervisor detected: KVM
Oct 01 18:32:23 haoladar.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
```

Рис. 3.17: Настройка постоянного хранения системного журнала journald

4 Контрольные вопросы

1. Какой файл используется для настройки rsyslogd?

Основной файл конфигурации службы – **/etc/rsyslog.conf**.

Дополнительные файлы с расширением **.conf** могут находиться в каталоге **/etc/rsyslog.d/**.

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

Сообщения, относящиеся к аутентификации пользователей, хранятся в файле **/var/log/secure**.

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

По умолчанию ротация логов выполняется **еженедельно**, что задаётся в файле **/etc/logrotate.conf** директивой **weekly**.

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

Необходимо добавить строку:

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

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

Для просмотра журнала в реальном времени используется команда:

journalctl -f

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

Команда имеет вид:

****journalctl _PID=1 –since “09:00” –until “15:00”****

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

Для этого используется команда:

journalctl -b

8. Какая процедура позволяет сделать журнал journald постоянным?

- Создать каталог **/var/log/journal** командой **mkdir -p /var/log/journal**
- Назначить права и владельца:
chown root:systemd-journal /var/log/journal
chmod 2755 /var/log/journal
- Применить изменения командой **killall -USR1 systemd-journald**
После этого журнал **journald** станет постоянным и будет сохраняться между перезагрузками системы.

5 Заключение

В ходе работы освоены приёмы администрирования системных журналов в Linux.

Настроено постоянное хранение логов **journald**, изучены методы фильтрации и просмотра сообщений с помощью **journalctl** и **rsyslog**, а также способы регистрации и анализа системных событий в реальном времени.