

Лабораторная работа №7

Управление журналами событий в системе

Шаханеоядж Хаоладар

5 октября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Основная цель

Получить навыки работы с журналами мониторинга событий и управления системными логами в Linux.

Ход выполнения работы

Мониторинг системных событий

```
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+bb000]
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 0x00000
00000450041c 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
3479:#012#0 0x00007f6f23897a3d syscall (libc.so.6 + 0x103a3d)#012#1 0x00000000004344e2 n/a (n/a + 0x0)#0
12#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+bb000]
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@17-3497-0.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. 1: Мониторинг системных событий в реальном времени

Мониторинг системных событий

```
Oct 1 18:39:17 haoladar systemd[1]: Started systemd-coredump@49-3856-0.service - Process Core Dump (PID 3856/UID 0).
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 VBoxClient[1dd1b,400000+bb000]
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#012Module libXau.so.6 from rom libXau-1.0.11-8.e110.x86_64#012Module libXch.so.1 from rom libXch-1.17.0-3.e110.
```

Рис. 2: Ошибка при попытке входа с неверным паролем

Мониторинг системных событий

```
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 0x0000000000041dd1b n/a (n/a + 0x0)#012#1 0x0000000000041dc94 n/a (n/a + 0x0)#012#2 0x0000000045041c n/a (n/a + 0x0)#012#3 0x000000000004355d0 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 0x000000000004344e2 n/a (n/a + 0x0)#012#2 0x00000000000450066 n/a (n/a + 0x0)#012#3 0x00000000000405123 n/a (n/a + 0x0)#012#4 0x00007f6f237be30e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x00007f6f237be3c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x000000000004044aa 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. 3: Сообщение logger hello в системном журнале

Мониторинг системных событий

```
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 op
ened 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(u
id=1000) by haoladar(uid=0)
Oct  1 18:35:07 haoladar gdm-password][1974]: pam_unix(gdm-password:session): session opened for user haolad
ar(uid=1000) by haoladar(uid=0)
Oct  1 18:35:07 haoladar gdm-password][1974]: gkr-pam: gnome-keyring-daemon started properly and unlocked ke
yring
Oct  1 18:35:11 haoladar gdm-launch-environment][1240]: pam_unix(gdm-launch-environment:session): session cl
osed 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
```

Рис. 4: Журнал безопасности /var/log/secure

Настройка rsyslog

```
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

apr-util-1.6.3-21.el10.x86_64
apr-util-openssl-1.6.3-21.el10.x86_64
httpd-core-2.4.63-1.el10_0.2.x86_64
httpd-tools-2.4.63-1.el10_0.2.x86_64
mod_lua-2.4.63-1.el10_0.2.x86_64

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. 5: Установка и запуск службы httpd

Настройка rsyslog

```
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] [lbmethod_heartbeat:notice] [pid 4405:tid 4405] AH02282: No slotmem from mod_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. 6: Журнал ошибок Apache

Настройка rsyslog

```
#  
# 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
```

1Help 2Save 3Mark 4Replace 5Copy 6Move 7Search 8Delete 9PullDown

Рис. 7: Добавление строки ErrorLog syslog:local1 в конфигурацию httpd

Настройка rsyslog

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

Рис. 8: Создание файла конфигурации rsyslog для httpd

Настройка rsyslog

```
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. 9: Создание файла debug.conf для регистрации отладочных сообщений

Настройка rsyslog

```
a 0x000:0#012#0 0x00000/T0TZ589/a#d syscall { libc.so.6 + 0x102a5d}#012#1 0x00000000004344e2 n/a (n/a + 0x0)##0
12#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 0x0000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Oct 1 18:49:35 haoladar systemd[1]: systemd-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 VBox
Client[1dd1b,400000+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 systemd-coredump@170-6316-0.service - Process Core Dump (PID 63
16/UID 0).
Oct 1 18:49:40 haoladar systemd-coredump[6317]: Process 6312 (VBoxClient) of user 1000 dumped core.#012#012
Module libXau.so.6 from rom libXau-1.0.11-8.el10.x86 64#012Module libxcb.so.1 from rom libxcb-1.17.0-3.el10.
```

Рис. 10: Отображение отладочного сообщения в системном журнале

Использование journalctl

```
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 0x00000000000100000-0x000000000dffeffff] usable
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x00000000dff0000-0x00000000dfffffff] 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 0x00000000ffc0000-0x00000000fffffff] 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: 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
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: 0xffffffffffffffff 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 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: 4096M
```

Рис. 11: Просмотр системного журнала с момента последней загрузки

Использование journalctl

```
+ 0x9511a)
105c3c)

03a3d)

+ 0x9511a)
105c3c)

03a3d)

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. 12: Просмотр возможных параметров фильтрации журнала

Использование journalctl

Рис. 13: Просмотр последних 20 строк журнала

Использование journalctl

```
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 driver
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 libX11.so.6 from rpm libX11-1.8.10-1.el7
                                                Module libffi.so.8 from rpm libffi-3.4.4-9.el7
                                                Module libwayland-client.so.0 from rpm wayland-1.16.0-1.el7
                                                Stack trace of thread 2800:
                                                #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 0x00007f6f2382911a start_thread (libc.so.6+0x2f4)
                                                #5 0x00007f6f23899c3c __clone3 (libc.so.6+0x2f4)

                                                Stack trace of thread 2799:
```

Рис. 14: Просмотр сообщений уровня ошибок

Использование journalctl

```
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-pro)  
Oct 01 18:32:23 haoladar.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0 root=UUID=4f3a23d0-0001-43e0-83c0-000000000000 ro  
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-provided physical RAM map:  
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbff] 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 0x000000000000f0000-0x000000000000ffff] reserved  
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x00000000000100000-0x000000000dffeffff] usable  
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x00000000dffff000-0x00000000dfffffff] ACPI da  
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 0x00000000fffc0000-0x00000000fffffff] reserved  
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x00000000100000000-0x0000000011fffffff] 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: 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  
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: 0xfffffffffffffff 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 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: 4096M
```

Рис. 15: Просмотр сообщений со вчерашнего дня

Использование journalctl

```
root@haoladar:/home/haoladar# journalctl --since yesterday -p err
Oct 01 18:32:24 haoladar.localdomain kernel: vmmwgfx 0000:00:02.0: [drm] *ERROR* vmmwgfx seems to be running
Oct 01 18:32:24 haoladar.localdomain kernel: vmmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely
Oct 01 18:32:24 haoladar.localdomain kernel: vmmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported
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: fail
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 dum
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 libX11.so.6 from rpm libX11-1.8.10-1.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 0x0000000000041dc94 n/a (n/a + 0x0)
#2 0x000000000045041c n/a (n/a + 0x0)
#3 0x00000000004355d0 n/a (n/a + 0x0)
```

Рис. 16: Просмотр сообщений об ошибках со вчерашнего дня

Использование journalctl

```
_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=0d27ca7ce57e47c8855449e23472568a
_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/rl_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. 17: Просмотр журнала службы SSH

Постоянный журнал journald

```
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.el1
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 0x00000000000f0000-0x000000000000ffff] reserved
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x000000000100000-0x00000000dffeffff] usable
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x00000000dfff0000-0x00000000dfffffff] ACPI da
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 0x00000000ffc00000-0x000000000fffffff] 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: 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 19:22:22 haoladar.localdomain kernel: kum_clock: Using mrcs 4b564d01 and 4b564d00
```

Рис. 18: Настройка постоянного хранения системного журнала journald

Итоги работы

Вывод

- Изучена работа с **rsyslog** и **systemd-journald**
- Настроено постоянное хранение логов
- Освоен мониторинг и фильтрация событий через **journalctl**
- Получены навыки анализа системных сообщений Linux