

# Презентация по лабораторной работе №7

Управление журналами событий в системе

---

Амина Аджигалиева

15 октября 2025

Российский университет дружбы народов, Москва, Россия

## Цель работы

---

Получить навыки работы с журналами мониторинга различных событий в системе.

## Ход выполнения работы

---

```
12#3 0x0000000000433500 n/a (n/a + 0x0)#012#4 0x00000132003c3118 static_thread (libc.so.6 + 0x33118)#012#5 0x0000
7f3200435c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 3630:#012#0 0x00007f3200433a3d syscall (
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 0x00007f320035a30e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x00
007f320035a3c9 __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 29 08:13:21 aradzhigalieva systemd[1]: systemd-coredump@27-3634-0.service: Deactivated successfully.
Sep 29 08:13:25 aradzhigalieva su[3621]: FAILED SU (to root) aradzhigalieva on pts/2
Sep 29 08:13:26 aradzhigalieva kernel: traps: VBoxClient[3645] trap int3 ip:41ddb sp:7f31f1d24cd0 error:0 in VBoxC
lient[1ddb,400000+bb000]
Sep 29 08:13:26 aradzhigalieva systemd-coredump[3646]: Process 3642 (VBoxClient) of user 1000 terminated abnormally
with signal 5/TRAP, processing...
Sep 29 08:13:26 aradzhigalieva systemd[1]: Started systemd-coredump@28-3646-0.service - Process Core Dump (PID 3646
/UID 0).
Sep 29 08:13:26 aradzhigalieva systemd-coredump[3647]: Process 3642 (VBoxClient) of user 1000 dumped core.#012#012M
```

Рис. 1: Сообщения о сбоях VBoxClient и вход под root

```
007f320035a3c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x00000000004044aa n/a (n/a + 0x1
object binary architecture: AMD x86-64
Sep 29 08:13:51 aradzhigalieva systemd[1]: systemd-coredump@33-3701-0.service: Deactivated successfully.
Sep 29 08:13:53 aradzhigalieva aradzhigalieva[3707]: hello
Sep 29 08:13:53 aradzhigalieva aradzhigalieva[3712]: hello
Sep 29 08:13:54 aradzhigalieva aradzhigalieva[3714]: hello
Sep 29 08:13:55 aradzhigalieva aradzhigalieva[3716]: hello
Sep 29 08:13:56 aradzhigalieva kernel: traps: VBoxClient[3721] trap int3 ip:41dd1b sp:7f31f1d24cd0 error:0
lient[1dd1b,400000+bb000]
Sep 29 08:13:56 aradzhigalieva systemd-coredump[3722]: Process 3718 (VBoxClient) of user 1000 terminated al
```

Рис. 2: Системные сообщения и ошибки VBoxClient

# Анализ системных журналов

```
root@aradzhigalieva:~# tail -n 20 /var/log/secure
Sep 29 08:10:34 aradzhigalieva sshd[1193]: Server listening on :: port 22.
Sep 29 08:10:34 aradzhigalieva (systemd)[1258]: pam_unix(systemd-user:session): session opened for user gdm(uid=42)
by gdm(uid=0)
Sep 29 08:10:34 aradzhigalieva gdm-launch-environment[1237]: pam_unix(gdm-launch-environment:session): session ope
ned for user gdm(uid=42) by (uid=0)
Sep 29 08:10:40 aradzhigalieva unix_chkpwd[1980]: password check failed for user (aradzhigalieva)
Sep 29 08:10:40 aradzhigalieva gdm-password[1973]: pam_unix(gdm-password:auth): authentication failure; logname= u
id=0 euid=0 tty=/dev/tty1 ruser= rhost= user=aradzhigalieva
Sep 29 08:10:40 aradzhigalieva gdm-password[1973]: gkr-pam: unable to locate daemon control file
Sep 29 08:10:40 aradzhigalieva gdm-password[1973]: gkr-pam: stashed password to try later in open session
Sep 29 08:10:52 aradzhigalieva gdm-password[1992]: gkr-pam: unable to locate daemon control file
Sep 29 08:10:52 aradzhigalieva gdm-password[1992]: gkr-pam: stashed password to try later in open session
Sep 29 08:10:52 aradzhigalieva (systemd)[2004]: pam_unix(systemd-user:session): session opened for user aradzhigali
eva(uid=1000) by aradzhigalieva(uid=0)
Sep 29 08:10:52 aradzhigalieva gdm-password[1992]: pam_unix(gdm-password:session): session opened for user aradzi
galieva(uid=1000) by aradzhigalieva(uid=0)
Sep 29 08:10:52 aradzhigalieva gdm-password[1992]: gkr-pam: gnome-keyring-daemon started properly and unlocked key
ring
Sep 29 08:11:02 aradzhigalieva gdm-launch-environment[1237]: pam_unix(gdm-launch-environment:session): session clo
sed for user gdm
Sep 29 08:12:33 aradzhigalieva (systemd)[3365]: pam_unix(systemd-user:session): session opened for user root(uid=0)
by root(uid=0)
Sep 29 08:12:33 aradzhigalieva su[3350]: pam_unix(su:session): session opened for user root(uid=0) by aradzhigali
euid=1000)
Sep 29 08:12:42 aradzhigalieva su[3445]: pam_unix(su:session): session opened for user root(uid=0) by aradzhigali
euid=1000)
Sep 29 08:12:47 aradzhigalieva su[3508]: pam_unix(su:session): session opened for user root(uid=0) by aradzhigali
euid=1000)
Sep 29 08:13:19 aradzhigalieva su[3508]: pam_unix(su:session): session closed for user root
Sep 29 08:13:22 aradzhigalieva unix_chkpwd[3640]: password check failed for user (root)
```

## Настройка регистрации через rsyslog

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

Рис. 4: Установка и запуск Apache



## Настройка регистрации через rsyslog

```
root@aradzhigalieva:/home/aradzhigalieva#  
root@aradzhigalieva:/home/aradzhigalieva# tail -f /var/log/httpd/error_log  
[Mon Sep 29 08:15:23.823745 2025] [suexec:notice] [pid 4153:tid 4153] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)  
[Mon Sep 29 08:15:23.867208 2025] [lbmethod_heartbeat:notice] [pid 4153:tid 4153] AH02282: No slotmem from mod_heartmonitor  
[Mon Sep 29 08:15:23.867764 2025] [systemd:notice] [pid 4153:tid 4153] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0  
[Mon Sep 29 08:15:23.870631 2025] [mpm_event:notice] [pid 4153:tid 4153] AH00489: Apache/2.4.63 (Rocky Linux) configured -- resuming normal operations  
[Mon Sep 29 08:15:23.870642 2025] [core:notice] [pid 4153:tid 4153] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
```


Рис. 5: Просмотр error\_log Apache

# Настройка регистрации через rsyslog

```
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
```

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

## Настройка регистрации через rsyslog



The screenshot shows a terminal window with three tabs. The active tab is titled 'aradzhigalieva@aradzhigalieva:/etc/rsyslog' and contains the following content:

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

Рис. 7: Создание правила для ошибок Apache

```
root@aradzhigalieva:/etc/rsyslog.d#  
root@aradzhigalieva:/etc/rsyslog.d# touch debug.conf  
root@aradzhigalieva:/etc/rsyslog.d# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf  
root@aradzhigalieva:/etc/rsyslog.d# █
```

Рис. 8: Создание файла debug.conf

```
007F320035a3c9 __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 29 08:22:26 aradzhigalieva systemd[1]: systemd-coredump@134-5888-0.service: Deactivated successfully.
Sep 29 08:22:26 aradzhigalieva root[5894]: Daemon Debug Message
Sep 29 08:22:27 aradzhigalieva root[5899]: Daemon Debug Message
Sep 29 08:22:28 aradzhigalieva root[5901]: Daemon Debug Message
Sep 29 08:22:31 aradzhigalieva kernel: traps: VBoxClient[5906] trap int3 ip:41dd1b sp:7f31fd24cd0 error:0 in VBoxC
lient[1dd1b,400000+bb000]
Sep 29 08:22:31 aradzhigalieva systemd-coredump[5907]: Process 5903 (VBoxClient) of user 1000 terminated abnormally
with signal 5/TRAP, processing...
Sep 29 08:22:31 aradzhigalieva systemd[1]: Started systemd-coredump@135-5907-0.service - Process Core Dump (PID 590
7/UID 0).
Sep 29 08:22:31 aradzhigalieva systemd-coredump[5908]: Process 5903 (VBoxClient) of user 1000 dumped core.#012#012M
odule libXv.so.6 from user libXv 1.0.11.0 elf64_x86_64#012Module libXv.so.1 from user libXv 1.17.0.2 elf64_x86_64#
```

Рис. 9: Проверка отладочного логирования

# Использование journalctl

```
root@aradzhigalieva:/home/aradzhigalieva# journalctl
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-provided physical RAM map:
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009bfff] usable
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff] reserved
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000ffffff] reserved
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x00000000001000000-0x000000000dffffffffff] usable
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x000000000dffff0000-0x000000000dffffffffff] ACPI data
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x00000000fec000000-0x00000000fec00ffff] reserved
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x00000000fee000000-0x00000000fee00ffff] reserved
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x00000000fffc00000-0x00000000ffffffffffff] reserved
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x00000000100000000-0x0000000011ffffffffff] usable
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: NX (Execute Disable) protection: active
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: APIC: Static calls initialized
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: SMBIOS 2.5 present.
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: DMI: Memory slots populated: 0/0
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: Hypervisor detected: KVM
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: kvm-clock: using sched offset of 4075594194 cycles
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: tsc: Detected 3187.200 MHz processor
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: total RAM covered: 4096M
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: Found optimal setting for mtrr clean up
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: gran_size: 64K chunk_size: 1G num_reg: 3
```

Рис. 10: Просмотр системного журнала

# Использование journalctl

```
x86_64
.23.0-2.el10.x86_64

0x9511a)
05c3c)

3a3d)

libc.so.6 + 0x2a30e)

2.34 (libc.so.6 + 0x2a3c9)

Sep 29 08:23:58 aradzhigalieva.localdomain systemd[1]: systemd-coredump@152-6138-0.service: Deactivated successfully.
root@aradzhigalieva:/home/aradzhigalieva#
```

```
Module libwayland-client.so.0 from rpm wayland-1

Stack trace of thread 6137:
#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  0x00007f32003c511a start_thread (libc.so.6 +
#5  0x00007f3200435c3c __clone3 (libc.so.6 + 0x1

Stack trace of thread 6134:
#0  0x00007f3200433a3d syscall (libc.so.6 + 0x10
#1  0x00000000004344e2 n/a (n/a + 0x0)
#2  0x0000000000450066 n/a (n/a + 0x0)
#3  0x0000000000405123 n/a (n/a + 0x0)
#4  0x00007f320035a30e __libc_start_call_main (l
#5  0x00007f320035a3c9 __libc_start_main@@GLIBC_
#6  0x00000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x86-64
```

Рис. 11: Сообщения об ошибках и дампы процессов

3a3d)

0x9511a)

05c3c)

3a3d)

libc.so.6 + 0x2a30e)

2.34 (libc.so.6 + 0x2a3c9)

Sep 29 08:24:13 aradzhigalieva.localdomain systemd[1]: systemd-coredump@155-6172-0.service: Deactivated successfully.  
■

Stack trace of thread 6169:

#0 0x00007f3200433a3d syscall (libc.so.6 + 0x10

#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 0x00007f32003c511a start\_thread (libc.so.6 +

#7 0x00007f3200435c3c \_\_clone3 (libc.so.6 + 0x1

Stack trace of thread 6168:

#0 0x00007f3200433a3d syscall (libc.so.6 + 0x10

#1 0x00000000004344e2 n/a (n/a + 0x0)

#2 0x0000000000450066 n/a (n/a + 0x0)

#3 0x0000000000405123 n/a (n/a + 0x0)

#4 0x00007f320035a30e \_\_libc\_start\_call\_main (l

#5 0x00007f320035a3c9 \_\_libc\_start\_main@@GLIBC\_

#6 0x00000000004044aa n/a (n/a + 0x0)

ELF object binary architecture: AMD x86-64



# Использование journalctl

```
root@aradzhigaliev: /home/aradzhigaliev# journalctl
Display all 128 possibilities? (y or n)
_AUDIT_LOGINUID=
_AUDIT_SESSION=
AVAILABLE=
AVAILABLE_PRETTY=
_BOOT_ID=
_CAP_EFFECTIVE=
_CMDLINE=
CODE_FILE=
CODE_FUNC=
CODE_LINE=
_COMM=
CONFIG_FILE=
CONFIG_LINE=
COREDUMP_CGROUP=
COREDUMP_CMDLINE=
COREDUMP_COMM=
COREDUMP_CWD=
COREDUMP_ENVIRON=
COREDUMP_EXE=
COREDUMP_FILENAME=
COREDUMP_GID=
COREDUMP_HOSTNAME=
COREDUMP_OPEN_FDS=
COREDUMP_OWNER_UID=
COREDUMP_PACKAGE_NAME=
CURRENT_USE_PRETTY=
DBUS_BROKER_LOG_DROPPED=
DBUS_BROKER_METRICS_DISPATCH_AVG=
DBUS_BROKER_METRICS_DISPATCH_COUNT=
DBUS_BROKER_METRICS_DISPATCH_MAX=
DBUS_BROKER_METRICS_DISPATCH_MIN=
DBUS_BROKER_METRICS_DISPATCH_STDDEV=
DISK_AVAILABLE=
DISK_AVAILABLE_PRETTY=
DISK_KEEP_FREE=
DISK_KEEP_FREE_PRETTY=
ERRNO=
_EXE=
_GID=
GLIB_DOMAIN=
GLIB_OLD_LOG_API=
_HOSTNAME=
INITRD_USEC=
INVOCATION_ID=
JOB_ID=
JOB_RESULT=
JOB_TYPE=
JOURNAL_NAME=
JOURNAL_PATH=
JOURNAL_REALTIME_TIMESTAMP=
KERNEL_DEVICE=
PODMAN_TIME=
PODMAN_TYPE=
PRIORITY=
REALMD_OPERATION=
_RUNTIME_SCOPE=
SEAT_ID=
_SELINUX_CONTEXT=
SESSION_ID=
_SOURCE_BOOTTIME_TIMESTAMP=
_SOURCE_MONOTONIC_TIMESTAMP=
_SOURCE_REALTIME_TIMESTAMP=
SSSD_DOMAIN=
SSSD_PRG_NAME=
_STREAM_ID=
SYSLOG_FACILITY=
SYSLOG_IDENTIFIER=
SYSLOG_PID=
SYSLOG_RAW=
SYSLOG_TIMESTAMP=
_SYSTEMD_CGROUP=
_SYSTEMD_INVOCATION_ID=
_SYSTEMD_OWNER_UID=
_SYSTEMD_SESSION=
_SYSTEMD_SLICE=
_SYSTEMD_UNIT=
```

Рис. 13: Отображение доступных фильтров

# Использование journalctl

```
root@aradzhigalieva:/home/aradzhigalieva#  
root@aradzhigalieva:/home/aradzhigalieva# journalctl _UID=0  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-journald[281]: Collecting audit messages is disabled.  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-journald[281]: Journal started  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-journald[281]: Runtime Journal (/run/log/journal/343a350182dc42b  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-modules-load[282]: Module 'msr' is built in  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-modules-load[282]: Inserted module 'fuse'  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-modules-load[282]: Module 'scsi_dh_alua' is built in  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-modules-load[282]: Module 'scsi_dh_emc' is built in  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-modules-load[282]: Module 'scsi_dh_rdac' is built in  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Finished systemd-vconsole-setup.service - Virtual Console S  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: dracut-cmdline-ask.service - dracut ask for additional cmdl  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Starting dracut-cmdline.service - dracut cmdline hook...  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-sysusers[295]: Creating group 'nobody' with GID 65534.  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-sysusers[295]: Creating group 'users' with GID 100.  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variables.  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-sysusers[295]: Creating group 'systemd-journal' with GID 190.  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Finished systemd-sysusers.service - Create System Users.  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create Static  
Sep 29 08:10:29 aradzhigalieva.localdomain dracut-cmdline[304]: dracut-105-4.el10_0  
Sep 29 08:10:29 aradzhigalieva.localdomain dracut-cmdline[304]: Using kernel command line parameters: BOOT_IMAGE  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev.service - Create Static  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Finished dracut-cmdline.service - dracut cmdline hook.  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Starting dracut-pre-udev.service - dracut pre-udev hook...  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Finished dracut-pre-udev.service - dracut pre-udev hook.  
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Starting systemd-udevdev.service - Rule-based Manager for Dev
```

Рис. 14: Просмотр событий UID=0

# Использование journalctl

```
root@aradzhigalieva: /home/aradzhigalieva#  
root@aradzhigalieva: /home/aradzhigalieva# journalctl -n 20  
Sep 29 08:25:14 aradzhigalieva.localdomain systemd-coredump[6337]: [?] Process 6332 (VBoxClient) of user 1000 dump  
Module libXau.so.6 from rpm libXau-1.0.11-8.el1  
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el1  
Module libX11.so.6 from rpm libX11-1.8.10-1.el1  
Module libffi.so.8 from rpm libffi-3.4.4-9.el10  
Module libwayland-client.so.0 from rpm wayland-  
Stack trace of thread 6335:  
#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 0x00007f32003c511a start_thread (libc.so.6  
#5 0x00007f3200435c3c __clone3 (libc.so.6 + 0x  
Stack trace of thread 6332:  
#0 0x00007f3200433a3d syscall (libc.so.6 + 0x1  
#1 0x00000000004344e2 n/a (n/a + 0x0)  
#2 0x0000000000450066 n/a (n/a + 0x0)  
#3 0x0000000000405123 n/a (n/a + 0x0)  
#4 0x00007f320035a30e __libc_start_call_main (  
#5 0x00007f320035a3c9 __libc_start_main@@GLIBC  
#6 0x00000000004044aa n/a (n/a + 0x0)  
ELF object binary architecture: AMD x86-64
```

Рис. 15: Вывод последних строк журнала

# Использование journalctl

```
root@aradzhigalieva:/home/aradzhigalieva# journalctl -p err
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported
Sep 29 08:10:32 aradzhigalieva.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Sep 29 08:10:33 aradzhigalieva.localdomain alsactl[932]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed
Sep 29 08:10:34 aradzhigalieva.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Sep 29 08:10:40 aradzhigalieva.localdomain gdm-password[1973]: gkr-pam: unable to locate daemon control file
Sep 29 08:10:52 aradzhigalieva.localdomain gdm-password[1992]: gkr-pam: unable to locate daemon control file
Sep 29 08:11:03 aradzhigalieva.localdomain systemd-coredump[2813]: [^] Process 2795 (VBoxClient) of user 1000 dump>

Module libXau.so.6 from rpm libXau-1.0.11-8.el1>
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el1>
Module libX11.so.6 from rpm libX11-1.8.10-1.el1>
Module libffi.so.8 from rpm libffi-3.4.4-9.el10>
Module libwayland-client.so.0 from rpm wayland->
Stack trace of thread 2798:
#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 0x00007f32003c511a start_thread (libc.so.6 >
#5 0x00007f3200435c3c __clone3 (libc.so.6 + 0x>

Stack trace of thread 2797:
#0 0x00007f3200433a3d syscall (libc.so.6 + 0x1>
#1 0x0000000004344e2 n/a (n/a + 0x0)
#2 0x000000000450066 n/a (n/a + 0x0)
#3 0x000000000416559 n/a (n/a + 0x0)
```

Рис. 16: Фильтрация по приоритету ошибок

# Использование journalctl

```
root@aradzhigalieva:/home/aradzhigalieva# journalctl --since yesterday
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-provided physical RAM map:
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbfff] usable
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff] reserved
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000ffffff] reserved
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x00000000001000000-0x0000000000dffff] usable
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x000000000dffff0000-0x000000000dffffff] ACPI data
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] reserved
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee0ffff] reserved
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x00000000100000000-0x0000000011ffffff] usable
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: NX (Execute Disable) protection: active
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: APIC: Static calls initialized
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: SMBIOS 2.5 present.
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: DMI: Memory slots populated: 0/0
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: Hypervisor detected: KVM
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: kvm-clock: using sched offset of 4075594194 cycles
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: tsc: Detected 3187.200 MHz processor
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: e820: update [mem 0x00000000-0x0000ffff] usable ==> reserved
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: e820: remove [mem 0x000a0000-0x000ffff] usable
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x40000000
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: total RAM covered: 4096M
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: Found optimal setting for mtrr clean up
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: gran_size: 64K chunk_size: 1G num_reg: 3
```

Рис. 17: События со вчерашнего дня

# Использование journalctl

```
root@aradzhigalieva:/home/aradzhigalieva# journalctl --since yesterday -p err
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running o
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely>
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported>
Sep 29 08:10:32 aradzhigalieva.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Sep 29 08:10:33 aradzhigalieva.localdomain alsactl[932]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: fail>
Sep 29 08:10:34 aradzhigalieva.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Sep 29 08:10:40 aradzhigalieva.localdomain gdm-password[1973]: gkr-pam: unable to locate daemon control file
Sep 29 08:10:52 aradzhigalieva.localdomain gdm-password[1992]: gkr-pam: unable to locate daemon control file
Sep 29 08:11:03 aradzhigalieva.localdomain systemd-coredump[2813]: [...] Process 2795 (VBoxClient) of user 1000 dump>

Module libXau.so.6 from rpm libXau-1.0.11-8.el1>
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el1>
Module libX11.so.6 from rpm libX11-1.8.10-1.el1>
Module libffi.so.8 from rpm libffi-3.4.4-9.el10>
Module libwayland-client.so.0 from rpm wayland->
Stack trace of thread 2798:
#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 0x00007f32003c511a start_thread (libc.so.6 >
#5 0x00007f3200435c3c __clone3 (libc.so.6 + 0x>

Stack trace of thread 2797:
#0 0x00007f3200433a3d syscall (libc.so.6 + 0x1>
#1 0x0000000004344e2 n/a (n/a + 0x0)
#2 0x000000000450066 n/a (n/a + 0x0)
#3 0x000000000416559 n/a (n/a + 0x0)
```

Рис. 18: Ошибки со вчерашнего дня

# Использование journalctl

```
Mon 2025-09-29 08:10:29.274409 MSK [s=b982d14e533447768cfc92e9877c7bb;i=1;b=1e229539ae9f4de9aac453a58766d518;m=128]
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
_PRIORITY=5
_SYSLOG_FACILITY=0
_SYSLOG_IDENTIFIER=kernel
MESSAGE=Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc
_BOOT_ID=1e229539ae9f4de9aac453a58766d518
_MACHINE_ID=343a350182dc4246a2a53c31ed9190c4
_HOSTNAME=aradzhigalieva.localdomain
_RUNTIME_SCOPE=initrd
Mon 2025-09-29 08:10:29.274422 MSK [s=b982d14e533447768cfc92e9877c7bb;i=2;b=1e229539ae9f4de9aac453a58766d518;m=128]
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
_SYSLOG_FACILITY=0
_SYSLOG_IDENTIFIER=kernel
_BOOT_ID=1e229539ae9f4de9aac453a58766d518
_MACHINE_ID=343a350182dc4246a2a53c31ed9190c4
_HOSTNAME=aradzhigalieva.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
Mon 2025-09-29 08:10:29.274427 MSK [s=b982d14e533447768cfc92e9877c7bb;i=3;b=1e229539ae9f4de9aac453a58766d518;m=128]
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
_SYSLOG_FACILITY=0
_SYSLOG_IDENTIFIER=kernel
```

lines 1-30

```
root@aradzhigalieva:/home/aradzhigalieva#  
root@aradzhigalieva:/home/aradzhigalieva# journalctl _SYSTEMD_UNIT=sshd.service  
Sep 29 08:10:34 aradzhigalieva.localdomain (sshd)[1193]: sshd.service: Referenced but unset environment variable e  
Sep 29 08:10:34 aradzhigalieva.localdomain sshd[1193]: Server listening on 0.0.0.0 port 22.  
Sep 29 08:10:34 aradzhigalieva.localdomain sshd[1193]: Server listening on :: port 22.  
lines 1-3/3 (END)
```

Рис. 20: Просмотр журнала sshd



```
-----@-----ig-----/-----ig-----
root@aradzhigalieva:/home/aradzhigalieva# mkdir -p /var/log/journal
root@aradzhigalieva:/home/aradzhigalieva# chown root:systemd-journal /var/log/journal/
root@aradzhigalieva:/home/aradzhigalieva# chmod 2755 /var/log/journal/
root@aradzhigalieva:/home/aradzhigalieva# killall -USR1 systemd-journald
root@aradzhigalieva:/home/aradzhigalieva# journalctl -b
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod>
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-provided physical RAM map:
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbff] usable
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff] reserved
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000ffffff] reserved
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x00000000000100000-0x000000000000dffff] usable
Sep 29 08:10:29 aradzhigalieva.localdomain kernel: BIOS-e820: [mem 0x00000000000dffff000-0x00000000000dffffffffff] ACPI data
```

Рис. 21: Создание постоянного журнала journald

## Вывод

---

В ходе выполнения лабораторной работы я изучила принципы работы системных журналов Linux и научилась настраивать их хранение и просмотр.

Я освоила использование `journalctl`, фильтрацию сообщений, настройку приоритетов, а также перенаправление логов веб-сервера Apache через `rsyslog`.

Был настроен постоянный журнал `journald`, что обеспечивает сохранность данных после перезагрузки.

Полученные знания и навыки важны для контроля, диагностики и администрирования Linux-систем.