

Лабораторная работа №7

Управление журналами событий в системе

Лабси Мохаммед

11 октября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

Ход выполнения работы

```
mlabsi@mlabsi:~$ su
Password:
root@mlabsi:/home/mlabsi# tail -f /var/log/messages
Oct 11 11:47:55 mlabsi kernel: traps: VBoxClient[3584] trap int3 ip:41dd1b sp:7f3b9ffb4cd0 error:0
in VBoxClient[1dd1b,400000+bb000]
Oct 11 11:47:55 mlabsi systemd-coredump[3585]: Process 3581 (VBoxClient) of user 1000 terminated ab
normally with signal 5/TRAP, processing...
Oct 11 11:47:55 mlabsi systemd[1]: Started systemd-coredump@38-3585-0.service - Process Core Dump (
PID 3585/UID 0).
Oct 11 11:47:55 mlabsi systemd-coredump[3586]: Process 3581 (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 libxc
b-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 3584:#012#0 0x00000000041dd1b n/a (n/a + 0x0)#012#1 0x0000
00000041dc94 n/a (n/a + 0x0)#012#2 0x000000000045041c n/a (n/a + 0x0)#012#3 0x00000000004355d0 n/
a (n/a + 0x0)#012#4 0x00007f3bae6c011a start_thread (libc.so.6 + 0x9511a)#012#5 0x00007f3bae730c3
c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 3581:#012#0 0x00007f3bae72ea3d sysc
all (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 0x00007f3bae65530e __libc_start_call_m
ain (libc.so.6 + 0x2a30e)#012#5 0x00007f3bae6553c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a
3c9)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Oct 11 11:47:55 mlabsi systemd[1]: systemd-coredump@38-3585-0.service: Deactivated successfully.
Oct 11 11:48:00 mlabsi kernel: traps: VBoxClient[3598] trap int3 ip:41dd1b sp:7f3b9ffb4cd0 error:0
in VBoxClient[1dd1b,400000+bb000]
```

Рис. 1: Мониторинг системных событий в реальном времени

```
Oct 11 11:48:20 mlabsi systemd[1]: session-c4.scope: Deactivated successfully.
Oct 11 11:48:20 mlabsi systemd-logind[886]: Session c4 logged out. Waiting for processes to exit.
Oct 11 11:48:20 mlabsi systemd-logind[886]: Removed session c4.
Oct 11 11:48:21 mlabsi systemd[1]: Starting fprintd.service - Fingerprint Authentication Daemon...
Oct 11 11:48:21 mlabsi systemd[1]: Started fprintd.service - Fingerprint Authentication Daemon.
Oct 11 11:48:25 mlabsi su[3658]: FAILED SU (to root) mlabsi on pts/2
Oct 11 11:48:25 mlabsi kernel: traps: VBoxClient[3671] trap int3 ip:41dd1b sp:7f3b9ffb4cd0 error:0
in VBoxClient[1dd1b,400000+bb000]
Oct 11 11:48:25 mlabsi systemd-coredump[3672]: Process 3668 (VBoxClient) of user 1000 terminated ab
normally with signal 5/TRAP, processing...
Oct 11 11:48:25 mlabsi systemd[1]: Started systemd-coredump@44-3672-0.service - Process Core Dump (
PID 3672/UID 0).
Oct 11 11:48:25 mlabsi systemd-coredump[3673]: Process 3668 (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 libxc
b-1.17.0-3.el10.x86_64#012Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Module libffi.
```

Рис. 2: Ошибка авторизации при вводе неправильного пароля root

```
all (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 0x00007f3bae65530e __libc_start_call_m
ain (libc.so.6 + 0x2a30e)#012#5 0x00007f3bae6553c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a
3c9)#012#6 0x0000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Oct 11 11:48:46 mlabsi systemd[1]: systemd-coredump@48-3717-0.service: Deactivated successfully.
Oct 11 11:48:49 mlabsi mlabsi[3723]: hello
Oct 11 11:48:51 mlabsi kernel: traps: VBoxClient[3728] trap int3 ip:41ddb sp:7f3b9ffb4cd0 error:0
in VBoxClient[1ddb,400000+bb000]
Oct 11 11:48:51 mlabsi systemd-coredump[3729]: Process 3725 (VBoxClient) of user 1000 terminated ab
normally with signal 5/TRAP, processing...
Oct 11 11:48:51 mlabsi systemd[1]: Started systemd-coredump@49-3729-0.service - Process Core Dump (
PID 3729/UID 0).
Oct 11 11:48:51 mlabsi systemd-coredump[3730]: Process 3725 (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 libxc
```

Рис. 3: Отображение пользовательского сообщения logger в системном журнале

Просмотр /var/log/secure

```
root@mlabsi:/home/mlabsi# tail -n 20 /var/log/secure
Oct 11 11:40:15 mlabsi su[3673]: pam_unix(su:session): session closed for user root
Oct 11 11:40:21 mlabsi su[5964]: pam_unix(su:session): session opened for user root(uid=0) by mlabsi(uid=1000)
Oct 11 11:43:45 mlabsi su[5964]: pam_unix(su:session): session closed for user root
Oct 11 11:44:09 mlabsi sshd[1178]: Server listening on 0.0.0.0 port 22.
Oct 11 11:44:09 mlabsi sshd[1178]: Server listening on :: port 22.
Oct 11 11:44:09 mlabsi (systemd)[1230]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm
(uid=0)
Oct 11 11:44:10 mlabsi gdm-launch-environment][1223]: pam_unix(gdm-launch-environment:session): session opened for
user gdm(uid=42) by (uid=0)
Oct 11 11:44:34 mlabsi gdm-password][1924]: gkr-pam: unable to locate daemon control file
Oct 11 11:44:34 mlabsi gdm-password][1924]: gkr-pam: stashed password to try later in open session
Oct 11 11:44:34 mlabsi (systemd)[1935]: pam_unix(systemd-user:session): session opened for user mlabsi(uid=1000) b
y mlabsi(uid=0)
Oct 11 11:44:34 mlabsi gdm-password][1924]: pam_unix(gdm-password:session): session opened for user mlabsi(uid=100
0) by mlabsi(uid=0)
Oct 11 11:44:34 mlabsi gdm-password][1924]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct 11 11:44:39 mlabsi gdm-launch-environment][1223]: pam_unix(gdm-launch-environment:session): session closed for
user gdm
Oct 11 11:47:37 mlabsi (systemd)[3399]: pam_unix(systemd-user:session): session opened for user root(uid=0) by roo
t(uid=0)
Oct 11 11:47:38 mlabsi su[3384]: pam_unix(su:session): session opened for user root(uid=0) by mlabsi(uid=1000)
Oct 11 11:47:48 mlabsi su[3492]: pam_unix(su:session): session opened for user root(uid=0) by mlabsi(uid=1000)
Oct 11 11:47:53 mlabsi su[3554]: pam_unix(su:session): session opened for user root(uid=0) by mlabsi(uid=1000)
Oct 11 11:48:20 mlabsi su[3554]: pam_unix(su:session): session closed for user root
Oct 11 11:48:23 mlabsi unix_chkpwd[3667]: password check failed for user (root)
Oct 11 11:48:23 mlabsi su[3658]: pam_unix(su:auth): authentication failure; logname=mlabsi uid=1000 euid=0 tty=/de
v/pts/2 ruser=mlabsi rhost= user=root
root@mlabsi:/home/mlabsi#
```

Рис. 4: Просмотр журнала /var/log/secure с записями об ошибках авторизации

Изменение правил rsyslog.conf

```
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

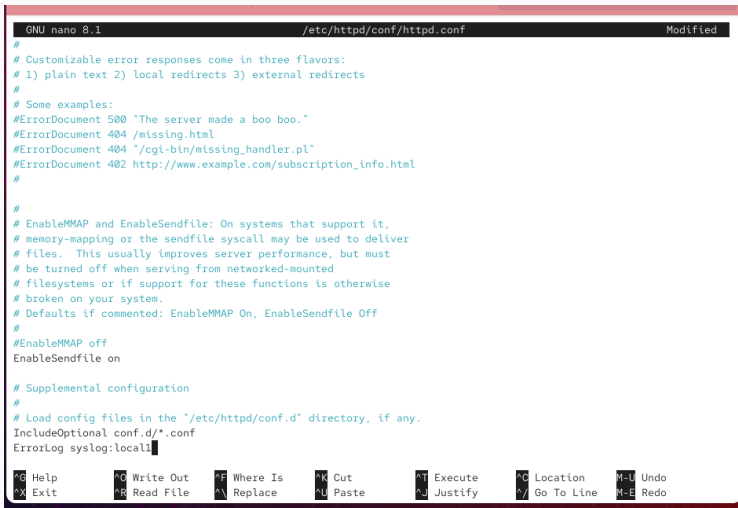
Complete!
root@mlabsi:/home/mlabsi# systemctl start httpd
root@mlabsi:/home/mlabsi# systemctl enable httpd
Created symlink '/etc/systemd/system/multi-user.target.wants/httpd.service' → '/usr/lib/systemd/system/httpd.service'.
root@mlabsi:/home/mlabsi#
```

Рис. 5: Установка и запуск службы Apache HTTPD

```
root@mlabs1:/home/mlabs1#  
root@mlabs1:/home/mlabs1# tail -f /var/log/httpd/error_log  
[Sat Oct 11 11:51:43.633306 2025] [suexec:notice] [pid 4354:tid 4354] AH01232: suEXEC mechanism enabled (wrapper:  
/usr/sbin/suexec)  
[Sat Oct 11 11:51:43.690045 2025] [lbmethod_heartbeat:notice] [pid 4354:tid 4354] AH02282: No slotmem from mod_he  
artmonitor  
[Sat Oct 11 11:51:43.691327 2025] [systemd:notice] [pid 4354:tid 4354] SELinux policy enabled; httpd running as co  
ntext system_u:system_r:httpd_t:s0  
[Sat Oct 11 11:51:43.694412 2025] [mpm_event:notice] [pid 4354:tid 4354] AH00489: Apache/2.4.63 (Rocky Linux) conf  
igured -- resuming normal operations  
[Sat Oct 11 11:51:43.694426 2025] [core:notice] [pid 4354:tid 4354] AH00094: Command line: '/usr/sbin/httpd -D FOR  
EGROUND'
```

Рис. 6: Мониторинг журнала ошибок Apache в режиме реального времени

Настройка передачи логов в syslog



```
GNU nano 8.1 /etc/httpd/conf/httpd.conf Modified
#
# Customizable error responses come in three flavors:
# 1) plain text 2) local redirects 3) external redirects
#
# 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-U Undo
^X Exit ^R Read File ^N Replace ^U Paste ^J Justify ^_ Go To Line M-E Redo

Рис. 7: Добавление перенаправления логов в syslog в конфигурации Apache

Конфигурация rsyslog для Apache



```
mlabsi@mlabsi:/etc/rsyslog.d - nano httpd.conf
mlabsi@mlabsi:/home/mlabsi | mlabsi@mlabsi:/home/mlabsi

GNU nano 8.1 httpd.conf
local1.* -/var/log/httpd-error.log
```

Рис. 8: Создание файла конфигурации для логов Apache в rsyslog

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

Рис. 9: Создание конфигурационного файла debug.conf для отладочных сообщений

```
3bae730c3c __clone3 (libc.so.6 + 0x105c3c)#012Stack trace of thread 5982:#012#0 0x00007f3bae72ea3d syscall (l  
libc.so.6 + 0x103a3d)#012#1 0x00000000004344e2 n/a (n/a + 0x0)#012#2 0x0000000000450066 n/a (n/a + 0x0)#012#3 0x  
0000000000405123 n/a (n/a + 0x0)#012#4 0x00007f3bae65530e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x0  
0007f3bae6553c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012E  
LF object binary architecture: AMD x86-64  
Oct 11 11:58:12 mlabsi systemd[1]: systemd-coredump@159-5986-0.service: Deactivated successfully.  
Oct 11 11:58:16 mlabsi root[5992]: Daemon Debug Message  
Oct 11 11:58:17 mlabsi kernel: traps: VBoxClient[5997] trap int3 ip:41ddb1b sp:7f3b9ffb4cd0 error:0 in VBoxClient[1  
ddb1b,400000+bb000]  
Oct 11 11:58:17 mlabsi systemd-coredump[5998]: Process 5994 (VBoxClient) of user 1000 terminated abnormally with s  
ignal 5/TRAP, processing...  
Oct 11 11:58:17 mlabsi systemd[1]: Started systemd-coredump@160-5998-0.service - Process Core Dump (PID 5998/UID 0  
).  
Oct 11 11:58:17 mlabsi systemd-coredump[5999]: Process 5994 (VBoxClient) of user 1000 dumped core.#012#012Module l
```

Рис. 10: Результат записи отладочного сообщения в лог /var/log/messages-debug

Использование journalctl

Просмотр журнала системы

```
root@mlabs1:/home/mlabs1# journalctl
Oct 11 11:43:59 mlabs1.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build0)
Oct 11 11:43:59 mlabs1.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_64
Oct 11 11:43:59 mlabs1.localdomain kernel: BIOS-provided physical RAM map:
Oct 11 11:43:59 mlabs1.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 11 11:43:59 mlabs1.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 11 11:43:59 mlabs1.localdomain kernel: BIOS-e820: [mem 0x000000000009f000-0x000000000000ffff] reserved
Oct 11 11:43:59 mlabs1.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dffff] usable
Oct 11 11:43:59 mlabs1.localdomain kernel: BIOS-e820: [mem 0x00000000dffff000-0x00000000dfffffff] ACPI data
Oct 11 11:43:59 mlabs1.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Oct 11 11:43:59 mlabs1.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Oct 11 11:43:59 mlabs1.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Oct 11 11:43:59 mlabs1.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff] usable
Oct 11 11:43:59 mlabs1.localdomain kernel: NX (Execute Disable) protection: active
Oct 11 11:43:59 mlabs1.localdomain kernel: APIC: Static calls initialized
Oct 11 11:43:59 mlabs1.localdomain kernel: SMBIOS 2.5 present.
Oct 11 11:43:59 mlabs1.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 11 11:43:59 mlabs1.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 11 11:43:59 mlabs1.localdomain kernel: Hypervisor detected: KVM
Oct 11 11:43:59 mlabs1.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 11 11:43:59 mlabs1.localdomain kernel: kvm-clock: using sched offset of 4547104750 cycles
Oct 11 11:43:59 mlabs1.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4
Oct 11 11:43:59 mlabs1.localdomain kernel: tsc: Detected 3187.204 MHz processor
Oct 11 11:43:59 mlabs1.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Oct 11 11:43:59 mlabs1.localdomain kernel: e820: remove [mem 0x000a0000-0x000ffff] usable
Oct 11 11:43:59 mlabs1.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 11 11:43:59 mlabs1.localdomain kernel: total RAM covered: 4096M
Oct 11 11:43:59 mlabs1.localdomain kernel: Found optimal setting for mtrr clean up
Oct 11 11:43:59 mlabs1.localdomain kernel: gran_size: 64K chunk_size: 1G num_reg: 3 los
```

Рис. 11: Просмотр журнала с момента последнего запуска системы

Мониторинг в реальном времени

```
Oct 11 12:00:55 mlabsi.localdomain systemd-coredump[6359]: [P] Process 6354 (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 6357:
                               #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  0x00007f3bae6c011a start_thread (libc.so.6 + 0x9511

                               a)

                               #5  0x00007f3bae730c3c __clone3 (libc.so.6 + 0x105c3c)

                               Stack trace of thread 6354:
                               #0  0x00007f3bae72ea3d syscall (libc.so.6 + 0x103a3d)
                               #1  0x0000000004344e2 n/a (n/a + 0x0)
                               #2  0x000000000450066 n/a (n/a + 0x0)
                               #3  0x000000000405123 n/a (n/a + 0x0)
                               #4  0x00007f3bae65530e __libc_start_call_main (libc.so.

                               6 + 0x2a30e)

                               #5  0x00007f3bae6553c9 __libc_start_main@@GLIBC_2.34 (l

                               ibc.so.6 + 0x2a3c9)

                               #6  0x0000000004044aa n/a (n/a + 0x0)
                               ELF object binary architecture: AMD x86-64

Oct 11 12:00:55 mlabsi.localdomain systemd[1]: systemd-coredump@191-6358-0.service: Deactivated successfully.
root@mlabsi:/home/mlabsi#
```

Рис. 12: Мониторинг системных событий в реальном времени через journalctl

Фильтрация и просмотр UID 0

```
-----/home/mlabsi# journalctl
root@mlabsi:/home/mlabsi# 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=    SEAT_ID=
```

Сообщения уровня ошибки

```
root@mlabsi:/home/mlabsi# journalctl -n 20
Oct 11 12:02:21 mlabsi.localdomain kernel: traps: VBoxClient[6573] trap int3 ip:41dd1b sp:7f3b9ffb4cd0 error:0 in>
Oct 11 12:02:21 mlabsi.localdomain systemd-coredump[6574]: Process 6570 (VBoxClient) of user 1000 terminated abno>
Oct 11 12:02:21 mlabsi.localdomain systemd[1]: Started systemd-coredump@208-6574-0.service - Process Core Dump (P>
Oct 11 12:02:21 mlabsi.localdomain systemd-coredump[6575]: [P] Process 6570 (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-
Stack trace of thread 6573:
#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  0x00007f3bae6c011a start_thread (libc.so.6 + 0x951)
#5  0x00007f3bae730c3c __clone3 (libc.so.6 + 0x105c3c)

Stack trace of thread 6571:
#0  0x00007f3bae72ea3d 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  0x00007f3bae6c011a start_thread (libc.so.6 + 0x951)
#7  0x00007f3bae730c3c __clone3 (libc.so.6 + 0x105c3c)
```

Рис. 14: Просмотр сообщений уровня ошибки в системном журнале

Сообщения со вчерашнего дня

```
root@mlabsi:/home/mlabsi#  
root@mlabsi:/home/mlabsi# journalctl -p err  
Oct 11 11:43:59 mlabsi.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an un  
Oct 11 11:43:59 mlabsi.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken.  
Oct 11 11:43:59 mlabsi.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graphi  
Oct 11 11:44:05 mlabsi.localdomain kernel: Warning: Unmaintained driver is detected: e1000  
Oct 11 11:44:06 mlabsi.localdomain alsactl[911]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to im  
Oct 11 11:44:09 mlabsi.localdomain kernel: Warning: Unmaintained driver is detected: ip_set  
Oct 11 11:44:34 mlabsi.localdomain gdm-password[1924]: gkr-pam: unable to locate daemon control file  
Oct 11 11:44:37 mlabsi.localdomain systemd[1935]: Failed to start app-gnome-gnome\x2dkeyring\x2dsecrets-2042.scop  
Oct 11 11:44:40 mlabsi.localdomain systemd-coredump[2771]: [?] Process 2741 (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-  
Stack trace of thread 2744:  
#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 0x00007f3bae6c011a start_thread (libc.so.6 + 0x951  
#5 0x00007f3bae730c3c __clone3 (libc.so.6 + 0x105c3c)  
  
Stack trace of thread 2741:  
#0 0x00007f3bae72ea3d syscall (libc.so.6 + 0x103a3d)  
#1 0x0000000004344e2 n/a (n/a + 0x0)  
#2 0x000000000450066 n/a (n/a + 0x0)  
#3 0x000000000405123 n/a (n/a + 0x0)
```

Рис. 15: Просмотр системных сообщений со вчерашнего дня

Ошибки со вчерашнего дня

```
root@mlabst: /home/mlabst# journalctl --since yesterday
Oct 11 11:43:59 mlabst.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build0
Oct 11 11:43:59 mlabst.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_
Oct 11 11:43:59 mlabst.localdomain kernel: BIOS-provided physical RAM map:
Oct 11 11:43:59 mlabst.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 11 11:43:59 mlabst.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 11 11:43:59 mlabst.localdomain kernel: BIOS-e820: [mem 0x000000000000f000-0x000000000000ffff] reserved
Oct 11 11:43:59 mlabst.localdomain kernel: BIOS-e820: [mem 0x0000000000010000-0x00000000000dffff] usable
Oct 11 11:43:59 mlabst.localdomain kernel: BIOS-e820: [mem 0x00000000000dff000-0x00000000000dffffff] ACPI data
Oct 11 11:43:59 mlabst.localdomain kernel: BIOS-e820: [mem 0x0000000000fec0000-0x0000000000fec0fff] reserved
Oct 11 11:43:59 mlabst.localdomain kernel: BIOS-e820: [mem 0x0000000000fee0000-0x0000000000fee0fff] reserved
Oct 11 11:43:59 mlabst.localdomain kernel: BIOS-e820: [mem 0x0000000000ffc0000-0x0000000000ffffff] reserved
Oct 11 11:43:59 mlabst.localdomain kernel: BIOS-e820: [mem 0x00000000010000000-0x00000000011ffffff] usable
Oct 11 11:43:59 mlabst.localdomain kernel: NX (Execute Disable) protection: active
Oct 11 11:43:59 mlabst.localdomain kernel: APIC: Static calls initialized
Oct 11 11:43:59 mlabst.localdomain kernel: SMBIOS 2.5 present.
Oct 11 11:43:59 mlabst.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 11 11:43:59 mlabst.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 11 11:43:59 mlabst.localdomain kernel: Hypervisor detected: KVM
Oct 11 11:43:59 mlabst.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 11 11:43:59 mlabst.localdomain kernel: kvm-clock: using sched offset of 4547104750 cycles
Oct 11 11:43:59 mlabst.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4
Oct 11 11:43:59 mlabst.localdomain kernel: tsc: Detected 3187.204 MHz processor
Oct 11 11:43:59 mlabst.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Oct 11 11:43:59 mlabst.localdomain kernel: e820: remove [mem 0x000a0000-0x000ffff] usable
Oct 11 11:43:59 mlabst.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 11 11:43:59 mlabst.localdomain kernel: total RAM covered: 4096M
Oct 11 11:43:59 mlabst.localdomain kernel: Found optimal setting for mtrr clean up
Oct 11 11:43:59 mlabst.localdomain kernel: gran_size: 64K chunk_size: 1G num_reg: 3 los
```

Рис. 16: Просмотр сообщений уровня ошибки со вчерашнего дня

```
_SOURCE_MONOTONIC_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=2d58672aff3745dd80c7e96eed8e4f56
_MACHINE_ID=c371d82aeddd4c358d0da59eb13ae51b
_HOSTNAME=mlabsi.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
Sat 2025-10-11 11:43:59.656303 MSK [s=430e5dc7a419407b8fa750bc257d7bd6;i=2;b=2d58672aff3745dd80c7e96eed8e4f56;m=8>
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=2d58672aff3745dd80c7e96eed8e4f56
root@mlabsi:/home/mlabsi# journalctl _SYSTEMD_UNIT=sshd.service
Oct 11 11:44:09 mlabsi.localdomain (sshd)[1178]: sshd.service: Referenced but unset environment variable evaluated
Oct 11 11:44:09 mlabsi.localdomain sshd[1178]: Server listening on 0.0.0.0 port 22.
Oct 11 11:44:09 mlabsi.localdomain sshd[1178]: Server listening on :: port 22.
...skipping...
Oct 11 11:44:09 mlabsi.localdomain (sshd)[1178]: sshd.service: Referenced but unset environment variable evaluated
Oct 11 11:44:09 mlabsi.localdomain sshd[1178]: Server listening on 0.0.0.0 port 22.
Oct 11 11:44:09 mlabsi.localdomain sshd[1178]: Server listening on :: port 22.
~
~
```

Рис. 17: Просмотр журнала службы SSH

Постоянный журнал journald

Настройка хранения логов

```
root@mlabsi:/home/mlabsi# mkdir -p /var/log/journal
root@mlabsi:/home/mlabsi# chown root:systemd-journal /var/log/journal/
root@mlabsi:/home/mlabsi# chmod 2755 /var/log/journal/
root@mlabsi:/home/mlabsi# killall -USR1 systemd-journald
root@mlabsi:/home/mlabsi# journalctl -b
Oct 11 11:43:59 mlabsi.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build0
Oct 11 11:43:59 mlabsi.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_
Oct 11 11:43:59 mlabsi.localdomain kernel: BIOS-provided physical RAM map:
Oct 11 11:43:59 mlabsi.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 11 11:43:59 mlabsi.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 11 11:43:59 mlabsi.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Oct 11 11:43:59 mlabsi.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] usable
Oct 11 11:43:59 mlabsi.localdomain kernel: BIOS-e820: [mem 0x000000000dff0000-0x000000000dffffff] ACPI data
Oct 11 11:43:59 mlabsi.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] reserved
Oct 11 11:43:59 mlabsi.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee0ffff] reserved
Oct 11 11:43:59 mlabsi.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Oct 11 11:43:59 mlabsi.localdomain kernel: BIOS-e820: [mem 0x0000000010000000-0x0000000011ffffff] usable
Oct 11 11:43:59 mlabsi.localdomain kernel: NX (Execute Disable) protection: active
Oct 11 11:43:59 mlabsi.localdomain kernel: APIC: Static calls initialized
```

Рис. 18: Настройка постоянного журнала journald и просмотр системных сообщений после перезапуска службы

Заключение

В ходе лабораторной работы были освоены принципы работы с системными журналами, фильтрации событий и настройки постоянного хранения логов с помощью **rsyslog** и **journald**.