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 abnormall
y with signal 5/TRAP, processing...
Oct  1 18:36:33 haoladar systemd[1]: Started systemd-coredump@16-3483-0.service - Process Core Dump (PID 348
3/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 libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Module libffi.so.8 from rpm libffi-3.4.
4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thr
ead 3482:#012#0  0x000000000041dd1b n/a (n/a + 0x0)#012#1  0x000000000041dc94 n/a (n/a + 0x0)#012#2  0x00000
0000045041c 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 threa
d 3479:#012#0  0x00007f6f23897a3d syscall (libc.so.6 + 0x103a3d)#012#1  0x000000000004344e2 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_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 18:36:33 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 abnormall
y with signal 5/TRAP, processing...
Oct  1 18:36:38 haoladar systemd[1]: Started systemd-coredump@17-3497-0.service - Process Core Dump (PID 349
7/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

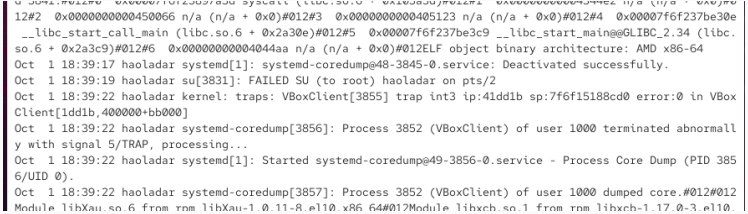

Рис. 2: Ошибка при попытке входа с неверным паролем

Рис. 3: Сообщение logger hello в системном журнале

Мониторинг системных событий

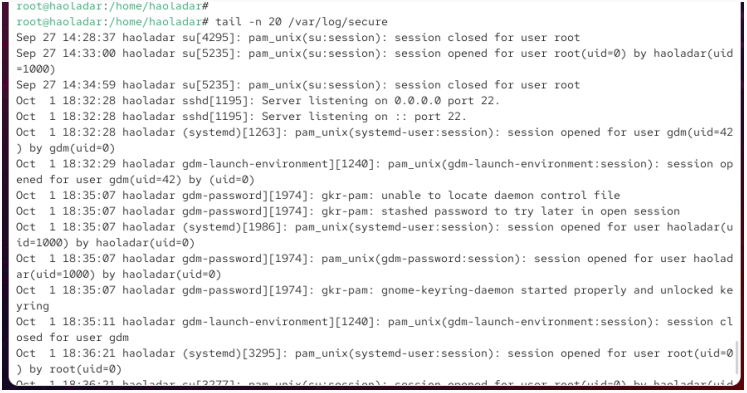

Рис. 4: Журнал безопасности /var/log/secure

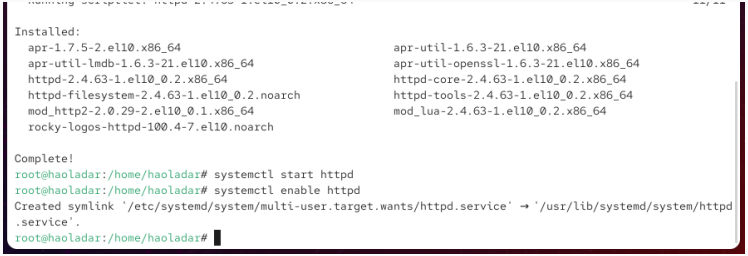

Рис. 5: Установка и запуск службы httpd

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 (wra
pper: /usr/sbin/suexec)
[Wed Oct 01 18:41:42.078182 2025] [lbmethod_heartbeat:notice] [pid 4405:tid 4405] AH02282: No slotmem from m
od_heartmonitor
[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

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

Настройка rsyslog

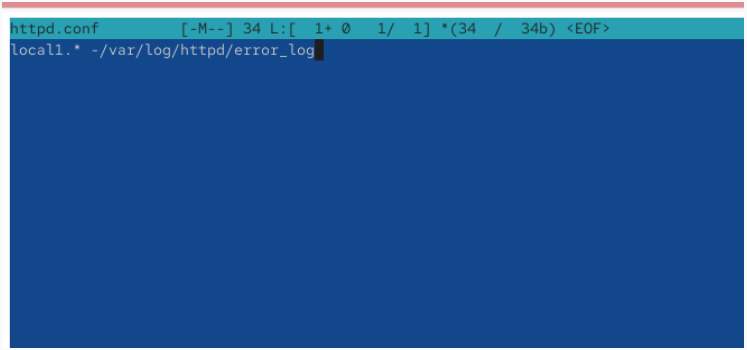

Рис. 8: Создание файла конфигурации rsyslog для httpd

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

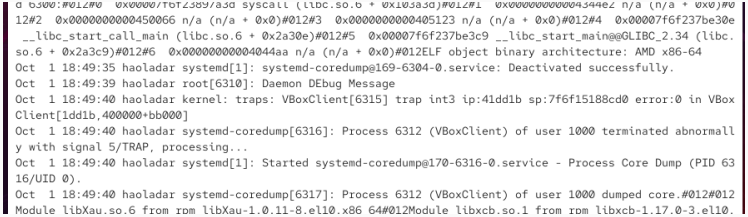

Рис. 10: Отображение отладочного сообщения в системном журнале

Использование journalctl

Рис. 11: Просмотр системного журнала с момента последней загрузки

Использование journalctl

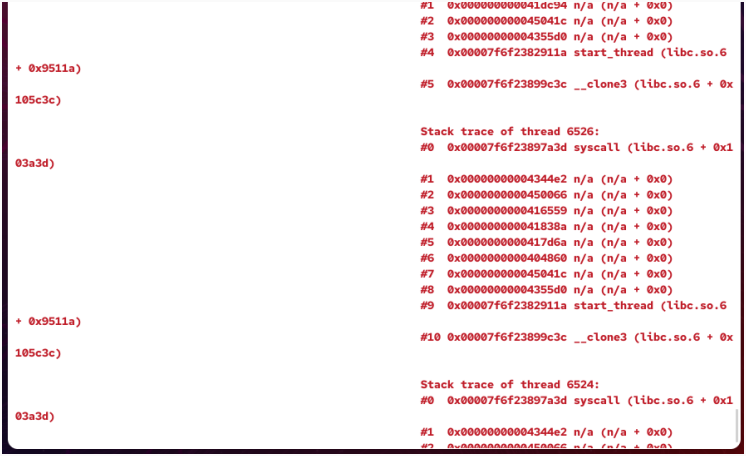

Рис. 12: Просмотр возможных параметров фильтрации журнала

Использование journalctl

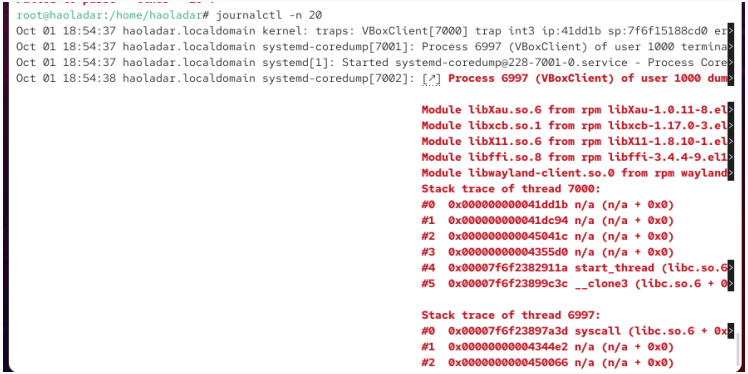

Рис. 13: Просмотр последних 20 строк журнала

Использование journalctl

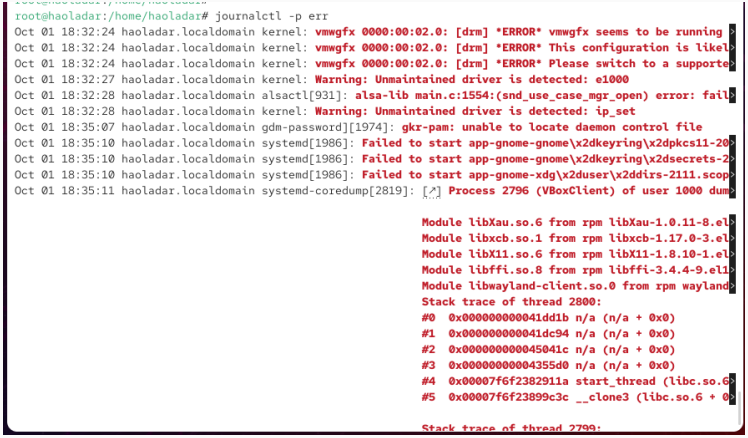

Рис. 14: Просмотр сообщений уровня ошибок

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.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 0x00000000000f0000-0x00000000000fffff] reserved
Oct 01 18:32:23 haoladar.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dffeffff] 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 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: 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: 0
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

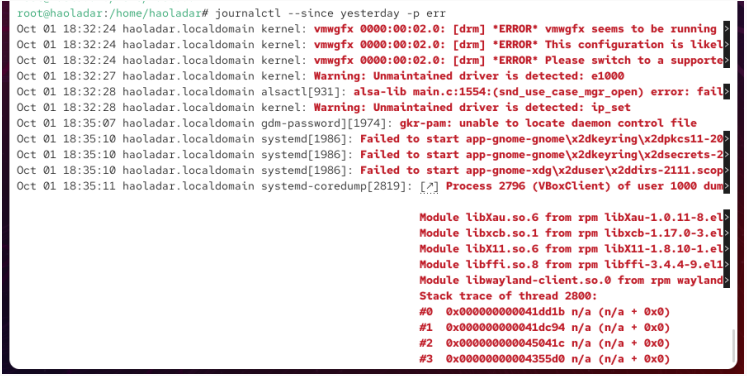

Рис. 16: Просмотр сообщений об ошибках со вчерашнего дня

Использование journalctl

Рис. 17: Просмотр журнала службы SSH

Постоянный журнал journald

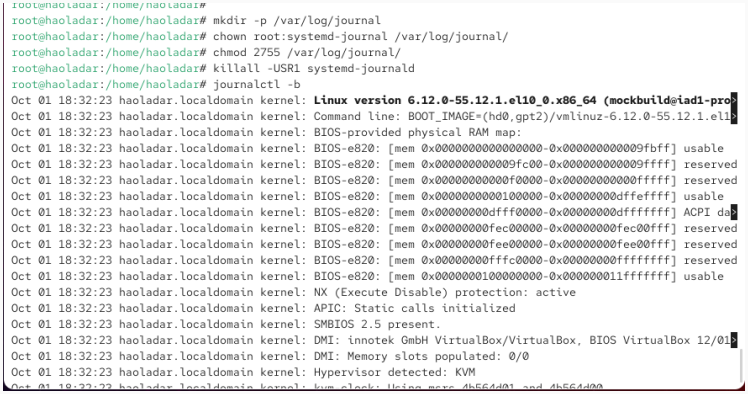

Рис. 18: Настройка постоянного хранения системного журнала journald

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