

Лабораторная работа №7

Управление журналами событий в системе

Руслан Алиев

16 декабря 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

Ход выполнения работы

Мониторинг системных событий

```
raliev@raliev:~$ su
Password:
root@raliev:/home/raliev# tail -f /var/log/messages
Oct 3 17:00:02 raliev kernel: traps: VBoxClient[6730] trap int3 ip:41ddb sp:7fc8e2435cd0 error:0 in VB
oxClient[1ddb,400000+bb000]
Oct 3 17:00:02 raliev systemd-coredump[6731]: Process 6727 (VBoxClient) of user 1000 terminated abnorma
lly with signal 5/TRAP, processing...
Oct 3 17:00:02 raliev systemd[1]: Started systemd-coredump@280-6731-0.service - Process Core Dump (PID
6731/UID 0).
Oct 3 17:00:02 raliev systemd-coredump[6732]: Process 6727 (VBoxClient) of user 1000 dumped core.#012#0
12Module 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 l
ibffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stac
k trace of thread 6730:#012#0 0x00000000041ddb n/a (n/a + 0x0)#012#1 0x00000000041dc94 n/a (n/a + 0
x0)#012#2 0x00000000045041c n/a (n/a + 0x0)#012#3 0x0000000004355d0 n/a (n/a + 0x0)#012#4 0x00007fc
8f0add1a start_thread (libc.so.6 + 0x9511a)#012#5 0x00007fc8f0b4dc3c __clone3 (libc.so.6 + 0x105c3c)#0
12#012Stack trace of thread 6727:#012#0 0x00007fc8f0b4ba3d syscall (libc.so.6 + 0x103a3d)#012#1 0x0000
000004344e2 n/a (n/a + 0x0)#012#2 0x000000000450066 n/a (n/a + 0x0)#012#3 0x000000000405123 n/a (n/
a + 0x0)#012#4 0x00007fc8f0a7230e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x00007fc8f0a723c
9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x0000000004044aa n/a (n/a + 0x0)#012ELF o
bject binary architecture: AMD x86-64
Oct 3 17:00:02 raliev systemd[1]: systemd-coredump@280-6731-0.service: Deactivated successfully.
Oct 3 17:00:07 raliev kernel: traps: VBoxClient[6742] trap int3 ip:41ddb sp:7fc8e2435cd0 error:0 in VB
oxClient[1ddb,400000+bb000]
Oct 3 17:00:07 raliev systemd-coredump[6743]: Process 6739 (VBoxClient) of user 1000 terminated abnorma
lly with signal 5/TRAP, processing...
Oct 3 17:00:07 raliev systemd[1]: Started systemd-coredump@281-6743-0.service - Process Core Dump (PID
6743/UID 0).
```

Рис. 1: Мониторинг /var/log/messages

```
Oct 3 17:00:38 raliiev systemd-coredump[6827]: Process 6822 (VBoxClient) of user 1000 dumped core.#012#0
12Module 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 l
ibffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stac
k trace of thread 6825:#012#0 0x00000000041dd1b n/a (n/a + 0x0)#012#1 0x00000000041dc94 n/a (n/a + 0
x0)#012#2 0x00000000045041c n/a (n/a + 0x0)#012#3 0x0000000004355d0 n/a (n/a + 0x0)#012#4 0x00007fc
8f0add11a start_thread (libc.so.6 + 0x9511a)#012#5 0x00007fc8f0b4dc3c __clone3 (libc.so.6 + 0x105c3c)#0
12#012Stack trace of thread 6823:#012#0 0x00007fc8f0b4ba3d syscall (libc.so.6 + 0x103a3d)#012#1 0x0000
00000434c30 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 0x00
007fc8f0add11a start_thread (libc.so.6 + 0x9511a)#012#7 0x00007fc8f0b4dc3c __clone3 (libc.so.6 + 0x105c
3c)#012#012Stack trace of thread 6822:#012#0 0x00007fc8f0b4ba3d syscall (libc.so.6 + 0x103a3d)#012#1 0
x0000000004344e2 n/a (n/a + 0x0)#012#2 0x000000000450066 n/a (n/a + 0x0)#012#3 0x000000000405123 n/
a (n/a + 0x0)#012#4 0x00007fc8f0a7230e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x00007fc8f0
a723c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x0000000004044aa n/a (n/a + 0x0)#012
ELF object binary architecture: AMD x86-64
Oct 3 17:00:38 raliiev systemd[1]: systemd-coredump@287-6826-0.service: Deactivated successfully.
Oct 3 17:00:38 raliiev su[6812]: FAILED SU (to root) raliiev on pts/2
```

Рис. 2: FAILED SU (to root)

```
aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Oct 3 17:01:04 raliiev systemd[1]: systemd-coredump@292-6895-0.service: Deactivated successfully.
Oct 3 17:01:06 raliiev systemd[1]: fprintd.service: Deactivated successfully.
Oct 3 17:01:07 raliiev raliiev[6904]: hello
Oct 3 17:01:09 raliiev kernel: traps: VBoxClient[6909] trap int3 ip:41ddb sp:7fc8e2435cd0 error:0 in VB
oxClient[1ddb,400000+bb000]
Oct 3 17:01:09 raliiev systemd-coredump[6910]: Process 6906 (VBoxClient) of user 1000 terminated abnorma
lly with signal 5/TRAP, processing...
Oct 3 17:01:09 raliiev systemd[1]: Started systemd-coredump@293-6910-0.service - Process Core Dump (PID
6910/UID 0).
Oct 3 17:01:09 raliiev systemd-coredump[6911]: Process 6906 (VBoxClient) of user 1000 dumped core.#012#0
12Module 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 l
```

Рис. 3: Сообщение logger hello

```
root@raliev:/home/raliev# tail -n 20 /var/log/secure
Oct 3 16:36:07 raliev gdm-password][1924]: gkr-pam: unable to locate daemon control file
Oct 3 16:36:07 raliev gdm-password][1924]: gkr-pam: stashed password to try later in open session
Oct 3 16:36:07 raliev (systemd)[1936]: pam_unix(systemd-user:session): session opened for user raliev(uid=1000) by raliev(uid=0)
Oct 3 16:36:07 raliev gdm-password][1924]: pam_unix(gdm-password:session): session opened for user raliev(uid=1000) by raliev(uid=0)
Oct 3 16:36:07 raliev gdm-password][1924]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct 3 16:36:13 raliev gdm-launch-environment][1212]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Oct 3 16:38:53 raliev (systemd)[3376]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)
Oct 3 16:38:53 raliev su[3351]: pam_unix(su:session): session opened for user root(uid=0) by raliev(uid=1000)
Oct 3 16:47:52 raliev su[3351]: pam_unix(su:session): session closed for user root
Oct 3 16:48:49 raliev su[4902]: pam_unix(su:session): session opened for user root(uid=0) by raliev(uid=1000)
Oct 3 16:53:07 raliev su[5521]: pam_unix(su:session): session opened for user root(uid=0) by raliev(uid=1000)
Oct 3 16:53:08 raliev su[4902]: pam_unix(su:session): session closed for user root
Oct 3 16:57:34 raliev su[5521]: pam_unix(su:session): session closed for user root
Oct 3 16:59:47 raliev (systemd)[6554]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)
```

Рис. 4: Журнал /var/log/secure

Настройка rsyslog (Apache)

```
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :                                1/1
  Installing     : apr-1.7.5-2.el10.x86_64        1/11
  Installing     : apr-util-lmdb-1.6.3-21.el10.x86_64 2/11
  Installing     : apr-util-openssl-1.6.3-21.el10.x86_64 3/11
  Installing     : apr-util-1.6.3-21.el10.x86_64     4/11
  Installing     : httpd-tools-2.4.63-1.el10_0.2.x86_64 5/11
  Installing     : rocky-logos-httpd-100.4-7.el10.noarch 6/11
Running scriptlet: httpd-filesystem-2.4.63-1.el10_0.2.noarch 7/11
  Installing     : httpd-filesystem-2.4.63-1.el10_0.2.noarch 7/11
  Installing     : httpd-core-2.4.63-1.el10_0.2.x86_64 8/11
  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-1.6.3-21.el10.x86_64
  apr-util-lmdb-1.6.3-21.el10.x86_64 apr-util-openssl-1.6.3-21.el10.x86_64
  httpd-2.4.63-1.el10_0.2.x86_64   httpd-core-2.4.63-1.el10_0.2.x86_64
  httpd-filesystem-2.4.63-1.el10_0.2.noarch httpd-tools-2.4.63-1.el10_0.2.x86_64
  mod_http2-2.0.29-2.el10_0.1.x86_64 mod_lua-2.4.63-1.el10_0.2.x86_64
  rocky-logos-httpd-100.4-7.el10.noarch

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

Рис. 5: Установка и запуск httpd

```
root@raliev:/home/raliev# tail -f /var/log/httpd/error_log
[Fri Oct 03 17:02:43.229529 2025] [suexec:notice] [pid 7330:tid 7330] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri Oct 03 17:02:43.275760 2025] [lbmethod_heartbeat:notice] [pid 7330:tid 7330] AH02282: No slotmem from mod_heartbeat
[Fri Oct 03 17:02:43.277016 2025] [systemd:notice] [pid 7330:tid 7330] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Fri Oct 03 17:02:43.278954 2025] [mpm_event:notice] [pid 7330:tid 7330] AH00489: Apache/2.4.63 (Rocky Linux) configured -- resuming normal operations
[Fri Oct 03 17:02:43.278970 2025] [core:notice] [pid 7330:tid 7330] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
```

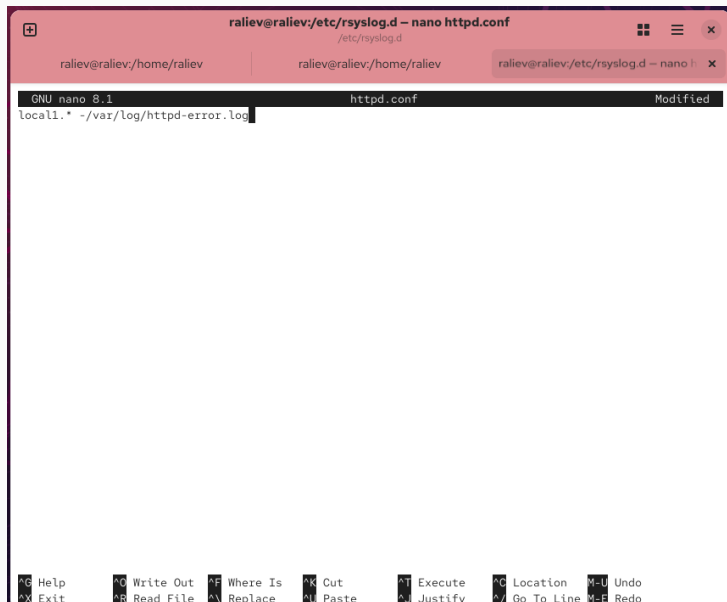
Рис. 6: Журнал ошибок httpd

Перенаправление логов Apache

```
raliev@raliev:/home/raliev  raliev@raliev:/home/raliev  raliev@raliev:/home/raliev – nano /etc/httpd/conf/httpd.conf x
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:local1
```

^G Help	^O Write Out	^F Where Is	^K Cut	^T Execute	^C Location	M-U Undo
^X Exit	^R Read File	^L Replace	^U Paste	^J Justify	^_ Go To Line	M-E Redo

Конфигурация rsyslog для Apache



The screenshot shows a terminal window with a nano editor editing the file `/etc/rsyslog.d/httpd.conf`. The window title is `raliev@raliev:/etc/rsyslog.d - nano httpd.conf`. The terminal shows the command `local1.* -/var/log/httpd-error.log` being entered. The nano editor's status bar at the bottom displays various keyboard shortcuts for editing and navigation.

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

Help Write Out Where Is Cut Execute Location M-U Undo
Exit Read File Replace Paste Justify Go To Line M-E Redo

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

Рис. 9: debug.conf для rsyslog

```
Oct 3 17:09:08 raliiev systemd[1]: systemd-coredump@387-8923-0.service: Deactivated successfully.
Oct 3 17:09:10 raliiev root[8930]: daemon debug message
Oct 3 17:09:13 raliiev kernel: traps: VBoxClient[8935] trap int3 ip:41dd1b sp:7fc8e2435cd0 error:0 in VB
oxClient[1dd1b,400000+bb000]
Oct 3 17:09:13 raliiev systemd-coredump[8936]: Process 8932 (VBoxClient) of user 1000 terminated abnorma
lly with signal 5/TRAP, processing...
Oct 3 17:09:13 raliiev systemd[1]: Started systemd-coredump@388-8936-0.service - Process Core Dump (PID
8936/UID 0).
Oct 3 17:09:13 raliiev systemd-coredump[8937]: Process 8932 (VBoxClient) of user 1000 dumped core.#012#0
12Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3
```

Рис. 10: Daemon Debug Message

Использование journalctl

```
root@raliev:/home/raliev# journalctl
Oct 03 16:35:43 raliev.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-p>
Oct 03 16:35:43 raliev.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.e>
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-provided physical RAM map:
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reser>
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reser>
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfeffff] usable
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x0000000000dfff0000-0x0000000000dfffffff] ACPI >
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000fec00ffff] reser>
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x000000000fee00000-0x000000000fee00ffff] reser>
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x000000000fffc0000-0x000000000fffffffff] reser>
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x00000000100000000-0x0000000011fffffffff] usable
Oct 03 16:35:43 raliev.localdomain kernel: NX (Execute Disable) protection: active
Oct 03 16:35:43 raliev.localdomain kernel: APIC: Static calls initialized
Oct 03 16:35:43 raliev.localdomain kernel: SMBIOS 2.5 present.
Oct 03 16:35:43 raliev.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/>
Oct 03 16:35:43 raliev.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 03 16:35:43 raliev.localdomain kernel: Hypervisor detected: KVM
Oct 03 16:35:43 raliev.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 03 16:35:43 raliev.localdomain kernel: kvm-clock: using sched offset of 8508347384 cycles
Oct 03 16:35:43 raliev.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles:>
Oct 03 16:35:43 raliev.localdomain kernel: tsc: Detected 3187.196 MHz processor
Oct 03 16:35:43 raliev.localdomain kernel: e820: update [mem 0x00000000-0x000000ffff] usable ==> reserved
Oct 03 16:35:43 raliev.localdomain kernel: e820: remove [mem 0x000a0000-0x0000fffff] usable
Oct 03 16:35:43 raliev.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 03 16:35:43 raliev.localdomain kernel: total RAM covered: 4096M
Oct 03 16:35:43 raliev.localdomain kernel: Found optimal setting for mtrr clean up
Oct 03 16:35:43 raliev.localdomain kernel: gran_size: 64K chunk_size: 1G num_reg: 3 >
```

Рис. 11: Журнал с момента загрузки

Journalctl без пейджера

```
6 + 0x9511a)
0x105c3c)

x103a3d)

6 + 0x9511a)
0x105c3c)

x103a3d)

(libc.so.6 + 0x2a30e)
BC_2.34 (libc.so.6 + 0x2a3c9)

Oct 03 17:14:09 raliev.localdomain systemd[1]: systemd-coredump@446-9578-0.service: Deactivated successfully.
root@raliev:/home/raliev#
```

```
#5 0x00007fc8f0b4dc3c __clone3 (libc.so.6 +

Stack trace of thread 9575:
#0 0x00007fc8f0b4ba3d syscall (libc.so.6 + 0
#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)
#5 0x00000000004355d0 n/a (n/a + 0x0)
#6 0x00007fc8f0add11a start_thread (libc.so.

#7 0x00007fc8f0b4dc3c __clone3 (libc.so.6 +

Stack trace of thread 9574:
#0 0x00007fc8f0b4ba3d syscall (libc.so.6 + 0
#1 0x00000000004344e2 n/a (n/a + 0x0)
#2 0x0000000000450066 n/a (n/a + 0x0)
#3 0x0000000000405123 n/a (n/a + 0x0)
#4 0x00007fc8f0a7230e __libc_start_call_main
#5 0x00007fc8f0a723c9 __libc_start_main@@GLIBC_2.34
#6 0x00000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x86-64
```

Рис. 12: -no-pager

Journalctl -f (реальное время)

```
l10.x86_64
10.x86_64
d-1.23.0-2.el10.x86_64

6 + 0x9511a)
0x105c3c)

x103a3d)

(libc.so.6 + 0x2a30e)
BC_2.34 (libc.so.6 + 0x2a3c9)

Oct 03 17:14:19 raliev.localdomain systemd[1]: systemd-coredump@448-9603-0.service: Deactivated successfully.
^C
root@raliev:/home/raliev#
```

Module libX11.so.6 from rpm libX11-1.8.10-1.e

Module libffi.so.8 from rpm libffi-3.4.4-9.el

Module libwayland-client.so.0 from rpm waylan

Stack trace of thread 9602:

#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 0x00007fc8f0add11a start_thread (libc.so.

#5 0x00007fc8f0b4dc3c __clone3 (libc.so.6 +

Stack trace of thread 9599:

#0 0x00007fc8f0b4ba3d syscall (libc.so.6 + 0

#1 0x0000000004344e2 n/a (n/a + 0x0)

#2 0x000000000450066 n/a (n/a + 0x0)

#3 0x000000000405123 n/a (n/a + 0x0)

#4 0x00007fc8f0a7230e __libc_start_call_main

#5 0x00007fc8f0a723c9 __libc_start_main@@GLI

#6 0x0000000004044aa n/a (n/a + 0x0)

ELF object binary architecture: AMD x86-64

Рис. 13: Режим реального времени

Фильтрация journalctl

```

root@raliev:/home/raliev# 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=

```

Фильтрация по UID=0

```
root@raliev:/home/raliev# journalctl _UID=0
Oct 03 16:35:43 raliev.localdomain systemd-journald[282]: Collecting audit messages is disabled.
Oct 03 16:35:43 raliev.localdomain systemd-journald[282]: Journal started
Oct 03 16:35:43 raliev.localdomain systemd-journald[282]: Runtime Journal (/run/log/journal/a210e53feae8
Oct 03 16:35:43 raliev.localdomain systemd-modules-load[283]: Module 'msr' is built in
Oct 03 16:35:43 raliev.localdomain systemd-modules-load[283]: Inserted module 'fuse'
Oct 03 16:35:43 raliev.localdomain systemd-modules-load[283]: Module 'scsi_dh_alua' is built in
Oct 03 16:35:43 raliev.localdomain systemd-modules-load[283]: Module 'scsi_dh_emc' is built in
Oct 03 16:35:43 raliev.localdomain systemd-modules-load[283]: Module 'scsi_dh_rdac' is built in
Oct 03 16:35:43 raliev.localdomain systemd-sysusers[295]: Creating group 'nobody' with GID 65534.
Oct 03 16:35:43 raliev.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variables.
Oct 03 16:35:43 raliev.localdomain systemd-sysusers[295]: Creating group 'users' with GID 100.
Oct 03 16:35:43 raliev.localdomain systemd-sysusers[295]: Creating group 'systemd-journal' with GID 190.
Oct 03 16:35:43 raliev.localdomain systemd[1]: Finished systemd-sysusers.service - Create System Users.
Oct 03 16:35:43 raliev.localdomain systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create Sta
Oct 03 16:35:43 raliev.localdomain systemd[1]: Finished systemd-vconsole-setup.service - Virtual Console
Oct 03 16:35:43 raliev.localdomain systemd[1]: dracut-cmdline-ask.service - dracut ask for additional co
Oct 03 16:35:43 raliev.localdomain systemd[1]: Starting dracut-cmdline.service - dracut cmdline hook...
Oct 03 16:35:43 raliev.localdomain dracut-cmdline[309]: dracut-105-4.el10_0
Oct 03 16:35:43 raliev.localdomain dracut-cmdline[309]: Using kernel command line parameters: BOOT_I
Oct 03 16:35:43 raliev.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev.service - Create Sta
Oct 03 16:35:43 raliev.localdomain systemd[1]: Finished dracut-cmdline.service - dracut cmdline hook.
Oct 03 16:35:43 raliev.localdomain systemd[1]: Starting dracut-pre-udev.service - dracut pre-udev hook.
Oct 03 16:35:43 raliev.localdomain systemd[1]: Finished dracut-pre-udev.service - dracut pre-udev hook.
Oct 03 16:35:43 raliev.localdomain systemd[1]: Starting systemd-udevd.service - Rule-based Manager for
Oct 03 16:35:43 raliev.localdomain systemd-udevd[408]: Using default interface naming scheme 'rhel-10.0
Oct 03 16:35:43 raliev.localdomain systemd[1]: Started systemd-udevd.service - Rule-based Manager for D
Oct 03 16:35:43 raliev.localdomain systemd[1]: dracut-pre-trigger.service - dracut pre-trigger hook was
Oct 03 16:35:43 raliev.localdomain systemd[1]: Starting systemd-udev-trigger.service - Coldplug All ude
```

Рис. 15: UID=0

Последние строки журнала

```
root@raliev:/home/raliev# journalctl -n 20
Oct 03 17:15:05 raliev.localdomain kernel: traps: VBoxClient[9707] trap int3 ip:41dd1b sp:7fc8e2435cd0 >
Oct 03 17:15:05 raliev.localdomain systemd-coredump[9708]: Process 9704 (VBoxClient) of user 1000 termi>
Oct 03 17:15:05 raliev.localdomain systemd[1]: Started systemd-coredump@457-9708-0.service - Process Co>
Oct 03 17:15:05 raliev.localdomain systemd-coredump[9709]: [?] Process 9704 (VBoxClient) of user 1000 d>

Module libXau.so.6 from rpm libXau-1.0.11-8.>
Module libxcb.so.1 from rpm libxcb-1.17.0-3.>
Module libX11.so.6 from rpm libX11-1.8.10-1.>
Module libffi.so.8 from rpm libffi-3.4.4-9.e>
Module libwayland-client.so.0 from rpm wayla>
Stack trace of thread 9707:
#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  0x00007fc8f0add11a start_thread (libc.so>
#5  0x00007fc8f0b4dc3c __clone3 (libc.so.6 +>

Stack trace of thread 9706:
#0  0x00007fc8f0b4ba3d syscall (libc.so.6 +>
#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)
#5  0x000000000417d6a n/a (n/a + 0x0)
```

Рис. 16: journalctl -n 20

Ошибки journalctl

```
root@raliev:/home/raliev# journalctl -p err
Oct 03 16:35:43 raliev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running
Oct 03 16:35:43 raliev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken
Oct 03 16:35:43 raliev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported configuration
Oct 03 16:35:50 raliev.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Oct 03 16:35:52 raliev.localdomain alsactl[922]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to create PCM object (rc: -1)
Oct 03 16:35:54 raliev.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Oct 03 16:36:07 raliev.localdomain gdm-password[1924]: gkr-pam: unable to locate daemon control file
Oct 03 16:36:14 raliev.localdomain systemd-coredump[2774]: Process 2749 (VBoxClient) of user 1000 dumped core.

Module libXau.so.6 from rpm libXau-1.0.11-8.el7.x86_64
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el7.x86_64
Module libX11.so.6 from rpm libX11-1.8.10-1.el7.x86_64
Module libffi.so.8 from rpm libffi-3.4.4-9.el7.x86_64
Module libwayland-client.so.0 from rpm wayland-1.18.0-1.el7.x86_64
Stack trace of thread 2753:
#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  0x00007fc8f0add11a start_thread (libc.so.6 + 0x7fc8f0add11a)
#5  0x00007fc8f0b4dc3c __clone3 (libc.so.6 + 0x7fc8f0b4dc3c)

Stack trace of thread 2749:
#0  0x00007fc8f0b4ba3d syscall (libc.so.6 + 0x7fc8f0b4ba3d)
#1  0x0000000004344e2 n/a (n/a + 0x0)
#2  0x000000000450066 n/a (n/a + 0x0)
#3  0x000000000405123 n/a (n/a + 0x0)
#4  0x00007fc8f0a7230e __libc_start_call_main (libc.so.6 + 0x7fc8f0a7230e)
#5  0x0000000000000000 0x0 (0x0 + 0x0)
```

Рис. 17: journalctl -p err

```
root@raliev:/home/raliev# journalctl --since yesterday
Oct 03 16:35:43 raliev.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prd)
Oct 03 16:35:43 raliev.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_64
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-provided physical RAM map:
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000009bfff] usable
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x00000000000009fc00-0x00000000000009ffff] reserved
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x000000000000f00000-0x000000000000ffffff] reserved
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x000000000001000000-0x000000000000dfffffff] usable
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x00000000000dfff00000-0x00000000000dffffff] ACPI
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x000000000fec000000-0x000000000fec00ffff] reserved
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x000000000fee000000-0x000000000fee00ffff] reserved
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x000000000fffc00000-0x000000000fffffffff] reserved
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x000000001000000000-0x0000000011ffffffff] usable
Oct 03 16:35:43 raliev.localdomain kernel: NX (Execute Disable) protection: active
Oct 03 16:35:43 raliev.localdomain kernel: APIC: Static calls initialized
Oct 03 16:35:43 raliev.localdomain kernel: SMBIOS 2.5 present.
Oct 03 16:35:43 raliev.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 03 16:35:43 raliev.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 03 16:35:43 raliev.localdomain kernel: Hypervisor detected: KVM
Oct 03 16:35:43 raliev.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 03 16:35:43 raliev.localdomain kernel: kvm-clock: using sched offset of 8508347384 cycles
Oct 03 16:35:43 raliev.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1000000000000000
Oct 03 16:35:43 raliev.localdomain kernel: tsc: Detected 3187.196 MHz processor
Oct 03 16:35:43 raliev.localdomain kernel: e820: update [mem 0x000000000-0x000000fff] usable ==> reserved
Oct 03 16:35:43 raliev.localdomain kernel: e820: remove [mem 0x000a00000-0x000ffffff] usable
Oct 03 16:35:43 raliev.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 03 16:35:43 raliev.localdomain kernel: total RAM covered: 4096M
Oct 03 16:35:43 raliev.localdomain kernel: Found optimal setting for mtrr clean up
Oct 03 16:35:43 raliev.localdomain kernel: gran_size: 64K chunk_size: 1G num_reg: 3
```

Рис. 18: –since yesterday

Ошибки со вчерашнего дня

```
root@raliev:~/home/raliev# journalctl --since yesterday -p err
Oct 03 16:35:43 raliev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running
Oct 03 16:35:43 raliev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken
Oct 03 16:35:43 raliev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported configuration
Oct 03 16:35:50 raliev.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Oct 03 16:35:52 raliev.localdomain alsactl[922]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to open PCM device
Oct 03 16:35:54 raliev.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Oct 03 16:36:07 raliev.localdomain gdm-password[1924]: gkr-pam: unable to locate daemon control file
Oct 03 16:36:14 raliev.localdomain systemd-coredump[2774]: [P] Process 2749 (VBoxClient) of user 1000 dumped core.

Module libXau.so.6 from rpm libXau-1.0.11-8.el7.x86_64
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el7.x86_64
Module libX11.so.6 from rpm libX11-1.8.10-1.el7.x86_64
Module libffi.so.8 from rpm libffi-3.4.4-9.el7.x86_64
Module libwayland-client.so.0 from rpm wayland-1.18.0-1.el7.x86_64
Stack trace of thread 2753:
#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  0x00007fc8f0add11a start_thread (libc.so.6 + 0x7fc8f0add11a)
#5  0x00007fc8f0b4dc3c __clone3 (libc.so.6 + 0x7fc8f0b4dc3c)

Stack trace of thread 2749:
#0  0x00007fc8f0b4ba3d syscall (libc.so.6 + 0x7fc8f0b4ba3d)
#1  0x0000000004344e2 n/a (n/a + 0x0)
#2  0x000000000450066 n/a (n/a + 0x0)
#3  0x000000000405123 n/a (n/a + 0x0)
#4  0x00007fc8f0a7230e __libc_start_call_main (libc.so.6 + 0x7fc8f0a7230e)
#5  0x0000000000000000 0x0 (n/a + 0x0)
```

Рис. 19: journalctl –since yesterday -p err

Подробный вывод journalctl

```
MESSAGE=Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux)
_BOOT_ID=ecae7e5faccf40a5a17d4615bd220020
_MACHINE_ID=a210e53feae6476da837fe226a86a941
_HOSTNAME=raliev.localdomain
_RUNTIME_SCOPE=initrd
Fri 2025-10-03 16:35:43.659184 MSK [s=08ea1295c5974efe8df1bc2bbc29f72c;i=2;b=ecae7e5faccf40a5a17d4615bd220020]
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=ecae7e5faccf40a5a17d4615bd220020
_MACHINE_ID=a210e53feae6476da837fe226a86a941
_HOSTNAME=raliev.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/r
Fri 2025-10-03 16:35:43.659189 MSK [s=08ea1295c5974efe8df1bc2bbc29f72c;i=3;b=ecae7e5faccf40a5a17d4615bd220020]
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=ecae7e5faccf40a5a17d4615bd220020
root@raliev:/home/raliev# journalctl _SYSTEMD_UNIT=sshd.service
Oct 03 16:35:54 raliev.localdomain (sshd)[1185]: sshd.service: Referenced but unset environment variable
Oct 03 16:35:54 raliev.localdomain sshd[1185]: Server listening on 0.0.0.0 port 22.
Oct 03 16:35:54 raliev.localdomain sshd[1185]: Server listening on :: port 22.
root@raliev:/home/raliev#
```

Рис. 20: journalctl -o verbose

Постоянный журнал journald

```
root@raliev:/home/raliev#  
root@raliev:/home/raliev# mkdir -p /var/log/journal  
root@raliev:/home/raliev# chown root:systemd-journal /var/log/journal/  
root@raliev:/home/raliev# chmod 2755 /var/log/journal/  
root@raliev:/home/raliev# killall -USR1 systemd-journald  
root@raliev:/home/raliev# journalctl -b  
Oct 03 16:35:43 raliev.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-p>  
Oct 03 16:35:43 raliev.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.e>  
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-provided physical RAM map:  
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable  
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reser>  
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reser>  
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] usable  
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x0000000000dffff000-0x0000000000dffffff] ACPI >  
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reser>  
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reser>  
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reser>  
Oct 03 16:35:43 raliev.localdomain kernel: BIOS-e820: [mem 0x0000000010000000-0x0000000011ffffff] usable  
Oct 03 16:35:43 raliev.localdomain kernel: NX (Execute Disable) protection: active  
Oct 03 16:35:43 raliev.localdomain kernel: APIC: Static calls initialized  
Oct 03 16:35:43 raliev.localdomain kernel: SMBIOS 2.5 present.  
Oct 03 16:35:43 raliev.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/>  
Oct 03 16:35:43 raliev.localdomain kernel: DMI: Memory slots populated: 0/0  
Oct 03 16:35:43 raliev.localdomain kernel: Hypervisor detected: KVM  
Oct 03 16:35:43 raliev.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00  
Oct 03 16:35:43 raliev.localdomain kernel: kvm-clock: using sched offset of 8508347384 cycles  
Oct 03 16:35:43 raliev.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles:>  
Oct 03 16:35:43 raliev.localdomain kernel: tsc: Detected 3187.196 MHz processor  
Oct 03 16:35:43 raliev.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved  
Oct 03 16:35:43 raliev.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable  
Oct 03 16:35:43 raliev.localdomain kernel: last pfn = 0x120000 max_arch_pfn = 0x400000000
```

Рис. 21: Создание постоянного журнала

Итоги работы

В ходе работы были изучены возможности администрирования журналов в Linux. Рассмотрены способы просмотра системных сообщений с использованием **rsyslog** и **systemd-journald**, а также настройка постоянного хранения логов и фильтрация событий.