

Презентация по лабораторной работе №7

Управление журналами событий в системе

Анна Саенко

3 октября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Получить навыки работы с журналами мониторинга различных событий в системе Linux.

- 1 Настроить мониторинг системных событий в реальном времени
- 2 Изменить правила конфигурации `rsyslog.conf`
- 3 Организовать отдельные журналы для ошибок и отладочных сообщений
- 4 Использовать инструмент `journalctl` для анализа журналов
- 5 Сделать хранение журнала `journald` постоянным

Ход выполнения работы

Мониторинг системных событий

```
root@aasaenko:/home/aasaenko# tail -f /var/log/messages
Sep 30 18:46:59 aasaenko kernel: traps: VBoxClient[3750] trap int3 ip:41dd1b sp:7f8584afbcd0 error:0 in VBoxClient[1dd1b,400000+bb000]
Sep 30 18:46:59 aasaenko systemd-coredump[3751]: Process 3747 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Sep 30 18:46:59 aasaenko systemd[1]: Started systemd-coredump@40-3751-0.service - Process Core Dump (PID 3751/UID 0).
Sep 30 18:46:59 aasaenko systemd-coredump[3752]: Process 3747 (VBoxClient) of user 1000 dumped core.#012#012Module 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 thread 3750:#012#0 0x00000000041dd1b n/a (n/a + 0x0)#012#1 0x00000000041dc94 n/a (n/a + 0x0)#012#2 0x00000000045041c n/a (n/a + 0x0)#012#3 0x0000000004355d0 n/a (n/a + 0x0)#012#4 0x00007f85931a211a start_thread (libc.so.6 + 0x9511a)#012#5 0x00007f8593212c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 3747:#012#0 0x00007f8593210a3d syscall (libc.so.6 + 0x103a3d)#012#1 0x0000000004344e2 n/a (n/a + 0x0)#012#2 0x000000000450066 n/a (n/a + 0x0)#012#3 0x000000000405123 n/a (n/a + 0x0)#012#4 0x00007f859313730e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x00007f85931373c9 __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
Sep 30 18:46:59 aasaenko systemd[1]: systemd-coredump@40-3751-0.service: Deactivated successfully.
Sep 30 18:47:04 aasaenko kernel: traps: VBoxClient[3763] trap int3 ip:41dd1b sp:7f8584afbcd0 error:0 in VBoxClient[1dd1b,400000+bb000]
Sep 30 18:47:04 aasaenko systemd-coredump[3764]: Process 3760 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Sep 30 18:47:04 aasaenko systemd[1]: Started systemd-coredump@41-3764-0.service - Process Core Dump (PID 3764/UID 0).
Sep 30 18:47:04 aasaenko systemd-coredump[3765]: Process 3760 (VBoxClient) of user 1000 dumped core.#012#012Module 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 thread 3763:#012#0 0x00000000041dd1b n/a (n/a + 0x0)#012#1 0x00000000041dc94 n/a (n/a + 0x0)#012#2 0x000000000
```

Рис. 1: Мониторинг системных сообщений в реальном времени

Ошибка при вводе неверного пароля

```
00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Sep 30 18:47:30 aasaenko systemd[1]: systemd-coredump@46-3831-0.service: Deactivated successfully.
Sep 30 18:47:30 aasaenko su[3817]: FAILED SU (to root) aasaenko on pts/2
Sep 30 18:47:35 aasaenko kernel: traps: VBoxClient[3841] trap int3 ip:41dd1b sp:7f8584afbcd0 error:0 in VBoxC
lient[1dd1b,400000+bb000]
Sep 30 18:47:35 aasaenko systemd-coredump[3842]: Process 3838 (VBoxClient) of user 1000 terminated abnormally
with signal 5/TRAP, processing...
Sep 30 18:47:35 aasaenko systemd[1]: Started systemd-coredump@47-3842-0.service - Process Core Dump (PID 3842
/UID 0).
```

Рис. 2: Ошибка при вводе неверного пароля

```
-----  
tart_call_main (libc.so.6 + 0x2a30e)#012#5  0x00007f85931373c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2  
a3c9)#012#6  0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64  
Sep 30 18:47:50 aasaenko systemd[1]: systemd-coredump@50-3872-0.service: Deactivated successfully.  
Sep 30 18:47:54 aasaenko aasaenko[3878]: hello  
Sep 30 18:47:55 aasaenko kernel: traps: VBoxClient[3886] trap int3 ip:41dd1b sp:7f8584afbcd0 error:0 in VBoxC  
lient[1dd1b,400000+bb000]  
Sep 30 18:47:55 aasaenko systemd-coredump[3887]: Process 3883 (VBoxClient) of user 1000 terminated abnormally  
with signal 5/TRAP, processing...  
Sep 30 18:47:55 aasaenko systemd[1]: Started systemd-coredump@51-3887-0.service - Process Core Dump (PID 3887  
/UID 0).
```

Рис. 3: Регистрируемое сообщение hello


```
root@aasaenko:/home/aasaenko# tail -n 20 /var/log/secure
Sep 25 11:07:51 aasaenko su[4426]: pam_unix(su:session): session opened for user root(uid=0) by aasaenko(uid=1000)
Sep 25 11:12:32 aasaenko su[4426]: pam_unix(su:session): session closed for user root
Sep 25 11:12:39 aasaenko su[5190]: pam_unix(su:session): session opened for user root(uid=0) by aasaenko(uid=1000)
Sep 30 18:42:46 aasaenko sshd[1184]: Server listening on 0.0.0.0 port 22.
Sep 30 18:42:46 aasaenko sshd[1184]: Server listening on :: port 22.
Sep 30 18:42:46 aasaenko (systemd)[1249]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)
Sep 30 18:42:46 aasaenko gdm-launch-environment[1228]: pam_unix(gdm-launch-environment:session): session opened for use
r gdm(uid=42) by (uid=0)
Sep 30 18:43:30 aasaenko gdm-password[1990]: gkr-pam: unable to locate daemon control file
Sep 30 18:43:30 aasaenko gdm-password[1990]: gkr-pam: stashed password to try later in open session
Sep 30 18:43:30 aasaenko (systemd)[2001]: pam_unix(systemd-user:session): session opened for user aasaenko(uid=1000) by
aasaenko(uid=0)
Sep 30 18:43:30 aasaenko gdm-password[1990]: pam_unix(gdm-password:session): session opened for user aasaenko(uid=1000)
by aasaenko(uid=0)
Sep 30 18:43:30 aasaenko gdm-password[1990]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Sep 30 18:43:35 aasaenko gdm-launch-environment[1228]: pam_unix(gdm-launch-environment:session): session closed for use
r gdm
Sep 30 18:46:13 aasaenko (systemd)[3509]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(ui
d=0)
Sep 30 18:46:13 aasaenko su[3484]: pam_unix(su:session): session opened for user root(uid=0) by aasaenko(uid=1000)
Sep 30 18:46:18 aasaenko su[3582]: pam_unix(su:session): session opened for user root(uid=0) by aasaenko(uid=1000)
Sep 30 18:46:23 aasaenko su[3643]: pam_unix(su:session): session opened for user root(uid=0) by aasaenko(uid=1000)
Sep 30 18:47:25 aasaenko su[3643]: pam_unix(su:session): session closed for user root
Sep 30 18:47:28 aasaenko unix_chkpwd[3826]: password check failed for user (root)
Sep 30 18:47:28 aasaenko su[3817]: pam_unix(su:auth): authentication failure; logname=aasaenko uid=1000 euid=0 tty=/dev/
pts/2 ruser=aasaenko rhost= user=root
root@aasaenko:/home/aasaenko#
```

120 x 33

Рис. 4: Просмотр файла secure

Установка и запуск httpd

```
Installed:
  apr-1.7.5-2.el10.x86_64          apr-util-1.6.3-21.el10.x86_64      apr-util-ldap-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@aasaenko:/home/aasaenko# systemctl start httpd
root@aasaenko:/home/aasaenko# systemctl enable httpd
Created symlink '/etc/systemd/system/multi-user.target.wants/httpd.service' → '/usr/lib/systemd/system/httpd.service'.
root@aasaenko:/home/aasaenko#
```

Рис. 5: Установка и запуск httpd

```
root@aasaenko:/home/aasaenko#  
root@aasaenko:/home/aasaenko# tail -f /var/log/httpd/error_log  
[Tue Sep 30 18:52:57.720801 2025] [suexec:notice] [pid 4869:tid 4869] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)  
[Tue Sep 30 18:52:57.770333 2025] [lbmethod_heartbeat:notice] [pid 4869:tid 4869] AH02282: No slotmem from mod_heartmonitor  
[Tue Sep 30 18:52:57.771160 2025] [systemd:notice] [pid 4869:tid 4869] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0  
[Tue Sep 30 18:52:57.773504 2025] [mpm_event:notice] [pid 4869:tid 4869] AH00489: Apache/2.4.63 (Rocky Linux) configured -- resuming normal operations  
[Tue Sep 30 18:52:57.773518 2025] [core:notice] [pid 4869:tid 4869] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 6: Мониторинг журнала ошибок Apache

Настройка ErrorLog через syslog

```
#  
# 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. 7: Добавление параметра ErrorLog в конфигурацию Apache

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

Рис. 8: Создание правила для перенаправления логов Apache

```
root@aasaenko:/home/aasaenko# mcedit /etc/httpd/conf/httpd.conf

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

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

Рис. 9: Создание правил для отладочного логирования

```
0x0)#012#3 0x00000000000405123 n/a (n/a + 0x0)#012#4 0x0000/r8b9313/30e __libc_start_call_main (libc.so.6 + 0x2a30e)#0
12#5 0x00007f85931373c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x00000000004044aa n/a (n/a + 0x0)#0
12ELF object binary architecture: AMD x86-64
Sep 30 18:58:48 aasaenko systemd[1]: systemd-coredump@179-6544-0.service: Deactivated successfully.
Sep 30 18:58:52 aasaenko root[6550]: Daemon Debug Message
Sep 30 18:58:53 aasaenko kernel: traps: VBoxClient[6555] trap int3 ip:41dd1b sp:7f8584afbcd0 error:0 in VBoxClient[1dd1b
,400000+bb000]
Sep 30 18:58:53 aasaenko systemd-coredump[6556]: Process 6552 (VBoxClient) of user 1000 terminated abnormally with signa
l 5/TRAP, processing...
Sep 30 18:58:53 aasaenko systemd[1]: Started systemd-coredump@180-6556-0.service - Process Core Dump (PID 6556/UID 0).
Sep 30 18:58:53 aasaenko systemd-coredump[6557]: Process 6552 (VBoxClient) of user 1000 dumped core.#012#012Module libXa
```

Рис. 10: Мониторинг и регистрация отладочного сообщения

Просмотр системного журнала

```
root@aasaenko:/home/aasaenko# journalctl
Sep 30 18:42:41 aasaenko.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.b
Sep 30 18:42:41 aasaenko.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_64 ro
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-provided physical RAM map:
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x000000000009f000-0x000000000000ffff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000dfff0000-0x0000000000dfffffff] ACPI data
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000fec00fff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x000000000fee00000-0x000000000fee00fff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x000000000fffc0000-0x000000000ffffffff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x00000000100000000-0x0000000011ffffffff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: NX (Execute Disable) protection: active
Sep 30 18:42:41 aasaenko.localdomain kernel: APIC: Static calls initialized
Sep 30 18:42:41 aasaenko.localdomain kernel: SMBIOS 2.5 present.
Sep 30 18:42:41 aasaenko.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 30 18:42:41 aasaenko.localdomain kernel: DMI: Memory slots populated: 0/0
Sep 30 18:42:41 aasaenko.localdomain kernel: Hypervisor detected: KVM
Sep 30 18:42:41 aasaenko.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Sep 30 18:42:41 aasaenko.localdomain kernel: kvm-clock: using sched offset of 4068452678 cycles
Sep 30 18:42:41 aasaenko.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb
Sep 30 18:42:41 aasaenko.localdomain kernel: tsc: Detected 3187.204 MHz processor
Sep 30 18:42:41 aasaenko.localdomain kernel: e820: update [mem 0x000000000-0x000000fff] usable ==> reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: e820: remove [mem 0x0000a0000-0x0000fffff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Sep 30 18:42:41 aasaenko.localdomain kernel: total RAM covered: 4096M
Sep 30 18:42:41 aasaenko.localdomain kernel: Found optimal setting for mtrr clean up
Sep 30 18:42:41 aasaenko.localdomain kernel: gran_size: 64K chunk_size: 1G num_reg: 3 lose co
Sep 30 18:42:41 aasaenko.localdomain kernel: MTRR map: 6 entries (3 fixed + 3 variable; max 35), built from 16 variables
Sep 30 18:42:41 aasaenko.localdomain kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
```

Рис. 11: Просмотр журнала событий

Вывод журнала без пейджера

```
0x2a30e)                                     #4  0x00007f859313730e __libc_start_call_main (@libc.so.0 +
                                           #5  0x00007f85931373c9 __libc_start_main@@GLIBC_2.34 (@libc.
so.6 + 0x2a3c9)                             #6  0x00000000004044aa n/a (n/a + 0x0)
                                           ELF object binary architecture: AMD x86-64
Sep 30 19:00:40 aasaenko.localdomain systemd[1]: systemd-coredump@201-6820-0.service: Deactivated successfully.
Sep 30 19:00:45 aasaenko.localdomain kernel: traps: VBoxClient[6844] trap int3 ip:41dd1b sp:7f8584afbcd0 error:0 in VBox
Client[1dd1b,400000+bb000]
Sep 30 19:00:45 aasaenko.localdomain systemd-coredump[6845]: Process 6841 (VBoxClient) of user 1000 terminated abnormall
y with signal 5/TRAP, processing...
Sep 30 19:00:45 aasaenko.localdomain systemd[1]: Started systemd-coredump@202-6845-0.service - Process Core Dump (PID 68
45/UID 0).
Sep 30 19:00:45 aasaenko.localdomain systemd-coredump[6846]: [?] Process 6841 (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.el1
0.x86_64

                                           Stack trace of thread 6844:
                                           #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  0x00007f85931a211a start_thread (@libc.so.6 + 0x9511a)
```

Рис. 12: Вывод журнала без пейджера

Режим реального времени в journalctl

```
root@aasaenko:/home/aasaenko#  
root@aasaenko:/home/aasaenko# journalctl -f  
Sep 30 19:01:00 aasaenko.localdomain systemd[1]: systemd-coredump@205-6883-0.service: Deactivated successfully.  
Sep 30 19:01:01 aasaenko.localdomain CROND[6890]: (root) CMD (run-parts /etc/cron.hourly)  
Sep 30 19:01:01 aasaenko.localdomain run-parts[6893]: (/etc/cron.hourly) starting 0anacron  
Sep 30 19:01:01 aasaenko.localdomain anacron[6903]: Anacron started on 2025-09-30  
Sep 30 19:01:01 aasaenko.localdomain anacron[6903]: Will run job `cron.daily' in 26 min.  
Sep 30 19:01:01 aasaenko.localdomain anacron[6903]: Will run job `cron.weekly' in 46 min.  
Sep 30 19:01:01 aasaenko.localdomain anacron[6903]: Will run job `cron.monthly' in 66 min.  
Sep 30 19:01:01 aasaenko.localdomain anacron[6903]: Jobs will be executed sequentially  
Sep 30 19:01:01 aasaenko.localdomain run-parts[6905]: (/etc/cron.hourly) finished 0anacron  
Sep 30 19:01:01 aasaenko.localdomain CROND[6889]: (root) CMDEND (run-parts /etc/cron.hourly)
```

Рис. 13: Режим реального времени в journalctl

Параметры фильтрации журнала

```
root@aasaenko:/home/aasaenko# journalctl
Display all 128 possibilities? (y or n)
_AUDIT_LOGINUID=
_AUDIT_SESSION=
AVAILABLE=
AVAILABLE_PRETTY=
_BOOT_ID=
_CAP_EFFECTIVE=
_CMDLINE=
CODE_FILE=
CODE_FUNC=
CODE_LINE=
_COMM=
CONFIG_FILE=
CONFIG_LINE=
COREDUMP_CGROUP=
COREDUMP_CMDLINE=
COREDUMP_COMM=
COREDUMP_CWD=
COREDUMP_ENVIRON=
COREDUMP_EXE=
COREDUMP_FILENAME=
COREDUMP_GID=
COREDUMP_HOSTNAME=
COREDUMP_OPEN_FDS=
COREDUMP_OWNER_UID=
COREDUMP_PACKAGE_JSON=
COREDUMP_PID=
CURRENT_USE_PRETTY=
DBUS_BROKER_LOG_DROPPED=
DBUS_BROKER_METRICS_DISPATCH_AVG=
DBUS_BROKER_METRICS_DISPATCH_COUNT=
DBUS_BROKER_METRICS_DISPATCH_MAX=
DBUS_BROKER_METRICS_DISPATCH_MIN=
DBUS_BROKER_METRICS_DISPATCH_STDDEV=
DISK_AVAILABLE=
DISK_AVAILABLE_PRETTY=
DISK_KEEP_FREE=
DISK_KEEP_FREE_PRETTY=
ERRNO=
_EXE=
_GID=
GLIB_DOMAIN=
GLIB_OLD_LOG_API=
_HOSTNAME=
INITRD_USEC=
INVOCATION_ID=
JOB_ID=
JOB_RESULT=
JOB_TYPE=
JOURNAL_NAME=
JOURNAL_PATH=
_KERNEL_DEVICE=
_KERNEL_SUBSYSTEM=
PODMAN_TIME=
PODMAN_TYPE=
PRIORITY=
REALMD_OPERATION=
_RUNTIME_SCOPE=
SEAT_ID=
_SELINUX_CONTEXT=
SESSION_ID=
_SOURCE_BOOTTIME_TIMESTAMP=
_SOURCE_MONOTONIC_TIMESTAMP=
_SOURCE_REALTIME_TIMESTAMP=
SSSD_DOMAIN=
SSSD_PRG_NAME=
_STREAM_ID=
SYSLOG_FACILITY=
SYSLOG_IDENTIFIER=
SYSLOG_PID=
SYSLOG_RAW=
SYSLOG_TIMESTAMP=
_SYSTEMD_CGROUP=
_SYSTEMD_INVOCATION_ID=
_SYSTEMD_OWNER_UID=
_SYSTEMD_SESSION=
_SYSTEMD_SLICE=
_SYSTEMD_UNIT=
_SYSTEMD_USER_SLICE=
```

Рис. 14: Просмотр доступных параметров фильтрации

```
root@aasaenko:/home/aasaenko# journalctl _UID=0
Sep 30 18:42:41 aasaenko.localdomain systemd-journald[283]: Collecting audit messages is disabled.
Sep 30 18:42:41 aasaenko.localdomain systemd-journald[283]: Journal started
Sep 30 18:42:41 aasaenko.localdomain systemd-journald[283]: Runtime Journal (/run/log/journal/4d1da01cd6b0424689deafc9e
Sep 30 18:42:41 aasaenko.localdomain systemd-modules-load[284]: Module 'msr' is built in
Sep 30 18:42:41 aasaenko.localdomain systemd-modules-load[284]: Inserted module 'fuse'
Sep 30 18:42:41 aasaenko.localdomain systemd-modules-load[284]: Module 'scsi_dh_alua' is built in
Sep 30 18:42:41 aasaenko.localdomain systemd-modules-load[284]: Module 'scsi_dh_emc' is built in
Sep 30 18:42:41 aasaenko.localdomain systemd-modules-load[284]: Module 'scsi_dh_rdac' is built in
Sep 30 18:42:41 aasaenko.localdomain systemd-sysusers[295]: Creating group 'nobody' with GID 65534.
Sep 30 18:42:41 aasaenko.localdomain systemd-sysusers[295]: Creating group 'users' with GID 100.
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variables.
Sep 30 18:42:41 aasaenko.localdomain systemd-sysusers[295]: Creating group 'systemd-journal' with GID 190.
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Finished systemd-sysusers.service - Create System Users.
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create Static Device Nodes
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Finished systemd-vconsole-setup.service - Virtual Console Setup.
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: dracut-cmdline-ask.service - dracut ask for additional cmdline parameters
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Starting dracut-cmdline.service - dracut cmdline hook...
Sep 30 18:42:41 aasaenko.localdomain dracut-cmdline[308]: dracut-105-4.el10_0
Sep 30 18:42:41 aasaenko.localdomain dracut-cmdline[308]: Using kernel command line parameters: BOOT_IMAGE=(hd0,gpt2)
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev.service - Create Static Device Nodes
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Finished dracut-cmdline.service - dracut cmdline hook.
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Starting dracut-pre-udev.service - dracut pre-udev hook...
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Finished dracut-pre-udev.service - dracut pre-udev hook.
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Starting systemd-udev.service - Rule-based Manager for Device Events and
Sep 30 18:42:41 aasaenko.localdomain systemd-udev[408]: Using default interface naming scheme 'rhel-10.0'.
Sep 30 18:42:41 aasaenko.localdomain systemd[1]: Started systemd-udev.service - Rule-based Manager for Device Events and
```

Рис. 15: Фильтрация журнала по UID

Последние 20 строк журнала

```
root@aasaenko:/home/aasaenko# journalctl -n 20
Sep 30 19:02:43 aasaenko.localdomain kernel: traps: VBoxClient[7122] trap int3 ip:41dd1b sp:7f8584afbcd0 error:0 in VBox
Sep 30 19:02:43 aasaenko.localdomain systemd-coredump[7123]: Process 7119 (VBoxClient) of user 1000 terminated abnormal
Sep 30 19:02:43 aasaenko.localdomain systemd[1]: Started systemd-coredump@225-7123-0.service - Process Core Dump (PID 7
Sep 30 19:02:43 aasaenko.localdomain systemd-coredump[7124]: [?] Process 7119 (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 7122:
                                #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  0x00007f85931a211a start_thread (libc.so.6 + 0x9511a)
                                #5  0x00007f8593212c3c __clone3 (libc.so.6 + 0x105c3c)

                                Stack trace of thread 7120:
                                #0  0x00007f8593210a3d syscall (libc.so.6 + 0x103a3d)
                                #1  0x000000000434c30 n/a (n/a + 0x0)
                                #2  0x000000000450bfb n/a (n/a + 0x0)
                                #3  0x00000000043566a n/a (n/a + 0x0)
                                #4  0x00000000045041c n/a (n/a + 0x0)
                                #5  0x0000000004355d0 n/a (n/a + 0x0)
                                #6  0x00007f85931a211a start_thread (libc.so.6 + 0x9511a)
```

Рис. 16: Просмотр последних 20 строк журнала

```
root@aasaenko:/home/aasaenko# journalctl -p err
Sep 30 18:42:42 aasaenko.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an unsupported device
Sep 30 18:42:42 aasaenko.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken.
Sep 30 18:42:42 aasaenko.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graphics device
Sep 30 18:42:45 aasaenko.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Sep 30 18:42:46 aasaenko.localdomain alsactl[957]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import module: snd-ice1712
Sep 30 18:42:46 aasaenko.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Sep 30 18:43:30 aasaenko.localdomain gdm-password[1990]: gkr-pam: unable to locate daemon control file
Sep 30 18:43:33 aasaenko.localdomain systemd[2001]: Failed to start app-gnome-gnome\x2dkeyring\x2dsecrets-2108.scope - Application is not supported
Sep 30 18:43:33 aasaenko.localdomain systemd[2001]: Failed to start app-gnome-xdg\x2duser\x2ddirs-2126.scope - Application is not supported
Sep 30 18:43:35 aasaenko.localdomain systemd-coredump[2800]: Process 2788 (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 2793:
                                     #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 0x000007f85931a211a start_thread (libc.so.6 + 0x9511a)
                                     #5 0x000007f8593212c3c __clone3 (libc.so.6 + 0x105c3c)

                                     Stack trace of thread 2788:
                                     #0 0x000007f8593210a3d syscall (libc.so.6 + 0x103a3d)
```

Рис. 17: Фильтрация по сообщениям с приоритетом “ошибка”

Сообщения со вчерашнего дня

```
-----
root@aasaenko:/home/aasaenko# journalctl --since yesterday
Sep 30 18:42:41 aasaenko.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.b
Sep 30 18:42:41 aasaenko.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_64 r
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-provided physical RAM map:
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000dff0000-0x0000000000dfffff] ACPI data
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000fec00fff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x000000000fee00000-0x000000000fee00fff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x000000000fffc0000-0x000000000ffffff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x00000000100000000-0x0000000011ffffff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: NX (Execute Disable) protection: active
Sep 30 18:42:41 aasaenko.localdomain kernel: APIC: Static calls initialized
Sep 30 18:42:41 aasaenko.localdomain kernel: SMBIOS 2.5 present.
Sep 30 18:42:41 aasaenko.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 30 18:42:41 aasaenko.localdomain kernel: DMI: Memory slots populated: 0/0
Sep 30 18:42:41 aasaenko.localdomain kernel: Hypervisor detected: KVM
Sep 30 18:42:41 aasaenko.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Sep 30 18:42:41 aasaenko.localdomain kernel: kvm-clock: using sched offset of 4068452678 cycles
Sep 30 18:42:41 aasaenko.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffff max_cycles: 0x1cd42e4dffb
Sep 30 18:42:41 aasaenko.localdomain kernel: tsc: Detected 3187.204 MHz processor
Sep 30 18:42:41 aasaenko.localdomain kernel: e820: update [mem 0x00000000-0x000000fff] usable ==> reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: e820: remove [mem 0x000a00000-0x000fffff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Sep 30 18:42:41 aasaenko.localdomain kernel: total RAM covered: 4096M
Sep 30 18:42:41 aasaenko.localdomain kernel: Found optimal setting for mtrr clean up
Sep 30 18:42:41 aasaenko.localdomain kernel: gran_size: 64K chunk_size: 10 num_reg: 3 lose co
Sep 30 18:42:41 aasaenko.localdomain kernel: MTRR map: 6 entries (3 fixed + 3 variable; max 35), built from 16 variables
Sep 30 18:42:41 aasaenko.localdomain kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
```

Рис. 18: Журнал со вчерашнего дня

Ошибки со вчерашнего дня

```
root@aasaenko:/home/aasaenko# journalctl --since yesterday -p err
Sep 30 18:42:42 aasaenko.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an unsupported
Sep 30 18:42:42 aasaenko.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken.
Sep 30 18:42:42 aasaenko.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graphics device
Sep 30 18:42:45 aasaenko.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Sep 30 18:42:46 aasaenko.localdomain alsactl[957]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import PCM
Sep 30 18:42:46 aasaenko.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Sep 30 18:43:30 aasaenko.localdomain gdm-password[1990]: gkr-pam: unable to locate daemon control file
Sep 30 18:43:33 aasaenko.localdomain systemd[2001]: Failed to start app-gnome-gnome\x2dkeyring\x2dsecrets-2108.scope - System
Sep 30 18:43:33 aasaenko.localdomain systemd[2001]: Failed to start app-gnome-xdg\x2duser\x2ddirs-2126.scope - Application
Sep 30 18:43:35 aasaenko.localdomain systemd-coredump[2800]: Process 2788 (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 2793:
#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  0x00007f85931a211a start_thread (libc.so.6 + 0x9511a)
#5  0x00007f8593212c3c __clone3 (libc.so.6 + 0x105c3c)

Stack trace of thread 2788:
#0  0x00007f8593210a3d 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  0x00007f859313730e __libc_start_call_main (libc.so.6 + 0x103a3d)
```

Рис. 19: Сообщения об ошибках со вчерашнего дня


```
_SOURCE_BOOTTIME_TIMESTAMP=0
Tue 2025-09-30 18:42:41.807213 MSK [s=dffc86b5ea7d44adbe60453ec325c33a;i=2;b=3fecebe220d5492c8996ede67293d253;m=eda4a;1
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=3fecebe220d5492c8996ede67293d253
_MACHINE_ID=4d1da01cd6b0424689deafc9e229859b
_HOSTNAME=aasaenko.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_vbox-root ro r
Tue 2025-09-30 18:42:41.807218 MSK [s=dffc86b5ea7d44adbe60453ec325c33a;i=3;b=3fecebe220d5492c8996ede67293d253;m=eda4e;1
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=3fecebe220d5492c8996ede67293d253
_MACHINE_ID=4d1da01cd6b0424689deafc9e229859b
root@aasaenko:/home/aasaenko#
```

Рис. 20: Детализированный вывод журнала

```
root@aasaenko:/home/aasaenko# journalctl _SYSTEMD_UNIT=sshd.service
Sep 30 18:42:46 aasaenko.localdomain (sshd)[1184]: sshd.service: Referenced but unset environment variable evaluates to
Sep 30 18:42:46 aasaenko.localdomain sshd[1184]: Server listening on 0.0.0.0 port 22.
Sep 30 18:42:46 aasaenko.localdomain sshd[1184]: Server listening on :: port 22.
root@aasaenko:/home/aasaenko#
```

Рис. 21: Просмотр журнала для sshd

Постоянное хранение journald

```
root@aasaenko:/home/aasaenko# mkdir -p /var/log/journal
root@aasaenko:/home/aasaenko# chown root:systemd-journal /var/log/journal/
root@aasaenko:/home/aasaenko# chmod 2755 /var/log/journal/
root@aasaenko:/home/aasaenko# killall -USR1 systemd-journal
root@aasaenko:/home/aasaenko# journalctl -b
Sep 30 18:42:41 aasaenko.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.b
Sep 30 18:42:41 aasaenko.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_64 ro
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-provided physical RAM map:
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbfff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x0000000000009fc000-0x0000000000009fffff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x000000000000f00000-0x000000000000ffffff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x000000000001000000-0x000000000000dfffffff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x00000000000dffff0000-0x00000000000dffffffffff] ACPI data
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x000000000fec000000-0x000000000fec00ffff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x000000000fee000000-0x000000000fee00ffff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x000000000fffc00000-0x000000000fffffffffff] reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: BIOS-e820: [mem 0x000000001000000000-0x0000000011fffffffffff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: NX (Execute Disable) protection: active
Sep 30 18:42:41 aasaenko.localdomain kernel: APIC: Static calls initialized
Sep 30 18:42:41 aasaenko.localdomain kernel: SMBIOS 2.5 present.
Sep 30 18:42:41 aasaenko.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 30 18:42:41 aasaenko.localdomain kernel: DMI: Memory slots populated: 0/0
Sep 30 18:42:41 aasaenko.localdomain kernel: Hypervisor detected: KVM
Sep 30 18:42:41 aasaenko.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Sep 30 18:42:41 aasaenko.localdomain kernel: kvm-clock: using sched offset of 4068452678 cycles
Sep 30 18:42:41 aasaenko.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb
Sep 30 18:42:41 aasaenko.localdomain kernel: tsc: Detected 3187.204 MHz processor
Sep 30 18:42:41 aasaenko.localdomain kernel: e820: update [mem 0x000000000-0x000000fff] usable ==> reserved
Sep 30 18:42:41 aasaenko.localdomain kernel: e820: remove [mem 0x000a00000-0x0000fffff] usable
Sep 30 18:42:41 aasaenko.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Sep 30 18:42:41 aasaenko.localdomain kernel: total RAM covered: 4096M
```

Рис. 22: Просмотр системного журнала с момента загрузки

Выводы по проделанной работе

В ходе лабораторной работы я освоила:

- мониторинг системных событий с помощью `tail` и `logger`;
- настройку и использование `rsyslog`;
- работу с системным журналом через `journalctl`;
- фильтрацию сообщений по UID, PID, приоритетам и времени;
- настройку постоянного хранения логов `journal`.

Полученные навыки помогут администрировать систему, анализировать события и обеспечивать контроль за её безопасностью.