

Отчёт по лабораторной работе №7

Управление журналами событий в системе

Борисенкова София Павловна

1 октября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

Выполнение лабораторной работы



```
root@localhost:~# sudo -i
spborisenkova@localhost:~$ whoami
spborisenkova
spborisenkova@localhost:~$ id
uid=1000(spborisenkova) gid=1000(spborisenkova) groups=1000(spborisenkova),10(wheel) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
spborisenkova@localhost:~$ sudo -i
[sudo] password for spborisenkova:
root@localhost:~# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
root@localhost:~# ezit
bash: ezit: command not found...
root@localhost:~#
```

Рис. 1: Ошибка аутентификации при su

```
0000000000000000 n/a (n/a + 0x0)0000000000000000 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9)
#012#5 0x00007fd708b283c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x0000000000004044
aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Sep 28 13:02:41 dsyakovleva systemd[1]: systemd-coredump@101-4924-0.service: Deactivated successfully.
Sep 28 13:02:44 dsyakovleva dsyakovleva[4930]: hello
Sep 28 13:02:45 dsyakovleva dsyakovleva[4932]: hello
Sep 28 13:02:45 dsyakovleva dsyakovleva[4939]: hello
Sep 28 13:02:46 dsyakovleva kernel: traps: VBoxClient[4944] trap int3 ip:41ddb sp:7fd6fa4cfcd0 error:
0 in VBoxClient[1ddb,400000+bb000]
Sep 28 13:02:46 dsyakovleva systemd-coredump[4945]: Process 4941 (VBoxClient) of user 1000 terminated
abnormally with signal 5/TRAP, processing...
Sep 28 13:02:46 dsyakovleva systemd[1]: Started systemd-coredump@102-4945-0.service - Process Core Dum
p (PID 4945/UID 0).
Sep 28 13:02:46 dsyakovleva systemd-coredump[4946]: Process 4941 (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 libwavland-client.so.0 from rpm wavland-1.23.0-2.el10.x
```

Рис. 2: Сообщение logger hello

```
root@dsyakovleva:/home/dsyakovleva# tail -n 20 /var/log/secure
Sep 23 14:43:07 dsyakovleva su[6243]: pam_unix(su:session): session closed for user root
Sep 28 12:52:40 dsyakovleva sshd[1242]: Server listening on 0.0.0.0 port 22.
Sep 28 12:52:40 dsyakovleva sshd[1242]: Server listening on :: port 22.
Sep 28 12:52:41 dsyakovleva (systemd)[1293]: pam_unix(systemd-user:session): session opened for user g
dm(uid=42) by gdm(uid=0)
Sep 28 12:52:43 dsyakovleva gdm-launch-environment][1286]: pam_unix(gdm-launch-environment:session): s
ession opened for user gdm(uid=42) by (uid=0)
Sep 28 12:53:08 dsyakovleva gdm-password][1962]: gkr-pam: unable to locate daemon control file
Sep 28 12:53:08 dsyakovleva gdm-password][1962]: gkr-pam: stashed password to try later in open sessio
n
Sep 28 12:53:08 dsyakovleva (systemd)[2020]: pam_unix(systemd-user:session): session opened for user d
syakovleva(uid=1000) by dsyakovleva(uid=0)
Sep 28 12:53:09 dsyakovleva gdm-password][1962]: pam_unix(gdm-password:session): session opened for us
er dsyakovleva(uid=1000) by dsyakovleva(uid=0)
Sep 28 12:53:09 dsyakovleva gdm-password][1962]: gkr-pam: gnome-keyring-daemon started properly and un
locked keyring
Sep 28 12:53:20 dsyakovleva gdm-launch-environment][1286]: pam_unix(gdm-launch-environment:session): s
ession closed for user gdm
Sep 28 13:00:14 dsyakovleva (systemd)[4472]: pam_unix(systemd-user:session): session opened for user r
oot(uid=0) by root(uid=0)
Sep 28 13:00:15 dsyakovleva su[4445]: pam_unix(su:session): session opened for user root(uid=0) by dsy
akovleva(uid=1000)
Sep 28 13:00:20 dsyakovleva su[4517]: pam_unix(su:session): session opened for user root(uid=0) by dsy
akovleva(uid=1000)
Sep 28 13:00:28 dsyakovleva su[4565]: pam_unix(su:session): session opened for user root(uid=0) by dsy
akovleva(uid=1000)
Sep 28 13:01:58 dsyakovleva su[4445]: pam_unix(su:session): session closed for user root
Sep 28 13:02:01 dsyakovleva unix_chkpwd[4819]: password check failed for user (root)
Sep 28 13:02:01 dsyakovleva su[4810]: pam_unix(su:auth): authentication failure; logname=dsyakovleva u
id=1000 euid=0 tty=/dev/pts/2 ruser=dsyakovleva rhost= user=root
Sep 28 13:02:07 dsyakovleva unix_chkpwd[4833]: password check failed for user (root)
Sep 28 13:02:07 dsyakovleva su[4831]: pam_unix(su:auth): authentication failure; logname=dsyakovleva u
id=1000 euid=0 tty=/dev/pts/2 ruser=dsyakovleva rhost= user=root
root@dsyakovleva:/home/dsyakovleva#
```

Изменение правил rsyslog.conf

```
Installing      : mod_http2-2.0.29-2.el10_0.1.x86_64          9/11
Installing      : mod_lua-2.4.63-1.el10_0.2.x86_64          10/11
Installing      : httpd-2.4.63-1.el10_0.2.x86_64             11/11
Running scriptlet: httpd-2.4.63-1.el10_0.2.x86_64            11/11

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

Рис. 4: Установка и запуск Apache

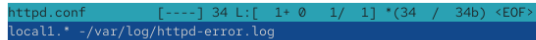

```
root@dsyakovleva:/home/dsyakovleva#  
root@dsyakovleva:/home/dsyakovleva# tail -f /var/log/httpd/error_log  
[Sun Sep 28 13:06:41.350959 2025] [suexec:notice] [pid 5702:tid 5702] AH01232: suEXEC mechanism enable  
d (wrapper: /usr/sbin/suexec)  
[Sun Sep 28 13:06:41.425686 2025] [lbmethod_heartbeat:notice] [pid 5702:tid 5702] AH02282: No slotmem  
from mod_heartbeat  
[Sun Sep 28 13:06:41.427898 2025] [systemd:notice] [pid 5702:tid 5702] SELinux policy enabled; httpd r  
unning as context system_u:system_r:httpd_t:s0  
[Sun Sep 28 13:06:41.436591 2025] [mpm_event:notice] [pid 5702:tid 5702] AH00489: Apache/2.4.63 (Rocky  
Linux) configured -- resuming normal operations  
[Sun Sep 28 13:06:41.436624 2025] [core:notice] [pid 5702:tid 5702] AH00094: Command line: '/usr/sbin/  
httpd -D FOREGROUND'  
^C  
root@dsyakovleva:/home/dsyakovleva#
```

Рис. 5: Просмотр error_log 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:local
```

Рис. 6: Настройка ErrorLog в httpd.conf

A screenshot of a text editor showing an rsyslog configuration rule. The rule is for the file httpd.conf and is located at line 34. The rule's condition is a logical AND of two parts: '1+ 0' and '1/ 1'. The action is to write the message to the file /var/log/httpd-error.log. The rule is terminated with '<EOF>'.

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

Рис. 7: Правило rsyslog для httpd

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

Рис. 8: Создание debug.conf

```
94 n/a (n/a + 0x0)#012#2 0x000000000045041c n/a (n/a + 0x0)#012#3 0x00000000004355d0 n/a (n/a + 0x0)
#012#4 0x00007fd708b9311a start_thread (libc.so.6 + 0x9511a)#012#5 0x00007fd708c03c3c __clone3 (libc
.so.6 + 0x105c3c)#012#012Stack trace of thread 8293:#012#0 0x00007fd708c01a3d syscall (libc.so.6 + 0x
103a3d)#012#1 0x00000000004344e2 n/a (n/a + 0x0)#012#2 0x0000000000450066 n/a (n/a + 0x0)#012#3 0x0
000000000416559 n/a (n/a + 0x0)#012#4 0x000000000041838a n/a (n/a + 0x0)#012#5 0x0000000000417d6a n/
a (n/a + 0x0)#012#6 0x0000000000404860 n/a (n/a + 0x0)#012#7 0x000000000045041c n/a (n/a + 0x0)#012#
8 0x00000000004355d0 n/a (n/a + 0x0)#012#9 0x00007fd708b9311a start_thread (libc.so.6 + 0x9511a)#012
#10 0x00007fd708c03c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 8291:#012#0 0x000
07fd708c01a3d syscall (libc.so.6 + 0x103a3d)#012#1 0x00000000004344e2 n/a (n/a + 0x0)#012#2 0x000000
0000450066 n/a (n/a + 0x0)#012#3 0x0000000000405123 n/a (n/a + 0x0)#012#4 0x00007fd708b2830e __libc_
start_call_main (libc.so.6 + 0x2a30e)#012#5 0x00007fd708b283c9 __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
Sep 28 13:19:09 dsyakovleva systemd[1]: systemd-coredump@282-8295-0.service: Deactivated successfully.
Sep 28 13:19:10 dsyakovleva dsyakovleva[8301]: Daemon Debug Message
```

Рис. 9: Сообщение Daemon Debug Message

Использование journalctl

```
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffffff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: NX (Execute Disable) protection: active
Sep 28 12:52:11 dsyakovleva.localdomain kernel: APIC: Static calls initialized
Sep 28 12:52:11 dsyakovleva.localdomain kernel: SMBIOS 2.5 present.
Sep 28 12:52:11 dsyakovleva.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualB
Sep 28 12:52:11 dsyakovleva.localdomain kernel: DMI: Memory slots populated: 0/0
Sep 28 12:52:11 dsyakovleva.localdomain kernel: Hypervisor detected: KVM
Sep 28 12:52:11 dsyakovleva.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Sep 28 12:52:11 dsyakovleva.localdomain kernel: kvm-clock: using sched offset of 12780091978 cycles
Sep 28 12:52:11 dsyakovleva.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_
Sep 28 12:52:11 dsyakovleva.localdomain kernel: tsc: Detected 2600.000 MHz processor
Sep 28 12:52:11 dsyakovleva.localdomain kernel: e820: update [mem 0x00000000-0x000000fff] usable ==> i
Sep 28 12:52:11 dsyakovleva.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Sep 28 12:52:11 dsyakovleva.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Sep 28 12:52:11 dsyakovleva.localdomain kernel: total RAM covered: 4096M
Sep 28 12:52:11 dsyakovleva.localdomain kernel: Found optimal setting for mtrr clean up
Sep 28 12:52:11 dsyakovleva.localdomain kernel: gran_size: 64K chunk_size: 1G num_re
Sep 28 12:52:11 dsyakovleva.localdomain kernel: MTRR map: 6 entries (3 fixed + 3 variable; max 35), b
Sep 28 12:52:11 dsyakovleva.localdomain kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP
Sep 28 12:52:11 dsyakovleva.localdomain kernel: e820: update [mem 0xe0000000-0xffffffff] usable ==> i
Sep 28 12:52:11 dsyakovleva.localdomain kernel: last_pfn = 0xe0000 max_arch_pfn = 0x400000000
Sep 28 12:52:11 dsyakovleva.localdomain kernel: found SMP MP-table at [mem 0x0009fbf0-0x0009fbff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: RAMDISK: [mem 0x343a1000-0x361c8fff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: ACPI: Early table checksum verification disabled
lines 1-35
```

Рис. 10: Просмотр журнала journalctl

```
.4-7.el10.x86_64
wayland-1.23.0-2.el10.x86_64

libc.so.6 + 0x9511a)
so.6 + 0x105c3c)

o.6 + 0x103a3d)

ll_main (libc.so.6 + 0x2a30e)
in@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)

6-64
Sep 28 13:22:20 dsyakovleva.localdomain systemd[1]: systemd-coredump@317-8745-0.service: Deactivated successfully.
root@dsyakovleva:/etc/rsyslog.d#
```

```
Module libwayland-client.so.0 from rpm

Stack trace of thread 8744:
#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  0x00007fd708b9311a start_thread (l

#5  0x00007fd708c03c3c __clone3 (libc.

Stack trace of thread 8741:
#0  0x00007fd708c01a3d syscall (libc.s
#1  0x0000000004344e2 n/a (n/a + 0x0)
#2  0x000000000450066 n/a (n/a + 0x0)
#3  0x000000000405123 n/a (n/a + 0x0)
#4  0x00007fd708b2830e __libc_start_ca
#5  0x00007fd708b283c9 __libc_start_ma
#6  0x0000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x8
```

Рис. 11: Вывод без пейджера

```
libc.so.6 + 0x9511a)
so.6 + 0x105c3c)
o.6 + 0x103a3d)
ll_main (libc.so.6 + 0x2a30e)
in@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)
6-64
Sep 28 13:22:42 dsyakovleva.localdomain systemd[1]: systemd-coredump@321-8820-0.service: Deactivated successfully.
```

```
#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 0x00007fd708b9311a start_thread (l
#5 0x00007fd708c03c3c __clone3 (libc.
Stack trace of thread 8816:
#0 0x00007fd708c01a3d syscall (libc.s
#1 0x00000000004344e2 n/a (n/a + 0x0)
#2 0x0000000000450066 n/a (n/a + 0x0)
#3 0x0000000000405123 n/a (n/a + 0x0)
#4 0x00007fd708b2830e __libc_start_ca
#5 0x00007fd708b283c9 __libc_start_ma
#6 0x00000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x8
```

Рис. 12: Режим реального времени

Использование journalctl

```
root@dsyakovleva:/etc/rsyslog.d#  
root@dsyakovleva:/etc/rsyslog.d# 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=  
COREDUMP_PROC_LIMITS=    _SELINUX_CONTEXT=  
COREDUMP_PROC_MAPS=      SESSION_ID=  
COREDUMP_PROC_MOUNTINFO= _SOURCE_BOOTTIME_TIMESTAMP=  
COREDUMP_PROC_STATUS=    _SOURCE_MONOTONIC_TIMESTAMP=
```

Использование journalctl

```
root@dsyakovleva:/etc/rsyslog.d# journalctl _UID=0
Sep 28 12:52:11 dsyakovleva.localdomain systemd-journald[303]: Collecting audit messages is disabled.
Sep 28 12:52:11 dsyakovleva.localdomain systemd-journald[303]: Journal started
Sep 28 12:52:11 dsyakovleva.localdomain systemd-journald[303]: Runtime Journal (/run/log/journal/c45e
Sep 28 12:52:11 dsyakovleva.localdomain systemd-modules-load[304]: Module 'msr' is built in
Sep 28 12:52:11 dsyakovleva.localdomain systemd-modules-load[304]: Inserted module 'fuse'
Sep 28 12:52:11 dsyakovleva.localdomain systemd-modules-load[304]: Module 'scsi_dh_alua' is built in
Sep 28 12:52:11 dsyakovleva.localdomain systemd-modules-load[304]: Module 'scsi_dh_emc' is built in
Sep 28 12:52:11 dsyakovleva.localdomain systemd-modules-load[304]: Module 'scsi_dh_rdac' is built in
Sep 28 12:52:11 dsyakovleva.localdomain systemd-sysusers[317]: Creating group 'nobody' with GID 65534.
Sep 28 12:52:11 dsyakovleva.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Va
Sep 28 12:52:11 dsyakovleva.localdomain systemd-sysusers[317]: Creating group 'users' with GID 100.
Sep 28 12:52:11 dsyakovleva.localdomain systemd-sysusers[317]: Creating group 'systemd-journal' with >
Sep 28 12:52:11 dsyakovleva.localdomain systemd[1]: Finished systemd-sysusers.service - Create System>
Sep 28 12:52:11 dsyakovleva.localdomain systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Cre>
Sep 28 12:52:12 dsyakovleva.localdomain systemd[1]: Finished systemd-vconsole-setup.service - Virtual>
Sep 28 12:52:12 dsyakovleva.localdomain systemd[1]: dracut-cmdline-ask.service - dracut ask for addit>
Sep 28 12:52:12 dsyakovleva.localdomain systemd[1]: Starting dracut-cmdline.service - dracut cmdline >
Sep 28 12:52:12 dsyakovleva.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev.service - Cre>
Sep 28 12:52:12 dsyakovleva.localdomain dracut-cmdline[332]: dracut-105-4.el10_0
Sep 28 12:52:12 dsyakovleva.localdomain dracut-cmdline[332]: Using kernel command line parameters: >
Sep 28 12:52:12 dsyakovleva.localdomain systemd[1]: Finished dracut-cmdline.service - dracut cmdline >
Sep 28 12:52:12 dsyakovleva.localdomain systemd[1]: Starting dracut-pre-udev.service - dracut pre-ude>
Sep 28 12:52:12 dsyakovleva.localdomain systemd[1]: Finished dracut-pre-udev.service - dracut pre-ude>
Sep 28 12:52:12 dsyakovleva.localdomain systemd[1]: Starting systemd-udev.service - Rule-based Manag>
```

Рис. 14: UID=0

Использование journalctl

```
root@dsyakovleva:/etc/rsyslog.d# journalctl -n 20
Sep 28 13:24:14 dsyakovleva.localdomain kernel: traps: VBoxClient[9077] trap int3 ip:41dd1b sp:7fd6fa>
Sep 28 13:24:14 dsyakovleva.localdomain systemd-coredump[9078]: Process 9074 (VBoxClient) of user 100>
Sep 28 13:24:14 dsyakovleva.localdomain systemd[1]: Started systemd-coredump@338-9078-0.service - Pro>
Sep 28 13:24:14 dsyakovleva.localdomain systemd-coredump[9080]: [...] Process 9074 (VBoxClient) of user>

Module libXau.so.6 from rpm libXau-1.>
Module libxcb.so.1 from rpm libxcb-1.>
Module libX11.so.6 from rpm libX11-1.>
Module libffi.so.8 from rpm libffi-3.>
Module libwayland-client.so.0 from rp>
Stack trace of thread 9077:
#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 0x00007fd708b9311a start_thread (>
#5 0x00007fd708c03c3c __clone3 (libc>

Stack trace of thread 9076:
#0 0x00007fd708c01a3d syscall (libc.>
#1 0x0000000004344e2 n/a (n/a + 0x0>
#2 0x000000000450066 n/a (n/a + 0x0>
#3 0x000000000416559 n/a (n/a + 0x0>
#4 0x00000000041838a n/a (n/a + 0x0>
```

Рис. 15: Последние 20 строк

Использование journalctl

```
-----
root@dsyakovleva:/etc/rsyslog.d# journalctl -p err
Sep 28 12:52:13 dsyakovleva.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be
Sep 28 12:52:13 dsyakovleva.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration
Sep 28 12:52:13 dsyakovleva.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a
Sep 28 12:52:29 dsyakovleva.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Sep 28 12:52:33 dsyakovleva.localdomain alsactl[961]: alsa-lib main.c:1554:(snd_use_case_mgr_open) er
Sep 28 12:52:39 dsyakovleva.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Sep 28 12:53:08 dsyakovleva.localdomain gdm-password[1962]: gkr-pam: unable to locate daemon control
Sep 28 12:53:28 dsyakovleva.localdomain systemd-coredump[2919]: [?] Process 2892 (VBoxClient) of user

Module libXau.so.6 from rpm libXau-1.
Module libxcb.so.1 from rpm libxcb-1.
Module libX11.so.6 from rpm libX11-1.
Module libffi.so.8 from rpm libffi-3.
Module libwayland-client.so.0 from rp
Stack trace of thread 2896:
#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  0x00007fd708b9311a start_thread (>
#5  0x00007fd708c03c3c __clone3 (libc>

Stack trace of thread 2895:
#0  0x00007fd708c01a3d syscall (libc.>
```

Рис. 16: Сообщения об ошибках

Использование journalctl

```
root@dsyakovleva:/etc/rsyslog.d#  
root@dsyakovleva:/etc/rsyslog.d# journalctl --since yesterday  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild)  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-provided physical RAM map:  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbf5  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000ffffff  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dfffff  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x00000000dffff0000-0x00000000dfffffff  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000fffffff  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: NX (Execute Disable) protection: active  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: APIC: Static calls initialized  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: SMBIOS 2.5 present.  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualB  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: DMI: Memory slots populated: 0/0  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: Hypervisor detected: KVM  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: kvm-clock: using sched offset of 12780091978 cycles  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_>  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: tsc: Detected 2600.000 MHz processor  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> 1x  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: e820: remove [mem 0x000a0000-0x000ffff] usable  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: total RAM covered: 4096M  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: Found optimal setting for mtrr clean up  
Sep 28 12:52:11 dsyakovleva.localdomain kernel: gran_size: 64K chunk_size: 1G num_res
```

Рис. 17: Со вчерашнего дня

Использование journalctl

```
root@dsyakovleva:/etc/rsyslog.d# journalctl --since yesterday -p err
Sep 28 12:52:13 dsyakovleva.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be
Sep 28 12:52:13 dsyakovleva.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration
Sep 28 12:52:13 dsyakovleva.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a
Sep 28 12:52:29 dsyakovleva.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Sep 28 12:52:33 dsyakovleva.localdomain alsactl[961]: alsa-lib main.c:1554:(snd_use_case_mgr_open) er
Sep 28 12:52:39 dsyakovleva.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Sep 28 12:53:08 dsyakovleva.localdomain gdm-password[1962]: gkr-pam: unable to locate daemon control
Sep 28 12:53:28 dsyakovleva.localdomain systemd-coredump[2919]: [?] Process 2892 (VBoxClient) of user

Module libXau.so.6 from rpm libXau-1.
Module libxcb.so.1 from rpm libxcb-1.
Module libX11.so.6 from rpm libX11-1.
Module libffi.so.8 from rpm libffi-3.
Module libwayland-client.so.0 from rp
Stack trace of thread 2896:
#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  0x00007fd708b9311a start_thread (>
#5  0x00007fd708c03c3c __clone3 (libc>

Stack trace of thread 2895:
#0  0x00007fd708c01a3d syscall (libc.>
#1  0x00000000004344e2 n/a (n/a + 0x0)
#2  0x0000000000450066 n/a (n/a + 0x0)
#3  0x0000000000416559 n/a (n/a + 0x0)
#4  0x000000000041838a n/a (n/a + 0x0)
```

Рис. 18: Ошибки со вчерашнего дня

Использование journalctl

```
SYSLOG_IDENTIFIER=kernel
MESSAGE=Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylin>
_BOOT_ID=5d214b2b8577473c95527448648f8c97
_MACHINE_ID=c45e6ab54e4b49419e9e0ed8a3067adb
_HOSTNAME=dsyakovleva.localdomain
_RUNTIME_SCOPE=initrd
Sun 2025-09-28 12:52:11.716156 MSK [s=7a5c03ff2d0a4ebeb0d612ca1e6bd408;i=2;b=5d214b2b8577473c95527448>
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=5d214b2b8577473c95527448648f8c97
_MACHINE_ID=c45e6ab54e4b49419e9e0ed8a3067adb
_HOSTNAME=dsyakovleva.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>
Sun 2025-09-28 12:52:11.716197 MSK [s=7a5c03ff2d0a4ebeb0d612ca1e6bd408;i=3;b=5d214b2b8577473c95527448>
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=5d214b2b8577473c95527448648f8c97
_MACHINE_ID=c45e6ab54e4b49419e9e0ed8a3067adb
_HOSTNAME=dsyakovleva.localdomain
_RUNTIME_SCOPE=initrd
PRIORITY=6
lines 1-35
```

Рис. 19: Подробный вывод verbose

```
root@dsyakovleva:/etc/rsyslog.d#  
root@dsyakovleva:/etc/rsyslog.d# journalctl _SYSTEMD_UNIT=sshd.service  
Sep 28 12:52:39 dsyakovleva.localdomain (sshd)[1242]: sshd.service: Referenced but unset environment  
Sep 28 12:52:40 dsyakovleva.localdomain sshd[1242]: Server listening on 0.0.0.0 port 22.  
Sep 28 12:52:40 dsyakovleva.localdomain sshd[1242]: Server listening on :: port 22.  
lines 1-3/3 (END)
```

Рис. 20: Журнал sshd


```
root@dsyakovleva:/etc/rsyslog.d#  
root@dsyakovleva:/etc/rsyslog.d# journalctl _SYSTEMD_UNIT=sshd.service  
Sep 28 12:52:39 dsyakovleva.localdomain (sshd)[1242]: sshd.service: Referenced but unset environment  
Sep 28 12:52:40 dsyakovleva.localdomain sshd[1242]: Server listening on 0.0.0.0 port 22.  
Sep 28 12:52:40 dsyakovleva.localdomain sshd[1242]: Server listening on :: port 22.  
root@dsyakovleva:/etc/rsyslog.d#  
root@dsyakovleva:/etc/rsyslog.d# mkdir -p /var/log/journal  
root@dsyakovleva:/etc/rsyslog.d# chown root:systemd-journal /var/log/journal/  
root@dsyakovleva:/etc/rsyslog.d# chmod 2755 /var/log/journal/  
root@dsyakovleva:/etc/rsyslog.d# killall -USR1 systemd-journald  
root@dsyakovleva:/etc/rsyslog.d# journalctl -b
```

Рис. 21: Создание каталога journald

```
root@dnyakovleva:/etc/rsyslog.d#  
root@dnyakovleva:/etc/rsyslog.d# mkdir -p /var/log/journal  
root@dnyakovleva:/etc/rsyslog.d# chown root:systemd-journal /var/log/journal/  
root@dnyakovleva:/etc/rsyslog.d# chmod 2755 /var/log/journal/  
root@dnyakovleva:/etc/rsyslog.d# killall -USR1 systemd-journald  
root@dnyakovleva:/etc/rsyslog.d# journalctl -b  
Sep 28 12:52:11 dnyakovleva.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild)  
Sep 28 12:52:11 dnyakovleva.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55  
Sep 28 12:52:11 dnyakovleva.localdomain kernel: BIOS-provided physical RAM map:  
Sep 28 12:52:11 dnyakovleva.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff]  
Sep 28 12:52:11 dnyakovleva.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff]  
Sep 28 12:52:11 dnyakovleva.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff]  
Sep 28 12:52:11 dnyakovleva.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff]  
Sep 28 12:52:11 dnyakovleva.localdomain kernel: BIOS-e820: [mem 0x0000000000dfff0000-0x0000000000dfffffff]  
Sep 28 12:52:11 dnyakovleva.localdomain kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000fec00fff]  
Sep 28 12:52:11 dnyakovleva.localdomain kernel: BIOS-e820: [mem 0x000000000fee00000-0x000000000fee00fff]  
Sep 28 12:52:11 dnyakovleva.localdomain kernel: BIOS-e820: [mem 0x000000000fffc0000-0x000000000fffffffff]  
Sep 28 12:52:11 dnyakovleva.localdomain kernel: BIOS-e820: [mem 0x00000000100000000-0x0000000011fffffffff]  
Sep 28 12:52:11 dnyakovleva.localdomain kernel: NX (Execute Disable) protection: active
```

Рис. 22: Активация journald

Контрольные вопросы

- Основной файл — `/etc/rsyslog.conf`
- Файлы правил — `/etc/rsyslog.d/`
- Журнал аутентификации - `/var/log/secure`

- По умолчанию — раз в неделю
- Хранение — 4 недели (`logrotate`)

- Режим реального времени: `journalctl -f`
- Сообщения PID 1 с 9:00 до 15:00:
`journalctl _PID=1 --since "09:00" --until "15:00"`
- После перезагрузки: `journalctl -b`

Итоги работы

Были приобретены навыки мониторинга системных журналов и настройки регистрации событий в Linux:

работа с `tail`, настройка `rsyslog`, использование `logger`, исследование логов при помощи `journalctl` и настройка постоянного хранения с помощью `journald`.