

Лабораторная работа №7

Управление журналами событий в системе

Анастасия Мазуркевич

15 октября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Получить навыки работы с системными журналами и их конфигурацией в Linux, научиться использовать `rsyslog` и `journalctl` для анализа событий.

Ход выполнения

Мониторинг системных сообщений

```
root@admazurkevich:/home/admazurkevich# tail -f /var/log/messages
Oct 1 11:17:34 admazurkevich systemd[1]: systemd-coredump@27-3580-0.service: Deactivated successfully.
Oct 1 11:17:39 admazurkevich chronyd[929]: Source 46.160.198.122 replaced with 2a12:4141:face:6::a (2.rocky.pool.ntp.org)
Oct 1 11:17:39 admazurkevich kernel: traps: VBoxClient[3592] trap int3 ip:41ddb sp:7f198c635cd0 error:0 in VBoxClient[400000+bb000]
Oct 1 11:17:39 admazurkevich systemd-coredump[3593]: Process 3589 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Oct 1 11:17:39 admazurkevich systemd[1]: Starting fwupd-refresh.service - Refresh fwupd metadata and update motd...
Oct 1 11:17:39 admazurkevich systemd[1]: Started systemd-coredump@28-3593-0.service - Process Core Dump (PID 3593/UID 0).
Oct 1 11:17:40 admazurkevich systemd[1]: fwupd-refresh.service: Deactivated successfully.
Oct 1 11:17:40 admazurkevich systemd[1]: Finished fwupd-refresh.service - Refresh fwupd metadata and update motd.
Oct 1 11:17:40 admazurkevich systemd-coredump[3595]: Process 3589 (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 3592:#012#0 0x0000000000041dd1b n/a (n/a + 0x0)#012#1 0x0000000000041dc94 n/a (n/a + 0x0)#012#2 0x0000000000045041c n/a (n/a + 0x0)#012#3 0x00000000004355d0 n/a (n/a + 0x0)#012#4 0x0000007f199ace611a start_thread (libc.so.6 + 0x9511a)#012#5 0x0000007f199ad56c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 3589:#012#0 0x0000007f199ad54a3d 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 0x0000007f199ac7b30e __libc_start_main (libc.so.6 + 0x2a30e)#012#5 0x0000007f199ac7b3c9 __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 11:17:40 admazurkevich systemd[1]: systemd-coredump@28-3593-0.service: Deactivated successfully.
Oct 1 11:17:45 admazurkevich kernel: traps: VBoxClient[3620] trap int3 ip:41ddb sp:7f198c635cd0 error:0 in VBoxClient[400000+bb000]
Oct 1 11:17:45 admazurkevich systemd-coredump[3621]: Process 3617 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Oct 1 11:17:45 admazurkevich systemd[1]: Started systemd-coredump@29-3621-0.service - Process Core Dump (PID 3621/UID 0).
Oct 1 11:17:45 admazurkevich systemd-coredump[3622]: Process 3617 (VBoxClient) of user 1000 dumped core.#012#012Module
```

Рис. 1: Мониторинг системных сообщений

```
Oct 1 11:18:25 admazurkevich systemd-coredump[3721]: Process 3717 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Oct 1 11:18:25 admazurkevich systemd[1]: Started systemd-coredump@37-3721-0.service - Process Core Dump (PID 3721/UID 0).
Oct 1 11:18:25 admazurkevich su[3714]: FAILED SU (to root) admazurkevich on pts/2
Oct 1 11:18:25 admazurkevich systemd-coredump[3722]: Process 3717 (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 3720:#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 0x000007f199ace611a start_thread (libc.so.6 + 0x9511a)#012#5 0x000007f199ad56c3c
```

Рис. 2: Сообщение об ошибке аутентификации

```
)#012#5 0x00007f199ac7b3c9 __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 11:18:56 admazurkevich systemd[1]: systemd-coredump@43-3786-0.service: Deactivated successfully.  
Oct 1 11:18:59 admazurkevich admazurkevich[3792]: hello  
Oct 1 11:18:59 admazurkevich admazurkevich[3794]: hello  
Oct 1 11:19:00 admazurkevich admazurkevich[3796]: hello  
Oct 1 11:19:01 admazurkevich kernel: traps: VBoxClient[3801] trap int3 ip:41ddb sp:7f198c635cd0 error:0 in VBoxClie  
nt[1ddb,400000+bb000]  
Oct 1 11:19:01 admazurkevich systemd-coredump[3802]: Process 3798 (VBoxClient) of user 1000 terminated abnormally wi
```

Рис. 3: Сообщение logger hello в журнале

```
root@admazurkevich:/home/admazurkevich# tail -n 20 /var/log/secure
Sep 25 15:15:47 admazurkevich su[4807]: pam_unix(su:session): session closed for user root
Oct  1 11:15:12 admazurkevich sshd[1192]: Server listening on 0.0.0.0 port 22.
Oct  1 11:15:12 admazurkevich sshd[1192]: Server listening on :: port 22.
Oct  1 11:15:12 admazurkevich (systemd)[1259]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by
gdm(uid=0)
Oct  1 11:15:12 admazurkevich gdm-launch-environment][1237]: pam_unix(gdm-launch-environment:session): session opened
for user gdm(uid=42) by (uid=0)
Oct  1 11:15:18 admazurkevich gdm-password][1958]: gkr-pam: unable to locate daemon control file
Oct  1 11:15:18 admazurkevich gdm-password][1958]: gkr-pam: stashed password to try later in open session
Oct  1 11:15:18 admazurkevich (systemd)[1985]: pam_unix(systemd-user:session): session opened for user admazurkevich(
uid=1000) by admazurkevich(uid=0)
Oct  1 11:15:18 admazurkevich gdm-password][1958]: pam_unix(gdm-password:session): session opened for user admazurkev
ich(uid=1000) by admazurkevich(uid=0)
Oct  1 11:15:18 admazurkevich gdm-password][1958]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyrin
g
Oct  1 11:15:22 admazurkevich gdm-launch-environment][1237]: pam_unix(gdm-launch-environment:session): session closed
for user gdm
Oct  1 11:17:18 admazurkevich (systemd)[3392]: pam_unix(systemd-user:session): session opened for user root(uid=0) by
root(uid=0)
Oct  1 11:17:18 admazurkevich su[3369]: pam_unix(su:session): session opened for user root(uid=0) by admazurkevich(ui
d=1000)
Oct  1 11:17:24 admazurkevich su[3474]: pam_unix(su:session): session opened for user root(uid=0) by admazurkevich(ui
d=1000)
Oct  1 11:17:28 admazurkevich su[3539]: pam_unix(su:session): session opened for user root(uid=0) by admazurkevich(ui
d=1000)
Oct  1 11:18:14 admazurkevich su[3539]: pam_unix(su:session): session closed for user root
Oct  1 11:18:17 admazurkevich unix_chkpwd[3702]: password check failed for user (root)
Oct  1 11:18:17 admazurkevich su[3683]: pam_unix(su:auth): authentication failure; logname=admazurkevich uid=1000 eui
d=0 tty=/dev/pts/2 ruser=admazurkevich rhost= user=root
Oct  1 11:18:23 admazurkevich unix_chkpwd[3716]: password check failed for user (root)
Oct  1 11:18:23 admazurkevich su[3714]: pam_unix(su:auth): authentication failure; logname=admazurkevich uid=1000 eui
d=0 tty=/dev/pts/2 ruser=admazurkevich rhost= user=root
root@admazurkevich:/home/admazurkevich#
```


Установка и запуск Apache

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

Рис. 5: Установка и запуск Apache

```
root@admazurkevich:/home/admazurkevich#  
root@admazurkevich:/home/admazurkevich# tail -f /var/log/httpd/error_log  
[Wed Oct 01 11:21:44.012487 2025] [suexec:notice] [pid 4402:tid 4402] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)  
[Wed Oct 01 11:21:44.046861 2025] [lbmethod_heartbeat:notice] [pid 4402:tid 4402] AH02282: No slotmem from mod_heartmonitor  
[Wed Oct 01 11:21:44.047560 2025] [systemd:notice] [pid 4402:tid 4402] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0  
[Wed Oct 01 11:21:44.049413 2025] [mpm_event:notice] [pid 4402:tid 4402] AH00489: Apache/2.4.63 (Rocky Linux) configured -- resuming normal operations  
[Wed Oct 01 11:21:44.049427 2025] [core:notice] [pid 4402:tid 4402] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 6: Журнал ошибок Apache

```
#
# 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 4Replac 5Copy 6Move 7Search 8Delete

Рис. 7: Добавление правила ErrorLog в httpd.conf



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

Рис. 8: Создание правила для логов Apache в rsyslog

```
root@admazurkevich:/home/admazurkevich#  
root@admazurkevich:/home/admazurkevich# cd /etc/rsyslog.d/  
root@admazurkevich:/etc/rsyslog.d# touch httpd.conf  
root@admazurkevich:/etc/rsyslog.d# mcedit httpd.conf  
  
root@admazurkevich:/etc/rsyslog.d# touch debug.conf  
root@admazurkevich:/etc/rsyslog.d# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf  
root@admazurkevich:/etc/rsyslog.d#
```

Рис. 9: Создание конфигурации debug.conf

Проверка отладочного сообщения

```
Oct 1 11:27:36 admazurkevich systemd-coredump[6076]: Process 6071 (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 6074:#012#0 0x0000000000041dd1b 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 0x00007f199ace611a start_thread (libc.so.6 + 0x9511a)#012#5 0x00007f199ad56c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 6071:#012#0 0x00007f199ad54a3d 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 0x00007f199ac7b30e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x00007f199ac7b3c9 __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 11:27:36 admazurkevich systemd[1]: systemd-coredump@145-6075-0.service: Deactivated successfully.
Oct 1 11:27:37 admazurkevich root[6081]: Daemon Debug Message
```

Рис. 10: Сообщение отладки в журнале

Просмотр системного журнала

```
root@admazurkevich:/home/admazurkevich# journalctl
Oct 01 11:15:07 admazurkevich.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-bu
Oct 01 11:15:07 admazurkevich.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.b
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-provided physical RAM map:
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x000000000009f000-0x000000000000ffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000000100000-0x0000000000dffff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000dfff0000-0x0000000000dffff] ACPI data
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000010000000-0x0000000011ffffff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: NX (Execute Disable) protection: active
Oct 01 11:15:07 admazurkevich.localdomain kernel: APIC: Static calls initialized
Oct 01 11:15:07 admazurkevich.localdomain kernel: SMBIOS 2.5 present.
Oct 01 11:15:07 admazurkevich.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 01 11:15:07 admazurkevich.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 01 11:15:07 admazurkevich.localdomain kernel: Hypervisor detected: KVM
Oct 01 11:15:07 admazurkevich.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 01 11:15:07 admazurkevich.localdomain kernel: kvm-clock: using sched offset of 4069948781 cycles
Oct 01 11:15:07 admazurkevich.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd
Oct 01 11:15:07 admazurkevich.localdomain kernel: tsc: Detected 3187.198 MHz processor
Oct 01 11:15:07 admazurkevich.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: e820: remove [mem 0x000a0000-0x000ffff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x40000000
Oct 01 11:15:07 admazurkevich.localdomain kernel: total RAM covered: 4096M
Oct 01 11:15:07 admazurkevich.localdomain kernel: Found optimal setting for mtrr clean up
Oct 01 11:15:07 admazurkevich.localdomain kernel: gran_size: 64K chunk_size: 1G num_reg: 3
Oct 01 11:15:07 admazurkevich.localdomain kernel: MTRR map: 6 entries (3 fixed + 3 variable; max 35), built from 16
Oct 01 11:15:07 admazurkevich.localdomain kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
```

Рис. 11: Просмотр системного журнала

Режим реального времени

```
6_64
_64
.0-2.el10.x86_64

9511a)
3c)

d)

.so.6 + 0x2a30e)
4 (libc.so.6 + 0x2a3c9)

Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86
Module libwayland-client.so.0 from rpm wayland-1.23

Stack trace of thread 6393:
#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 0x00007f199ace611a start_thread (libc.so.6 + 0x
#5 0x00007f199ad56c3c __clone3 (libc.so.6 + 0x105c

Stack trace of thread 6390:
#0 0x00007f199ad54a3d syscall (libc.so.6 + 0x103a3
#1 0x0000000004344e2 n/a (n/a + 0x0)
#2 0x000000000450066 n/a (n/a + 0x0)
#3 0x000000000405123 n/a (n/a + 0x0)
#4 0x00007f199ac7b30e __libc_start_call_main (libc
#5 0x00007f199ac7b3c9 __libc_start_main@@GLIBC_2.3
#6 0x0000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x86-64

Oct 01 11:29:44 admazurkevich.localdomain systemd[1]: systemd-coredump@170-6394-0.service: Deactivated successfully.
```

Рис. 12: Режим просмотра журнала в реальном времени

Фильтрация параметров

```
root@admazurkevich:/home/admazurkevich# journalctl
Display all 131 possibilities? (y or n)
_AUDIT_LOGINUID=
_AUDIT_SESSION=
AVAILABLE=
AVAILABLE_PRETTY=
_BOOT_ID=
_CAP_EFFECTIVE=
_CMDLINE=
CODE_FILE=
CODE_FUNC=
CODE_LINE=
_COMM=
COMMAND=
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=
COREDUMP_PROC_AUXV=
COREDUMP_PROC_CGROUP=
COREDUMP_PROC_LIMITS=
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=
EXIT_CODE=
EXIT_STATUS=
_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=
KERNEL_USEC=
LEADER=
PODMAN_EVENT=
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=
_SYSTEMD_USER_UNIT=
THREAD_ID=
TID=
```

Рис. 13: Фильтрация журнала по параметрам

```

root@admazurkevich:/home/admazurkevich# journalctl _UID=0
Oct 01 11:15:07 admazurkevich.localdomain systemd-journald[280]: Collecting audit messages is disabled.
Oct 01 11:15:07 admazurkevich.localdomain systemd-journald[280]: Journal started
Oct 01 11:15:07 admazurkevich.localdomain systemd-journald[280]: Runtime Journal (/run/log/journal/c9e273a9076042e78
Oct 01 11:15:07 admazurkevich.localdomain systemd-modules-load[281]: Module 'msr' is built in
Oct 01 11:15:07 admazurkevich.localdomain systemd-modules-load[281]: Inserted module 'fuse'
Oct 01 11:15:07 admazurkevich.localdomain systemd-modules-load[281]: Module 'scsi_dh_alua' is built in
Oct 01 11:15:07 admazurkevich.localdomain systemd-modules-load[281]: Module 'scsi_dh_emc' is built in
Oct 01 11:15:07 admazurkevich.localdomain systemd-modules-load[281]: Module 'scsi_dh_rdac' is built in
Oct 01 11:15:07 admazurkevich.localdomain systemd-sysusers[293]: Creating group 'nobody' with GID 65534.
Oct 01 11:15:07 admazurkevich.localdomain systemd-sysusers[293]: Creating group 'users' with GID 100.
Oct 01 11:15:07 admazurkevich.localdomain systemd-sysusers[293]: Creating group 'systemd-journal' with GID 190.
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Finished systemd-sysusers.service - Create System Users.
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create Static De
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variables.
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Finished systemd-vconsole-setup.service - Virtual Console Setup
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: dracut-cmdline-ask.service - dracut ask for additional cmdline
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Starting dracut-cmdline.service - dracut cmdline hook...
Oct 01 11:15:07 admazurkevich.localdomain dracut-cmdline[307]: dracut-105-4.el10_0
Oct 01 11:15:07 admazurkevich.localdomain dracut-cmdline[307]: Using kernel command line parameters: BOOT_IMAGE=(
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev.service - Create Static De
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Finished dracut-cmdline.service - dracut cmdline hook.
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Starting dracut-pre-udev.service - dracut pre-udev hook...
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Finished dracut-pre-udev.service - dracut pre-udev hook.
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Starting systemd-udev.service - Rule-based Manager for Device
Oct 01 11:15:07 admazurkevich.localdomain systemd-udev[408]: Using default interface naming scheme 'rhel-10.0'.
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Started systemd-udev.service - Rule-based Manager for Device

```

Рис. 14: Журнал для UID 0

Последние строки журнала

```
root@admazurkevich:/home/admazurkevich#  
root@admazurkevich:/home/admazurkevich# journalctl -n 20  
Oct 01 11:31:27 admazurkevich.localdomain systemd-coredump[6626]: [?] Process 6621 (VBoxClient) of user 1000 dumped >  
  
Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x>  
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x>  
Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x>  
Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x8>  
Module libwayland-client.so.0 from rpm wayland-1.2>  
Stack trace of thread 6624:  
#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 0x00007f199ace611a start_thread (libc.so.6 + 0>  
#5 0x00007f199ad56c3c __clone3 (libc.so.6 + 0x105>  
  
Stack trace of thread 6622:  
#0 0x00007f199ad54a3d syscall (libc.so.6 + 0x103a>  
#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 0x00007f199ace611a start_thread (libc.so.6 + 0>  
#7 0x00007f199ad56c3c __clone3 (libc.so.6 + 0x105>  
  
Stack trace of thread 6621:  
#0 0x00007f199ad54a3d syscall (libc.so.6 + 0x103a>
```

Рис. 15: Вывод последних строк журнала

```
root@admazurkevich:/home/admazurkevich# journalctl -p err
Oct 01 11:15:07 admazurkevich.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on a
Oct 01 11:15:07 admazurkevich.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken
Oct 01 11:15:07 admazurkevich.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graphics
Oct 01 11:15:10 admazurkevich.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Oct 01 11:15:12 admazurkevich.localdomain alsactl[925]: alsalib main.c:1554:(snd_use_case_mgr_open) error: failed to
Oct 01 11:15:12 admazurkevich.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Oct 01 11:15:14 admazurkevich.localdomain systemd-coredump[1751]: [?] Process 439 (plymouthd) of user 0 dumped core.

                               Module libpcre2-8.so.0 from rpm pcre2-10.44-1.el10.x86_64
                               Module libbrotlicommon.so.1 from rpm brotli-1.1.0-6.el10.x86_64
                               Module libgraphite2.so.3 from rpm graphite2-1.3.14-2.el10.x86_64
                               Module libglib-2.0.so.0 from rpm glib2-2.80.4-4.el10.x86_64
                               Module libbrotlidedec.so.1 from rpm brotli-1.1.0-6.el10.x86_64
                               Module libharfbuzz.so.0 from rpm harfbuzz-8.4.0-6.el10.x86_64
                               Module libbz2.so.1 from rpm bzip2-1.0.8-25.el10.x86_64
                               Module libfreetype.so.6 from rpm freetype-2.13.2-8.el10.x86_64
                               Module label-freetype.so from rpm plymouth-24.004.60-13.el10.x86_64
                               Module libz.so.1 from rpm zlib-ng-2.2.3-1.el10.x86_64
                               Module libpng16.so.16 from rpm libpng-1.6.40-8.el10.x86_64
                               Module libply-splash-graphics.so.5 from rpm plymouth-24.004.60-13.el10.x86_64
                               Module two-step.so from rpm plymouth-24.004.60-13.el10.x86_64
                               Module libdrm.so.2 from rpm libdrm-2.4.123-1.el10.x86_64
                               Module drm.so from rpm plymouth-24.004.60-13.el10.x86_64
                               Module libcap.so.2 from rpm libcap-2.69-7.el10.x86_64
                               Module libudev.so.1 from rpm systemd-257-9.el10.x86_64
                               Module libxkbcommon.so.0 from rpm libxkbcommon-1.7.0-1.el10.x86_64
                               Module libevdev.so.2 from rpm libevdev-1.13.1-6.el10.x86_64
                               Module libply-splash-core.so.5 from rpm plymouth-24.004.60-13.el10.x86_64
                               Module libply.so.5 from rpm plymouth-24.004.60-13.el10.x86_64
                               Stack trace of thread 439:
```

Рис. 16: Сообщения уровня ошибки

Сообщения со вчерашнего дня

```
root@admazurkevich:/home/admazurkevich#  
root@admazurkevich:/home/admazurkevich# journalctl --since yesterday  
Oct 01 11:15:07 admazurkevich.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-bu  
Oct 01 11:15:07 admazurkevich.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x  
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-provided physical RAM map:  
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable  
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved  
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved  
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] usable  
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000dffff000-0x0000000000dffffff] ACPI data  
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000fec00fff] reserved  
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x000000000fee00000-0x000000000fee00fff] reserved  
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x000000000fffc0000-0x000000000ffffffff] reserved  
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000100000000-0x0000000011ffffffff] usable  
Oct 01 11:15:07 admazurkevich.localdomain kernel: NX (Execute Disable) protection: active  
Oct 01 11:15:07 admazurkevich.localdomain kernel: APIC: Static calls initialized  
Oct 01 11:15:07 admazurkevich.localdomain kernel: SMBIOS 2.5 present.  
Oct 01 11:15:07 admazurkevich.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006  
Oct 01 11:15:07 admazurkevich.localdomain kernel: DMI: Memory slots populated: 0/0  
Oct 01 11:15:07 admazurkevich.localdomain kernel: Hypervisor detected: KVM  
Oct 01 11:15:07 admazurkevich.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00  
Oct 01 11:15:07 admazurkevich.localdomain kernel: kvm-clock: using sched offset of 4069948781 cycles  
Oct 01 11:15:07 admazurkevich.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd  
Oct 01 11:15:07 admazurkevich.localdomain kernel: tsc: Detected 3187.198 MHz processor  
Oct 01 11:15:07 admazurkevich.localdomain kernel: e820: update [mem 0x000000000-0x000000fff] usable ==> reserved  
Oct 01 11:15:07 admazurkevich.localdomain kernel: e820: remove [mem 0x000a00000-0x0000fffff] usable  
Oct 01 11:15:07 admazurkevich.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000  
Oct 01 11:15:07 admazurkevich.localdomain kernel: total RAM covered: 4096M  
Oct 01 11:15:07 admazurkevich.localdomain kernel: Found optimal setting for mtrr clean up  
Oct 01 11:15:07 admazurkevich.localdomain kernel: gran_size: 64K chunk_size: 1G num_reg: 3  
Oct 01 11:15:07 admazurkevich.localdomain kernel: MTRR map: 6 entries (3 fixed + 3 variable; max 35), built from 16  
Oct 01 11:15:07 admazurkevich.localdomain kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
```

Рис. 17: Сообщения со вчерашнего дня

Ошибки со вчерашнего дня

```
root@admazurkevich:/home/admazurkevich# journalctl --since yesterday -p err
Oct 01 11:15:07 admazurkevich.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on a
Oct 01 11:15:07 admazurkevich.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely br
Oct 01 11:15:07 admazurkevich.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported gr
Oct 01 11:15:10 admazurkevich.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Oct 01 11:15:12 admazurkevich.localdomain alsactl[925]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to
Oct 01 11:15:12 admazurkevich.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Oct 01 11:15:14 admazurkevich.localdomain systemd-coredump[1751]: [?] Process 439 (plymouthd) of user 0 dumped core.

                               Module libpcr2-8.so.0 from rpm pcr2-10.44-1.el10
                               Module libbrotlicommon.so.1 from rpm brotli-1.1.0-
                               Module libgraphite2.so.3 from rpm graphite2-1.3.14
                               Module libglib-2.0.so.0 from rpm glib2-2.80.4-4.el
                               Module libbrotlidec.so.1 from rpm brotli-1.1.0-6.e
                               Module libharfbuzz.so.0 from rpm harfbuzz-8.4.0-6.
                               Module libbz2.so.1 from rpm bzip2-1.0.8-25.el10.x8
                               Module libfreetype.so.6 from rpm freetype-2.13.2-8
                               Module label-freetype.so from rpm plymouth-24.004.
                               Module libz.so.1 from rpm zlib-ng-2.2.3-1.el10.x86
                               Module libpng16.so.16 from rpm libpng-1.6.40-8.el1
                               Module libply-splash-graphics.so.5 from rpm plymou
                               Module two-step.so from rpm plymouth-24.004.60-13.
                               Module libdrm.so.2 from rpm libdrm-2.4.123-1.el10.
                               Module drm.so from rpm plymouth-24.004.60-13.el10.
                               Module libcap.so.2 from rpm libcap-2.69-7.el10.x86
                               Module libudev.so.1 from rpm systemd-257-9.el10_0.
                               Module libxkbcommon.so.0 from rpm libxkbcommon-1.7
                               Module libevdev.so.2 from rpm libevdev-1.13.1-6.el
                               Module libply-splash-core.so.5 from rpm plymouth-2
                               Module libply.so.5 from rpm plymouth-24.004.60-13.
                               Stack trace of thread 439:
```

Рис. 18: Ошибки со вчерашнего дня

Детализированный вывод

```
Wed 2025-10-01 11:15:07.666131 MSK [s=d1fb3a047b71437aa5a221c0d1f4918a;i=1;b=553eeab0b76a42bfa2e62e229ac7ddfa;m=769c]
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
PRIORITY=5
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
MESSAGE=Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (G
_BOOT_ID=553eeab0b76a42bfa2e62e229ac7ddfa
_MACHINE_ID=c9e273a9076042e7849804b1c4762ff4
_HOSTNAME=admazurkevich.localdomain
_RUNTIME_SCOPE=initrd
Wed 2025-10-01 11:15:07.666144 MSK [s=d1fb3a047b71437aa5a221c0d1f4918a;i=2;b=553eeab0b76a42bfa2e62e229ac7ddfa;m=769c]
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=553eeab0b76a42bfa2e62e229ac7ddfa
_MACHINE_ID=c9e273a9076042e7849804b1c4762ff4
_HOSTNAME=admazurkevich.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 r
Wed 2025-10-01 11:15:07.666149 MSK [s=d1fb3a047b71437aa5a221c0d1f4918a;i=3;b=553eeab0b76a42bfa2e62e229ac7ddfa;m=769c]
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=553eeab0b76a42bfa2e62e229ac7ddfa
_MACHINE_ID=c9e273a9076042e7849804b1c4762ff4
_HOSTNAME=admazurkevich.localdomain
root@admazurkevich:/home/admazurkevich#
```

Рис. 19: Детализированный вывод журнала

```
root@admazurkevich:/home/admazurkevich#  
root@admazurkevich:/home/admazurkevich#  
root@admazurkevich:/home/admazurkevich# journalctl _SYSTEMD_UNIT=sshd.service  
Oct 01 11:15:12 admazurkevich.localdomain (sshd)[1192]: sshd.service: Referenced but unset environment variable eval  
Oct 01 11:15:12 admazurkevich.localdomain sshd[1192]: Server listening on 0.0.0.0 port 22.  
Oct 01 11:15:12 admazurkevich.localdomain sshd[1192]: Server listening on :: port 22.  
lines 1-3/3 (END)
```

Рис. 20: Журнал работы SSHD

Постоянное хранение журналов

```
root@admazurkevich:/home/admazurkevich#
root@admazurkevich:/home/admazurkevich# mkdir -p /var/log/journal
root@admazurkevich:/home/admazurkevich# chown root:systemd-journal /var/log/journal/
root@admazurkevich:/home/admazurkevich# chmod 2755 /var/log/journal/
root@admazurkevich:/home/admazurkevich# killall -USR1 systemd-journald
root@admazurkevich:/home/admazurkevich# journalctl -b
Oct 01 11:15:07 admazurkevich.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-bu
Oct 01 11:15:07 admazurkevich.localdomain kernel: Command line: BOOT_IMAGE=(hd,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-provided physical RAM map:
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000009fbff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000000009fc00-0x00000000000009ffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000000009f000-0x0000000000000fffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000000100000-0x0000000000000dfffff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000000dffff000-0x0000000000000dffffff] ACPI data
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000fec00fff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x000000000fee00000-0x000000000fee00fff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x000000000fffc0000-0x000000000fffffffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000100000000-0x000000001fffffffff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: NX (Execute Disable) protection: active
Oct 01 11:15:07 admazurkevich.localdomain kernel: APIC: Static calls initialized
Oct 01 11:15:07 admazurkevich.localdomain kernel: SMBIOS 2.5 present.
Oct 01 11:15:07 admazurkevich.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 01 11:15:07 admazurkevich.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 01 11:15:07 admazurkevich.localdomain kernel: Hypervisor detected: KVM
Oct 01 11:15:07 admazurkevich.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 01 11:15:07 admazurkevich.localdomain kernel: kvm-clock: using sched offset of 4069948781 cycles
Oct 01 11:15:07 admazurkevich.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd
Oct 01 11:15:07 admazurkevich.localdomain kernel: tsc: Detected 3187.198 MHz processor
Oct 01 11:15:07 admazurkevich.localdomain kernel: e820: update [mem 0x000000000-0x000000fff] usable ==> reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: e820: remove [mem 0x000a00000-0x0000fffff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 01 11:15:07 admazurkevich.localdomain kernel: total RAM covered: 4096M
```

Рис. 21: Перенос журналов и вывод сообщений загрузки

Выводы по проделанной работе

В ходе лабораторной работы были освоены приёмы работы с системными журналами Linux. Была выполнена настройка перенаправления логов веб-сервера Apache в отдельные файлы, создан отладочный журнал, а также освоены фильтрация и просмотр событий через `journalctl`.

Полученные навыки позволяют эффективно контролировать работу системы и администрировать сервисы.