Отчёт по лабораторной работе №7

Управление журналами событий в системе

Борисенкова София Павловна

1 октября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Цель

Получить навыки работы с журналами мониторинга различных событий в системе.

Выполнение лабораторной работы

Мониторинг системных событий

Рис. 1: Ошибка аутентификации при su

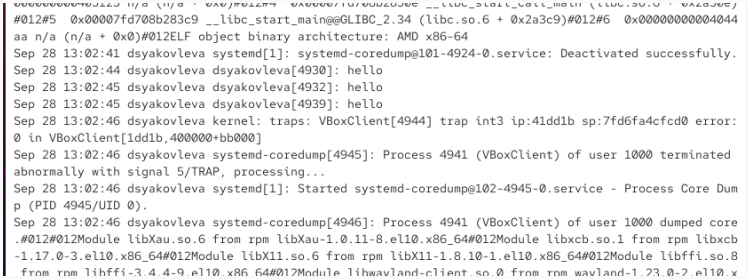

Рис. 2: Сообщение logger hello

Мониторинг системных событий

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

Изменение правил rsyslog.conf

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

Installed:
  apr-1.7.5-2.el10.x86_64                      apr-util-1.6.3-21.el10.x86_64
  apr-util-lmdb-1.6.3-21.el10.x86_64           apr-util-openssl-1.6.3-21.el10.x86_64
  httpd-2.4.63-1.el10_0.2.x86_64               httpd-core-2.4.63-1.el10_0.2.x86_64
  httpd-filesystem-2.4.63-1.el10_0.2.noarch    httpd-tools-2.4.63-1.el10_0.2.x86_64
  mod_http2-2.0.29-2.el10_0.1.x86_64           mod_lua-2.4.63-1.el10_0.2.x86_64
  rocky-logos-httpd-100.4-7.el10.noarch

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

Рис. 4: Установка и запуск Apache

Изменение правил rsyslog.conf

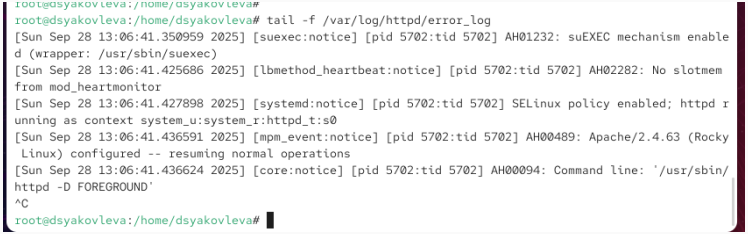

Рис. 5: Просмотр error_log Apache

Изменение правил rsyslog.conf

Рис. 6: Настройка ErrorLog в httpd.conf

Изменение правил rsyslog.conf

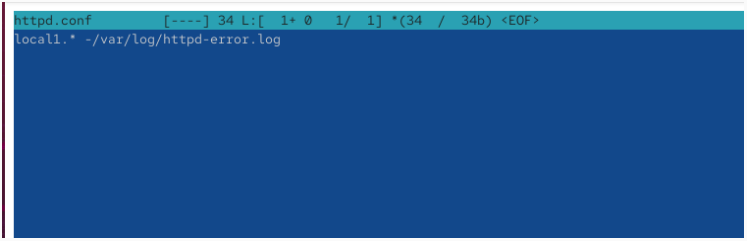

Рис. 7: Правило rsyslog для httpd

Изменение правил rsyslog.conf

```
root@dsyakovleva:/home/dsyakovleva#
root@dsyakovleva:/home/dsyakovleva# mcedit /etc/httpd/conf/httpd.conf

root@dsyakovleva:/home/dsyakovleva#
root@dsyakovleva:/home/dsyakovleva# cd /etc/rsyslog.d/
root@dsyakovleva:/etc/rsyslog.d# touch httpd.conf
root@dsyakovleva:/etc/rsyslog.d# mcedit httpd.conf

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

Рис. 8: Создание debug.conf

Изменение правил rsyslog.conf

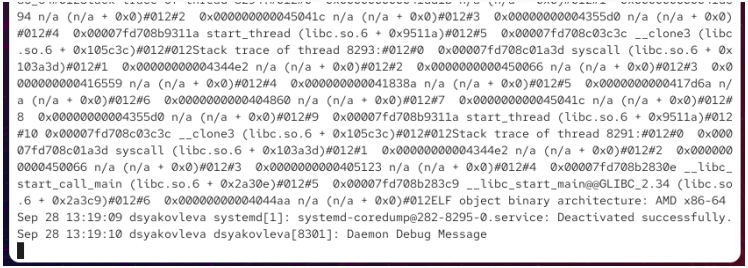

Рис. 9: Сообщение Daemon Debug Message

Использование journalctl

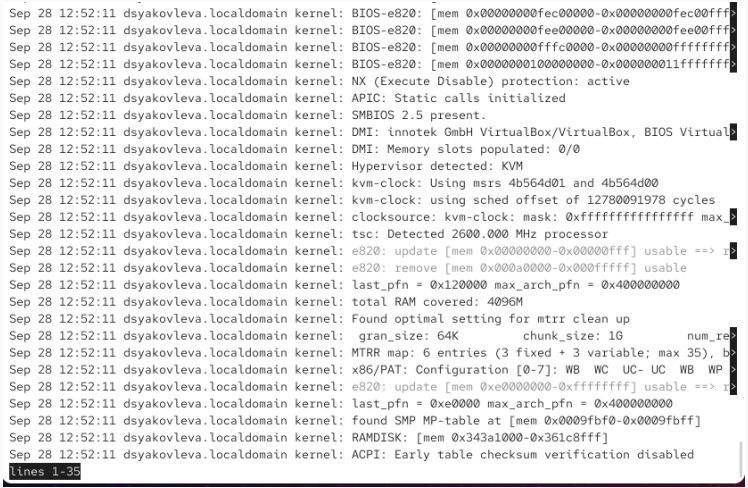

Рис. 10: Просмотр журнала journalctl

Использование journalctl

```
.4-9.el10.x86_64
                                                    Module libwayland-client.so.0 from rpm
 wayland-1.23.0-2.el10.x86_64
                                                    Stack trace of thread 8744:
                                                    #0  0x000000000041dd1b n/a (n/a + 0x0)
                                                    #1  0x000000000041dc94 n/a (n/a + 0x0)
                                                    #2  0x000000000045041c n/a (n/a + 0x0)
                                                    #3  0x00000000004355d0 n/a (n/a + 0x0)
                                                    #4  0x00007fd708b9311a start_thread (l
ibc.so.6 + 0x9511a)
                                                    #5  0x00007fd708c03c3c __clone3 (libc.
so.6 + 0x105c3c)

                                                    Stack trace of thread 8741:
                                                    #0  0x00007fd708c01a3d syscall (libc.s
o.6 + 0x103a3d)
                                                    #1  0x00000000004344e2 n/a (n/a + 0x0)
                                                    #2  0x0000000000450066 n/a (n/a + 0x0)
                                                    #3  0x0000000000405123 n/a (n/a + 0x0)
                                                    #4  0x00007fd708b2830e __libc_start_ca
ll_main (libc.so.6 + 0x2a30e)
                                                    #5  0x00007fd708b283c9 __libc_start_ma
in@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)
                                                    #6  0x00000000004044aa n/a (n/a + 0x0)
                                                    ELF object binary architecture: AMD x8
6-64
Sep 28 13:22:20 dsyakovleva.localdomain systemd[1]: systemd-coredump@317-8745-0.service: Deactivated s
uccessfully.
root@dsyakovleva:/etc/rsyslog.d#
```

Рис. 11: Вывод без пейджера

Использование journalctl

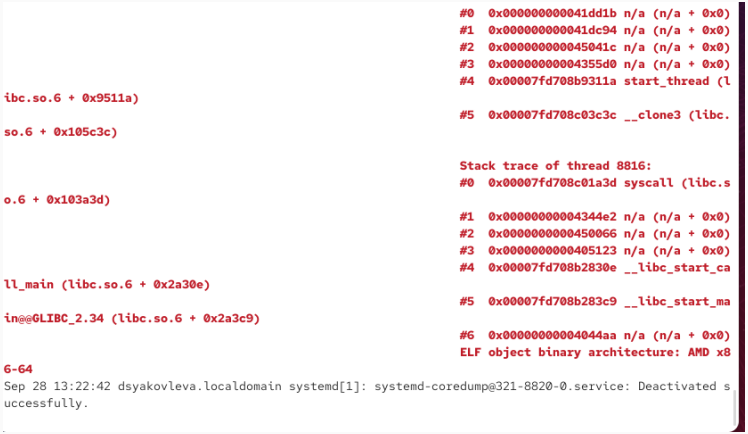

Рис. 12: Режим реального времени

Использование journalctl

```
root@dsyakovleva:/etc/rsyslog.d#
root@dsyakovleva:/etc/rsyslog.d# journalctl
Display all 128 possibilities? (y or n)
_AUDIT_LOGINUID=                    JOB_TYPE=
_AUDIT_SESSION=                     JOURNAL_NAME=
AVAILABLE=                          JOURNAL_PATH=
AVAILABLE_PRETTY=                   _KERNEL_DEVICE=
_BOOT_ID=                           _KERNEL_SUBSYSTEM=
_CAP_EFFECTIVE=                     KERNEL_USEC=
_CMDLINE=                           LEADER=
CODE_FILE=                          LIMIT=
CODE_FUNC=                          LIMIT_PRETTY=
CODE_LINE=                          _LINE_BREAK=
_COMM=                              _MACHINE_ID=
CONFIG_FILE=                        MAX_USE=
CONFIG_LINE=                        MAX_USE_PRETTY=
COREDUMP_CGROUP=                    MEMORY_PEAK=
COREDUMP_CMDLINE=                   MEMORY_SWAP_PEAK=
COREDUMP_COMM=                      MESSAGE=
COREDUMP_CWD=                       MESSAGE_ID=
COREDUMP_ENVIRON=                   NM_DEVICE=
COREDUMP_EXE=                       NM_LOG_DOMAINS=
COREDUMP_FILENAME=                  NM_LOG_LEVEL=
COREDUMP_GID=                       _PID=
COREDUMP_HOSTNAME=                  PODMAN_EVENT=
COREDUMP_OPEN_FDS=                  PODMAN_TIME=
COREDUMP_OWNER_UID=                 PODMAN_TYPE=
COREDUMP_PACKAGE_JSON=              PRIORITY=
COREDUMP_PID=                       REALMD_OPERATION=
COREDUMP_PROC_AUXV=                 _RUNTIME_SCOPE=
COREDUMP_PROC_CGROUP=               SEAT_ID=
COREDUMP_PROC_LIMITS=               _SELINUX_CONTEXT=
COREDUMP_PROC_MAPS=                 SESSION_ID=
COREDUMP_PROC_MOUNTINFO=            _SOURCE_BOOTTIME_TIMESTAMP=
COREDUMP_PROC_STATUS=               _SOURCE_MONOTONIC_TIMESTAMP=
```

Использование journalctl

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

Рис. 14: UID=0

Использование journalctl

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

                                                                Module libXau.so.6 from rpm libXau-1.
                                                                Module libxcb.so.1 from rpm libxcb-1.
                                                                Module libX11.so.6 from rpm libX11-1.
                                                                Module libffi.so.8 from rpm libffi-3.
                                                                Module libwayland-client.so.0 from rp
                                                                Stack trace of thread 9077:
                                                                #0  0x000000000041dd1b n/a (n/a + 0x0)
                                                                #1  0x000000000041dc94 n/a (n/a + 0x0)
                                                                #2  0x000000000045041c n/a (n/a + 0x0)
                                                                #3  0x00000000004355d0 n/a (n/a + 0x0)
                                                                #4  0x00007fd708b9311a start_thread (
                                                                #5  0x00007fd708c03c3c __clone3 (libc

                                                                Stack trace of thread 9076:
                                                                #0  0x00007fd708c01a3d syscall (libc.
                                                                #1  0x00000000004344e2 n/a (n/a + 0x0)
                                                                #2  0x000000000045006б n/a (n/a + 0x0)
                                                                #3  0x0000000000416559 n/a (n/a + 0x0)
                                                                #4  0x000000000041838a n/a (n/a + 0x0)
```

Рис. 15: Последние 20 строк

Использование journalctl

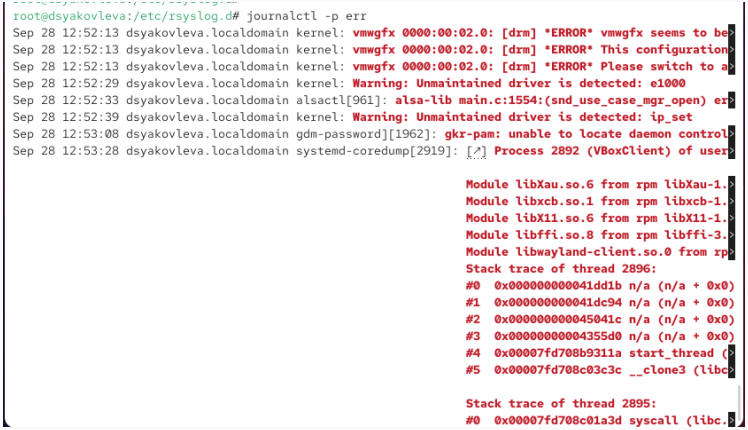

Рис. 16: Сообщения об ошибках

Использование journalctl

```
root@dsyakovleva:/etc/rsyslog.d#
root@dsyakovleva:/etc/rsyslog.d# journalctl --since yesterday
Sep 28 12:52:11 dsyakovleva.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@
Sep 28 12:52:11 dsyakovleva.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-provided physical RAM map:
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dffeffff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x00000000dfff0000-0x00000000dfffffff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: NX (Execute Disable) protection: active
Sep 28 12:52:11 dsyakovleva.localdomain kernel: APIC: Static calls initialized
Sep 28 12:52:11 dsyakovleva.localdomain kernel: SMBIOS 2.5 present.
Sep 28 12:52:11 dsyakovleva.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS Virtual
Sep 28 12:52:11 dsyakovleva.localdomain kernel: DMI: Memory slots populated: 0/0
Sep 28 12:52:11 dsyakovleva.localdomain kernel: Hypervisor detected: KVM
Sep 28 12:52:11 dsyakovleva.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Sep 28 12:52:11 dsyakovleva.localdomain kernel: kvm-clock: using sched offset of 12780091978 cycles
Sep 28 12:52:11 dsyakovleva.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_
Sep 28 12:52:11 dsyakovleva.localdomain kernel: tsc: Detected 2600.000 MHz processor
Sep 28 12:52:11 dsyakovleva.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> r
Sep 28 12:52:11 dsyakovleva.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Sep 28 12:52:11 dsyakovleva.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Sep 28 12:52:11 dsyakovleva.localdomain kernel: total RAM covered: 4096M
Sep 28 12:52:11 dsyakovleva.localdomain kernel: Found optimal setting for mtrr clean up
Sep 28 12:52:11 dsyakovleva.localdomain kernel:  gran_size: 64K         chunk_size: 1G         num_re
```

Рис. 17: Со вчерашнего дня

Использование journalctl

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

                                                    Module libXau.so.6 from rpm libXau-1.
                                                    Module libxcb.so.1 from rpm libxcb-1.
                                                    Module libX11.so.6 from rpm libX11-1.
                                                    Module libffi.so.8 from rpm libffi-3.
                                                    Module libwayland-client.so.0 from rp
                                                    Stack trace of thread 2896:
                                                    #0  0x00000000041dd1b n/a (n/a + 0x0)
                                                    #1  0x00000000041dc94 n/a (n/a + 0x0)
                                                    #2  0x000000000045041c n/a (n/a + 0x0)
                                                    #3  0x00000000004355d0 n/a (n/a + 0x0)
                                                    #4  0x00007fd708b9311a start_thread (
                                                    #5  0x00007fd708c03c3c __clone3 (libc

                                                    Stack trace of thread 2895:
                                                    #0  0x00007fd708c01a3d syscall (libc.
                                                    #1  0x00000000004344e2 n/a (n/a + 0x0)
                                                    #2  0x0000000000450066 n/a (n/a + 0x0)
                                                    #3  0x0000000000416559 n/a (n/a + 0x0)
                                                    #4  0x00000000041838a n/a (n/a + 0x0)
```

Рис. 18: Ошибки со вчерашнего дня

Использование journalctl

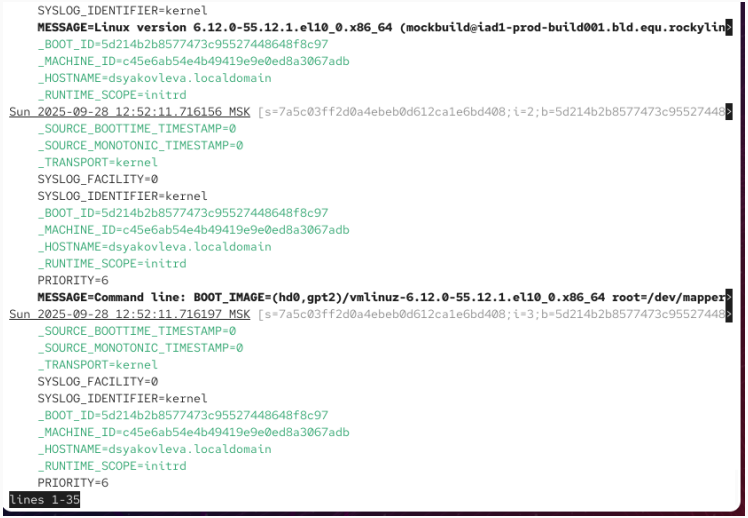

Рис. 19: Подробный вывод verbose

Использование journalctl

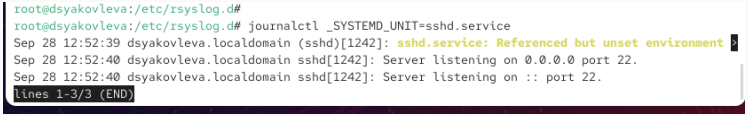

Рис. 20: Журнал sshd

Постоянный журнал journald

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

Рис. 21: Создание каталога journald

Постоянный журнал journald

```
root@dsyakovleva:/etc/rsyslog.d#
root@dsyakovleva:/etc/rsyslog.d# mkdir -p /var/log/journal
root@dsyakovleva:/etc/rsyslog.d# chown root:systemd-journal /var/log/journal/
root@dsyakovleva:/etc/rsyslog.d# chmod 2755 /var/log/journal/
root@dsyakovleva:/etc/rsyslog.d# killall -USR1 systemd-journald
root@dsyakovleva:/etc/rsyslog.d# journalctl -b
Sep 28 12:52:11 dsyakovleva.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@
Sep 28 12:52:11 dsyakovleva.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55@
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-provided physical RAM map:
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dffeffff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x00000000dfff0000-0x00000000dfffffff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff]
Sep 28 12:52:11 dsyakovleva.localdomain kernel: NX (Execute Disable) protection: active
```

Рис. 22: Активация journald

Контрольные вопросы

Конфигурация rsyslog

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

Ротация журналов

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

journalctl

- Режим реального времени: `journalctl -f`
- Сообщения PID 1 с 9:00 до 15:00:

  ```
  journalctl _PID=1 --since "09:00" --until "15:00"
  ```
- После перезагрузки: `journalctl -b`

Итоги работы

Вывод

Были приобретены навыки мониторинга системных журналов и настройки регистрации событий в Linux:
работа с `tail`, настройка `rsyslog`, использование `logger`, исследование логов при помощи `journalctl` и настройка постоянного хранения с помощью `journald`.