Лабораторная работа №7

Управление журналами событий в системе

Ришард Когенгар

20 января 2026

Российский университет дружбы народов, Москва, Россия

Цель работы

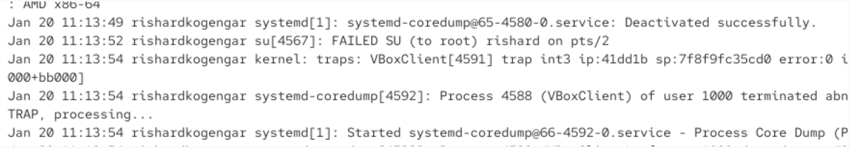
Основная цель

Получить навыки работы с журналами мониторинга различных событий в системе: - просмотр и анализ журналов - мониторинг в реальном времени - настройка rsyslog и journald

Ход выполнения работы

Ошибка аутентификации su

- В 3-й вкладке выполнен выход из root (Ctrl + d)
- Повторная попытка su с неверным паролем
- В журнале появляется сообщение вида FAILED SU (to root) username …
- Событие фиксируется в /var/log/messages

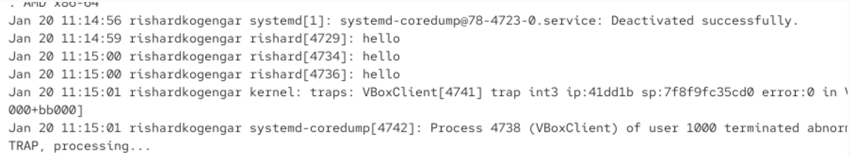


```
: AMD x86-64
Jan 20 11:13:49 rishardkogengar systemd[1]: systemd-coredump@65-4580-0.service: Deactivated successfully.
Jan 20 11:13:52 rishardkogengar su[4567]: FAILED SU (to root) rishard on pts/2
Jan 20 11:13:54 rishardkogengar kernel: traps: VBoxClient[4591] trap int3 ip:41dd1b sp:7f8f9fc35cd0 error:0 i
000+bb000]
Jan 20 11:13:54 rishardkogengar systemd-coredump[4592]: Process 4588 (VBoxClient) of user 1000 terminated abn
TRAP, processing...
Jan 20 11:13:54 rishardkogengar systemd[1]: Started systemd-coredump@66-4592-0.service - Process Core Dump (P
```

Рис. 1: Ошибка аутентификации su фиксируется в журнале

Регистрация сообщения через logger

- В 3-й вкладке из-под пользователя отправлено сообщение в журнал (logger hello)
- Во 2-й вкладке оно отображается сразу (режим реального времени)
- Сообщение также записывается в /var/log/messages

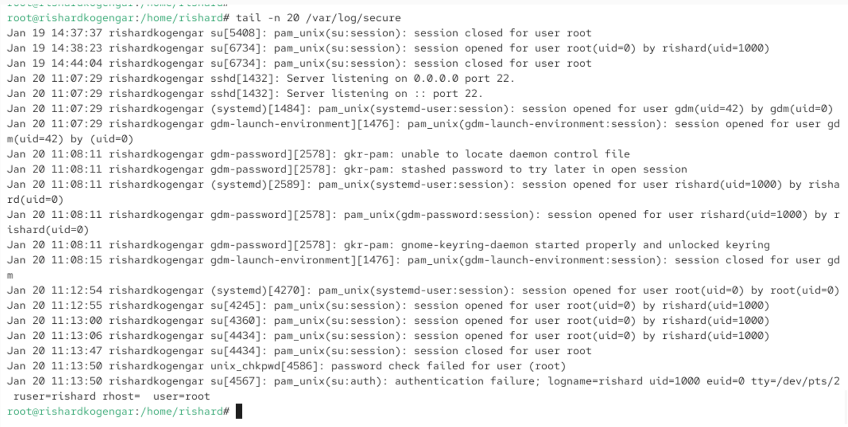


```
. AMD x86-64
Jan 20 11:14:56 rishardkogengar systemd[1]: systemd-coredump@78-4723-0.service: Deactivated successfully.
Jan 20 11:14:59 rishardkogengar rishard[4729]: hello
Jan 20 11:15:00 rishardkogengar rishard[4734]: hello
Jan 20 11:15:00 rishardkogengar rishard[4736]: hello
Jan 20 11:15:01 rishardkogengar kernel: traps: VBoxClient[4741] trap int3 ip:41dd1b sp:7f8f9fc35cd0 error:0 in \
000+bb000]
Jan 20 11:15:01 rishardkogengar systemd-coredump[4742]: Process 4738 (VBoxClient) of user 1000 terminated abnor
TRAP, processing...
```

Рис. 2: Сообщение logger в системном журнале

Просмотр журнала безопасности /var/log/secure

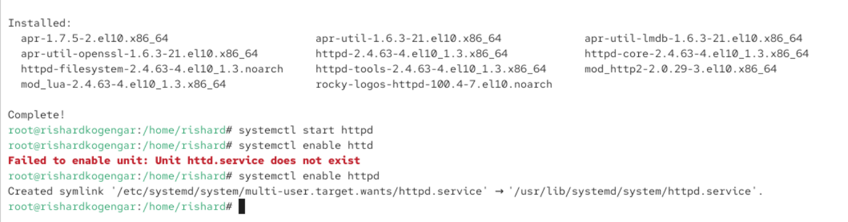
- Остановлен мониторинг /var/log/messages (Ctrl + c)
- Просмотрены последние 20 строк журнала безопасности
- В журнале присутствуют записи об ошибке авторизации su



```
root@rishardkogengar:/home/rishard#
root@rishardkogengar:/home/rishard# tail -n 20 /var/log/secure
Jan 19 14:37:37 rishardkogengar su[5408]: pam_unix(su:session): session closed for user root
Jan 19 14:38:23 rishardkogengar su[6734]: pam_unix(su:session): session opened for user root(uid=0) by rishard(uid=1000)
Jan 19 14:44:04 rishardkogengar su[6734]: pam_unix(su:session): session closed for user root
Jan 20 11:07:29 rishardkogengar sshd[1432]: Server listening on 0.0.0.0 port 22.
Jan 20 11:07:29 rishardkogengar sshd[1432]: Server listening on :: port 22.
Jan 20 11:07:29 rishardkogengar (systemd)[1484]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)
Jan 20 11:07:29 rishardkogengar gdm-launch-environment][1476]: pam_unix(gdm-launch-environment:session): session opened for user gd
m(uid=42) by (uid=0)
Jan 20 11:08:11 rishardkogengar gdm-password][2578]: gkr-pam: unable to locate daemon control file
Jan 20 11:08:11 rishardkogengar gdm-password][2578]: gkr-pam: stashed password to try later in open session
Jan 20 11:08:11 rishardkogengar (systemd)[2589]: pam_unix(systemd-user:session): session opened for user rishard(uid=1000) by risha
rd(uid=0)
Jan 20 11:08:11 rishardkogengar gdm-password][2578]: pam_unix(gdm-password:session): session opened for user rishard(uid=1000) by r
ishard(uid=0)
Jan 20 11:08:11 rishardkogengar gdm-password][2578]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Jan 20 11:08:15 rishardkogengar gdm-launch-environment][1476]: pam_unix(gdm-launch-environment:session): session closed for user gd
m
Jan 20 11:12:54 rishardkogengar (systemd)[4270]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)
Jan 20 11:12:55 rishardkogengar su[4245]: pam_unix(su:session): session opened for user root(uid=0) by rishard(uid=1000)
Jan 20 11:13:00 rishardkogengar su[4360]: pam_unix(su:session): session opened for user root(uid=0) by rishard(uid=1000)
Jan 20 11:13:06 rishardkogengar su[4434]: pam_unix(su:session): session opened for user root(uid=0) by rishard(uid=1000)
Jan 20 11:13:47 rishardkogengar su[4434]: pam_unix(su:session): session closed for user root
Jan 20 11:13:50 rishardkogengar unix_chkpwd[4586]: password check failed for user (root)
Jan 20 11:13:50 rishardkogengar su[4567]: pam_unix(su:auth): authentication failure; logname=rishard uid=1000 euid=0 tty=/dev/pts/2
 ruser=rishard rhost=  user=root
root@rishardkogengar:/home/rishard# █
```

Установка и запуск Apache (httpd)

- Установлен пакет httpd
- Служба запущена и включена в автозагрузку
- Проверена корректность состояния службы

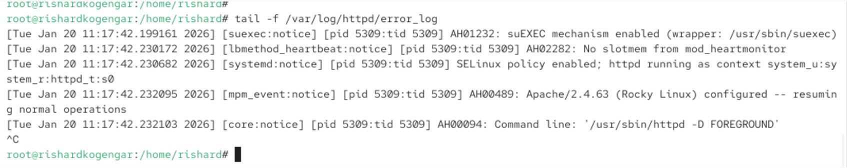


```
Installed:
  apr-1.7.5-2.el10.x86_64                       apr-util-1.6.3-21.el10.x86_64             apr-util-lmdb-1.6.3-21.el10.x86_64
  apr-util-openssl-1.6.3-21.el10.x86_64         httpd-2.4.63-4.el10_1.3.x86_64            httpd-core-2.4.63-4.el10_1.3.x86_64
  httpd-filesystem-2.4.63-4.el10_1.3.noarch     httpd-tools-2.4.63-4.el10_1.3.x86_64      mod_http2-2.0.29-3.el10.x86_64
  mod_lua-2.4.63-4.el10_1.3.x86_64              rocky-logos-httpd-100.4-7.el10.noarch

Complete!
root@rishardkogengar:/home/rishard# systemctl start httpd
root@rishardkogengar:/home/rishard# systemctl enable httd
Failed to enable unit: Unit httd.service does not exist
root@rishardkogengar:/home/rishard# systemctl enable httpd
Created symlink '/etc/systemd/system/multi-user.target.wants/httpd.service' → '/usr/lib/systemd/system/httpd.service'.
root@rishardkogengar:/home/rishard# █
```

Рис. 4: Установка и запуск Apache

Просмотр журнала ошибок Apache

- Выполнен просмотр журнала /var/log/httpd/error_log
- Зафиксированы сообщения о запуске и работе httpd

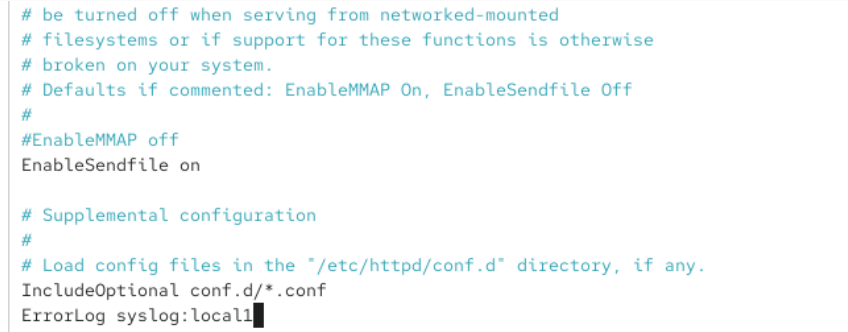


```
root@rishardkogengar:/home/rishard#
root@rishardkogengar:/home/rishard# tail -f /var/log/httpd/error_log
[Tue Jan 20 11:17:42.199161 2026] [suexec:notice] [pid 5309:tid 5309] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Tue Jan 20 11:17:42.230172 2026] [lbmethod_heartbeat:notice] [pid 5309:tid 5309] AH02282: No slotmem from mod_heartmonitor
[Tue Jan 20 11:17:42.230682 2026] [systemd:notice] [pid 5309:tid 5309] SELinux policy enabled; httpd running as context system_u:sy
stem_r:httpd_t:s0
[Tue Jan 20 11:17:42.232095 2026] [mpm_event:notice] [pid 5309:tid 5309] AH00489: Apache/2.4.63 (Rocky Linux) configured -- resumin
g normal operations
[Tue Jan 20 11:17:42.232103 2026] [core:notice] [pid 5309:tid 5309] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
^C
root@rishardkogengar:/home/rishard# 
```

Рис. 5: Журнал ошибок Apache

Перенаправление ErrorLog в syslog

- Открыт файл /etc/httpd/conf/httpd.conf
- Добавлена строка ErrorLog syslog:local1
- Apache начинает отправлять сообщения в syslog с использованием local1

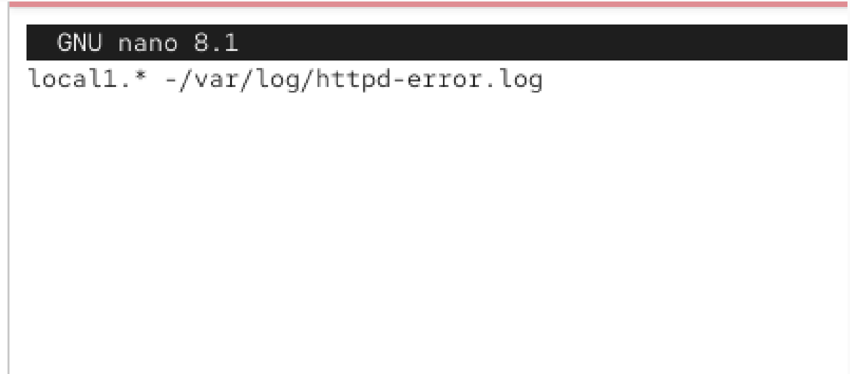


```
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults if commented: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
EnableSendfile on

# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
ErrorLog syslog:local1
```

Рис. 6: Изменение httpd.conf: ErrorLog syslog:local1

Правило rsyslog для local1

- В /etc/rsyslog.d создан файл httpd.conf
- Добавлено правило: local1.* -> /var/log/httpd-error.log
- Это обеспечивает отдельный файл лога для сообщений httpd через syslog

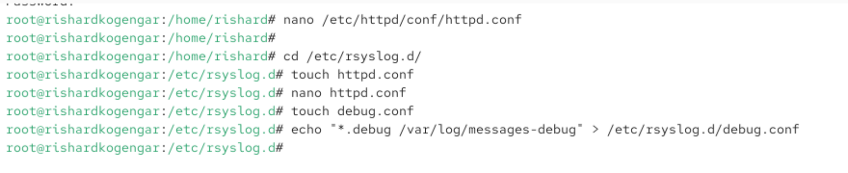


```
  GNU nano 8.1
local1.* -/var/log/httpd-error.log
```

Рис. 7: Правило rsyslog для Apache

Настройка debug-логирования

- В /etc/rsyslog.d создан файл debug.conf
- Добавлено правило: *.debug -> /var/log/messages-debug
- Перезапущена служба rsyslog для применения правил

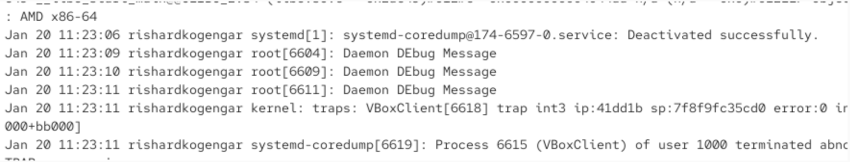


```
Password:
root@rishardkogengar:/home/rishard# nano /etc/httpd/conf/httpd.conf
root@rishardkogengar:/home/rishard#
root@rishardkogengar:/home/rishard# cd /etc/rsyslog.d/
root@rishardkogengar:/etc/rsyslog.d# touch httpd.conf
root@rishardkogengar:/etc/rsyslog.d# nano httpd.conf
root@rishardkogengar:/etc/rsyslog.d#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

Рис. 8: Создание debug.conf и настройка отладочного лога

Проверка: сообщение daemon.debug

- Запущен мониторинг /var/log/messages-debug
- Отправлено тестовое сообщение уровня daemon.debug
- Сообщение отображается в отдельном отладочном журнале

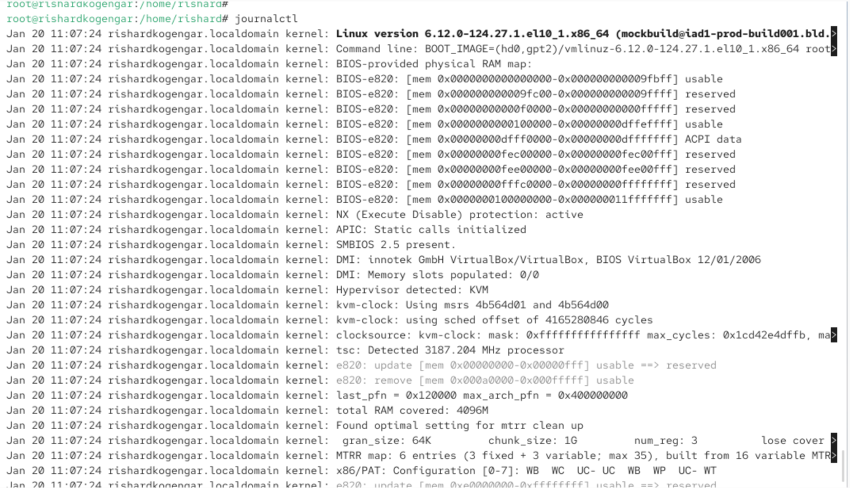


```
: AMD x86-64
Jan 20 11:23:06 rishardkogengar systemd[1]: systemd-coredump@174-6597-0.service: Deactivated successfully.
Jan 20 11:23:09 rishardkogengar root[6604]: Daemon DEbug Message
Jan 20 11:23:10 rishardkogengar root[6609]: Daemon DEbug Message
Jan 20 11:23:11 rishardkogengar root[6611]: Daemon DEbug Message
Jan 20 11:23:11 rishardkogengar kernel: traps: VBoxClient[6618] trap int3 ip:41dd1b sp:7f8f9fc35cd0 error:0 ir
000+bb000]
Jan 20 11:23:11 rishardkogengar systemd-coredump[6619]: Process 6615 (VBoxClient) of user 1000 terminated abnc
```

Рис. 9: Проверка отладочного сообщения в messages-debug

Просмотр журнала с момента загрузки системы

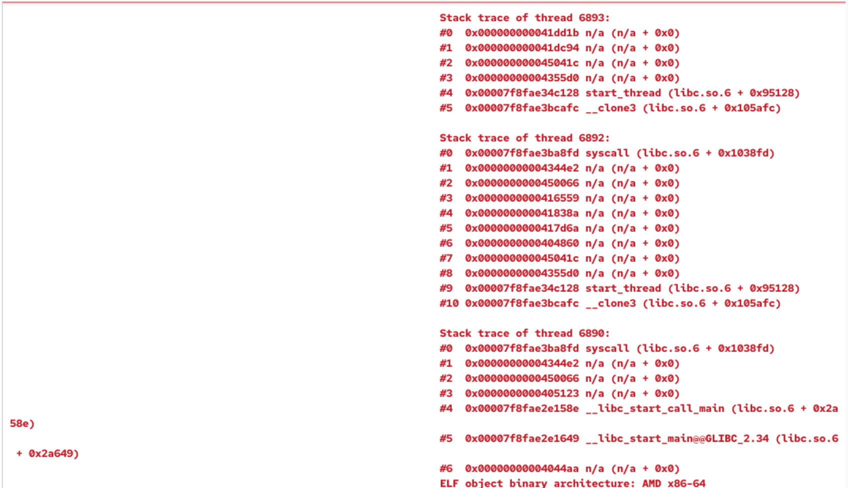
- Выполнен просмотр журнала journald за текущую загрузку
- Отображены сообщения ядра и системных служб



```
root@rishardkogengar:/home/rishard#
root@rishardkogengar:/home/rishard# journalctl
Jan 20 11:07:24 rishardkogengar.localdomain kernel: Linux version 6.12.0-124.27.1.el10_1.x86_64 (mockbuild@iad1-prod-build001.bld.>
Jan 20 11:07:24 rishardkogengar.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-124.27.1.el10_1.x86_64 root>
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-provided physical RAM map:
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dffeffff] usable
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x00000000dfff0000-0x00000000dfffffff] ACPI data
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff] usable
Jan 20 11:07:24 rishardkogengar.localdomain kernel: NX (Execute Disable) protection: active
Jan 20 11:07:24 rishardkogengar.localdomain kernel: APIC: Static calls initialized
Jan 20 11:07:24 rishardkogengar.localdomain kernel: SMBIOS 2.5 present.
Jan 20 11:07:24 rishardkogengar.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Jan 20 11:07:24 rishardkogengar.localdomain kernel: DMI: Memory slots populated: 0/0
Jan 20 11:07:24 rishardkogengar.localdomain kernel: Hypervisor detected: KVM
Jan 20 11:07:24 rishardkogengar.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Jan 20 11:07:24 rishardkogengar.localdomain kernel: kvm-clock: using sched offset of 4165280846 cycles
Jan 20 11:07:24 rishardkogengar.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, ma>
Jan 20 11:07:24 rishardkogengar.localdomain kernel: tsc: Detected 3187.204 MHz processor
Jan 20 11:07:24 rishardkogengar.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Jan 20 11:07:24 rishardkogengar.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Jan 20 11:07:24 rishardkogengar.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Jan 20 11:07:24 rishardkogengar.localdomain kernel: total RAM covered: 4096M
Jan 20 11:07:24 rishardkogengar.localdomain kernel: Found optimal setting for mtrr clean up
Jan 20 11:07:24 rishardkogengar.localdomain kernel:  gran_size: 64K         chunk_size: 1G         num_reg: 3          lose cover >
Jan 20 11:07:24 rishardkogengar.localdomain kernel: MTRR map: 6 entries (3 fixed + 3 variable; max 35), built from 16 variable MTR>
Jan 20 11:07:24 rishardkogengar.localdomain kernel: x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WP  UC- WT
Jan 20 11:07:24 rishardkogengar.localdomain kernel: e820: update [mem 0xe0000000-0xffffffff] usable ==> reserved
```

Просмотр журнала без пейджера

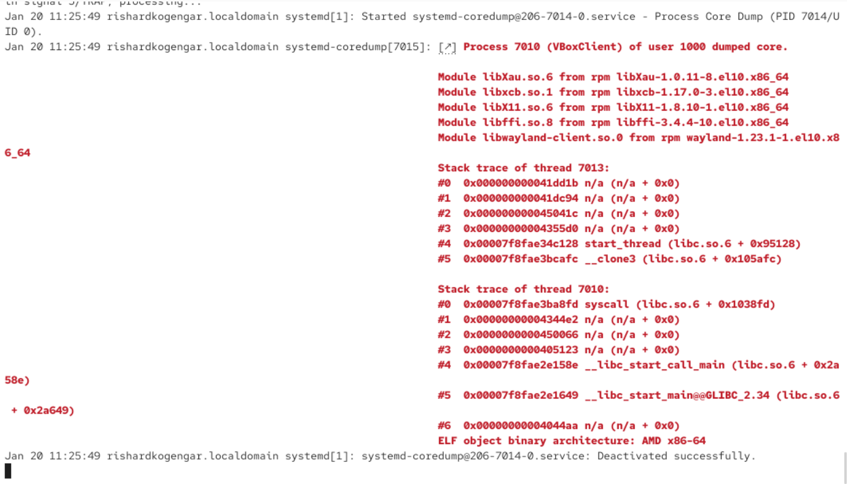
- Выполнен вывод журнала без использования пейджера
- Удобно для перенаправления и быстрой обработки вывода



```
Stack trace of thread 6893:
#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  0x00007f8fae34c128 start_thread (libc.so.6 + 0x95128)
#5  0x00007f8fae3bcafc __clone3 (libc.so.6 + 0x105afc)

Stack trace of thread 6892:
#0  0x00007f8fae3ba8fd syscall (libc.so.6 + 0x1038fd)
#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)
#5  0x0000000000417d6a n/a (n/a + 0x0)
#6  0x0000000000404860 n/a (n/a + 0x0)
#7  0x000000000045041c n/a (n/a + 0x0)
#8  0x00000000004355d0 n/a (n/a + 0x0)
#9  0x00007f8fae34c128 start_thread (libc.so.6 + 0x95128)
#10 0x00007f8fae3bcafc __clone3 (libc.so.6 + 0x105afc)

Stack trace of thread 6890:
#0  0x00007f8fae3ba8fd syscall (libc.so.6 + 0x1038fd)
#1  0x00000000004344e2 n/a (n/a + 0x0)
#2  0x0000000000450066 n/a (n/a + 0x0)
#3  0x0000000000405123 n/a (n/a + 0x0)
#4  0x00007f8fae2e158e __libc_start_call_main (libc.so.6 + 0x2a
58e)
#5  0x00007f8fae2e1649 __libc_start_main@@GLIBC_2.34 (libc.so.6
 + 0x2a649)
#6  0x00000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x86-64
```

Режим реального времени

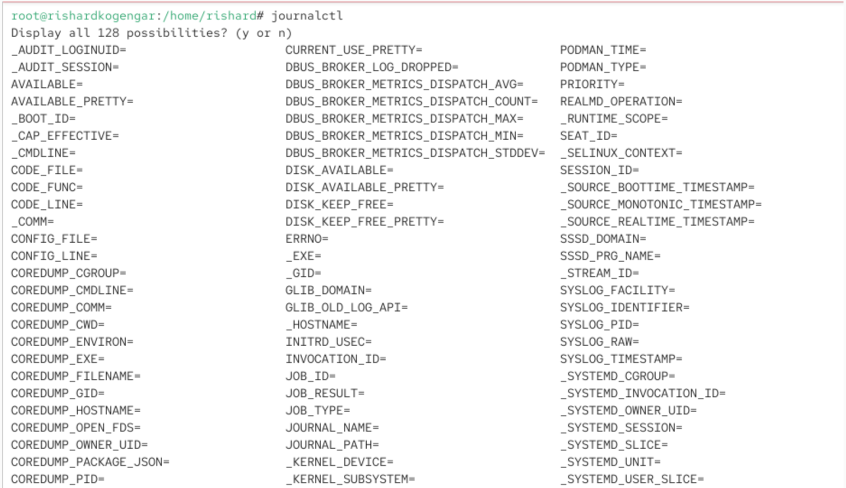
- Включён режим слежения за журналом в реальном времени (journalctl -f)
- Просмотр остановлен вручную (Ctrl + c)



```
th signal 5/TRAP, processing...
Jan 20 11:25:49 rishardkogengar.localdomain systemd[1]: Started systemd-coredump@206-7014-0.service - Process Core Dump (PID 7014/U
ID 0).
Jan 20 11:25:49 rishardkogengar.localdomain systemd-coredump[7015]: [↗] Process 7010 (VBoxClient) of user 1000 dumped core.

                                                                    Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64
                                                                    Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64
                                                                    Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64
                                                                    Module libffi.so.8 from rpm libffi-3.4.4-10.el10.x86_64
                                                                    Module libwayland-client.so.0 from rpm wayland-1.23.1-1.el10.x8
6_64
                                                                    Stack trace of thread 7013:
                                                                    #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  0x00007f8fae34c128 start_thread (libc.so.6 + 0x95128)
                                                                    #5  0x00007f8fae3bcafc __clone3 (libc.so.6 + 0x105afc)

                                                                    Stack trace of thread 7010:
                                                                    #0  0x00007f8fae3ba8fd syscall (libc.so.6 + 0x1038fd)
                                                                    #1  0x00000000004344e2 n/a (n/a + 0x0)
                                                                    #2  0x0000000000450066 n/a (n/a + 0x0)
                                                                    #3  0x0000000000405123 n/a (n/a + 0x0)
                                                                    #4  0x00007f8fae2e158e __libc_start_call_main (libc.so.6 + 0x2a
58e)
                                                                    #5  0x00007f8fae2e1649 __libc_start_main@@GLIBC_2.34 (libc.so.6
 + 0x2a649)
                                                                    #6  0x00000000004044aa n/a (n/a + 0x0)
                                                                    ELF object binary architecture: AMD x86-64
Jan 20 11:25:49 rishardkogengar.localdomain systemd[1]: systemd-coredump@206-7014-0.service: Deactivated successfully.
█
```

Доступные поля фильтрации

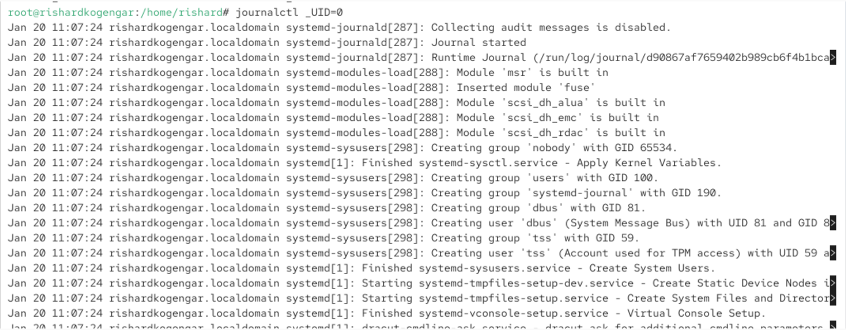
- Выполнен вывод возможных параметров фильтрации (Tab-автодополнение)
- Показаны поля: PID, PRIORITY, UID, UNIT и др.



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

Фильтрация по UID 0

- Просмотрены события, относящиеся к UID=0
- В журнале видны системные действия суперпользователя и служб

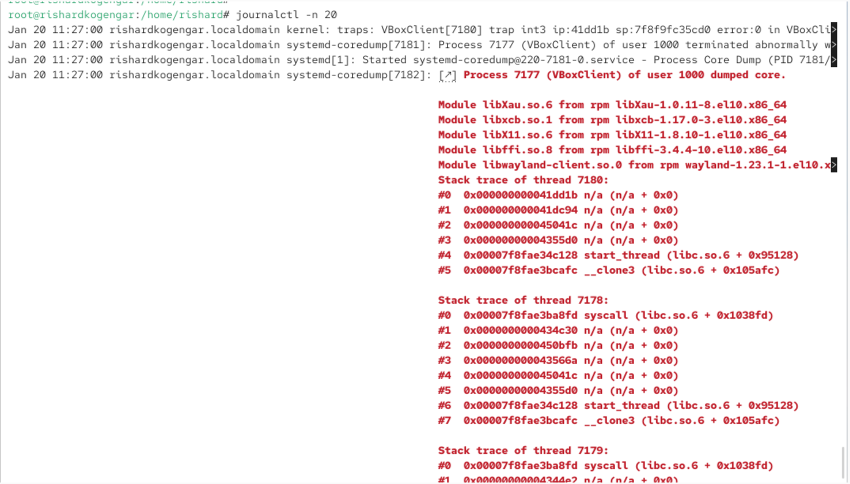


```
root@rishardkogengar:/home/rishard# journalctl _UID=0
Jan 20 11:07:24 rishardkogengar.localdomain systemd-journald[287]: Collecting audit messages is disabled.
Jan 20 11:07:24 rishardkogengar.localdomain systemd-journald[287]: Journal started
Jan 20 11:07:24 rishardkogengar.localdomain systemd-journald[287]: Runtime Journal (/run/log/journal/d90867af7659402b989cb6f4b1bca>
Jan 20 11:07:24 rishardkogengar.localdomain systemd-modules-load[288]: Module 'msr' is built in
Jan 20 11:07:24 rishardkogengar.localdomain systemd-modules-load[288]: Inserted module 'fuse'
Jan 20 11:07:24 rishardkogengar.localdomain systemd-modules-load[288]: Module 'scsi_dh_alua' is built in
Jan 20 11:07:24 rishardkogengar.localdomain systemd-modules-load[288]: Module 'scsi_dh_emc' is built in
Jan 20 11:07:24 rishardkogengar.localdomain systemd-modules-load[288]: Module 'scsi_dh_rdac' is built in
Jan 20 11:07:24 rishardkogengar.localdomain systemd-sysusers[298]: Creating group 'nobody' with GID 65534.
Jan 20 11:07:24 rishardkogengar.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variables.
Jan 20 11:07:24 rishardkogengar.localdomain systemd-sysusers[298]: Creating group 'users' with GID 100.
Jan 20 11:07:24 rishardkogengar.localdomain systemd-sysusers[298]: Creating group 'systemd-journal' with GID 190.
Jan 20 11:07:24 rishardkogengar.localdomain systemd-sysusers[298]: Creating group 'dbus' with GID 81.
Jan 20 11:07:24 rishardkogengar.localdomain systemd-sysusers[298]: Creating user 'dbus' (System Message Bus) with UID 81 and GID 8>
Jan 20 11:07:24 rishardkogengar.localdomain systemd-sysusers[298]: Creating group 'tss' with GID 59.
Jan 20 11:07:24 rishardkogengar.localdomain systemd-sysusers[298]: Creating user 'tss' (Account used for TPM access) with UID 59 a>
Jan 20 11:07:24 rishardkogengar.localdomain systemd[1]: Finished systemd-sysusers.service - Create System Users.
Jan 20 11:07:24 rishardkogengar.localdomain systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create Static Device Nodes i>
Jan 20 11:07:24 rishardkogengar.localdomain systemd[1]: Starting systemd-tmpfiles-setup.service - Create System Files and Director>
Jan 20 11:07:24 rishardkogengar.localdomain systemd[1]: Finished systemd-vconsole-setup.service - Virtual Console Setup.
Jan 20 11:07:24 rishardkogengar.localdomain systemd[1]: dracut-cmdline-ask.service - dracut ask for additional cmdline parameters >
```

Рис. 14: journalctl _UID=0

Последние 20 строк журнала

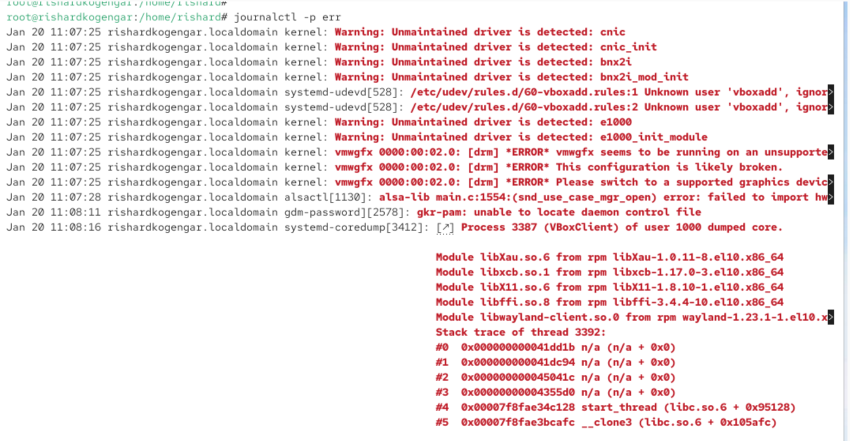
- Выполнен вывод последних 20 сообщений журнала
- Удобно для быстрого анализа последних событий



```
root@rishardkogengar:/home/rishard#
root@rishardkogengar:/home/rishard# journalctl -n 20
Jan 20 11:27:00 rishardkogengar.localdomain kernel: traps: VBoxClient[7180] trap int3 ip:41dd1b sp:7f8f9fc35cd0 error:0 in VBoxCli>
Jan 20 11:27:00 rishardkogengar.localdomain systemd-coredump[7181]: Process 7177 (VBoxClient) of user 1000 terminated abnormally w>
Jan 20 11:27:00 rishardkogengar.localdomain systemd[1]: Started systemd-coredump@220-7181-0.service - Process Core Dump (PID 7181/>
Jan 20 11:27:00 rishardkogengar.localdomain systemd-coredump[7182]: [↗] Process 7177 (VBoxClient) of user 1000 dumped core.

                                                                    Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64
                                                                    Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64
                                                                    Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64
                                                                    Module libffi.so.8 from rpm libffi-3.4.4-10.el10.x86_64
                                                                    Module libwayland-client.so.0 from rpm wayland-1.23.1-1.el10.x>
                                                                    Stack trace of thread 7180:
                                                                    #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  0x00007f8fae34c128 start_thread (libc.so.6 + 0x95128)
                                                                    #5  0x00007f8fae3bcafc __clone3 (libc.so.6 + 0x105afc)

                                                                    Stack trace of thread 7178:
                                                                    #0  0x00007f8fae3ba8fd syscall (libc.so.6 + 0x1038fd)
                                                                    #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  0x00007f8fae34c128 start_thread (libc.so.6 + 0x95128)
                                                                    #7  0x00007f8fae3bcafc __clone3 (libc.so.6 + 0x105afc)

                                                                    Stack trace of thread 7179:
                                                                    #0  0x00007f8fae3ba8fd syscall (libc.so.6 + 0x1038fd)
                                                                    #1  0x00000000004344e2 n/a (n/a + 0x0)
```

Сообщения только с ошибками

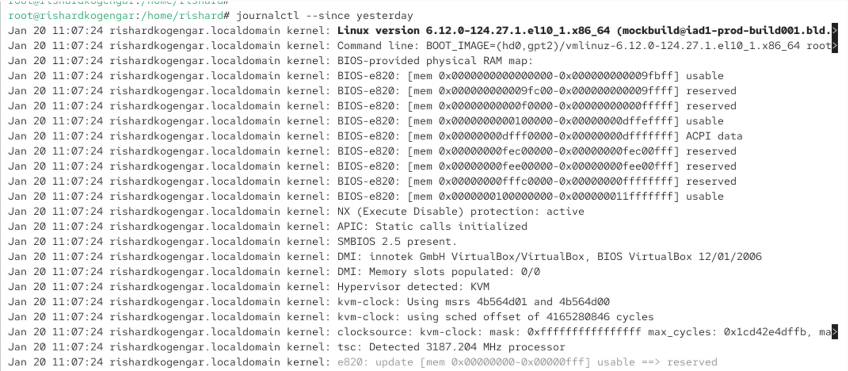
- Включена фильтрация по приоритету err
- Зафиксированы ошибки драйверов/служб и core dump процессов



```
root@rishardkogengar:/home/rishard#
root@rishardkogengar:/home/rishard# journalctl -p err
Jan 20 11:07:25 rishardkogengar.localdomain kernel: Warning: Unmaintained driver is detected: cnic
Jan 20 11:07:25 rishardkogengar.localdomain kernel: Warning: Unmaintained driver is detected: cnic_init
Jan 20 11:07:25 rishardkogengar.localdomain kernel: Warning: Unmaintained driver is detected: bnx2i
Jan 20 11:07:25 rishardkogengar.localdomain kernel: Warning: Unmaintained driver is detected: bnx2i_mod_init
Jan 20 11:07:25 rishardkogengar.localdomain systemd-udevd[528]: /etc/udev/rules.d/60-vboxadd.rules:1 Unknown user 'vboxadd', ignor>
Jan 20 11:07:25 rishardkogengar.localdomain systemd-udevd[528]: /etc/udev/rules.d/60-vboxadd.rules:2 Unknown user 'vboxadd', ignor>
Jan 20 11:07:25 rishardkogengar.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Jan 20 11:07:25 rishardkogengar.localdomain kernel: Warning: Unmaintained driver is detected: e1000_init_module
Jan 20 11:07:25 rishardkogengar.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an unsupporte>
Jan 20 11:07:25 rishardkogengar.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken.
Jan 20 11:07:25 rishardkogengar.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graphics devic>
Jan 20 11:07:28 rishardkogengar.localdomain alsactl[1130]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import hw>
Jan 20 11:08:11 rishardkogengar.localdomain gdm-password][2578]: gkr-pam: unable to locate daemon control file
Jan 20 11:08:16 rishardkogengar.localdomain systemd-coredump[3412]: [↗] Process 3387 (VBoxClient) of user 1000 dumped core.

                                                                    Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64
                                                                    Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64
                                                                    Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64
                                                                    Module libffi.so.8 from rpm libffi-3.4.4-10.el10.x86_64
                                                                    Module libwayland-client.so.0 from rpm wayland-1.23.1-1.el10.x>
                                                                    Stack trace of thread 3392:
                                                                    #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  0x00007f8fae34c128 start_thread (libc.so.6 + 0x95128)
                                                                    #5  0x00007f8fae3bcafc __clone3 (libc.so.6 + 0x105afc)
```

Просмотр за период времени

- Выполнен просмотр сообщений, записанных со вчерашнего дня
- Использован параметр –since yesterday

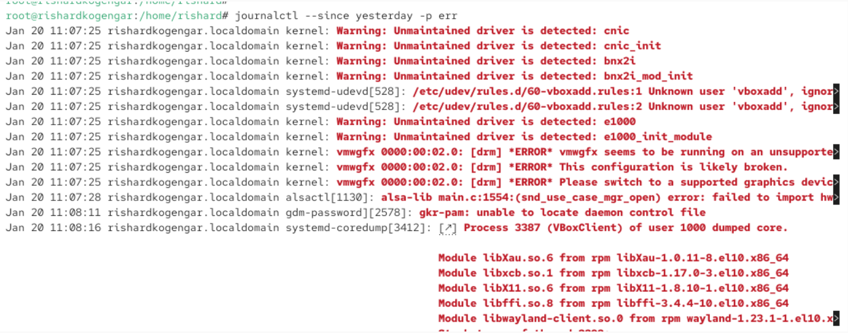


```
root@rishardkogengar:/home/rishard#
root@rishardkogengar:/home/rishard# journalctl --since yesterday
Jan 20 11:07:24 rishardkogengar.localdomain kernel: Linux version 6.12.0-124.27.1.el10_1.x86_64 (mockbuild@iad1-prod-build001.bld.>
Jan 20 11:07:24 rishardkogengar.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-124.27.1.el10_1.x86_64 root>
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-provided physical RAM map:
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dffeffff] usable
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x00000000dfff0000-0x00000000dfffffff] ACPI data
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff] usable
Jan 20 11:07:24 rishardkogengar.localdomain kernel: NX (Execute Disable) protection: active
Jan 20 11:07:24 rishardkogengar.localdomain kernel: APIC: Static calls initialized
Jan 20 11:07:24 rishardkogengar.localdomain kernel: SMBIOS 2.5 present.
Jan 20 11:07:24 rishardkogengar.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Jan 20 11:07:24 rishardkogengar.localdomain kernel: DMI: Memory slots populated: 0/0
Jan 20 11:07:24 rishardkogengar.localdomain kernel: Hypervisor detected: KVM
Jan 20 11:07:24 rishardkogengar.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Jan 20 11:07:24 rishardkogengar.localdomain kernel: kvm-clock: using sched offset of 4165280846 cycles
Jan 20 11:07:24 rishardkogengar.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, ma>
Jan 20 11:07:24 rishardkogengar.localdomain kernel: tsc: Detected 3187.204 MHz processor
Jan 20 11:07:24 rishardkogengar.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
```

Рис. 17: journalctl –since yesterday

Ошибки за период времени

- Отображены только сообщения уровня err со вчерашнего дня
- Комбинация параметров –since и -p err

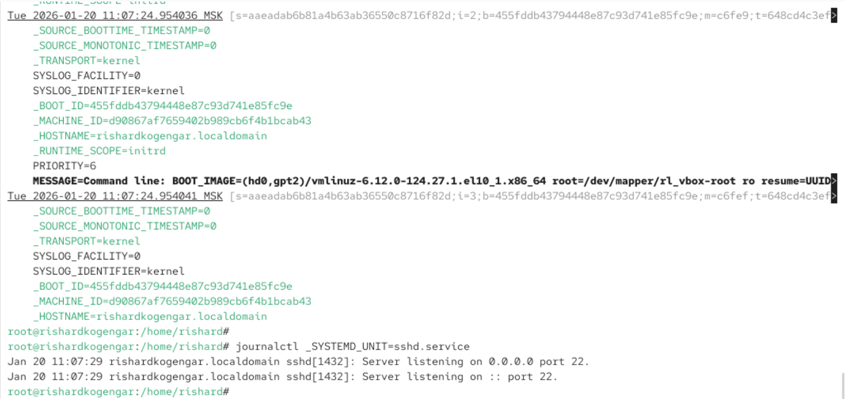


```
root@rishardkogengar:/home/rishard#
root@rishardkogengar:/home/rishard# journalctl --since yesterday -p err
Jan 20 11:07:25 rishardkogengar.localdomain kernel: Warning: Unmaintained driver is detected: cnic
Jan 20 11:07:25 rishardkogengar.localdomain kernel: Warning: Unmaintained driver is detected: cnic_init
Jan 20 11:07:25 rishardkogengar.localdomain kernel: Warning: Unmaintained driver is detected: bnx2i
Jan 20 11:07:25 rishardkogengar.localdomain kernel: Warning: Unmaintained driver is detected: bnx2i_mod_init
Jan 20 11:07:25 rishardkogengar.localdomain systemd-udevd[528]: /etc/udev/rules.d/60-vboxadd.rules:1 Unknown user 'vboxadd', ignor>
Jan 20 11:07:25 rishardkogengar.localdomain systemd-udevd[528]: /etc/udev/rules.d/60-vboxadd.rules:2 Unknown user 'vboxadd', ignor>
Jan 20 11:07:25 rishardkogengar.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Jan 20 11:07:25 rishardkogengar.localdomain kernel: Warning: Unmaintained driver is detected: e1000_init_module
Jan 20 11:07:25 rishardkogengar.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an unsupporte>
Jan 20 11:07:25 rishardkogengar.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken.
Jan 20 11:07:25 rishardkogengar.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graphics devic>
Jan 20 11:07:28 rishardkogengar.localdomain alsactl[1130]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import hw>
Jan 20 11:08:11 rishardkogengar.localdomain gdm-password][2578]: gkr-pam: unable to locate daemon control file
Jan 20 11:08:16 rishardkogengar.localdomain systemd-coredump[3412]: [↗] Process 3387 (VBoxClient) of user 1000 dumped core.

                                                                    Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64
                                                                    Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64
                                                                    Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64
                                                                    Module libffi.so.8 from rpm libffi-3.4.4-10.el10.x86_64
                                                                    Module libwayland-client.so.0 from rpm wayland-1.23.1-1.el10.x>
```

Рис. 18: journalctl –since yesterday -p err

Подробный вывод (verbose)

- Включён формат подробного вывода (-o verbose)
- Отображаются дополнительные поля события (BOOT_ID, TRANSPORT, PRIORITY и т.д.)

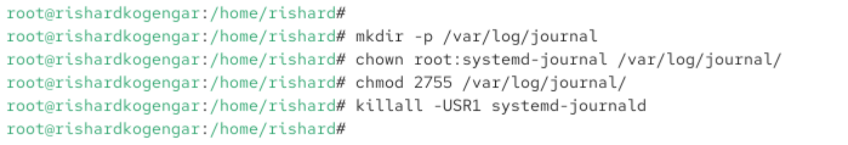


```
    _RUNTIME_SCOPE=initrd
Tue 2026-01-20 11:07:24.954036 MSK [s=aaeadab6b81a4b63ab36550c8716f82d;i=2;b=455fddb43794448e87c93d741e85fc9e;m=c6fe9;t=648cd4c3ef>
    _SOURCE_BOOTTIME_TIMESTAMP=0
    _SOURCE_MONOTONIC_TIMESTAMP=0
    _TRANSPORT=kernel
    SYSLOG_FACILITY=0
    SYSLOG_IDENTIFIER=kernel
    _BOOT_ID=455fddb43794448e87c93d741e85fc9e
    _MACHINE_ID=d90867af7659402b989cb6f4b1bcab43
    _HOSTNAME=rishardkogengar.localdomain
    _RUNTIME_SCOPE=initrd
    PRIORITY=6
    MESSAGE=Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-124.27.1.el10_1.x86_64 root=/dev/mapper/rl_vbox-root ro resume=UUID>
Tue 2026-01-20 11:07:24.954041 MSK [s=aaeadab6b81a4b63ab36550c8716f82d;i=3;b=455fddb43794448e87c93d741e85fc9e;m=c6fef;t=648cd4c3ef>
    _SOURCE_BOOTTIME_TIMESTAMP=0
    _SOURCE_MONOTONIC_TIMESTAMP=0
    _TRANSPORT=kernel
    SYSLOG_FACILITY=0
    SYSLOG_IDENTIFIER=kernel
    _BOOT_ID=455fddb43794448e87c93d741e85fc9e
    _MACHINE_ID=d90867af7659402b989cb6f4b1bcab43
    _HOSTNAME=rishardkogengar.localdomain
root@rishardkogengar:/home/rishard#
root@rishardkogengar:/home/rishard# journalctl _SYSTEMD_UNIT=sshd.service
Jan 20 11:07:29 rishardkogengar.localdomain sshd[1432]: Server listening on 0.0.0.0 port 22.
Jan 20 11:07:29 rishardkogengar.localdomain sshd[1432]: Server listening on :: port 22.
root@rishardkogengar:/home/rishard#
```

Рис. 19: journalctl -o verbose

Включение постоянного хранения

- Создан каталог /var/log/journal
- Назначены права: root:systemd-journal
- Установлены права доступа (режим 2755)
- Для применения изменений отправлен сигнал USR1 службе systemd-journald



```
root@rishardkogengar:/home/rishard#
root@rishardkogengar:/home/rishard# mkdir -p /var/log/journal
root@rishardkogengar:/home/rishard# chown root:systemd-journal /var/log/journal/
root@rishardkogengar:/home/rishard# chmod 2755 /var/log/journal/
root@rishardkogengar:/home/rishard# killall -USR1 systemd-journald
root@rishardkogengar:/home/rishard#
```

Рис. 20: Создание /var/log/journal и применение изменений

Итоги работы

Вывод

- Освоен мониторинг системных событий и событий безопасности
- Настроено перенаправление логов Apache через syslog (local1)
- Создан отдельный отладочный журнал для *.debug
- Изучены ключевые режимы journalctl и фильтрация
- Включено постоянное хранение journald на диске