Лабораторная работа №7

Управление журналами событий в системе

Щемелев Илья Владимирович

Российский университет дружбы народов, Москва, Россия

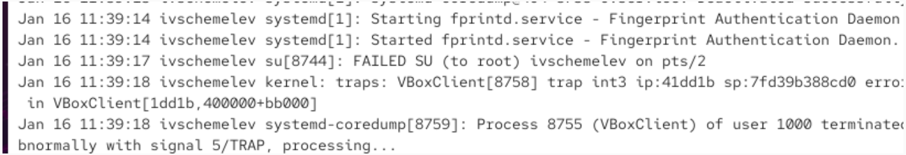
Цель работы

Формулировка цели

Получить практические навыки работы с системными журналами Linux, включая мониторинг событий, настройку rsyslog, анализ журналов с помощью journalctl и организацию постоянного хранения журнала systemd.

Ход выполнения работы

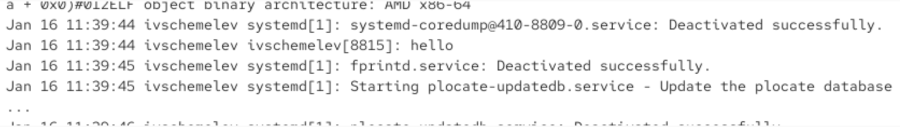
Отслеживание системных сообщений в реальном времени



```
Jan 16 11:39:14 ivschemelev systemd[1]: Starting fprintd.service - Fingerprint Authentication Daemon
Jan 16 11:39:14 ivschemelev systemd[1]: Started fprintd.service - Fingerprint Authentication Daemon.
Jan 16 11:39:17 ivschemelev su[8744]: FAILED SU (to root) ivschemelev on pts/2
Jan 16 11:39:18 ivschemelev kernel: traps: VBoxClient[8758] trap int3 ip:41dd1b sp:7fd39b388cd0 erro
 in VBoxClient[1dd1b,400000+bb000]
Jan 16 11:39:18 ivschemelev systemd-coredump[8759]: Process 8755 (VBoxClient) of user 1000 terminate
bnormally with signal 5/TRAP, processing...
```

Рис. 1: Мониторинг файла /var/log/messages

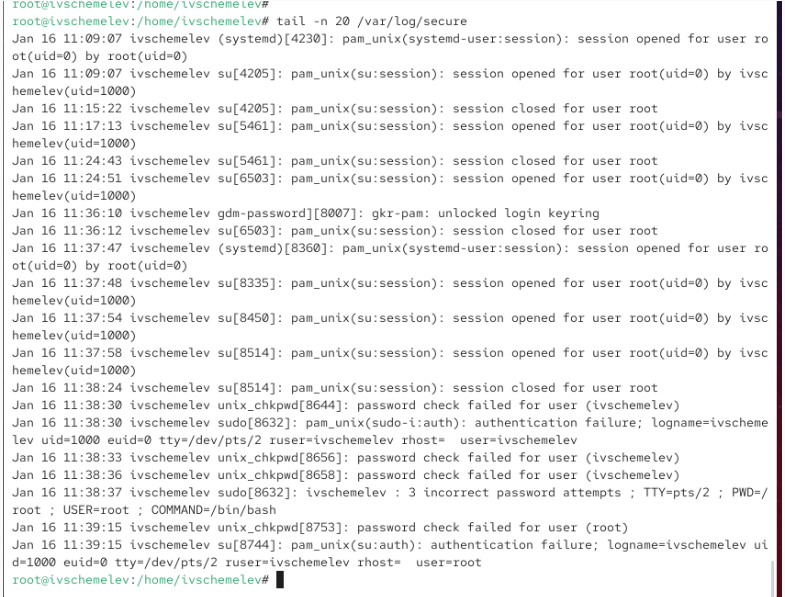
Пользовательское сообщение журнала



```
a + 0x0)#012ELF object binary architecture: AMD x86-64
Jan 16 11:39:44 ivschemelev systemd[1]: systemd-coredump@410-8809-0.service: Deactivated successfully.
Jan 16 11:39:44 ivschemelev ivschemelev[8815]: hello
Jan 16 11:39:45 ivschemelev systemd[1]: fprintd.service: Deactivated successfully.
Jan 16 11:39:45 ivschemelev systemd[1]: Starting plocate-updatedb.service - Update the plocate database
...
Jan 16 11:39:46 ivschemelev systemd[1]: plocate-updatedb.service: Deactivated successfully.
```

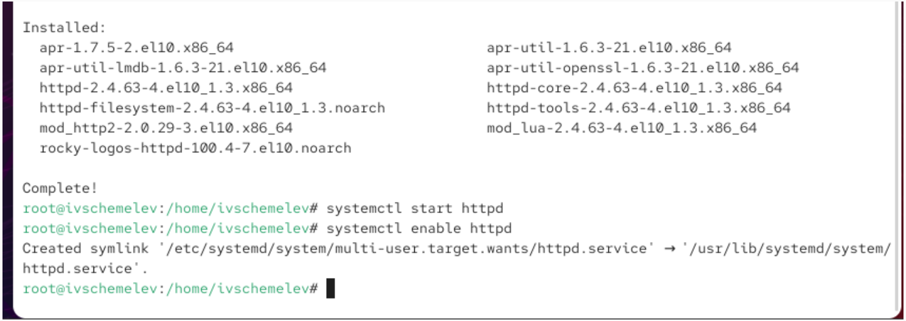
Рис. 2: Сообщение, добавленное в системный журнал

Журнал безопасности



```
root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# tail -n 20 /var/log/secure
Jan 16 11:09:07 ivschemelev (systemd)[4230]: pam_unix(systemd-user:session): session opened for user ro
ot(uid=0) by root(uid=0)
Jan 16 11:09:07 ivschemelev su[4205]: pam_unix(su:session): session opened for user root(uid=0) by ivsc
hemelev(uid=1000)
Jan 16 11:15:22 ivschemelev su[4205]: pam_unix(su:session): session closed for user root
Jan 16 11:17:13 ivschemelev su[5461]: pam_unix(su:session): session opened for user root(uid=0) by ivsc
hemelev(uid=1000)
Jan 16 11:24:43 ivschemelev su[5461]: pam_unix(su:session): session closed for user root
Jan 16 11:24:51 ivschemelev su[6503]: pam_unix(su:session): session opened for user root(uid=0) by ivsc
hemelev(uid=1000)
Jan 16 11:36:10 ivschemelev gdm-password][8007]: gkr-pam: unlocked login keyring
Jan 16 11:36:12 ivschemelev su[6503]: pam_unix(su:session): session closed for user root
Jan 16 11:37:47 ivschemelev (systemd)[8360]: pam_unix(systemd-user:session): session opened for user ro
ot(uid=0) by root(uid=0)
Jan 16 11:37:48 ivschemelev su[8335]: pam_unix(su:session): session opened for user root(uid=0) by ivsc
hemelev(uid=1000)
Jan 16 11:37:54 ivschemelev su[8450]: pam_unix(su:session): session opened for user root(uid=0) by ivsc
hemelev(uid=1000)
Jan 16 11:37:58 ivschemelev su[8514]: pam_unix(su:session): session opened for user root(uid=0) by ivsc
hemelev(uid=1000)
Jan 16 11:38:24 ivschemelev su[8514]: pam_unix(su:session): session closed for user root
Jan 16 11:38:30 ivschemelev unix_chkpwd[8644]: password check failed for user (ivschemelev)
Jan 16 11:38:30 ivschemelev sudo[8632]: pam_unix(sudo-i:auth): authentication failure; logname=ivscheme
lev uid=1000 euid=0 tty=/dev/pts/2 ruser=ivschemelev rhost=  user=ivschemelev
Jan 16 11:38:33 ivschemelev unix_chkpwd[8656]: password check failed for user (ivschemelev)
Jan 16 11:38:36 ivschemelev unix_chkpwd[8658]: password check failed for user (ivschemelev)
Jan 16 11:38:37 ivschemelev sudo[8632]: ivschemelev : 3 incorrect password attempts ; TTY=pts/2 ; PWD=/
root ; USER=root ; COMMAND=/bin/bash
Jan 16 11:39:15 ivschemelev unix_chkpwd[8753]: password check failed for user (root)
Jan 16 11:39:15 ivschemelev su[8744]: pam_unix(su:auth): authentication failure; logname=ivschemelev ui
d=1000 euid=0 tty=/dev/pts/2 ruser=ivschemelev rhost=  user=root
root@ivschemelev:/home/ivschemelev#
```

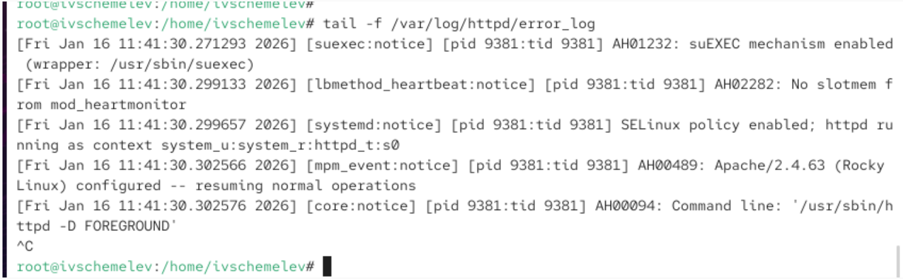
Установка и запуск Apache HTTP Server



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

Рис. 4: Установка Apache

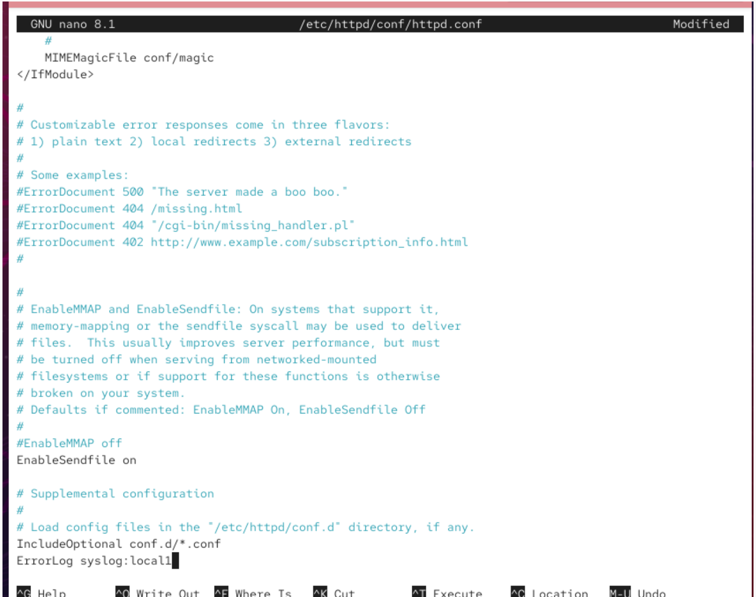
Журнал ошибок Apache



```
root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# tail -f /var/log/httpd/error_log
[Fri Jan 16 11:41:30.271293 2026] [suexec:notice] [pid 9381:tid 9381] AH01232: suEXEC mechanism enabled
 (wrapper: /usr/sbin/suexec)
[Fri Jan 16 11:41:30.299133 2026] [lbmethod_heartbeat:notice] [pid 9381:tid 9381] AH02282: No slotmem f
rom mod_heartmonitor
[Fri Jan 16 11:41:30.299657 2026] [systemd:notice] [pid 9381:tid 9381] SELinux policy enabled; httpd ru
nning as context system_u:system_r:httpd_t:s0
[Fri Jan 16 11:41:30.302566 2026] [mpm_event:notice] [pid 9381:tid 9381] AH00489: Apache/2.4.63 (Rocky
Linux) configured -- resuming normal operations
[Fri Jan 16 11:41:30.302576 2026] [core:notice] [pid 9381:tid 9381] AH00094: Command line: '/usr/sbin/h
ttpd -D FOREGROUND'
^C
root@ivschemelev:/home/ivschemelev# 
```

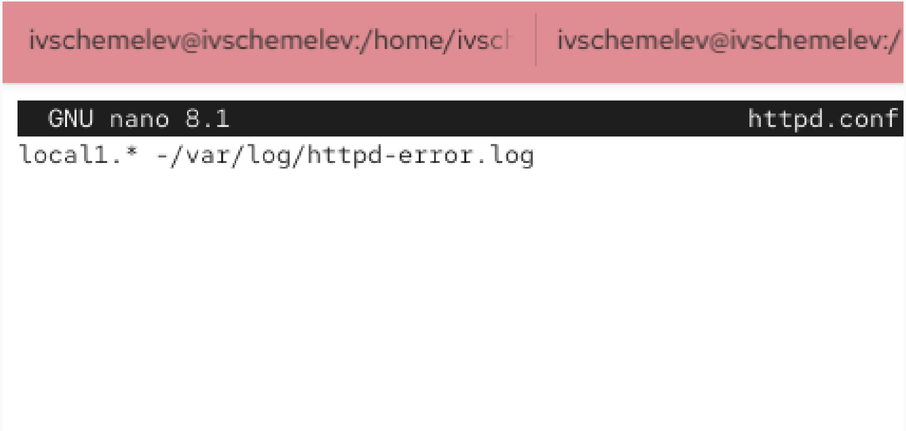
Рис. 5: Журнал ошибок Apache

Перенаправление логов Apache в syslog



```
 GNU nano 8.1                    /etc/httpd/conf/httpd.conf                    Modified
    #
    MIMEMagicFile conf/magic
</IfModule>

#
# 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
```

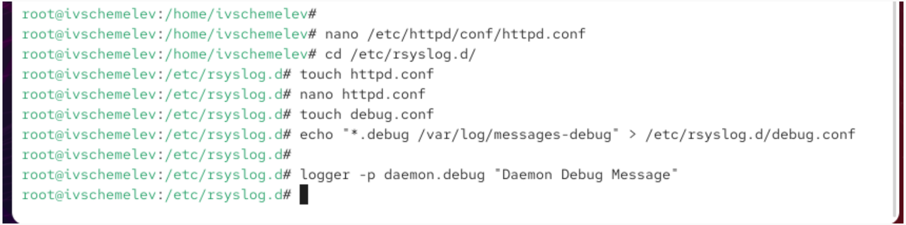
Настройка rsyslog для Apache



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

Рис. 7: Конфигурация rsyslog

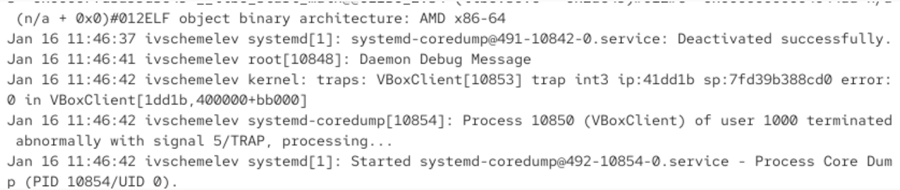
Журнал отладочных сообщений



```
root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# nano /etc/httpd/conf/httpd.conf
root@ivschemelev:/home/ivschemelev# cd /etc/rsyslog.d/
root@ivschemelev:/etc/rsyslog.d# touch httpd.conf
root@ivschemelev:/etc/rsyslog.d# nano httpd.conf
root@ivschemelev:/etc/rsyslog.d# touch debug.conf
root@ivschemelev:/etc/rsyslog.d# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
root@ivschemelev:/etc/rsyslog.d#
root@ivschemelev:/etc/rsyslog.d# logger -p daemon.debug "Daemon Debug Message"
root@ivschemelev:/etc/rsyslog.d# 
```

Рис. 8: Файл debug-журнала

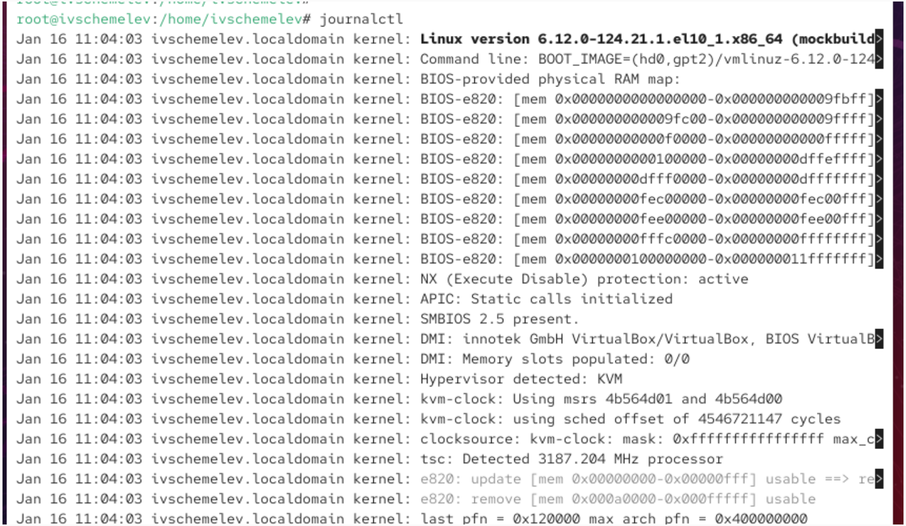
Журнал отладочных сообщений



```
 (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Jan 16 11:46:37 ivschemelev systemd[1]: systemd-coredump@491-10842-0.service: Deactivated successfully.
Jan 16 11:46:41 ivschemelev root[10848]: Daemon Debug Message
Jan 16 11:46:42 ivschemelev kernel: traps: VBoxClient[10853] trap int3 ip:41dd1b sp:7fd39b388cd0 error:
0 in VBoxClient[1dd1b,400000+bb000]
Jan 16 11:46:42 ivschemelev systemd-coredump[10854]: Process 10850 (VBoxClient) of user 1000 terminated
 abnormally with signal 5/TRAP, processing...
Jan 16 11:46:42 ivschemelev systemd[1]: Started systemd-coredump@492-10854-0.service - Process Core Dum
p (PID 10854/UID 0).
```

Рис. 9: Мониторинг debug-журнала

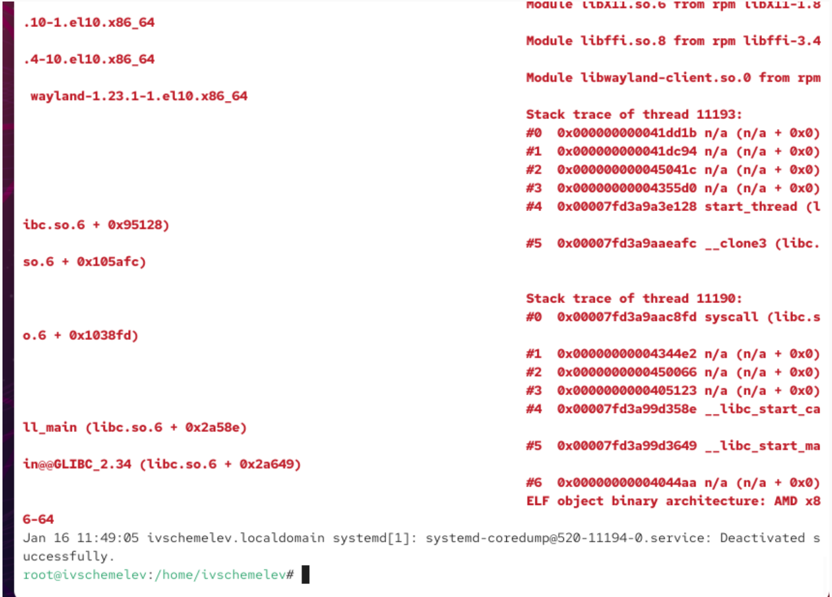
Просмотр журнала с момента загрузки



```
root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# journalctl
Jan 16 11:04:03 ivschemelev.localdomain kernel: Linux version 6.12.0-124.21.1.el10_1.x86_64 (mockbuild>
Jan 16 11:04:03 ivschemelev.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-124>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-provided physical RAM map:
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dffeffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000dfff0000-0x00000000dfffffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: NX (Execute Disable) protection: active
Jan 16 11:04:03 ivschemelev.localdomain kernel: APIC: Static calls initialized
Jan 16 11:04:03 ivschemelev.localdomain kernel: SMBIOS 2.5 present.
Jan 16 11:04:03 ivschemelev.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualB>
Jan 16 11:04:03 ivschemelev.localdomain kernel: DMI: Memory slots populated: 0/0
Jan 16 11:04:03 ivschemelev.localdomain kernel: Hypervisor detected: KVM
Jan 16 11:04:03 ivschemelev.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Jan 16 11:04:03 ivschemelev.localdomain kernel: kvm-clock: using sched offset of 4546721147 cycles
Jan 16 11:04:03 ivschemelev.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_c>
Jan 16 11:04:03 ivschemelev.localdomain kernel: tsc: Detected 3187.204 MHz processor
Jan 16 11:04:03 ivschemelev.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> re>
Jan 16 11:04:03 ivschemelev.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Jan 16 11:04:03 ivschemelev.localdomain kernel: last pfn = 0x120000 max arch pfn = 0x400000000
```

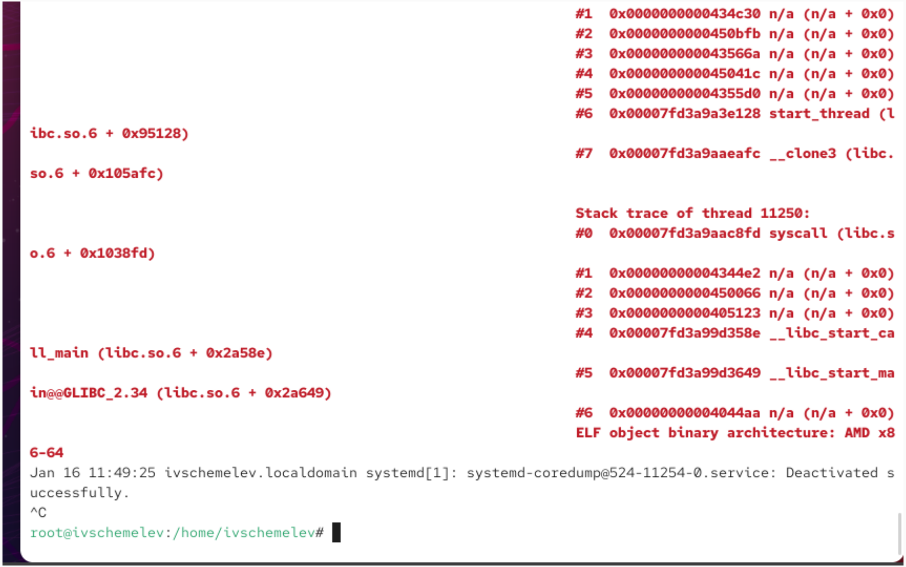
Рис. 10: Журнал с момента загрузки

Вывод без пейджера



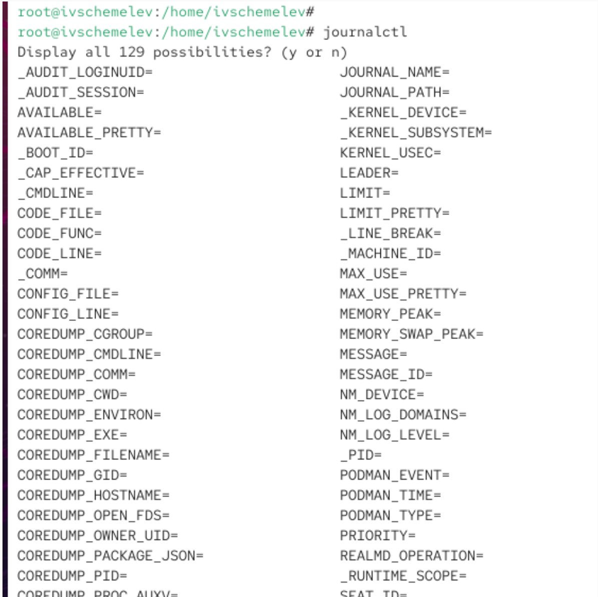
```
                                                                 Module libX11.so.6 from rpm libX11-1.8
.10-1.el10.x86_64

                                                                 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.x86_64

                                                                 Stack trace of thread 11193:
                                                                 #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  0x00007fd3a9a3e128 start_thread (l
ibc.so.6 + 0x95128)
                                                                 #5  0x00007fd3a9aaeafc __clone3 (libc.
so.6 + 0x105afc)

                                                                 Stack trace of thread 11190:
                                                                 #0  0x00007fd3a9aac8fd syscall (libc.s
o.6 + 0x1038fd)
                                                                 #1  0x00000000004344e2 n/a (n/a + 0x0)
                                                                 #2  0x0000000000450066 n/a (n/a + 0x0)
                                                                 #3  0x0000000000405123 n/a (n/a + 0x0)
                                                                 #4  0x00007fd3a99d358e __libc_start_ca
ll_main (libc.so.6 + 0x2a58e)
                                                                 #5  0x00007fd3a99d3649 __libc_start_ma
in@@GLIBC_2.34 (libc.so.6 + 0x2a649)
                                                                 #6  0x00000000004044aa n/a (n/a + 0x0)
                                                                 ELF object binary architecture: AMD x8
6-64
Jan 16 11:49:05 ivschemelev.localdomain systemd[1]: systemd-coredump@520-11194-0.service: Deactivated s
uccessfully.
root@ivschemelev:/home/ivschemelev#
```

Мониторинг в реальном времени



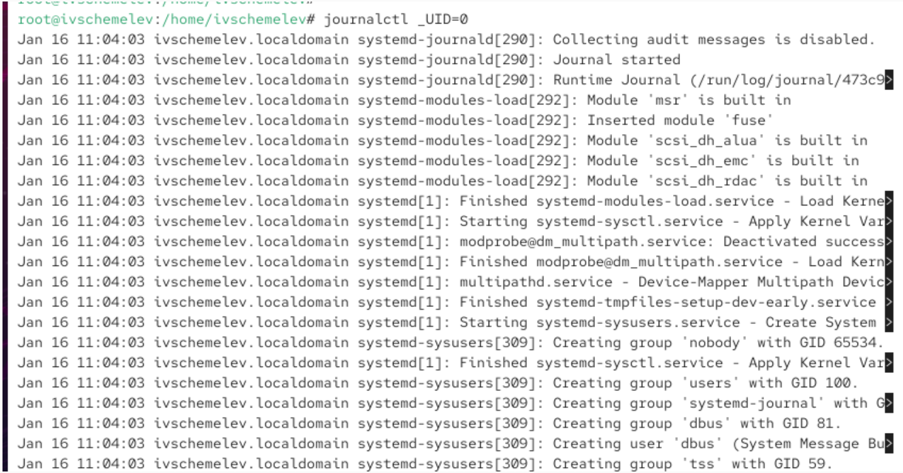
```
                                                                 #1  0x0000000000434c30 n/a (n/a + 0x0)
                                                                 #2  0x0000000000450bfb n/a (n/a + 0x0)
                                                                 #3  0x000000000043566a n/a (n/a + 0x0)
                                                                 #4  0x000000000045041c n/a (n/a + 0x0)
                                                                 #5  0x00000000004355d0 n/a (n/a + 0x0)
                                                                 #6  0x00007fd3a9a3e128 start_thread (l
ibc.so.6 + 0x95128)
                                                                 #7  0x00007fd3a9aaeafc __clone3 (libc.
so.6 + 0x105afc)

                                                                 Stack trace of thread 11250:
                                                                 #0  0x00007fd3a9aac8fd syscall (libc.s
o.6 + 0x1038fd)
                                                                 #1  0x00000000004344e2 n/a (n/a + 0x0)
                                                                 #2  0x0000000000450066 n/a (n/a + 0x0)
                                                                 #3  0x0000000000405123 n/a (n/a + 0x0)
                                                                 #4  0x00007fd3a99d358e __libc_start_ca
ll_main (libc.so.6 + 0x2a58e)
                                                                 #5  0x00007fd3a99d3649 __libc_start_ma
in@@GLIBC_2.34 (libc.so.6 + 0x2a649)
                                                                 #6  0x00000000004044aa n/a (n/a + 0x0)
                                                                 ELF object binary architecture: AMD x8
6-64
Jan 16 11:49:25 ivschemelev.localdomain systemd[1]: systemd-coredump@524-11254-0.service: Deactivated s
uccessfully.
^C
root@ivschemelev:/home/ivschemelev#
```

Параметры фильтрации journalctl



```
root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# journalctl
Display all 129 possibilities? (y or n)
_AUDIT_LOGINUID=                        JOURNAL_NAME=
_AUDIT_SESSION=                         JOURNAL_PATH=
AVAILABLE=                              _KERNEL_DEVICE=
AVAILABLE_PRETTY=                       _KERNEL_SUBSYSTEM=
_BOOT_ID=                               KERNEL_USEC=
_CAP_EFFECTIVE=                         LEADER=
_CMDLINE=                               LIMIT=
CODE_FILE=                              LIMIT_PRETTY=
CODE_FUNC=                              _LINE_BREAK=
CODE_LINE=                              _MACHINE_ID=
_COMM=                                  MAX_USE=
CONFIG_FILE=                            MAX_USE_PRETTY=
CONFIG_LINE=                            MEMORY_PEAK=
COREDUMP_CGROUP=                        MEMORY_SWAP_PEAK=
COREDUMP_CMDLINE=                       MESSAGE=
COREDUMP_COMM=                          MESSAGE_ID=
COREDUMP_CWD=                           NM_DEVICE=
COREDUMP_ENVIRON=                       NM_LOG_DOMAINS=
COREDUMP_EXE=                           NM_LOG_LEVEL=
COREDUMP_FILENAME=                      _PID=
COREDUMP_GID=                           PODMAN_EVENT=
COREDUMP_HOSTNAME=                      PODMAN_TIME=
COREDUMP_OPEN_FDS=                      PODMAN_TYPE=
COREDUMP_OWNER_UID=                     PRIORITY=
COREDUMP_PACKAGE_JSON=                  REALMD_OPERATION=
COREDUMP_PID=                           _RUNTIME_SCOPE=
COREDUMP_PROC_AUXV=                     SEAT_ID=
```

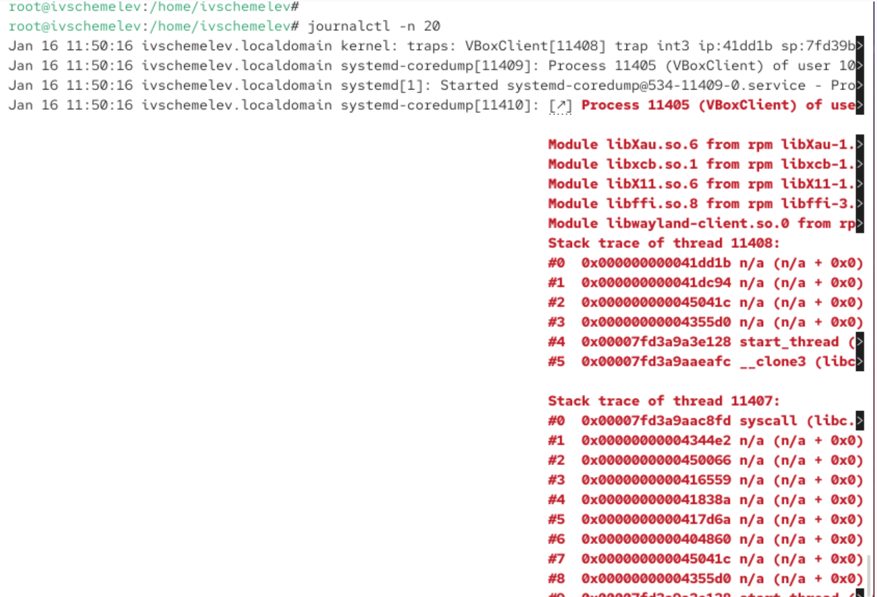
Фильтрация по пользователю UID 0



```
root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# journalctl _UID=0
Jan 16 11:04:03 ivschemelev.localdomain systemd-journald[290]: Collecting audit messages is disabled.
Jan 16 11:04:03 ivschemelev.localdomain systemd-journald[290]: Journal started
Jan 16 11:04:03 ivschemelev.localdomain systemd-journald[290]: Runtime Journal (/run/log/journal/473c9>
Jan 16 11:04:03 ivschemelev.localdomain systemd-modules-load[292]: Module 'msr' is built in
Jan 16 11:04:03 ivschemelev.localdomain systemd-modules-load[292]: Inserted module 'fuse'
Jan 16 11:04:03 ivschemelev.localdomain systemd-modules-load[292]: Module 'scsi_dh_alua' is built in
Jan 16 11:04:03 ivschemelev.localdomain systemd-modules-load[292]: Module 'scsi_dh_emc' is built in
Jan 16 11:04:03 ivschemelev.localdomain systemd-modules-load[292]: Module 'scsi_dh_rdac' is built in
Jan 16 11:04:03 ivschemelev.localdomain systemd[1]: Finished systemd-modules-load.service - Load Kerne>
Jan 16 11:04:03 ivschemelev.localdomain systemd[1]: Starting systemd-sysctl.service - Apply Kernel Var>
Jan 16 11:04:03 ivschemelev.localdomain systemd[1]: modprobe@dm_multipath.service: Deactivated success>
Jan 16 11:04:03 ivschemelev.localdomain systemd[1]: Finished modprobe@dm_multipath.service - Load Kern>
Jan 16 11:04:03 ivschemelev.localdomain systemd[1]: multipathd.service - Device-Mapper Multipath Devic>
Jan 16 11:04:03 ivschemelev.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev-early.service >
Jan 16 11:04:03 ivschemelev.localdomain systemd[1]: Starting systemd-sysusers.service - Create System >
Jan 16 11:04:03 ivschemelev.localdomain systemd-sysusers[309]: Creating group 'nobody' with GID 65534.
Jan 16 11:04:03 ivschemelev.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Var>
Jan 16 11:04:03 ivschemelev.localdomain systemd-sysusers[309]: Creating group 'users' with GID 100.
Jan 16 11:04:03 ivschemelev.localdomain systemd-sysusers[309]: Creating group 'systemd-journal' with G>
Jan 16 11:04:03 ivschemelev.localdomain systemd-sysusers[309]: Creating group 'dbus' with GID 81.
Jan 16 11:04:03 ivschemelev.localdomain systemd-sysusers[309]: Creating user 'dbus' (System Message Bu>
Jan 16 11:04:03 ivschemelev.localdomain systemd-sysusers[309]: Creating group 'tss' with GID 59.
```

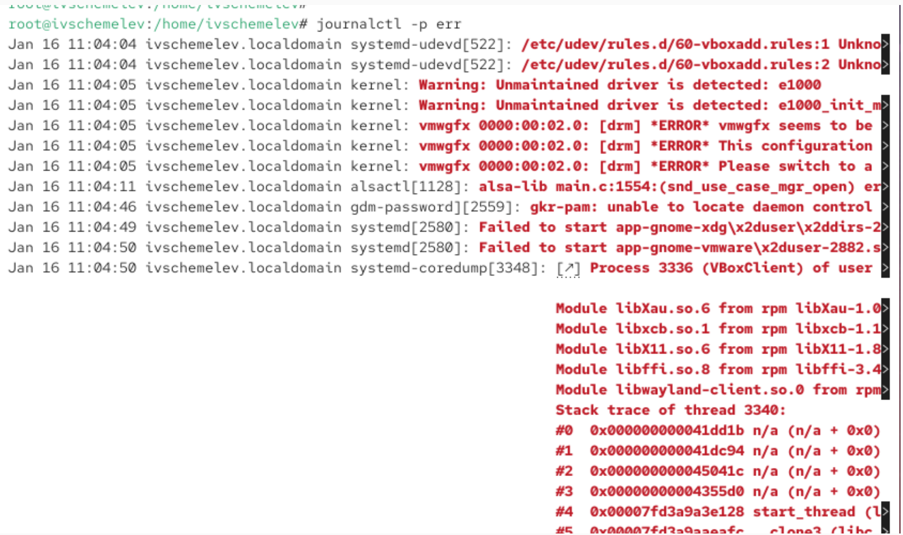
Рис. 14: События UID 0

Последние записи журнала



```
root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# journalctl -n 20
Jan 16 11:50:16 ivschemelev.localdomain kernel: traps: VBoxClient[11408] trap int3 ip:41dd1b sp:7fd39b>
Jan 16 11:50:16 ivschemelev.localdomain systemd-coredump[11409]: Process 11405 (VBoxClient) of user 10>
Jan 16 11:50:16 ivschemelev.localdomain systemd[1]: Started systemd-coredump@534-11409-0.service - Pro>
Jan 16 11:50:16 ivschemelev.localdomain systemd-coredump[11410]: [↗] Process 11405 (VBoxClient) of use>

                                                                 Module libXau.so.6 from rpm libXau-1.>
                                                                 Module libxcb.so.1 from rpm libxcb-1.>
                                                                 Module libX11.so.6 from rpm libX11-1.>
                                                                 Module libffi.so.8 from rpm libffi-3.>
                                                                 Module libwayland-client.so.0 from rp>
                                                                 Stack trace of thread 11408:
                                                                 #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  0x00007fd3a9a3e128 start_thread (>
                                                                 #5  0x00007fd3a9aaeafc __clone3 (libc>

                                                                 Stack trace of thread 11407:
                                                                 #0  0x00007fd3a9aac8fd syscall (libc.>
                                                                 #1  0x00000000004344e2 n/a (n/a + 0x0)
                                                                 #2  0x0000000000450066 n/a (n/a + 0x0)
                                                                 #3  0x0000000000416559 n/a (n/a + 0x0)
                                                                 #4  0x000000000041838a n/a (n/a + 0x0)
                                                                 #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  0x00007fd3a9a3e128 start_thread (>
```

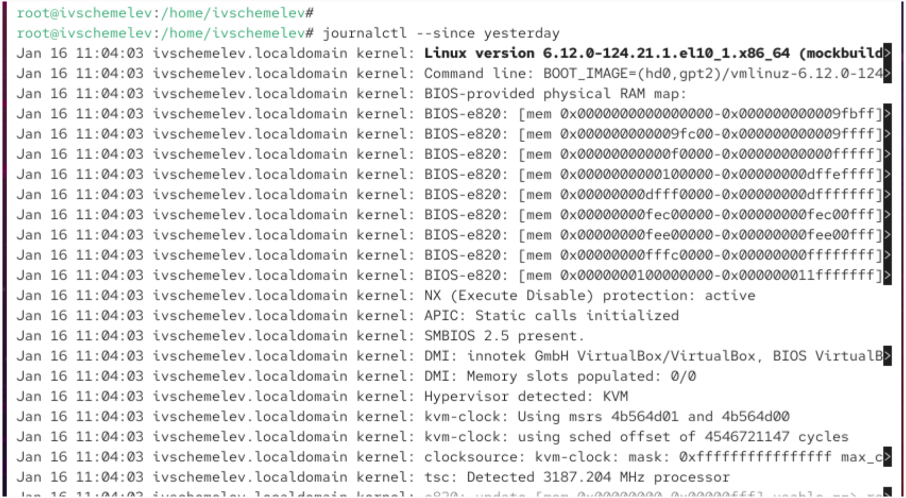
Сообщения с приоритетом ошибок



```
root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# journalctl -p err
Jan 16 11:04:04 ivschemelev.localdomain systemd-udevd[522]: /etc/udev/rules.d/60-vboxadd.rules:1 Unkno>
Jan 16 11:04:04 ivschemelev.localdomain systemd-udevd[522]: /etc/udev/rules.d/60-vboxadd.rules:2 Unkno>
Jan 16 11:04:05 ivschemelev.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Jan 16 11:04:05 ivschemelev.localdomain kernel: Warning: Unmaintained driver is detected: e1000_init_m>
Jan 16 11:04:05 ivschemelev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be >
Jan 16 11:04:05 ivschemelev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration >
Jan 16 11:04:05 ivschemelev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a >
Jan 16 11:04:11 ivschemelev.localdomain alsactl[1128]: alsa-lib main.c:1554:(snd_use_case_mgr_open) er>
Jan 16 11:04:46 ivschemelev.localdomain gdm-password][2559]: gkr-pam: unable to locate daemon control >
Jan 16 11:04:49 ivschemelev.localdomain systemd[2580]: Failed to start app-gnome-xdg\x2duser\x2ddirs-2>
Jan 16 11:04:50 ivschemelev.localdomain systemd[2580]: Failed to start app-gnome-vmware\x2duser-2882.s>
Jan 16 11:04:50 ivschemelev.localdomain systemd-coredump[3348]: [↗] Process 3336 (VBoxClient) of user >

                                                                   Module libXau.so.6 from rpm libXau-1.0>
                                                                   Module libxcb.so.1 from rpm libxcb-1.1>
                                                                   Module libX11.so.6 from rpm libX11-1.8>
                                                                   Module libffi.so.8 from rpm libffi-3.4>
                                                                   Module libwayland-client.so.0 from rpm>
                                                                   Stack trace of thread 3340:
                                                                   #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  0x00007fd3a9a3e128 start_thread (l>
                                                                   #5  0x00007fd3a9aaeafc __clone3 (libc >
```

Рис. 16: Ошибки системы

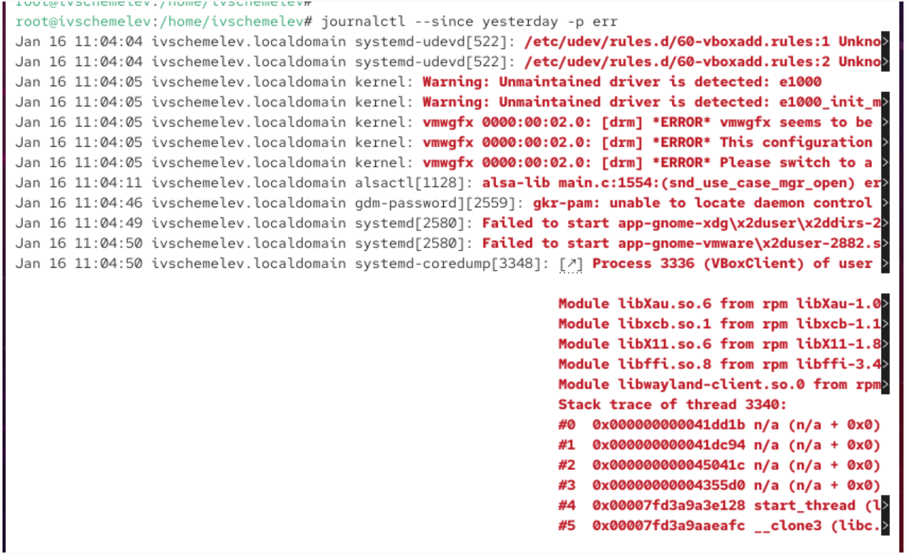
Журнал за вчерашний день



```
root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# journalctl --since yesterday
Jan 16 11:04:03 ivschemelev.localdomain kernel: Linux version 6.12.0-124.21.1.el10_1.x86_64 (mockbuild>
Jan 16 11:04:03 ivschemelev.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-124>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-provided physical RAM map:
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dffeffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000dfff0000-0x00000000dfffffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: NX (Execute Disable) protection: active
Jan 16 11:04:03 ivschemelev.localdomain kernel: APIC: Static calls initialized
Jan 16 11:04:03 ivschemelev.localdomain kernel: SMBIOS 2.5 present.
Jan 16 11:04:03 ivschemelev.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualB>
Jan 16 11:04:03 ivschemelev.localdomain kernel: DMI: Memory slots populated: 0/0
Jan 16 11:04:03 ivschemelev.localdomain kernel: Hypervisor detected: KVM
Jan 16 11:04:03 ivschemelev.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Jan 16 11:04:03 ivschemelev.localdomain kernel: kvm-clock: using sched offset of 4546721147 cycles
Jan 16 11:04:03 ivschemelev.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_c>
Jan 16 11:04:03 ivschemelev.localdomain kernel: tsc: Detected 3187.204 MHz processor
Jan 16 11:04:03 ivschemelev.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> re>
```

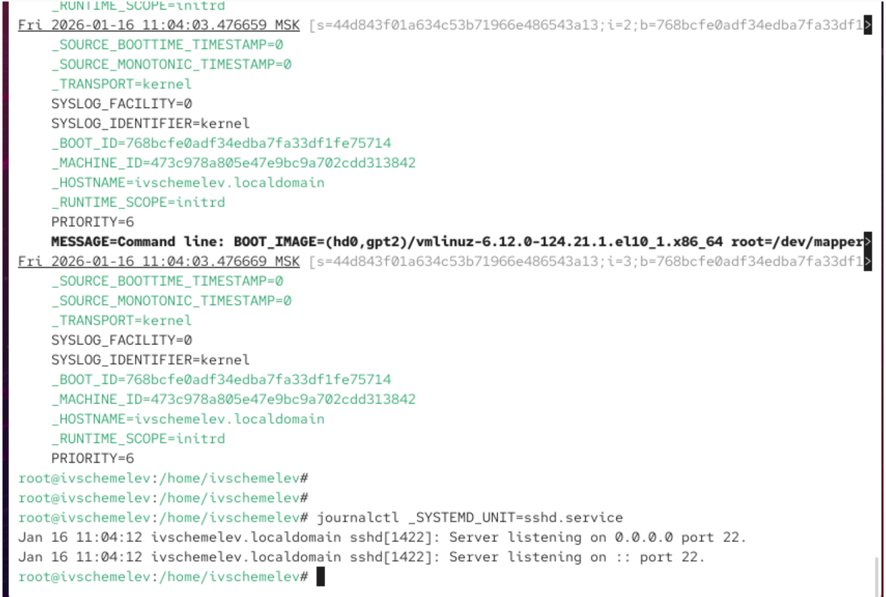
Рис. 17: Сообщения со вчерашнего дня

Ошибки за вчерашний день



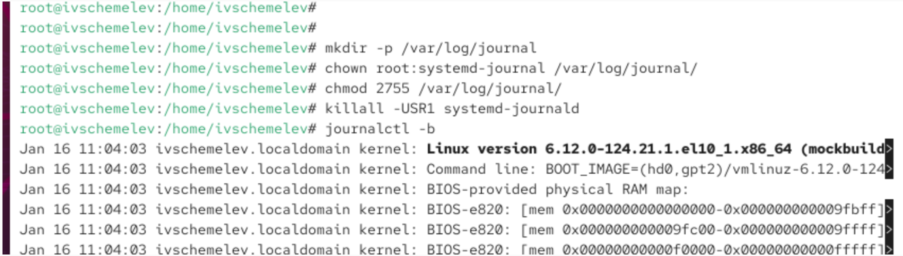
```
root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# journalctl --since yesterday -p err
Jan 16 11:04:04 ivschemelev.localdomain systemd-udevd[522]: /etc/udev/rules.d/60-vboxadd.rules:1 Unkno>
Jan 16 11:04:04 ivschemelev.localdomain systemd-udevd[522]: /etc/udev/rules.d/60-vboxadd.rules:2 Unkno>
Jan 16 11:04:05 ivschemelev.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Jan 16 11:04:05 ivschemelev.localdomain kernel: Warning: Unmaintained driver is detected: e1000_init_m>
Jan 16 11:04:05 ivschemelev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be >
Jan 16 11:04:05 ivschemelev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration >
Jan 16 11:04:05 ivschemelev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a >
Jan 16 11:04:11 ivschemelev.localdomain alsactl[1128]: alsa-lib main.c:1554:(snd_use_case_mgr_open) er>
Jan 16 11:04:46 ivschemelev.localdomain gdm-password][2559]: gkr-pam: unable to locate daemon control >
Jan 16 11:04:49 ivschemelev.localdomain systemd[2580]: Failed to start app-gnome-xdg\x2duser\x2ddirs-2>
Jan 16 11:04:50 ivschemelev.localdomain systemd[2580]: Failed to start app-gnome-vmware\x2duser-2882.s>
Jan 16 11:04:50 ivschemelev.localdomain systemd-coredump[3348]: [↗] Process 3336 (VBoxClient) of user >

                                                                Module libXau.so.6 from rpm libXau-1.0>
                                                                Module libxcb.so.1 from rpm libxcb-1.1>
                                                                Module libX11.so.6 from rpm libX11-1.8>
                                                                Module libffi.so.8 from rpm libffi-3.4>
                                                                Module libwayland-client.so.0 from rpm>
                                                                Stack trace of thread 3340:
                                                                #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  0x00007fd3a9a3e128 start_thread (l>
                                                                #5  0x00007fd3a9aaeafc __clone3 (libc.>
```

Расширенный формат журнала



```
    _RUNTIME_SCOPE=initrd
Fri 2026-01-16 11:04:03.476659 MSK [s=44d843f01a634c53b71966e486543a13;i=2;b=768bcfe0adf34edba7fa33df1>
    _SOURCE_BOOTTIME_TIMESTAMP=0
    _SOURCE_MONOTONIC_TIMESTAMP=0
    _TRANSPORT=kernel
    SYSLOG_FACILITY=0
    SYSLOG_IDENTIFIER=kernel
    _BOOT_ID=768bcfe0adf34edba7fa33df1fe75714
    _MACHINE_ID=473c978a805e47e9bc9a702cdd313842
    _HOSTNAME=ivschemelev.localdomain
    _RUNTIME_SCOPE=initrd
    PRIORITY=6
    MESSAGE=Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-124.21.1.el10_1.x86_64 root=/dev/mapper>
Fri 2026-01-16 11:04:03.476669 MSK [s=44d843f01a634c53b71966e486543a13;i=3;b=768bcfe0adf34edba7fa33df1>
    _SOURCE_BOOTTIME_TIMESTAMP=0
    _SOURCE_MONOTONIC_TIMESTAMP=0
    _TRANSPORT=kernel
    SYSLOG_FACILITY=0
    SYSLOG_IDENTIFIER=kernel
    _BOOT_ID=768bcfe0adf34edba7fa33df1fe75714
    _MACHINE_ID=473c978a805e47e9bc9a702cdd313842
    _HOSTNAME=ivschemelev.localdomain
    _RUNTIME_SCOPE=initrd
    PRIORITY=6
root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# journalctl _SYSTEMD_UNIT=sshd.service
Jan 16 11:04:12 ivschemelev.localdomain sshd[1422]: Server listening on 0.0.0.0 port 22.
Jan 16 11:04:12 ivschemelev.localdomain sshd[1422]: Server listening on :: port 22.
root@ivschemelev:/home/ivschemelev#
```

Проверка постоянного журнала



```
root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# mkdir -p /var/log/journal
root@ivschemelev:/home/ivschemelev# chown root:systemd-journal /var/log/journal/
root@ivschemelev:/home/ivschemelev# chmod 2755 /var/log/journal/
root@ivschemelev:/home/ivschemelev# killall -USR1 systemd-journald
root@ivschemelev:/home/ivschemelev# journalctl -b
Jan 16 11:04:03 ivschemelev.localdomain kernel: Linux version 6.12.0-124.21.1.el10_1.x86_64 (mockbuild>
Jan 16 11:04:03 ivschemelev.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-124>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-provided physical RAM map:
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff]>
```

Рис. 20: Постоянный журнал journald

Итоги работы

Заключение

В ходе лабораторной работы были изучены механизмы журналирования в операционной системе Linux. Освоены:

- мониторинг журналов в реальном времени;
- настройка rsyslog и перенаправление логов служб;
- анализ системных событий с помощью journalctl;
- организация постоянного хранения журнала systemd-journald.

Полученные навыки необходимы для администрирования и диагностики серверных и пользовательских Linux-систем.