

Отчёт по лабораторной работе №7

Управление журналами событий в системе

Максат Хемраев

Содержание

1	Цель работы	5
2	Отчёт по выполнению работы	6
2.1	Мониторинг журнала системных событий в реальном времени . .	6
2.2	Изменение правил rsyslog.conf	8
2.3	Использование journalctl	11
2.4	Постоянный журнал journald	15
3	Контрольные вопросы	17
3.0.1	1. Какой файл используется для настройки rsyslogd?	17
3.0.2	2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?	17
3.0.3	3. Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?	17
3.0.4	4. Какую строку следует добавить в конфигурацию для записи всех сообщений с приоритетом info в файл /var/log/messages.info?	18
3.0.5	5. Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?	18
3.0.6	6. Какая команда позволяет вам видеть все сообщения журнала, которые были написаны для PID 1 между 9:00 и 15:00?	18
3.0.7	7. Какая команда позволяет вам видеть сообщения journald после последней перезагрузки системы?	18
3.0.8	8. Какая процедура позволяет сделать журнал journald постоянным?	19
4	Заключение	20

Список иллюстраций

2.1	Мониторинг системных сообщений	6
2.2	Ошибка аутентификации при su	7
2.3	Проверка журнала /var/log/secure	8
2.4	Установка и запуск Apache	8
2.5	Просмотр журнала ошибок Apache	9
2.6	Редактирование httpd.conf	9
2.7	Создание файла httpd.conf для rsyslog	10
2.8	Создание правила для отладки	10
2.9	Проверка отладочного сообщения	11
2.10	Просмотр журнала systemd	11
2.11	Фильтрация по параметрам	12
2.12	Фильтрация по UID 0	13
2.13	Последние 20 строк журнала	13
2.14	Ошибки в журнале	14
2.15	Сообщения со вчерашнего дня	14
2.16	Просмотр событий для sshd	15
2.17	Просмотр журнала текущей загрузки	16

Список таблиц

1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

2 Отчёт по выполнению работы

2.1 Мониторинг журнала системных событий в реальном времени

1. В трёх вкладках терминала были получены полномочия администратора с помощью команды `su -`.
2. Во второй вкладке терминала был запущен мониторинг системных сообщений в реальном времени.

Это позволило отслеживать любые события, которые фиксируются в файле журнала: `tail -f /var/log/messages`.

```
Sep 30 11:02:38 mhemraev packagekitd[1351]: Failed to get cache filename for cups-filesystem
Sep 30 11:02:38 mhemraev packagekitd[1351]: Failed to get cache filename for cmake-filesystem
Sep 30 11:02:38 mhemraev packagekitd[1351]: Failed to get cache filename for kernel
Sep 30 11:02:40 mhemraev su[3412]: FAILED SU (to root) mhemraev on pts/2
Sep 30 11:02:42 mhemraev kernel: traps: VBoxClient[3441] trap int3 ip:41dd1b sp:7eff4cbb4cd0 error:0 in VBoxClient[1dd1b,400000+bb000]
Sep 30 11:02:42 mhemraev systemd-coredump[3442]: Process 3438 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Sep 30 11:02:42 mhemraev systemd[1]: Started systemd-coredump@18-3442-0.service - Process Core Dump (PID 3442/UID 0).
Sep 30 11:02:42 mhemraev systemd-coredump[3443]: Process 3438 (VBoxClient) of user 1000 dumped core.#012#012Module 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#012Module 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#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 3441:
:#012#0 0x000000000041dd1b n/a (n/a + 0x0)#012#1 0x000000000041dc94 n/a (n/a + 0x0)#012#2 0x000000000045041
```

Рис. 2.1: Мониторинг системных сообщений

3. В третьей вкладке терминала была выполнена попытка перехода к суперпользователю с заведомо неверным паролем.

В результате в окне с мониторингом отобразилось сообщение об ошибке авторизации:

«FAILED SU (to root) mhemraev on pts/2».

```

a30e)#012#5 0x00007eff5b2063c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x00000000004044aa
n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Sep 30 11:03:22 mhemraev systemd[1]: systemd-coredump@26-3526-0.service: Deactivated successfully.
Sep 30 11:03:24 mhemraev mhemraev[3532]: hello

Sep 30 11:03:27 mhemraev kernel: traps: VBoxClient[3537] trap int3 ip:41ddb1b sp:7eff4cbb4cd0 error:0 in VBoxCl
ient[1ddb1b,400000+bb000]
Sep 30 11:03:27 mhemraev systemd-coredump[3538]: Process 3534 (VBoxClient) of user 1000 terminated abnormally
with signal 5/TRAP, processing...
Sep 30 11:03:27 mhemraev systemd[1]: Started systemd-coredump@27-3538-0.service - Process Core Dump (PID 3538/
UID 0).
Sep 30 11:03:27 mhemraev systemd-coredump[3539]: Process 3534 (VBoxClient) of user 1000 dumped core.#012#012Mo
dule 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#012Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Module libffi.so.8 from rpm libffi-3.4.4-9.el
10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 3537
:#012#0 0x000000000041ddb1 n/a (n/a + 0x0)#012#1 0x000000000041dc94 n/a (n/a + 0x0)#012#2 0x000000000045041

```

Рис. 2.2: Ошибка аутентификации при su

4. Затем, находясь под учётной записью обычного пользователя, была выпол-
нена команда `logger hello`.

Сообщение `hello` отобразилось в окне мониторинга и одновременно было
записано в файл `/var/log/messages`.

5. После этого мониторинг сообщений `/var/log/messages` был остановлен со-
четанием клавиш **Ctrl + C**.

Далее был выполнен анализ журнала безопасности с помощью просмотра
последних строк файла `/var/log/secure`:

`tail -n 20 /var/log/secure`.

На экране отобразились записи, связанные с неудачными попытками авто-
ризации и действиями с полномочиями суперпользователя.

```

root@mhemraev:/home/mhemraev# tail -n 20 /var/log/secure
Sep 30 11:00:20 mhemraev sshd[1152]: Server listening on 0.0.0.0 port 22.
Sep 30 11:00:20 mhemraev sshd[1152]: Server listening on :: port 22.
Sep 30 11:00:20 mhemraev (systemd)[1225]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm
(uid=0)
Sep 30 11:00:20 mhemraev gdm-launch-environment[1196]: pam_unix(gdm-launch-environment:session): session opened for
user gdm(uid=42) by (uid=0)
Sep 30 11:00:54 mhemraev unix_chkpwd[1923]: password check failed for user (mhemraev)
Sep 30 11:00:54 mhemraev gdm-password[1906]: pam_unix(gdm-password:auth): authentication failure; logname= uid=0 eu
id=0 tty=/dev/tty1 ruser= rhost= user=mhemraev
Sep 30 11:00:54 mhemraev gdm-password[1906]: gkr-pam: unable to locate daemon control file
Sep 30 11:00:54 mhemraev gdm-password[1906]: gkr-pam: stashed password to try later in open session
Sep 30 11:00:59 mhemraev gdm-password[1926]: gkr-pam: unable to locate daemon control file
Sep 30 11:00:59 mhemraev gdm-password[1926]: gkr-pam: stashed password to try later in open session
Sep 30 11:00:59 mhemraev (systemd)[1936]: pam_unix(systemd-user:session): session opened for user mhemraev(uid=1000)
by mhemraev(uid=0)
Sep 30 11:00:59 mhemraev gdm-password[1926]: pam_unix(gdm-password:session): session opened for user mhemraev(uid=1
000) by mhemraev(uid=0)
Sep 30 11:00:59 mhemraev gdm-password[1926]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Sep 30 11:01:10 mhemraev gdm-launch-environment[1196]: pam_unix(gdm-launch-environment:session): session closed for
user gdm
Sep 30 11:01:24 mhemraev (systemd)[3042]: pam_unix(systemd-user:session): session opened for user root(uid=0) by roo
t(uid=0)
Sep 30 11:01:24 mhemraev su[3011]: pam_unix(su:session): session opened for user root(uid=0) by mhemraev(uid=1000)
Sep 30 11:01:35 mhemraev su[3130]: pam_unix(su:session): session opened for user root(uid=0) by mhemraev(uid=1000)
Sep 30 11:01:45 mhemraev su[3213]: pam_unix(su:session): session opened for user root(uid=0) by mhemraev(uid=1000)
Sep 30 11:02:35 mhemraev su[3213]: pam_unix(su:session): session closed for user root
Sep 30 11:02:38 mhemraev su[3412]: pam_unix(su:auth): authentication failure; logname=mhemraev uid=1000 euid=0 tty=/
dev/pts/2 ruser=mhemraev rhost= user=root
root@mhemraev:/home/mhemraev#

```

Рис. 2.3: Проверка журнала /var/log/secure

2.2 Изменение правил rsyslog.conf

1. В первой вкладке терминала была выполнена установка веб-сервера Apache.

После завершения установки служба httpd была запущена и добавлена в автозагрузку.

```

Installed:
apr-1.7.5-2.el10.x86_64
apr-util-1.6.3-21.el10.x86_64
httpd-2.4.63-1.el10_0.2.x86_64
httpdfilesystem-2.4.63-1.el10_0.2.noarch
mod_http2-2.0.29-2.el10_0.1.x86_64
rocky-logos-httpd-100.4-7.el10.noarch

apr-util-1.6.3-21.el10.x86_64
apr-util-openssl-1.6.3-21.el10.x86_64
httpd-core-2.4.63-1.el10_0.2.x86_64
httpd-tools-2.4.63-1.el10_0.2.x86_64
mod_lua-2.4.63-1.el10_0.2.x86_64

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

```

Рис. 2.4: Установка и запуск Apache

2. Во второй вкладке терминала был просмотрен журнал ошибок веб-службы с помощью трассировки файла /var/log/httpd/error_log.

На экране отобразились сообщения о запуске и настройке httpd.


```
root@mhemraev:/home/mhemraev# tail -f /var/log/httpd/error_log
[Tue Sep 30 11:07:40.958701 2025] [suexec:notice] [pid 4327:tid 4327] AH01232: suEXEC mechanism enabled (wrapper: /u
sr/sbin/suexec)
[Tue Sep 30 11:07:41.001282 2025] [lbmethod_heartbeat:notice] [pid 4327:tid 4327] AH02282: No slotmem from mod_heart
monitor
[Tue Sep 30 11:07:41.001961 2025] [systemd:notice] [pid 4327:tid 4327] SELinux policy enabled; httpd running as cont
ext system_u:system_r:httpd_t:s0
[Tue Sep 30 11:07:41.003891 2025] [mpm_event:notice] [pid 4327:tid 4327] AH00489: Apache/2.4.63 (Rocky Linux) config
ured -- resuming normal operations
[Tue Sep 30 11:07:41.003902 2025] [core:notice] [pid 4327:tid 4327] AH00094: Command line: '/usr/sbin/httpd -D FOREG
ROUND'
```

Рис. 2.5: Просмотр журнала ошибок Apache

3. В третьей вкладке терминала был открыт конфигурационный файл `/etc/httpd/conf/httpd.conf`.

В его конец была добавлена строка `ErrorLog syslog:local1`, что перенаправило регистрацию ошибок веб-сервера через `syslog`.

```
httpd.conf [----] 22 L:[331+28 359/359] *(12027/12027b) mhemraev@m
httpd.conf

#
# 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

1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search
```

Рис. 2.6: Редактирование `httpd.conf`

4. В каталоге `/etc/rsyslog.d` был создан файл `httpd.conf`.

В нём прописано правило `local1.* -/var/log/httpd-error.log`, которое направляет все сообщения объекта **local1** в отдельный файл журнала ошибок Apache.

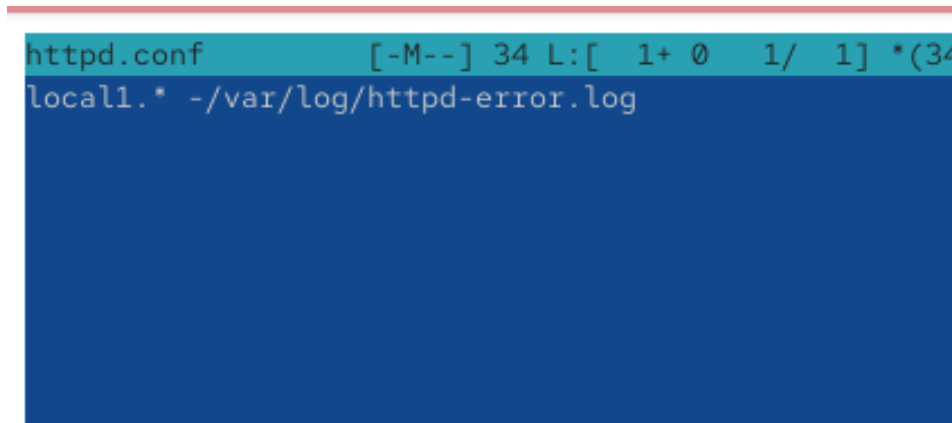


Рис. 2.7: Создание файла `httpd.conf` для `rsyslog`

5. В первой вкладке терминала были перезапущены службы **rsyslog** и **httpd** для применения новых правил.

После этого сообщения об ошибках веб-сервера стали записываться в файл `/var/log/httpd-error.log`.

6. В каталоге `/etc/rsyslog.d` был также создан файл `debug.conf`.

В нём прописано правило `*.debug /var/log/messages-debug`, что позволяет перенаправлять все отладочные сообщения в отдельный лог.

```
root@mhemraev:~# cd /etc/rsyslog.d/
root@mhemraev:/etc/rsyslog.d# touch httpd.conf
root@mhemraev:/etc/rsyslog.d# mcedit httpd.conf

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

Рис. 2.8: Создание правила для отладки

7. После перезапуска службы `rsyslog` был включён мониторинг отладочных сообщений с помощью команды `tail -f /var/log/messages-debug`.

- В третьей вкладке терминала была отправлена отладочная запись:

`logger -p daemon.debug "Daemon Debug Message".`

Сообщение успешно появилось в журнале `/var/log/messages-debug`, что подтверждает корректность настроек.

```
x103a3d)#012#1 0x000000000004344e2 n/a (n/a + 0x0)#012#2 0x000000000004b0bb n/a (n/a + 0x0)#012#3 0x0000000000041b5
59 n/a (n/a + 0x0)#012#4 0x0000000000041838a n/a (n/a + 0x0)#012#5 0x00000000000417d6a n/a (n/a + 0x0)#012#6 0x0000
0000000404860 n/a (n/a + 0x0)#012#7 0x0000000000045041c n/a (n/a + 0x0)#012#8 0x000000000004355d0 n/a (n/a + 0x0)#012
#9 0x00000eff5b27111a start_thread (libc.so.6 + 0x9511a)#012#10 0x00000eff5b2e1c3c __clone3 (libc.so.6 + 0x105c3c)#
012#012Stack trace of thread 5674:#012#0 0x00000eff5b2dfa3d syscall (libc.so.6 + 0x103a3d)#012#1 0x000000000004344e
2 n/a (n/a + 0x0)#012#2 0x00000000000450066 n/a (n/a + 0x0)#012#3 0x00000000000405123 n/a (n/a + 0x0)#012#4 0x00000
eff5b20630e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x00000eff5b2063c9 __libc_start_main@GLIBC_2.34 (li
bc.so.6 + 0x2a3c9)#012#6 0x000000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Sep 30 11:12:51 mhemraev systemd[1]: systemd-coredump@138-5678-0.service: Deactivated successfully.
Sep 30 11:12:53 mhemraev root[5684]: Daemon Debug Message
```

Рис. 2.9: Проверка отладочного сообщения

2.3 Использование journalctl

- Во второй вкладке терминала был просмотрен журнал с событиями, начи-
ная с момента последней загрузки системы.

Для перемещения использовались клавиши Enter (построчно) и пробел (постранично), выход осуществлялся клавишей q.

```
root@mhemraev:/home/mhemraev# journalctl
Sep 30 11:00:15 mhemraev.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build0
Sep 30 11:00:15 mhemraev.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_6
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-provided physical RAM map:
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x00000000000a0000-0x00000000000fffff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x00000000000100000-0x000000000007fffff] usable
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x000000000007ffff000-0x000000000007fffff] ACPI data
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000fec00fff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x000000000fee00000-0x000000000fee00fff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x000000000ffc00000-0x000000000ffc00fff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: NX (Execute Disable) protection: active
Sep 30 11:00:15 mhemraev.localdomain kernel: APIC: Static calls initialized
Sep 30 11:00:15 mhemraev.localdomain kernel: SMBIOS 2.5 present.
Sep 30 11:00:15 mhemraev.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 30 11:00:15 mhemraev.localdomain kernel: DMI: Memory slots populated: 0/0
Sep 30 11:00:15 mhemraev.localdomain kernel: Hypervisor detected: KVM
Sep 30 11:00:15 mhemraev.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Sep 30 11:00:15 mhemraev.localdomain kernel: kvm-clock: using sched offset of 4365313689 cycles
Sep 30 11:00:15 mhemraev.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4
Sep 30 11:00:15 mhemraev.localdomain kernel: tsc: Detected 3187.202 MHz processor
Sep 30 11:00:15 mhemraev.localdomain kernel: e820: update [mem 0x00000000-0x000000fff] usable ==> reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: e820: remove [mem 0x0000a0000-0x0000fffff] usable
Sep 30 11:00:15 mhemraev.localdomain kernel: last_pfn = 0x80000 max_arch_pfn = 0x400000000
Sep 30 11:00:15 mhemraev.localdomain kernel: MTRR map: 4 entries (3 fixed + 1 variable; max 35) built from 16 vari
```

Рис. 2.10: Просмотр журнала systemd

- Журнал был выведен в консоль без применения постраничного пейджера.

Это позволило отобразить все записи сплошным списком: `journalctl --no-pager`.

3. Для наблюдения за событиями в реальном времени был активирован режим: `journalctl -f`.

Прерывание вывода выполнялось комбинацией **Ctrl + C**.

4. Для изучения доступных параметров фильтрации журнала была введена команда `journalctl` и дважды нажата клавиша **Tab**, что показало список из 128 возможных атрибутов.

```
root@mhemraev:/home/mhemraev# 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=
```

Рис. 2.11: Фильтрация по параметрам

5. Далее был выполнен просмотр событий только для **UID 0** (суперпользователь).

```

root@mhemraev:/home/mhemraev# journalctl _UID=0
Sep 30 11:00:15 mhemraev.localdomain systemd-journald[261]: Collecting audit messages is disabled.
Sep 30 11:00:15 mhemraev.localdomain systemd-journald[261]: Journal started
Sep 30 11:00:15 mhemraev.localdomain systemd-journald[261]: Runtime Journal (/run/log/journal/c69c609d0a8742be8f2a1
Sep 30 11:00:15 mhemraev.localdomain systemd-modules-load[263]: Module 'msr' is built in
Sep 30 11:00:15 mhemraev.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev-early.service - Create Static
Sep 30 11:00:15 mhemraev.localdomain systemd[1]: Starting systemd-sysusers.service - Create System Users...
Sep 30 11:00:15 mhemraev.localdomain systemd-modules-load[263]: Inserted module 'fuse'
Sep 30 11:00:15 mhemraev.localdomain systemd-modules-load[263]: Module 'scsi_dh_alua' is built in
Sep 30 11:00:15 mhemraev.localdomain systemd-modules-load[263]: Module 'scsi_dh_emc' is built in
Sep 30 11:00:15 mhemraev.localdomain systemd-modules-load[263]: Module 'scsi_dh_rdac' is built in
Sep 30 11:00:15 mhemraev.localdomain systemd[1]: Finished systemd-modules-load.service - Load Kernel Modules.
Sep 30 11:00:15 mhemraev.localdomain systemd[1]: Starting systemd-sysctl.service - Apply Kernel Variables...
Sep 30 11:00:15 mhemraev.localdomain systemd-sysusers[274]: Creating group 'nobody' with GID 65534.
Sep 30 11:00:15 mhemraev.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variables.
Sep 30 11:00:15 mhemraev.localdomain systemd-sysusers[274]: Creating group 'users' with GID 100.
Sep 30 11:00:15 mhemraev.localdomain systemd-sysusers[274]: Creating group 'systemd-journal' with GID 190.
Sep 30 11:00:15 mhemraev.localdomain systemd[1]: Finished systemd-sysusers.service - Create System Users.
Sep 30 11:00:15 mhemraev.localdomain systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create Static Device
Sep 30 11:00:15 mhemraev.localdomain systemd[1]: Finished systemd-vconsole-setup.service - Virtual Console Setup.
Sep 30 11:00:15 mhemraev.localdomain systemd[1]: dracut-cmdline-ask.service - dracut ask for additional cmdline par
Sep 30 11:00:15 mhemraev.localdomain systemd[1]: Starting dracut-cmdline.service - dracut cmdline hook...
Sep 30 11:00:15 mhemraev.localdomain dracut-cmdline[286]: dracut-105-4.el10_0
Sep 30 11:00:15 mhemraev.localdomain dracut-cmdline[286]: Using kernel command line parameters: BOOT_IMAGE=(hd0
Sep 30 11:00:15 mhemraev.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev.service - Create Static Device
Sep 30 11:00:15 mhemraev.localdomain systemd[1]: Finished dracut-cmdline.service - dracut cmdline hook.

```

Рис. 2.12: Фильтрация по UID 0

6. Для отображения последних строк журнала была использована команда:
journalctl -n 20.

```

root@mhemraev:/home/mhemraev# journalctl -n 20
Sep 30 11:15:13 mhemraev.localdomain systemd-coredump[5999]: [P] Process 5994 (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-3.4.4-9.el10.x86_64
                               Module libwayland-client.so.0 from rpm wayland-1.23.0-
Stack trace of thread 5997:
#0  0x00000000041dd1b n/a (n/a + 0x0)
#1  0x00000000041dc94 n/a (n/a + 0x0)
#2  0x00000000045041c n/a (n/a + 0x0)
#3  0x0000000004355d0 n/a (n/a + 0x0)
#4  0x00007eff5b27111a start_thread (libc.so.6 + 0x951
#5  0x00007eff5b2e1c3c __clone3 (libc.so.6 + 0x105c3c)

Stack trace of thread 5994:
#0  0x00007eff5b2dfa3d syscall (libc.so.6 + 0x103a3d)
#1  0x0000000004344e2 n/a (n/a + 0x0)
#2  0x000000000450066 n/a (n/a + 0x0)
#3  0x000000000405123 n/a (n/a + 0x0)
#4  0x00007eff5b20630e __libc_start_call_main (libc.so
#5  0x00007eff5b2063c9 __libc_start_main@GLIBC_2.34 (p
#6  0x0000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x86-64
Sep 30 11:15:13 mhemraev.localdomain systemd[1]: systemd-coredump@166-5998-0.service: Deactivated successfully.

```

Рис. 2.13: Последние 20 строк журнала

7. Для просмотра исключительно сообщений об ошибках был применён
 фильтр по приоритету: **journalctl -p err.**

```

root@mhemraev:/home/mhemraev# journalctl -p err
Sep 30 11:00:16 mhemraev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an un
Sep 30 11:00:16 mhemraev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken.
Sep 30 11:00:16 mhemraev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graphi
Sep 30 11:00:18 mhemraev.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Sep 30 11:00:19 mhemraev.localdomain alsactl[887]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to im
Sep 30 11:00:20 mhemraev.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Sep 30 11:00:54 mhemraev.localdomain gdm-password[1906]: gkr-pam: unable to locate daemon control file
Sep 30 11:00:59 mhemraev.localdomain gdm-password[1926]: gkr-pam: unable to locate daemon control file
Sep 30 11:01:09 mhemraev.localdomain systemd[1936]: Failed to start app-gnome-user\x2ddirs\x2dupdate\x2dgtk-2234.sc
Sep 30 11:01:10 mhemraev.localdomain systemd-coredump[2759]: Process 2744 (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-3.4.4-9.el10.x86_64
                               Module libwayland-client.so.0 from rpm wayland-1.23.0-5
                               Stack trace of thread 2747:
                               #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 0x00000000004355d0 n/a (n/a + 0x0)
                               #5 0x00000000004355d0 n/a (n/a + 0x0)
                               Stack trace of thread 2746:
                               #0 0x00000000004355d0 n/a (n/a + 0x0)
                               #1 0x00000000004344e2 n/a (n/a + 0x0)
                               #2 0x0000000000450066 n/a (n/a + 0x0)
                               #3 0x00000000004355d0 n/a (n/a + 0x0)
                               #4 0x00000000004355d0 n/a (n/a + 0x0)
                               #5 0x00000000004355d0 n/a (n/a + 0x0)

```

Рис. 2.14: Ошибки в журнале

8. Для анализа сообщений за определённый период времени была использо-
вана опция `--since`.

Были просмотрены все события начиная со вчерашнего дня: `journalctl`
`--since yesterday`.

```

root@mhemraev:/home/mhemraev# journalctl --since yesterday
Sep 30 11:00:15 mhemraev.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iadi-prod-build0
Sep 30 11:00:15 mhemraev.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_6
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-provided physical RAM map:
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x000000000009ffff-0x00000000000fffff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x00000000000fffff-0x00000000000fffff] usable
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x00000000000fffff-0x00000000000fffff] ACPI data
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x00000000000fffff-0x00000000000fffff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x00000000000fffff-0x00000000000fffff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x00000000000fffff-0x00000000000fffff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: NX (Execute Disable) protection: active
Sep 30 11:00:15 mhemraev.localdomain kernel: APIC: Static calls initialized
Sep 30 11:00:15 mhemraev.localdomain kernel: SMBIOS 2.5 present.
Sep 30 11:00:15 mhemraev.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 30 11:00:15 mhemraev.localdomain kernel: DMI: Memory slots populated: 0/0
Sep 30 11:00:15 mhemraev.localdomain kernel: Hypervisor detected: KVM
Sep 30 11:00:15 mhemraev.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Sep 30 11:00:15 mhemraev.localdomain kernel: kvm-clock: using sched offset of 4365313689 cycles
Sep 30 11:00:15 mhemraev.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4
Sep 30 11:00:15 mhemraev.localdomain kernel: tsc: Detected 3187.202 MHz processor
Sep 30 11:00:15 mhemraev.localdomain kernel: e820: update [mem 0x00000000-0x00000000] usable ==> reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: e820: remove [mem 0x00000000-0x00000000] usable
Sep 30 11:00:15 mhemraev.localdomain kernel: last_pfn = 0x80000 max_arch_pfn = 0x400000000
Sep 30 11:00:15 mhemraev.localdomain kernel: MTRR map: 4 entries (3 fixed + 1 variable; max 35) built from 16 vari

```

Рис. 2.15: Сообщения со вчерашнего дня

9. Для получения сообщений с уровнем ошибки начиная со вчерашнего дня
использовалась команда:

```
journalctl --since yesterday -p err.
```

10. Для получения детальной информации о событиях был использован вывод в расширенном формате:

```
journalctl -o verbose.
```

11. Для изучения информации о модуле sshd были просмотрены соответствующие записи:

```
journalctl _SYSTEMD_UNIT=sshd.service.
```

```

    _SOURCE_BOOTTIME_TIMESTAMP=0
    _SOURCE_MONOTONIC_TIMESTAMP=0
    _TRANSPORT=kernel
    SYSLOG_FACILITY=0
    SYSLOG_IDENTIFIER=kernel
    _BOOT_ID=1d5ee01a6db1475ca697b01ca33b4470
    _MACHINE_ID=c69c609d0a8742be8f2a1e4538ef6441
    _HOSTNAME=mhemraev.localdomain
    _RUNTIME_SCOPE=initrd
    _PRIORITY=6
    MESSAGE=Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_64 root=/dev/mapper/rl_vbox-root
Tue 2025-09-30 11:00:15.734488 MSK [s=88cff91ce96e4368bd3be1aca512d1eb;i=2;b=1d5ee01a6db1475ca697b01ca33b4470;m=bb6
    _SOURCE_BOOTTIME_TIMESTAMP=0
    _SOURCE_MONOTONIC_TIMESTAMP=0
    _TRANSPORT=kernel
    SYSLOG_FACILITY=0
    SYSLOG_IDENTIFIER=kernel
root@mhemraev:/home/mhemraev# journalctl _SYSTEMD_UNIT=sshd.service
Sep 30 11:00:20 mhemraev.localdomain (sshd)[1152]: sshd.service: Referenced but unset environment variable evaluate
Sep 30 11:00:20 mhemraev.localdomain sshd[1152]: Server listening on 0.0.0.0 port 22.
Sep 30 11:00:20 mhemraev.localdomain sshd[1152]: Server listening on :: port 22.
root@mhemraev:/home/mhemraev#
```

Рис. 2.16: Просмотр событий для sshd

2.4 Постоянный журнал journald

1. В терминале были получены полномочия администратора.
2. Для хранения записей журнала был создан каталог /var/log/journal.
3. Были скорректированы права доступа к каталогу, чтобы служба **systemd-journald** могла записывать данные:

- назначен владелец и группа root:systemd-journal;
- установлены права доступа 2755.

4. Для применения изменений служба **systemd-journald** была уведомлена сигналом:

```
killall -USR1 systemd-journald.
```

После этого служба начала вести постоянный журнал.

5. Для проверки работы был выполнен просмотр записей текущей загрузки с помощью команды:

```
journalctl -b.
```

На экране отобразились системные сообщения, начиная с последнего запуска.

```
root@mhemraev:/home/mhemraev# journalctl -b
Sep 30 11:00:15 mhemraev.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build0
Sep 30 11:00:15 mhemraev.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_6
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-provided physical RAM map:
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000009fbff] usable
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x00000000000009fc00-0x00000000000009ffff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x0000000000000f0000-0x0000000000000fffff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x00000000000100000-0x000000000007fffff] usable
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x000000000007ffff0000-0x000000000007ffffffffff] ACPI data
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000fec00ffff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x000000000fee00000-0x000000000fee00ffff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x000000000fffc0000-0x000000000fffc0ffff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: NX (Execute Disable) protection: active
Sep 30 11:00:15 mhemraev.localdomain kernel: APIC: Static calls initialized
Sep 30 11:00:15 mhemraev.localdomain kernel: SMBIOS 2.5 present.
Sep 30 11:00:15 mhemraev.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 30 11:00:15 mhemraev.localdomain kernel: DMI: Memory slots populated: 0/0
Sep 30 11:00:15 mhemraev.localdomain kernel: Hypervisor detected: KVM
Sep 30 11:00:15 mhemraev.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Sep 30 11:00:15 mhemraev.localdomain kernel: kvm-clock: using sched offset of 4365313689 cycles
Sep 30 11:00:15 mhemraev.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4
Sep 30 11:00:15 mhemraev.localdomain kernel: tsc: Detected 3187.202 MHz processor
```

Рис. 2.17: Просмотр журнала текущей загрузки

3 Контрольные вопросы

3.0.1 1. Какой файл используется для настройки rsyslogd?

- Основной файл конфигурации: `/etc/rsyslog.conf`
 - Дополнительные файлы: каталог `/etc/rsyslog.d/`
-

3.0.2 2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?

- Сообщения об аутентификации хранятся в `/var/log/secure`
-

3.0.3 3. Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?

- По умолчанию ротация выполняется еженедельно
 - Настройки определяются в `/etc/logrotate.conf`
-

3.0.4 4. Какую строку следует добавить в конфигурацию для записи всех сообщений с приоритетом info в файл /var/log/messages.info?

- В конфигурации следует прописать правило: *.info /var/log/messages.info
-

3.0.5 5. Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?

- Для rsyslog используется команда tail -f /var/log/messages
 - Для journald — команда journalctl -f
-

3.0.6 6. Какая команда позволяет вам видеть все сообщения журнала, которые были написаны для PID 1 между 9:00 и 15:00?

- journalctl _PID=1 –since “09:00” –until “15:00”
-

3.0.7 7. Какая команда позволяет вам видеть сообщения journald после последней перезагрузки системы?

- journalctl -b
-

3.0.8 8. Какая процедура позволяет сделать журнал journald постоянным?

- Создать каталог /var/log/journal
- Назначить владельца root:systemd-journal
- Установить права доступа 2755
- Перезапустить journald сигналом USR1
- После этого записи журнала сохраняются постоянно

4 Заключение

В ходе работы были изучены основы журналирования в Linux, рассмотрены методы настройки службы rsyslog и systemd-journald, а также способы фильтрации и просмотра системных сообщений. Получены навыки создания постоянного журнала и применения правил для разделения логов по уровням важности.