Лабораторная работа №7

Управление журналами событий в системе

Анастасия Мазуркевич

15 октября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Цель лабораторной работы

Получить навыки работы с системными журналами и их конфигурацией в Linux, научиться использовать rsyslog и journalctl для анализа событий.

Ход выполнения

Мониторинг системных сообщений

```
root@admazurkevich:/home/admazurkevich# tail -f /var/log/messages
Oct  1 11:17:34 admazurkevich systemd[1]: systemd-coredump@27-3580-0.service: Deactivated successfully.
Oct  1 11:17:39 admazurkevich chronyd[929]: Source 46.160.198.122 replaced with 2a12:4141:face:6::a (2.rocky.pool.ntp
.org)
Oct  1 11:17:39 admazurkevich kernel: traps: VBoxClient[3592] trap int3 ip:41dd1b sp:7f198c635cd0 error:0 in VBoxClie
nt[1dd1b,400000+bb000]
Oct  1 11:17:39 admazurkevich systemd-coredump[3593]: Process 3589 (VBoxClient) of user 1000 terminated abnormally wi
th signal 5/TRAP, processing...
Oct  1 11:17:39 admazurkevich systemd[1]: Starting fwupd-refresh.service - Refresh fwupd metadata and update motd...
Oct  1 11:17:39 admazurkevich systemd[1]: Started systemd-coredump@28-3593-0.service - Process Core Dump (PID 3593/UI
D 0).
Oct  1 11:17:40 admazurkevich systemd[1]: fwupd-refresh.service: Deactivated successfully.
Oct  1 11:17:40 admazurkevich systemd[1]: Finished fwupd-refresh.service - Refresh fwupd metadata and update motd.
Oct  1 11:17:40 admazurkevich systemd-coredump[3595]: Process 3589 (VBoxClient) of user 1000 dumped core.#012#012Modu
le libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Mod
ule libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012Mod
ule libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 3592:#012#0  0x000000000041
dd1b n/a (n/a + 0x0)#012#1  0x000000000041dc94 n/a (n/a + 0x0)#012#2  0x000000000045041c n/a (n/a + 0x0)#012#3  0x000
000000044355d0 n/a (n/a + 0x0)#012#4  0x00007f199ace611a start_thread (libc.so.6 + 0x9511a)#012#5  0x00007f199ad56c3c
__clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 3589:#012#0  0x00007f199ad54a3d syscall (libc.so.6 + 0x1
03a3d)#012#1  0x0000000000044344e2 n/a (n/a + 0x0)#012#2  0x0000000000450066 n/a (n/a + 0x0)#012#3  0x0000000000405123
n/a (n/a + 0x0)#012#4  0x00007f199ac7b30e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5  0x00007f199ac7b3c9 __li
bc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6  0x0000000000044aa n/a (n/a + 0x0)#012ELF object binary archit
ecture: AMD x86-64
Oct  1 11:17:40 admazurkevich systemd[1]: systemd-coredump@28-3593-0.service: Deactivated successfully.
Oct  1 11:17:45 admazurkevich kernel: traps: VBoxClient[3620] trap int3 ip:41dd1b sp:7f198c635cd0 error:0 in VBoxClie
nt[1dd1b,400000+bb000]
Oct  1 11:17:45 admazurkevich systemd-coredump[3621]: Process 3617 (VBoxClient) of user 1000 terminated abnormally wi
th signal 5/TRAP, processing...
Oct  1 11:17:45 admazurkevich systemd[1]: Started systemd-coredump@29-3621-0.service - Process Core Dump (PID 3621/UI
D 0).
Oct  1 11:17:45 admazurkevich systemd-coredump[3622]: Process 3617 (VBoxClient) of user 1000 dumped core.#012#012Modu
```

Рис. 1: Мониторинг системных сообщений

Ошибка при вводе пароля

```
Oct  1 11:18:25 admazurkevich systemd-coredump[3721]: Process 3717 (VBoxClient) of user 1000 terminated abnormally wi
th signal 5/TRAP, processing...
Oct  1 11:18:25 admazurkevich systemd[1]: Started systemd-coredump@37-3721-0.service - Process Core Dump (PID 3721/UI
D 0).
Oct  1 11:18:25 admazurkevich su[3714]: FAILED SU (to root) admazurkevich on pts/2
Oct  1 11:18:25 admazurkevich systemd-coredump[3722]: Process 3717 (VBoxClient) of user 1000 dumped core.#012#012Modu
le libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Mod
ule libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012Mod
ule libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 3720:#012#0  0x000000000041
dd1b n/a (n/a + 0x0)#012#1  0x000000000041dc94 n/a (n/a + 0x0)#012#2  0x000000000045041c n/a (n/a + 0x0)#012#3  0x000
00000004355d0 n/a (n/a + 0x0)#012#4  0x00007f199ace611a start_thread (libc.so.6 + 0x9511a)#012#5  0x00007f199ad56c3c
```

Рис. 2: Сообщение об ошибке аутентификации

Использование logger

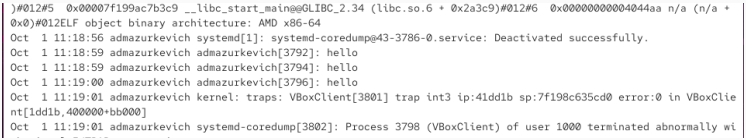

Рис. 3: Сообщение logger hello в журнале

Просмотр secure

```
root@admazurkevich:/home/admazurkevich# tail -n 20 /var/log/secure
Sep 25 15:15:47 admazurkevich su[4807]: pam_unix(su:session): session closed for user root
Oct  1 11:15:12 admazurkevich sshd[1192]: Server listening on 0.0.0.0 port 22.
Oct  1 11:15:12 admazurkevich sshd[1192]: Server listening on :: port 22.
Oct  1 11:15:12 admazurkevich (systemd)[1259]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by
 gdm(uid=0)
Oct  1 11:15:12 admazurkevich gdm-launch-environment][1237]: pam_unix(gdm-launch-environment:session): session opened
 for user gdm(uid=42) by (uid=0)
Oct  1 11:15:18 admazurkevich gdm-password][1958]: gkr-pam: unable to locate daemon control file
Oct  1 11:15:18 admazurkevich gdm-password][1958]: gkr-pam: stashed password to try later in open session
Oct  1 11:15:18 admazurkevich (systemd)[1985]: pam_unix(systemd-user:session): session opened for user admazurkevich(
uid=1000) by admazurkevich(uid=0)
Oct  1 11:15:18 admazurkevich gdm-password][1958]: pam_unix(gdm-password:session): session opened for user admazurkev
ich(uid=1000) by admazurkevich(uid=0)
Oct  1 11:15:18 admazurkevich gdm-password][1958]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyrin
g
Oct  1 11:15:22 admazurkevich gdm-launch-environment][1237]: pam_unix(gdm-launch-environment:session): session closed
 for user gdm
Oct  1 11:17:18 admazurkevich (systemd)[3392]: pam_unix(systemd-user:session): session opened for user root(uid=0) by
 root(uid=0)
Oct  1 11:17:18 admazurkevich su[3369]: pam_unix(su:session): session opened for user root(uid=0) by admazurkevich(ui
d=1000)
Oct  1 11:17:24 admazurkevich su[3474]: pam_unix(su:session): session opened for user root(uid=0) by admazurkevich(ui
d=1000)
Oct  1 11:17:28 admazurkevich su[3539]: pam_unix(su:session): session opened for user root(uid=0) by admazurkevich(ui
d=1000)
Oct  1 11:18:14 admazurkevich su[3539]: pam_unix(su:session): session closed for user root
Oct  1 11:18:17 admazurkevich unix_chkpwd[3702]: password check failed for user (root)
Oct  1 11:18:17 admazurkevich su[3683]: pam_unix(su:auth): authentication failure; logname=admazurkevich uid=1000 eui
d=0 tty=/dev/pts/2 ruser=admazurkevich rhost=  user=root
Oct  1 11:18:23 admazurkevich unix_chkpwd[3716]: password check failed for user (root)
Oct  1 11:18:23 admazurkevich su[3714]: pam_unix(su:auth): authentication failure; logname=admazurkevich uid=1000 eui
d=0 tty=/dev/pts/2 ruser=admazurkevich rhost=  user=root
root@admazurkevich:/home/admazurkevich#
```

Рис. 4: Фрагмент журнала secure

Установка и запуск Apache

Рис. 5: Установка и запуск Apache

Журнал ошибок Apache

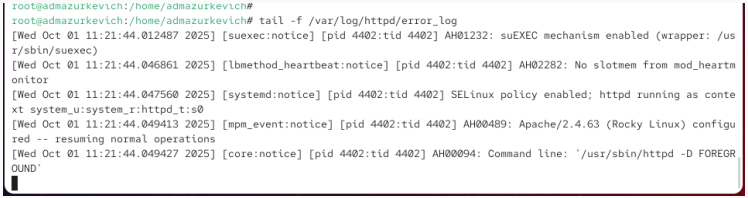

Рис. 6: Журнал ошибок Apache

Перенаправление логов Apache

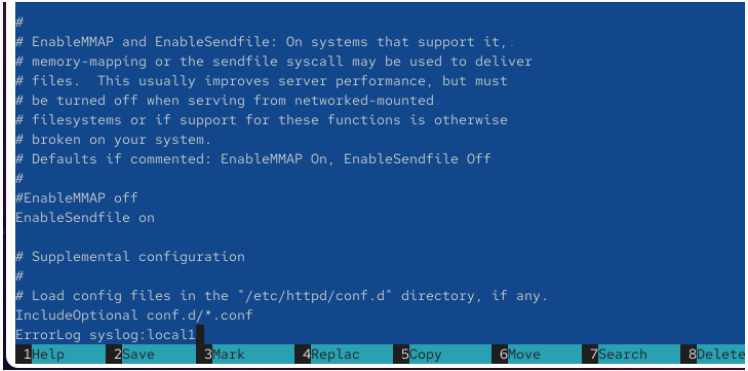

Рис. 7: Добавление правила ErrorLog в httpd.conf

Создание правила rsyslog

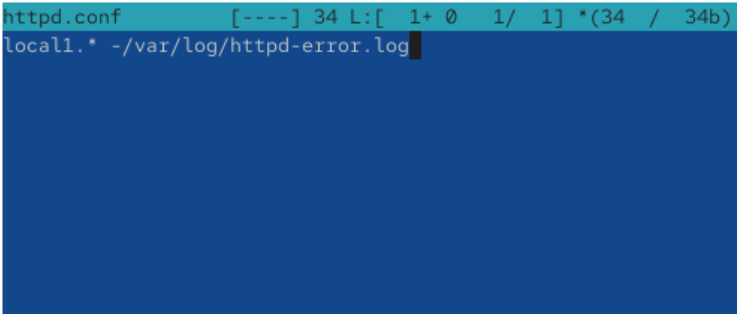

Рис. 8: Создание правила для логов Apache в rsyslog

Конфигурация отладочного журнала

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

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

Рис. 9: Создание конфигурации debug.conf

Проверка отладочного сообщения

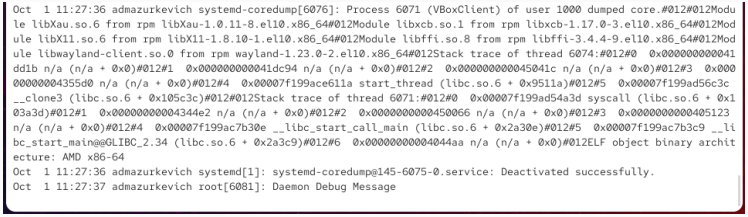

Рис. 10: Сообщение отладки в журнале

Просмотр системного журнала

```
root@admazurkevich:/home/admazurkevich# journalctl
Oct 01 11:15:07 admazurkevich.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-bu
Oct 01 11:15:07 admazurkevich.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-provided physical RAM map:
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dffeffff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000dfff0000-0x00000000dfffffff] ACPI data
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: NX (Execute Disable) protection: active
Oct 01 11:15:07 admazurkevich.localdomain kernel: APIC: Static calls initialized
Oct 01 11:15:07 admazurkevich.localdomain kernel: SMBIOS 2.5 present.
Oct 01 11:15:07 admazurkevich.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 01 11:15:07 admazurkevich.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 01 11:15:07 admazurkevich.localdomain kernel: Hypervisor detected: KVM
Oct 01 11:15:07 admazurkevich.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 01 11:15:07 admazurkevich.localdomain kernel: kvm-clock: using sched offset of 4069948781 cycles
Oct 01 11:15:07 admazurkevich.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd
Oct 01 11:15:07 admazurkevich.localdomain kernel: tsc: Detected 3187.198 MHz processor
Oct 01 11:15:07 admazurkevich.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 01 11:15:07 admazurkevich.localdomain kernel: total RAM covered: 4096M
Oct 01 11:15:07 admazurkevich.localdomain kernel: Found optimal setting for mtrr clean up
Oct 01 11:15:07 admazurkevich.localdomain kernel:  gran_size: 64K         chunk_size: 1G         num_reg: 3
Oct 01 11:15:07 admazurkevich.localdomain kernel: MTRR map: 6 entries (3 fixed + 3 variable; max 35), built from 16
Oct 01 11:15:07 admazurkevich.localdomain kernel: x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WP  UC- WT
```

Рис. 11: Просмотр системного журнала

Режим реального времени

Рис. 12: Режим просмотра журнала в реальном времени

Фильтрация параметров

```
root@admazurkevich:/home/admazurkevich# journalctl
Display all 131 possibilities? (y or n)
_AUDIT_LOGINUID=                    CURRENT_USE_PRETTY=                    PODMAN_EVENT=
_AUDIT_SESSION=                     DBUS_BROKER_LOG_DROPPED=               PODMAN_TIME=
AVAILABLE=                          DBUS_BROKER_METRICS_DISPATCH_AVG=      PODMAN_TYPE=
AVAILABLE_PRETTY=                   DBUS_BROKER_METRICS_DISPATCH_COUNT=    PRIORITY=
_BOOT_ID=                           DBUS_BROKER_METRICS_DISPATCH_MAX=      REALMD_OPERATION=
_CAP_EFFECTIVE=                     DBUS_BROKER_METRICS_DISPATCH_MIN=      _RUNTIME_SCOPE=
_CMDLINE=                           DBUS_BROKER_METRICS_DISPATCH_STDDEV=   SEAT_ID=
CODE_FILE=                          DISK_AVAILABLE=                        _SELINUX_CONTEXT=
CODE_FUNC=                          DISK_AVAILABLE_PRETTY=                 SESSION_ID=
CODE_LINE=                          DISK_KEEP_FREE=                        _SOURCE_BOOTTIME_TIMESTAMP=
_COMM=                              DISK_KEEP_FREE_PRETTY=                 _SOURCE_MONOTONIC_TIMESTAMP=
COMMAND=                            ERRNO=                                 _SOURCE_REALTIME_TIMESTAMP=
CONFIG_FILE=                        _EXE=                                  SSSD_DOMAIN=
CONFIG_LINE=                        EXIT_CODE=                             SSSD_PRG_NAME=
COREDUMP_CGROUP=                    EXIT_STATUS=                           _STREAM_ID=
COREDUMP_CMDLINE=                   _GID=                                  SYSLOG_FACILITY=
COREDUMP_COMM=                      GLIB_DOMAIN=                           SYSLOG_IDENTIFIER=
COREDUMP_CWD=                       GLIB_OLD_LOG_API=                      SYSLOG_PID=
COREDUMP_ENVIRON=                   _HOSTNAME=                             SYSLOG_RAW=
COREDUMP_EXE=                       INITRD_USEC=                           SYSLOG_TIMESTAMP=
COREDUMP_FILENAME=                  INVOCATION_ID=                         _SYSTEMD_CGROUP=
COREDUMP_GID=                       JOB_ID=                                _SYSTEMD_INVOCATION_ID=
COREDUMP_HOSTNAME=                  JOB_RESULT=                            _SYSTEMD_OWNER_UID=
COREDUMP_OPEN_FDS=                  JOB_TYPE=                              _SYSTEMD_SESSION=
COREDUMP_OWNER_UID=                 JOURNAL_NAME=                          _SYSTEMD_SLICE=
COREDUMP_PACKAGE_JSON=              JOURNAL_PATH=                          _SYSTEMD_UNIT=
COREDUMP_PID=                       _KERNEL_DEVICE=                        _SYSTEMD_USER_SLICE=
COREDUMP_PROC_AUXV=                 _KERNEL_SUBSYSTEM=                     _SYSTEMD_USER_UNIT=
COREDUMP_PROC_CGROUP=               KERNEL_USEC=                           THREAD_ID=
COREDUMP_PROC_LIMITS=               LEADER=                                TID=
```

Рис. 13: Фильтрация журнала по параметрам

События UID=0

```
root@admazurkevich:/home/admazurkevich# journalctl _UID=0
Oct 01 11:15:07 admazurkevich.localdomain systemd-journald[280]: Collecting audit messages is disabled.
Oct 01 11:15:07 admazurkevich.localdomain systemd-journald[280]: Journal started
Oct 01 11:15:07 admazurkevich.localdomain systemd-journald[280]: Runtime Journal (/run/log/journal/c9e273a9076042e78
Oct 01 11:15:07 admazurkevich.localdomain systemd-modules-load[281]: Module 'msr' is built in
Oct 01 11:15:07 admazurkevich.localdomain systemd-modules-load[281]: Inserted module 'fuse'
Oct 01 11:15:07 admazurkevich.localdomain systemd-modules-load[281]: Module 'scsi_dh_alua' is built in
Oct 01 11:15:07 admazurkevich.localdomain systemd-modules-load[281]: Module 'scsi_dh_emc' is built in
Oct 01 11:15:07 admazurkevich.localdomain systemd-modules-load[281]: Module 'scsi_dh_rdac' is built in
Oct 01 11:15:07 admazurkevich.localdomain systemd-sysusers[293]: Creating group 'nobody' with GID 65534.
Oct 01 11:15:07 admazurkevich.localdomain systemd-sysusers[293]: Creating group 'users' with GID 100.
Oct 01 11:15:07 admazurkevich.localdomain systemd-sysusers[293]: Creating group 'systemd-journal' with GID 190.
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Finished systemd-sysusers.service - Create System Users.
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create Static De
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variables.
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Finished systemd-vconsole-setup.service - Virtual Console Setu
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: dracut-cmdline-ask.service - dracut ask for additional cmdline
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Starting dracut-cmdline.service - dracut cmdline hook...
Oct 01 11:15:07 admazurkevich.localdomain dracut-cmdline[307]: dracut-105-4.el10_0
Oct 01 11:15:07 admazurkevich.localdomain dracut-cmdline[307]: Using kernel command line parameters:    BOOT_IMAGE=(
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev.service - Create Static De
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Finished dracut-cmdline.service - dracut cmdline hook.
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Starting dracut-pre-udev.service - dracut pre-udev hook...
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Finished dracut-pre-udev.service - dracut pre-udev hook.
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Starting systemd-udevd.service - Rule-based Manager for Device
Oct 01 11:15:07 admazurkevich.localdomain systemd-udevd[408]: Using default interface naming scheme 'rhel-10.0'.
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Started systemd-udevd.service - Rule-based Manager for Device
```

Рис. 14: Журнал для UID 0

Последние строки журнала

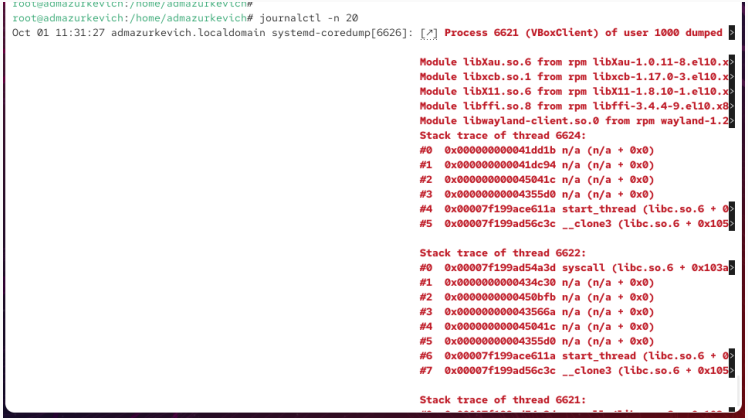

Рис. 15: Вывод последних строк журнала

Сообщения об ошибках

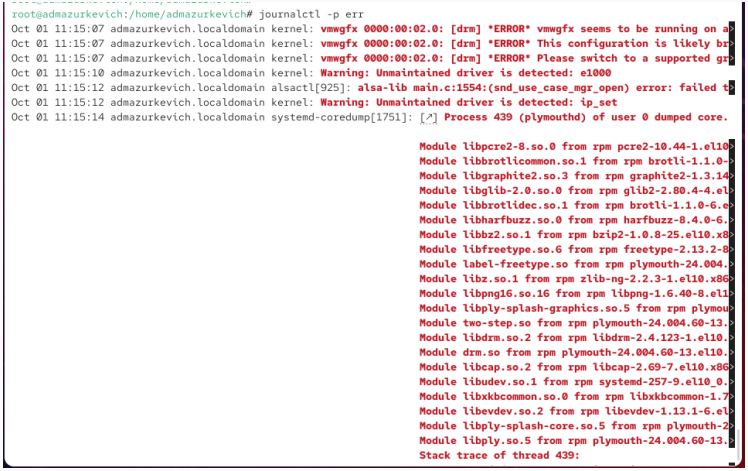

Рис. 16: Сообщения уровня ошибки

Сообщения со вчерашнего дня

```
root@admazurkevich:/home/admazurkevich#
root@admazurkevich:/home/admazurkevich# journalctl --since yesterday
Oct 01 11:15:07 admazurkevich.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-bu>
Oct 01 11:15:07 admazurkevich.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.>
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-provided physical RAM map:
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dffeffff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000dfff0000-0x00000000dfffffff] ACPI data
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: NX (Execute Disable) protection: active
Oct 01 11:15:07 admazurkevich.localdomain kernel: APIC: Static calls initialized
Oct 01 11:15:07 admazurkevich.localdomain kernel: SMBIOS 2.5 present.
Oct 01 11:15:07 admazurkevich.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 01 11:15:07 admazurkevich.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 01 11:15:07 admazurkevich.localdomain kernel: Hypervisor detected: KVM
Oct 01 11:15:07 admazurkevich.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 01 11:15:07 admazurkevich.localdomain kernel: kvm-clock: using sched offset of 4069948781 cycles
Oct 01 11:15:07 admazurkevich.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd>
Oct 01 11:15:07 admazurkevich.localdomain kernel: tsc: Detected 3187.198 MHz processor
Oct 01 11:15:07 admazurkevich.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 01 11:15:07 admazurkevich.localdomain kernel: total RAM covered: 4096M
Oct 01 11:15:07 admazurkevich.localdomain kernel: Found optimal setting for mtrr clean up
Oct 01 11:15:07 admazurkevich.localdomain kernel:  gran_size: 64K         chunk_size: 1G         num_reg: 3         >
Oct 01 11:15:07 admazurkevich.localdomain kernel: MTRR map: 6 entries (3 fixed + 3 variable; max 35), built from 16 >
Oct 01 11:15:07 admazurkevich.localdomain kernel: x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WP  UC- WT
```

Рис. 17: Сообщения со вчерашнего дня

Ошибки со вчерашнего дня

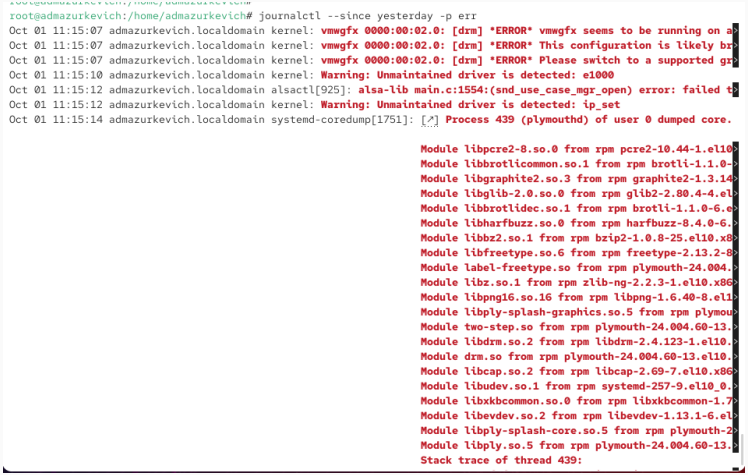

Рис. 18: Ошибки со вчерашнего дня

Детализированный вывод

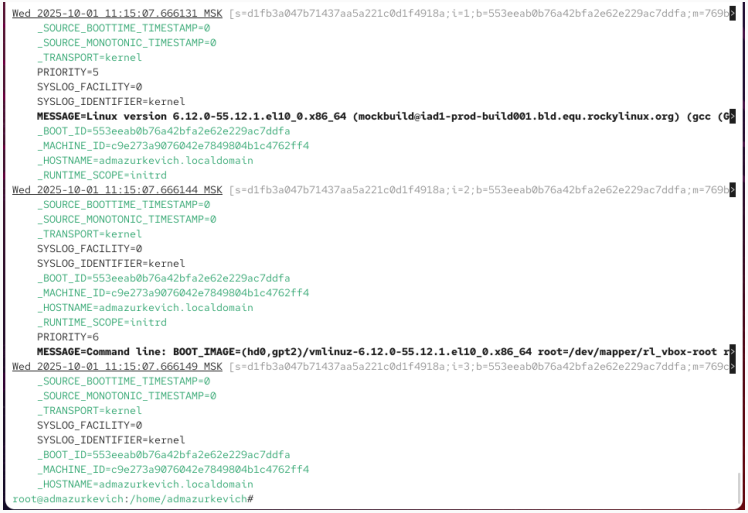

Рис. 19: Детализированный вывод журнала

Журнал работы SSHD

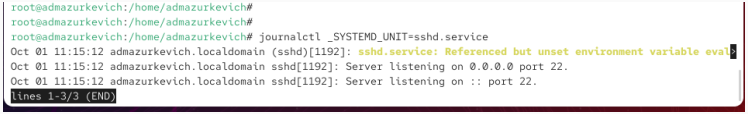

Рис. 20: Журнал работы SSHD

Постоянное хранение журналов

```
root@admazurkevich:/home/admazurkevich#
root@admazurkevich:/home/admazurkevich# mkdir -p /var/log/journal
root@admazurkevich:/home/admazurkevich# chown root:systemd-journal /var/log/journal/
root@admazurkevich:/home/admazurkevich# chmod 2755 /var/log/journal/
root@admazurkevich:/home/admazurkevich# killall -USR1 systemd-journald
root@admazurkevich:/home/admazurkevich# journalctl -b
Oct 01 11:15:07 admazurkevich.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-bu
Oct 01 11:15:07 admazurkevich.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-provided physical RAM map:
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dffeffff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000dfff0000-0x00000000dfffffff] ACPI data
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: NX (Execute Disable) protection: active
Oct 01 11:15:07 admazurkevich.localdomain kernel: APIC: Static calls initialized
Oct 01 11:15:07 admazurkevich.localdomain kernel: SMBIOS 2.5 present.
Oct 01 11:15:07 admazurkevich.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 01 11:15:07 admazurkevich.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 01 11:15:07 admazurkevich.localdomain kernel: Hypervisor detected: KVM
Oct 01 11:15:07 admazurkevich.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 01 11:15:07 admazurkevich.localdomain kernel: kvm-clock: using sched offset of 4069948781 cycles
Oct 01 11:15:07 admazurkevich.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd
Oct 01 11:15:07 admazurkevich.localdomain kernel: tsc: Detected 3187.198 MHz processor
Oct 01 11:15:07 admazurkevich.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 01 11:15:07 admazurkevich.localdomain kernel: total RAM covered: 4096M
```

Рис. 21: Перенос журналов и вывод сообщений загрузки

Выводы по проделанной работе

Вывод

В ходе лабораторной работы были освоены приёмы работы с системными журналами Linux. Была выполнена настройка перенаправления логов веб-сервера Apache в отдельные файлы, создан отладочный журнал, а также освоены фильтрация и просмотр событий через `journalctl`.

Полученные навыки позволяют эффективно контролировать работу системы и администрировать сервисы.