

Лабораторная работа №7

Управление журналами событий в системе

Турсунов Мухамметназар

10 октября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Получить навыки работы с системными журналами Linux, включая настройку служб **rsyslog** и **systemd-journald**, а также анализ событий при помощи утилиты **journalctl**.

Ход выполнения работы

Мониторинг системных событий

```
root@mtursunov:/home/mtursunov# tail -f /var/log/messages
Oct 10 11:59:18 mtursunov systemd-coredump[3862]: Process 3858 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Oct 10 11:59:18 mtursunov systemd[1]: Started systemd-coredump@25-3862-0.service - Process Core Dump (PID 3862/UID 0).
Oct 10 11:59:18 mtursunov systemd-coredump[3863]: Process 3858 (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 3861:#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 0x00007fd4e16d3b68 start_thread (libc.so.6 + 0x94b68)#012#5 0x00007fd4e17446bc __clone3 (libc.so.6 + 0x1056bc)#012#012Stack trace of thread 3859:#012#0 0x00007fd4e17424bd syscall (libc.so.6 + 0x1034bd)#012#1 0x000000000434c30 n/a (n/a + 0x0)#012#2 0x000000000450bfb n/a (n/a + 0x0)#012#3 0x00000000043566a n/a (n/a + 0x0)#012#4 0x00000000045041c n/a (n/a + 0x0)#012#5 0x0000000004355d0 n/a (n/a + 0x0)#012#6 0x00007fd4e16d3b68 start_thread (libc.so.6 + 0x94b68)#012#7 0x00007fd4e17446bc __clone3 (libc.so.6 + 0x1056bc)#012#012Stack trace of thread 3858:#012#0 0x00007fd4e17424bd syscall (libc.so.6 + 0x1034bd)#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 0x00007fd4e166930e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x00007fd4e16693c9 __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 10 11:59:18 mtursunov systemd[1]: systemd-coredump@25-3862-0.service: Deactivated successfully.
Oct 10 11:59:21 mtursunov systemd[1]: fprintd.service: Deactivated successfully.
Oct 10 11:59:23 mtursunov kernel: traps: VBoxClient[3878] trap int3 ip:41dd1b sp:7fd4d2fb4cd0 error:0 in VBoxClient[1dd1b,400000+bb000]
Oct 10 11:59:23 mtursunov systemd-coredump[3879]: Process 3875 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Oct 10 11:59:23 mtursunov systemd[1]: Started systemd-coredump@26-3879-0.service - Process Core Dump (PID 3879/UID 0).
```

Рис. 1: Мониторинг системных событий через tail -f /var/log/messages

Ошибка авторизации su -

```
000000004344e2 n/a (n/a + 0x0)#012#2 0x000000000450066 n/a (n/a + 0x0)#012#3 0x000000000405123 n/a
(n/a + 0x0)#012#4 0x00007fd4e166930e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x00007fd4e166
93c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x0000000004044aa n/a (n/a + 0x0)#012EL
F object binary architecture: AMD x86-64
Oct 10 12:00:24 mtursunov systemd[1]: systemd-coredump@38-4013-0.service: Deactivated successfully.
Oct 10 12:00:27 mtursunov su[4000]: FAILED SU (to root) mtursunov on pts/2
Oct 10 12:00:29 mtursunov kernel: traps: VBoxClient[4024] trap int3 ip:41dd1b sp:7fd4d2fb4cd0 error:0 in
VBoxClient[1dd1b,400000+bb000]
Oct 10 12:00:29 mtursunov systemd-coredump[4025]: Process 4021 (VBoxClient) of user 1000 terminated abno
rmally with signal 5/TRAP, processing...
Oct 10 12:00:29 mtursunov systemd[1]: Started systemd-coredump@39-4025-0.service - Process Core Dump (PI
D 4025/UID 0).
Oct 10 12:00:29 mtursunov systemd-coredump[4026]: Process 4021 (VBoxClient) of user 1000 dumped core.#01
```

Рис. 2: Ошибка авторизации при попытке su -

```
libc.so.6 + 0x1054bd) #012#1 0x00000000004544e2 n/a (n/a + 0x0) #012#2 0x00000000004500bb n/a (n/a + 0x0)
) #012#3 0x0000000000405123 n/a (n/a + 0x0) #012#4 0x00007fd4e166930e __libc_start_call_main (libc.so.6
+ 0x2a30e) #012#5 0x00007fd4e16693c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9) #012#6 0x000000
00004044aa n/a (n/a + 0x0) #012ELF object binary architecture: AMD x86-64
Oct 10 12:02:02 mtursunov systemd[1]: systemd-coredump@57-4230-0.service: Deactivated successfully.
Oct 10 12:02:03 mtursunov mtursunov[4236]: hello
Oct 10 12:02:07 mtursunov kernel: traps: VBoxClient[4241] trap int3 ip:41dd1b sp:7fd4d2fb4cd0 error:0 in
VBoxClient[1dd1b,400000+bb000]
Oct 10 12:02:07 mtursunov systemd-coredump[4242]: Process 4238 (VBoxClient) of user 1000 terminated abno
rmally with signal 5/TRAP, processing...
Oct 10 12:02:07 mtursunov systemd[1]: Started systemd-coredump@58-4242-0.service - Process Core Dump (PI
D 4242/UID 0).
```

Рис. 3: Результат работы команды logger hello

```
root@mtursunov:/home/mtursunov# tail -n 20 /var/log/secure
Oct 10 11:47:01 mtursunov su[5607]: pam_unix(su:session): session opened for user root(uid=0) by mtursunov(uid=1000)
Oct 10 11:51:50 mtursunov su[5607]: pam_unix(su:session): session closed for user root
Oct 10 11:51:56 mtursunov su[6299]: pam_unix(su:session): session opened for user root(uid=0) by mtursunov(uid=1000)
Oct 10 11:55:54 mtursunov sshd[1207]: Server listening on 0.0.0.0 port 22.
Oct 10 11:55:54 mtursunov sshd[1207]: Server listening on :: port 22.
Oct 10 11:55:55 mtursunov (systemd)[1332]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)
Oct 10 11:55:56 mtursunov gdm-launch-environment[1251]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=42) by (uid=0)
Oct 10 11:57:04 mtursunov gdm-password[2342]: gkr-pam: unable to locate daemon control file
Oct 10 11:57:04 mtursunov gdm-password[2342]: gkr-pam: stashed password to try later in open session
Oct 10 11:57:04 mtursunov (systemd)[2353]: pam_unix(systemd-user:session): session opened for user mtursunov(uid=1000) by mtursunov(uid=0)
Oct 10 11:57:04 mtursunov gdm-password[2342]: pam_unix(gdm-password:session): session opened for user mtursunov(uid=1000) by mtursunov(uid=0)
Oct 10 11:57:04 mtursunov gdm-password[2342]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct 10 11:57:09 mtursunov gdm-launch-environment[1251]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Oct 10 11:58:53 mtursunov (systemd)[3659]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)
Oct 10 11:58:53 mtursunov su[3634]: pam_unix(su:session): session opened for user root(uid=0) by mtursunov(uid=1000)
Oct 10 11:58:59 mtursunov su[3729]: pam_unix(su:session): session opened for user root(uid=0) by mtursunov(uid=1000)
Oct 10 11:59:03 mtursunov su[3793]: pam_unix(su:session): session opened for user root(uid=0) by mtursunov(uid=1000)
Oct 10 12:00:23 mtursunov su[3793]: pam_unix(su:session): session closed for user root
Oct 10 12:00:26 mtursunov unix_chkpwd[40103]: password check failed for user (root)
```



```
root@mtursunov:/home/mtursunov#  
root@mtursunov:/home/mtursunov# tail -f /var/log/httpd/error_log  
[Fri Oct 10 12:06:42.261083 2025] [suexec:notice] [pid 5065:tid 5065] AH01232: suEXEC mechanism enabled  
(wrapper: /usr/sbin/suexec)  
[Fri Oct 10 12:06:42.315202 2025] [lbmethod_heartbeat:notice] [pid 5065:tid 5065] AH02282: No slotmem fr  
om mod_heartbeat  
[Fri Oct 10 12:06:42.316145 2025] [systemd:notice] [pid 5065:tid 5065] SELinux policy enabled; httpd run  
ning as context system_u:system_r:httpd_t:s0  
[Fri Oct 10 12:06:42.317775 2025] [mpm_event:notice] [pid 5065:tid 5065] AH00489: Apache/2.4.63 (Rocky L  
inux) configured -- resuming normal operations  
[Fri Oct 10 12:06:42.317794 2025] [core:notice] [pid 5065:tid 5065] AH00094: Command line: '/usr/sbin/ht  
tpd -D FOREGROUND'
```

Рис. 5: Мониторинг журнала ошибок Apache

Перенаправление логов Apache в системный журнал

```
#
# Some examples:
#ErrorDocument 500 "The server made a boo boo."
#ErrorDocument 404 /missing.html
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#ErrorDocument 402 http://www.example.com/subscription_info.html
#

#
# 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:local
```

^G Help

^O Write Out

^F Where Is

^K Cut

^T Execute

^C Location

M

^X Exit

^R Read File

^N Replace

^U Paste

^J Justify

^/ Go To Line

M

Создание собственного файла логов Apache



```
mtursunov@mtursunov:/etc/rsyslog.d - nano httpd.conf
/etc/rsyslog.d
mtursunov@mtursunov:/home/mtursunov | mtursunov@mtursunov:/home/mtursunov:
GNU nano 8.1 httpd.conf
local1.* -/var/log/httpd-error.log
```

Рис. 7: Создание правила для перенаправления логов Apache

Перезапуск служб rsyslog и httpd

```
root@mtursunov:/home/mtursunov# nano /etc/httpd/conf/httpd.conf
root@mtursunov:/home/mtursunov#
root@mtursunov:/home/mtursunov# cd /etc/rsyslog.d/
root@mtursunov:/etc/rsyslog.d# touch httpd.conf
root@mtursunov:/etc/rsyslog.d# nano httpd.conf
root@mtursunov:/etc/rsyslog.d#
root@mtursunov:/etc/rsyslog.d# systemctl restart rsyslog.service
root@mtursunov:/etc/rsyslog.d# systemctl restart httpd
root@mtursunov:/etc/rsyslog.d#
root@mtursunov:/etc/rsyslog.d# touch debug.conf
root@mtursunov:/etc/rsyslog.d# echo "*.debug /var/log/messages-debug" > debug.conf
root@mtursunov:/etc/rsyslog.d# systemctl restart httpd
root@mtursunov:/etc/rsyslog.d# systemctl restart rsyslog.service
root@mtursunov:/etc/rsyslog.d# █
```

Рис. 8: Перезапуск служб rsyslog и httpd

Запись отладочного сообщения

```
VBoxClient[1dd1b,400000+bb000]
Oct 10 12:13:16 mtursunov systemd-coredump[6880]: Process 6876 (VBoxClient) of user 1000 terminated abno
rmally with signal 5/TRAP, processing...
Oct 10 12:13:16 mtursunov systemd[1]: Started systemd-coredump@189-6880-0.service - Process Core Dump (P
ID 6880/UID 0).
Oct 10 12:13:16 mtursunov root[6883]: Daemon Debug Message
Oct 10 12:13:16 mtursunov systemd-coredump[6881]: Process 6876 (VBoxClient) of user 1000 dumped core.#01
2#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 rp
m libffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012S
tack trace of thread 6879:#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 0x0000
7f44e1643b68 start_thread (/lib64/libc.so.6 + 0x04b68)#012#5 0x00007f44e17445ba __libc_start_main (/lib64/libc.so.6 + 0x1056ba)
```

Рис. 9: Результат регистрации отладочного сообщения через logger

Работа с journalctl

Общий просмотр журнала

```
root@mtursunov:/home/mtursunov# journalctl
Oct 10 11:55:42 mtursunov.localdomain kernel: Linux version 6.12.0-55.37.1.el10_0.x86_64 (mockbuild@iad>
Oct 10 11:55:42 mtursunov.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.37.>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-provided physical RAM map:
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009bfbb] us>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] re>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] re>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] us>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x0000000000dfff0000-0x0000000000dfffffff] AC>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] re>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] re>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] re>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x0000000010000000-0x0000000011ffffffff] us>
Oct 10 11:55:42 mtursunov.localdomain kernel: NX (Execute Disable) protection: active
Oct 10 11:55:42 mtursunov.localdomain kernel: APIC: Static calls initialized
Oct 10 11:55:42 mtursunov.localdomain kernel: SMBIOS 2.5 present.
Oct 10 11:55:42 mtursunov.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox >
Oct 10 11:55:42 mtursunov.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 10 11:55:42 mtursunov.localdomain kernel: Hypervisor detected: KVM
Oct 10 11:55:42 mtursunov.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 10 11:55:42 mtursunov.localdomain kernel: kvm-clock: using sched offset of 4573410790 cycles
Oct 10 11:55:42 mtursunov.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycl>
Oct 10 11:55:42 mtursunov.localdomain kernel: tsc: Detected 3187.206 MHz processor
Oct 10 11:55:42 mtursunov.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reser>
Oct 10 11:55:42 mtursunov.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Oct 10 11:55:42 mtursunov.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 10 11:55:42 mtursunov.localdomain kernel: total RAM covered: 4096M
Oct 10 11:55:42 mtursunov.localdomain kernel: Found optimal setting for mtrr clean up
Oct 10 11:55:42 mtursunov.localdomain kernel: page size: 64K chunk size: 1G sum page: 28
```

Рис. 10: Просмотр системного журнала с момента загрузки

Просмотр журнала в реальном времени

```
Oct 10 12:16:20 mtursunov.localdomain kernel: traps: VBoxClient[7331] trap int3 ip:41dd1b sp:7fd4d2fb4cd
0 error:0 in VBoxClient[1dd1b,400000+bb000]
Oct 10 12:16:20 mtursunov.localdomain systemd-coredump[7332]: Process 7328 (VBoxClient) of user 1000 ter
minated abnormally with signal 5/TRAP, processing...
Oct 10 12:16:20 mtursunov.localdomain systemd[1]: Started systemd-coredump@225-7332-0.service - Process
Core Dump (PID 7332/UID 0).
Oct 10 12:16:20 mtursunov.localdomain systemd-coredump[7333]: [^] Process 7328 (VBoxClient) of user 1000
dumped core.

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

so.6 + 0x94b68)                               Stack trace of thread 7331:
+ 0x1056bc)                                  #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  0x00007fd4e16d3b68 start_thread (libc.
                                              #5  0x00007fd4e17446bc __clone3 (libc.so.6

                                              Stack trace of thread 7330:
                                              #0  0x00007fd4e17424bd syscall (libc.so.6
```

Рис. 11: Просмотр журнала в реальном времени

Параметры фильтрации journalctl

```
Oct 10 12:17:26 mtursunov.localdomain systemd-coredump[7471]: Process 7466 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Oct 10 12:17:26 mtursunov.localdomain systemd[1]: Started systemd-coredump@238-7470-0.service - Process Core Dump (PID 7470/UID 0).
Oct 10 12:17:26 mtursunov.localdomain systemd-coredump[7471]: [^] Process 7466 (VBoxClient) of user 1000 dumped core.

                                     Module libXau.so.6 from rpm libXau-1.0.11-
                                     Module libxcb.so.1 from rpm libxcb-1.17.0-
                                     Module libX11.so.6 from rpm libX11-1.8.10-
                                     Module libffi.so.8 from rpm libffi-3.4.4-9
                                     Module libwayland-client.so.0 from rpm way
                                     Stack trace of thread 7469:
                                     #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  0x00007fd4e16d3b68 start_thread (libc.
                                     #5  0x00007fd4e17446bc __clone3 (libc.so.6
                                     Stack trace of thread 7466:
                                     #0  0x00007fd4e17424bd syscall (libc.so.6
                                     #1  0x00000000004344e2 n/a (n/a + 0x0)

8.el10.x86_64
3.el10.x86_64
1.el10.x86_64
.el10.x86_64
land-1.23.0-2.el10.x86_64

so.6 + 0x94b68)
+ 0x1056bc)
+ 0x1034bd)
```

Рис. 12: Отображение параметров фильтрации journalctl

```
root@mtursunov:~# journalctl
root@mtursunov:/home/mtursunov# journalctl
Display all 128 possibilities? (y or n)
_AUDIT_LOGINUID=                                JOB_TYPE=
_AUDIT_SESSION=                                JOURNAL_NAME=
AVAILABLE=                                       JOURNAL_PATH=
AVAILABLE_PRETTY=                               _KERNEL_DEVICE=
_BOOT_ID=                                       _KERNEL_SUBSYSTEM=
_CAP_EFFECTIVE=                                KERNEL_USEC=
_CMDLINE=                                       LEADER=
CODE_FILE=                                     LIMIT=
CODE_FUNC=                                    LIMIT_PRETTY=
CODE_LINE=                                     _LINE_BREAK=
_COMM=                                         _MACHINE_ID=
CONFIG_FILE=                                  MAX_USE=
CONFIG_LINE=                                  MAX_USE_PRETTY=
COREDUMP_CGROUP=                              MEMORY_PEAK=
COREDUMP_CMDLINE=                             MEMORY_SWAP_PEAK=
COREDUMP_COMM=                                MESSAGE=
COREDUMP_CWD=                                 MESSAGE_ID=
COREDUMP_ENVIRON=                             NM_DEVICE=
COREDUMP_EXE=                                 NM_LOG_DOMAINS=
COREDUMP_FILENAME=                            NM_LOG_LEVEL=
COREDUMP_GID=                                 _PID=
COREDUMP_HOSTNAME=                            PODMAN_EVENT=
COREDUMP_OPEN_FDS=                           PODMAN_TIME=
COREDUMP_OWNER_UID=                           PODMAN_TYPE=
COREDUMP_PACKAGE_JSON=                       PRIORITY=
COREDUMP_PID=                                 REALMD_OPERATION=
COREDUMP_PROC_AUXV=                           _RUNTIME_SCOPE=
COREDUMP_PROC_CGROUP=                         _SYSTEMD_CGROUP=
```

Последние строки журнала

```
root@mtursunov:/home/mtursunov# journalctl _UID=0
Oct 10 11:55:42 mtursunov.localdomain systemd-journald[280]: Collecting audit messages is disabled.
Oct 10 11:55:42 mtursunov.localdomain systemd-journald[280]: Journal started
Oct 10 11:55:42 mtursunov.localdomain systemd-journald[280]: Runtime Journal (/run/log/journal/a055ff80>
Oct 10 11:55:42 mtursunov.localdomain systemd-modules-load[281]: Module 'msr' is built in
Oct 10 11:55:42 mtursunov.localdomain systemd-modules-load[281]: Inserted module 'fuse'
Oct 10 11:55:42 mtursunov.localdomain systemd-modules-load[281]: Module 'scsi_dh_alua' is built in
Oct 10 11:55:42 mtursunov.localdomain systemd-modules-load[281]: Module 'scsi_dh_emc' is built in
Oct 10 11:55:42 mtursunov.localdomain systemd-modules-load[281]: Module 'scsi_dh_rdac' is built in
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Starting systemd-sysusers.service - Create System Use>
Oct 10 11:55:42 mtursunov.localdomain systemd-sysusers[296]: Creating group 'nobody' with GID 65534.
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variab>
Oct 10 11:55:42 mtursunov.localdomain systemd-sysusers[296]: Creating group 'users' with GID 100.
Oct 10 11:55:42 mtursunov.localdomain systemd-sysusers[296]: Creating group 'systemd-journal' with GID >
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Finished systemd-sysusers.service - Create System Use>
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create >
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Finished systemd-vconsole-setup.service - Virtual Con>
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: dracut-cmdline-ask.service - dracut ask for additiona>
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Starting dracut-cmdline.service - dracut cmdline hook>
Oct 10 11:55:42 mtursunov.localdomain dracut-cmdline[308]: dracut-105-4.el10_0
Oct 10 11:55:42 mtursunov.localdomain dracut-cmdline[308]: Using kernel command line parameters: BOO>
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev.service - Create >
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Finished dracut-cmdline.service - dracut cmdline hook.
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Starting dracut-pre-udev.service - dracut pre-udev ho>
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Finished dracut-pre-udev.service - dracut pre-udev ho>
```

Рис. 14: Отображение последних 20 строк журнала

```
root@mtursunov:/home/mtursunov# journalctl -n 20
Oct 10 12:18:53 mtursunov.localdomain kernel: traps: VBoxClient[7660] trap int3 ip:41dd1b sp:7fd4d2fb4c>
Oct 10 12:18:53 mtursunov.localdomain systemd-coredump[7661]: Process 7657 (VBoxClient) of user 1000 te>
Oct 10 12:18:53 mtursunov.localdomain systemd[1]: Started systemd-coredump@255-7661-0.service - Process>
Oct 10 12:18:53 mtursunov.localdomain systemd-coredump[7664]: [..] Process 7657 (VBoxClient) of user 100>

Module libXau.so.6 from rpm libXau-1.0.11>
Module libxcb.so.1 from rpm libxcb-1.17.0>
Module libX11.so.6 from rpm libX11-1.8.10>
Module libffi.so.8 from rpm libffi-3.4.4->
Module libwayland-client.so.0 from rpm wa>
Stack trace of thread 7660:
#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 0x00007fd4e16d3b68 start_thread (libc>
#5 0x00007fd4e17446bc __clone3 (libc.so.>

Stack trace of thread 7658:
#0 0x00007fd4e17424bd syscall (libc.so.6>
#1 0x0000000000434c30 n/a (n/a + 0x0)
#2 0x0000000000450bfb n/a (n/a + 0x0)
#3 0x000000000043566a n/a (n/a + 0x0)
#4 0x000000000045041c n/a (n/a + 0x0)
```

Рис. 15: Просмотр сообщений об ошибках

Просмотр по времени

```
root@mtursunov: /home/mtursunov# journalctl -p err
Oct 10 11:55:42 mtursunov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be run>
Oct 10 11:55:42 mtursunov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is >
Oct 10 11:55:42 mtursunov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a sup>
Oct 10 11:55:49 mtursunov.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Oct 10 11:55:51 mtursunov.localdomain alsactl[917]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error:>
Oct 10 11:57:04 mtursunov.localdomain gdm-password[2342]: gkr-pam: unable to locate daemon control file
Oct 10 11:57:10 mtursunov.localdomain systemd-coredump[3187]: [?] Process 3158 (VBoxClient) of user 100>

Module libXau.so.6 from rpm libXau-1.0.11>
Module libxcb.so.1 from rpm libxcb-1.17.0>
Module libX11.so.6 from rpm libX11-1.8.10>
Module libffi.so.8 from rpm libffi-3.4.4->
Module libwayland-client.so.0 from rpm wa>

Stack trace of thread 3161:
#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  0x00007fd4e16d3b68 start_thread (libc>
#5  0x00007fd4e17446bc __clone3 (libc.so.>

Stack trace of thread 3158:
#0  0x00007fd4e17424bd syscall (libc.so.6>
#1  0x00000000004344e2 n/a (n/a + 0x0)
```

Рис. 16: Просмотр журнала с фильтром по времени

Ошибки со вчерашнего дня

```
root@mtursunov:/home/mtursunov# journalctl --since yesterday
Oct 10 11:55:42 mtursunov.localdomain kernel: Linux version 6.12.0-55.37.1.el10_0.x86_64 (mockbuild@iad
Oct 10 11:55:42 mtursunov.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.37.>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-provided physical RAM map:
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] us>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] re>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] re>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfefff] us>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000dffff000-0x00000000dfffffff] AC>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] re>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] re>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] re>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x0000000010000000-0x0000000011fffffff] us>
Oct 10 11:55:42 mtursunov.localdomain kernel: NX (Execute Disable) protection: active
Oct 10 11:55:42 mtursunov.localdomain kernel: APIC: Static calls initialized
Oct 10 11:55:42 mtursunov.localdomain kernel: SMBIOS 2.5 present.
Oct 10 11:55:42 mtursunov.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox >
Oct 10 11:55:42 mtursunov.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 10 11:55:42 mtursunov.localdomain kernel: Hypervisor detected: KVM
Oct 10 11:55:42 mtursunov.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 10 11:55:42 mtursunov.localdomain kernel: kvm-clock: using sched offset of 4573410790 cycles
Oct 10 11:55:42 mtursunov.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycl>
Oct 10 11:55:42 mtursunov.localdomain kernel: tsc: Detected 3187.206 MHz processor
Oct 10 11:55:42 mtursunov.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> rese>
Oct 10 11:55:42 mtursunov.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Oct 10 11:55:42 mtursunov.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 10 11:55:42 mtursunov.localdomain kernel: total RAM covered: 4096M
Oct 10 11:55:42 mtursunov.localdomain kernel: Found optimal setting for mtrr clean up
Oct 10 11:55:42 mtursunov.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> rese>
```

Рис. 17: Просмотр ошибок со вчерашнего дня

Подробный вывод (verbose)

```
root@mtursunov:/home/mtursunov# journalctl --since yesterday -p err
Oct 10 11:55:42 mtursunov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be run>
Oct 10 11:55:42 mtursunov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is >
Oct 10 11:55:42 mtursunov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a sup>
Oct 10 11:55:49 mtursunov.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Oct 10 11:55:51 mtursunov.localdomain alsactl[917]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error:>
Oct 10 11:57:04 mtursunov.localdomain gdm-password[2342]: gkr-pam: unable to locate daemon control file
Oct 10 11:57:10 mtursunov.localdomain systemd-coredump[3187]: [..] Process 3158 (VBoxClient) of user 100>

Module libXau.so.6 from rpm libXau-1.0.11>
Module libxcb.so.1 from rpm libxcb-1.17.0>
Module libX11.so.6 from rpm libX11-1.8.10>
Module libffi.so.8 from rpm libffi-3.4.4->
Module libwayland-client.so.0 from rpm wa>
Stack trace of thread 3161:
#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  0x00007fd4e16d3b68 start_thread (libc>
#5  0x00007fd4e17446bc __clone3 (libc.so.>

Stack trace of thread 3158:
#0  0x00007fd4e17424bd syscall (libc.so.6>
#1  0x0000000004344a2 n/a (n/a + 0x0)
#2  0x000000000450066 n/a (n/a + 0x0)
#3  0x000000000405123 n/a (n/a + 0x0)
#4  0x00007fd4e166930e __libc_start_call_>
#5  0x00007fd4e166930e __libc_start_main
```

Рис. 18: Режим подробного вывода verbose

```
_RUNTIME_SCOPE=initrd
Fri 2025-10-10 11:55:42.723607 MSK [s=18507d14dc3449e39968f5c00a0bf2de;i=2;b=e5d51ff71c3049c58f1cdc5764>
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=e5d51ff71c3049c58f1cdc5764919953
_MACHINE_ID=a055ff809d5a4a55b89dacba4a93a2a5
_HOSTNAME=mtursunov.localdomain
_RUNTIME_SCOPE=initrd
PRIORITY=6
MESSAGE=Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.37.1.el10_0.x86_64 root=/dev/mapper/r
Fri 2025-10-10 11:55:42.723613 MSK [s=18507d14dc3449e39968f5c00a0bf2de;i=3;b=e5d51ff71c3049c58f1cdc5764>
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
root@mtursunov:/home/mtursunov# journalctl _SYSTEMD_UNIT=sshd.service
Oct 10 11:55:54 mtursunov.localdomain (sshd)[1207]: sshd.service: Referenced but unset environment var
Oct 10 11:55:54 mtursunov.localdomain sshd[1207]: Server listening on 0.0.0.0 port 22.
Oct 10 11:55:54 mtursunov.localdomain sshd[1207]: Server listening on :: port 22.
root@mtursunov:/home/mtursunov#
```

Рис. 19: Просмотр событий службы SSHD

Постоянный журнал journald

Создание постоянного журнала

```
root@mtursunov:/home/mtursunov#  
root@mtursunov:/home/mtursunov# mkdir -p /var/log/journal  
root@mtursunov:/home/mtursunov# chown root:systemd-journal /var/log/journal/  
root@mtursunov:/home/mtursunov# chmod 775 /var/log/journal/  
root@mtursunov:/home/mtursunov# killall -USR1 systemd-journald  
root@mtursunov:/home/mtursunov# journalctl -b  
Oct 10 11:55:42 mtursunov.localdomain kernel: Linux version 6.12.0-55.37.1.el10_0.x86_64 (mockbuild@iad>  
Oct 10 11:55:42 mtursunov.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.37.>  
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-provided physical RAM map:  
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] us>  
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] re>  
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000ffff] re>  
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dffff] us>  
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000dffff000-0x00000000dfffffff] AC>  
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] re>  
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee0ffff] re>  
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] re>  
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x0000000010000000-0x0000000011fffffff] us>  
Oct 10 11:55:42 mtursunov.localdomain kernel: NX (Execute Disable) protection: active  
Oct 10 11:55:42 mtursunov.localdomain kernel: APIC: Static calls initialized  
Oct 10 11:55:42 mtursunov.localdomain kernel: SMBIOS 2.5 present.  
Oct 10 11:55:42 mtursunov.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox >  
Oct 10 11:55:42 mtursunov.localdomain kernel: DMI: Memory slots populated: 0/0  
Oct 10 11:55:42 mtursunov.localdomain kernel: Hypervisor detected: KVM  
Oct 10 11:55:42 mtursunov.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
```

Рис. 20: Настройка постоянного журнала journald

Итоги работы

В ходе работы были изучены механизмы регистрации и хранения системных событий в Linux. Были освоены приёмы настройки **rsyslog**, перенаправления логов веб-службы Apache и фильтрации сообщений по уровням приоритета.

Также исследованы возможности **journalctl** по просмотру, фильтрации и анализу событий, а система журналирования **journald** была настроена на постоянное хранение логов.