

Отчёт по лабораторной работе №7

Управление журналами событий в системе

Эзиз Хатамов

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	12
2.4	Постоянный журнал journald	19
3	Контрольные вопросы	21
4	Заключение	24

Список иллюстраций

2.1	Мониторинг системных событий через <code>tail -f /var/log/messages</code> . . .	6
2.2	Ошибка при попытке получить права <code>root</code> с неверным паролем . .	7
2.3	Фиксация пользовательского сообщения в системном журнале че- рез <code>logger</code>	7
2.4	Просмотр последних строк файла <code>/var/log/secure</code>	8
2.5	Установка и запуск веб-сервера <code>Apache</code>	9
2.6	Мониторинг журнала ошибок <code>Apache</code>	9
2.7	Добавление строки <code>ErrorLog syslog:local1</code> в конфигурацию <code>Apache</code> .	10
2.8	Создание конфигурационного файла <code>httpd.conf</code> в <code>/etc/rsyslog.d</code> . . .	11
2.9	Создание файлов конфигурации <code>httpd.conf</code> и <code>debug.conf</code> , настройка вывода сообщений уровня <code>debug</code>	11
2.10	Проверка работы отладочного логирования в <code>messages-debug</code> . . .	12
2.11	Просмотр системного журнала с момента загрузки системы	13
2.12	Просмотр системного журнала	13
2.13	Просмотр системного журнала	14
2.14	Просмотр доступных параметров фильтрации <code>journalctl</code>	15
2.15	Просмотр событий для пользователя <code>root</code> (UID 0)	15
2.16	Просмотр последних строк системного журнала	16
2.17	Вывод сообщений уровня ошибок	17
2.18	Фильтрация сообщений об ошибках со вчерашнего дня	18
2.19	Просмотр подробной информации о событиях с параметром <code>verbose</code> .	18
2.20	Настройка постоянного хранения журнала <code>journald</code>	20

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 права администратора с помощью команды `su -`.

После успешного ввода пароля был осуществлён вход под пользователем `root`.

2. Во второй вкладке был запущен мониторинг системных событий в реальном времени с помощью команды `tail -f /var/log/messages`.

На экране начали отображаться текущие системные сообщения, включая информацию о работе служб и процессах пользователя.

```
root@ehatamov:/home/ehatamov# tail -f /var/log/messages
Oct 2 17:03:43 ehatamov systemd[1992]: Starting gvfs-metadata.service - Virtual filesystem metadata service...
Oct 2 17:03:43 ehatamov systemd[1992]: Started gvfs-metadata.service - Virtual filesystem metadata service.
Oct 2 17:03:44 ehatamov PackageKit[1407]: uid 1000 is trying to obtain org.freedesktop.packagekit.system-sources-refresh auth (only trusted:0)
Oct 2 17:03:44 ehatamov PackageKit[1407]: uid 1000 obtained auth for org.freedesktop.packagekit.system-sources-refresh
Oct 2 17:03:44 ehatamov systemd[1]: fprintd.service: Deactivated successfully.
Oct 2 17:03:45 ehatamov kernel: traps: VBoxClient[3408] trap int3 ip:41dd1b sp:7fdadef4fcd0 error:0 in VBoxClient[1dd1b,400000+bb000]
Oct 2 17:03:45 ehatamov systemd-coredump[3409]: Process 3405 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Oct 2 17:03:45 ehatamov systemd[1]: Started systemd-coredump@12-3409-0.service - Process Core Dump (PID 3409/UID 0).
Oct 2 17:03:45 ehatamov systemd-coredump[3410]: Process 3405 (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 3408:#012#0 0x000000000041dd1b n/a (n/a + 0x0)#012#1 0x000000000041dc94 n/a (n/a + 0x0)#012#2 0x000000000045041c n/a (n/a + 0x0)#012#3 0x00000000004355d0 n/a (n/a + 0x0)#012#4 0x00007fdaed5f211a start_thread (libc.so.6 + 0x9511a)#012#5 0x00007fdaed662c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 3405:#012#0 0x00007fdaed660a3d syscall (libc.so.6 + 0x103a3d)#012#1 0x00000000004344e2 n/a (n/a + 0x0)#012#2 0x0000000000450066 n/a (n/a + 0x0)#012#3 0x0000000000405123 n/a (n/a + 0x0)#012#4 0x00007fdaed58730e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x00007fdaed5873c9 __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
Oct 2 17:03:45 ehatamov systemd[1]: systemd-coredump@12-3409-0.service: Deactivated successfully.
Oct 2 17:03:50 ehatamov kernel: traps: VBoxClient[3430] trap int3 ip:41dd1b sp:7fdadef4fcd0 error:0 in VBoxClient[1dd1b,400000+bb000]
```

Рис. 2.1: Мониторинг системных событий через `tail -f /var/log/messages`

3. В третьей вкладке из оболочки пользователя была выполнена попытка по-

строк файла `/var/log/secure` с помощью команды `tail -n 20 /var/log/secure`.

В результате отобразились записи, подтверждающие предыдущие действия — успешные и неудачные попытки входа, а также обращения к системным службам.

```
root@ehatamov:~/home/ehatamov# tail -n 20 /var/log/secure
Sep 27 13:16:47 ehatamov su[7952]: pam_unix(su:session): session opened for user root(uid=0) by ehatamov(uid=1000)
Oct  2 17:02:32 ehatamov sshd[1196]: Server listening on 0.0.0.0 port 22.
Oct  2 17:02:32 ehatamov sshd[1196]: Server listening on :: port 22.
Oct  2 17:02:32 ehatamov (systemd)[1281]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)
Oct  2 17:02:32 ehatamov gdm-launch-environment[1262]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=42) by (uid=0)
Oct  2 17:02:38 ehatamov gdm-password[1962]: gkr-pam: unable to locate daemon control file
Oct  2 17:02:38 ehatamov gdm-password[1962]: gkr-pam: stashed password to try later in open session
Oct  2 17:02:38 ehatamov (systemd)[1992]: pam_unix(systemd-user:session): session opened for user ehatamov(uid=1000) by ehatamov(uid=0)
Oct  2 17:02:38 ehatamov gdm-password[1962]: pam_unix(gdm-password:session): session opened for user ehatamov(uid=1000) by ehatamov(uid=0)
Oct  2 17:02:38 ehatamov gdm-password[1962]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct  2 17:02:43 ehatamov gdm-launch-environment[1262]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Oct  2 17:03:15 ehatamov (systemd)[3170]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)
Oct  2 17:03:15 ehatamov su[3136]: pam_unix(su:session): session opened for user root(uid=0) by ehatamov(uid=1000)
Oct  2 17:03:23 ehatamov su[3258]: pam_unix(su:session): session opened for user root(uid=0) by ehatamov(uid=1000)
Oct  2 17:03:29 ehatamov su[3319]: pam_unix(su:session): session opened for user root(uid=0) by ehatamov(uid=1000)
Oct  2 17:05:02 ehatamov su[3319]: pam_unix(su:session): session closed for user root
Oct  2 17:05:04 ehatamov unix_chkpwd[3636]: password check failed for user (root)
Oct  2 17:05:04 ehatamov su[3627]: pam_unix(su:auth): authentication failure; logname=ehatamov uid=1000 euid=0 tty=/dev/pts/2 ruser=ehatamov rhost= user=root
Oct  2 17:05:27 ehatamov unix_chkpwd[3695]: password check failed for user (root)
Oct  2 17:05:27 ehatamov su[3683]: pam_unix(su:auth): authentication failure; logname=ehatamov uid=1000 euid=0 tty=/dev/pts/2 ruser=ehatamov rhost= user=root
root@ehatamov:~/home/ehatamov#
```

Рис. 2.4: Просмотр последних строк файла `/var/log/secure`

2.2 Изменение правил `rsyslog.conf`

1. В первой вкладке терминала был установлен веб-сервер Apache с помощью команды `dnf -y install httpd`.

После завершения установки служба была запущена и добавлена в автозагрузку при помощи команд `systemctl start httpd` и `systemctl enable httpd`. Успешное выполнение команд подтвердило корректную установку и активацию сервиса.


```

Transaction test succeeded.
Running transaction
  Preparing      :                                1/11
  Installing     : apr-1.7.5-2.el10.x86_64        1/11
  Installing     : apr-util-ldap-1.6.3-21.el10.x86_64 2/11
  Installing     : apr-util-openssl-1.6.3-21.el10.x86_64 3/11
  Installing     : apr-util-1.6.3-21.el10.x86_64    4/11
  Installing     : httpd-tools-2.4.63-1.el10_0.2.x86_64 5/11
  Installing     : rocky-logos-httpd-100.4-7.el10.noarch 6/11
Running scriptlet: httpd-filesystem-2.4.63-1.el10_0.2.noarch 7/11
  Installing     : httpd-filesystem-2.4.63-1.el10_0.2.noarch 7/11
  Installing     : httpd-core-2.4.63-1.el10_0.2.x86_64 8/11
  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-ldap-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@ehatamov:/home/ehatamov# systemctl start httpd
root@ehatamov:/home/ehatamov# systemctl enable httpd
Created symlink '/etc/systemd/system/multi-user.target.wants/httpd.service' → '/usr/lib/systemd/system/httpd.service'.
root@ehatamov:/home/ehatamov# █

```

Рис. 2.5: Установка и запуск веб-сервера Apache

- Во второй вкладке был запущен мониторинг журнала ошибок веб-службы Apache: `tail -f /var/log/httpd/error_log`.

В журнале отобразились стандартные служебные сообщения о запуске Apache и активации модулей.

```

root@ehatamov:/home/ehatamov#
root@ehatamov:/home/ehatamov# tail -f /var/log/httpd/error_log
[Thu Oct 02 17:08:30.586176 2025] [suexec:notice] [pid 4317:tid 4317] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Thu Oct 02 17:08:30.633469 2025] [lbmethod_heartbeat:notice] [pid 4317:tid 4317] AH02282: No slotmem from mod_heartbeat
[Thu Oct 02 17:08:30.634129 2025] [systemd:notice] [pid 4317:tid 4317] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Thu Oct 02 17:08:30.636475 2025] [mpm_event:notice] [pid 4317:tid 4317] AH00489: Apache/2.4.63 (Rocky Linux) configured -- resuming normal operations
[Thu Oct 02 17:08:30.636487 2025] [core:notice] [pid 4317:tid 4317] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
root@ehatamov:/home/ehatamov# █

```

Рис. 2.6: Мониторинг журнала ошибок Apache

- В третьей вкладке терминала в файле `/etc/httpd/conf/httpd.conf` была добавлена строка `ErrorLog syslog:local1`.

Это позволило перенаправить сообщения об ошибках веб-службы в системный журнал через механизм `syslog`.

```
#
# 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
```

Рис. 2.7: Добавление строки ErrorLog syslog:local1 в конфигурацию Apache

4. Для настройки приёма сообщений от Apache в каталоге /etc/rsyslog.d был создан новый файл конфигурации httpd.conf. В него была добавлена строка local1.* -/var/log/httpd-error.log, направляющая все сообщения категории local1 в отдельный лог-файл /var/log/httpd-error.log.

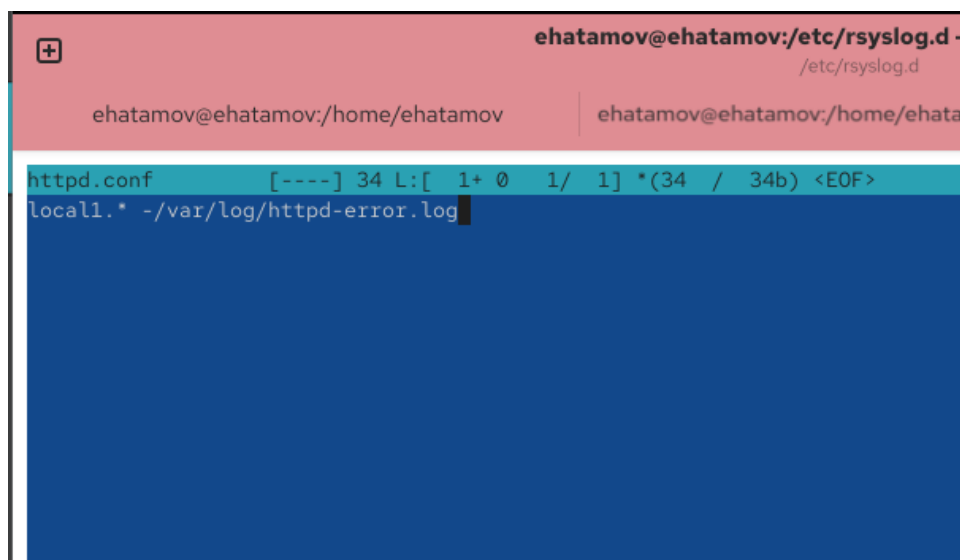


Рис. 2.8: Создание конфигурационного файла httpd.conf в /etc/rsyslog.d

5. После внесения изменений служба rsyslog была перезапущена с помощью команды `systemctl restart rsyslog.service` для применения новых настроек.

6. Далее был создан отдельный файл конфигурации `debug.conf` для мониторинга отладочной информации.

В этот файл была добавлена строка `“.debug /var/log/messages-debug”`, направляющая все сообщения уровня `debug` в файл `/var/log/messages-debug`. После редактирования службы `rsyslog` была снова перезапущена.

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

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

Рис. 2.9: Создание файлов конфигурации `httpd.conf` и `debug.conf`, настройка вывода сообщений уровня `debug`

7. Для проверки работы механизма логирования был запущен мониторинг отладочного журнала командой `tail -f /var/log/messages-debug`.

Затем было создано тестовое сообщение через команду `logger -p`

daemon.debug “Daemon debug message”.

В окне мониторинга появилось сообщение от root, подтверждающее успешную запись события в отладочный лог.

```
rocessing...
Oct  2 17:13:43 ehatamov systemd[1]: Started systemd-coredump@129-5924-0.service - Process Core Dump (PID 5924/UID 0).
Oct  2 17:13:43 ehatamov systemd-coredump[5925]: Process 5920 (VBoxClient) of user 1000 dumped core.#012#012Module libXau
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
.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 wi
3.0-2.el10.x86_64#012Stack trace of thread 5923:#012#0 0x000000000041dd1b n/a (n/a + 0x0)#012#1 0x000000000041dc94 n/a (
)#012#2 0x000000000045041c n/a (n/a + 0x0)#012#3 0x00000000004355d0 n/a (n/a + 0x0)#012#4 0x00007fdaed5f211a start_thr
so.6 + 0x9511a)#012#5 0x00007fdaed662c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 5920:#012#0 0x0000
a3d syscall (libc.so.6 + 0x103a3d)#012#1 0x00000000004344e2 n/a (n/a + 0x0)#012#2 0x0000000000450066 n/a (n/a + 0x0)#01
000000405123 n/a (n/a + 0x0)#012#4 0x00007fdaed58730e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x00007fdaed5f
bc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architectu
6-64
Oct  2 17:13:43 ehatamov systemd[1]: systemd-coredump@129-5924-0.service: Deactivated successfully.
Oct  2 17:13:46 ehatamov root[5930]: Daemon debug message
```

Рис. 2.10: Проверка работы отладочного логирования в messages-debug

2.3 Использование journalctl

1. Во второй вкладке терминала было выполнено отображение содержимого системного журнала с момента последнего запуска системы с помощью команды journalctl.

В выводе отображались записи ядра и системных служб, включая данные о конфигурации виртуальной машины, аппаратных компонентах и запуске ядра.

```

root@ehatamov:/home/ehatamov# journalctl
Oct 02 17:02:27 ehatamov.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rock
Oct 02 17:02:27 ehatamov.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_64 root=/dev/mas
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-provided physical RAM map:
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbfff] usable
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x0000000000009fc000-0x0000000000009fffff] reserved
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x000000000000f00000-0x000000000000ffffff] reserved
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x000000000001000000-0x000000000000dfffffff] usable
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x000000000dffff0000-0x000000000dffffffffff] ACPI data
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x00000000fec000000-0x00000000fec00fffff] reserved
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x00000000fee000000-0x00000000fee00fffff] reserved
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x00000000fffc00000-0x00000000ffffffffff] reserved
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x00000000100000000-0x0000000011ffffff] usable
Oct 02 17:02:27 ehatamov.localdomain kernel: NX (Execute Disable) protection: active
Oct 02 17:02:27 ehatamov.localdomain kernel: APIC: Static calls initialized
Oct 02 17:02:27 ehatamov.localdomain kernel: SMBIOS 2.5 present.
Oct 02 17:02:27 ehatamov.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 02 17:02:27 ehatamov.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 02 17:02:27 ehatamov.localdomain kernel: Hypervisor detected: KVM
Oct 02 17:02:27 ehatamov.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 02 17:02:27 ehatamov.localdomain kernel: kvm-clock: using sched offset of 4082479414 cycles
Oct 02 17:02:27 ehatamov.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle:
Oct 02 17:02:27 ehatamov.localdomain kernel: tsc: Detected 3187.196 MHz processor
Oct 02 17:02:27 ehatamov.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Oct 02 17:02:27 ehatamov.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Oct 02 17:02:27 ehatamov.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 02 17:02:27 ehatamov.localdomain kernel: total RAM covered: 4096M
Oct 02 17:02:27 ehatamov.localdomain kernel: Found optimal setting for mtrr clean up
Oct 02 17:02:27 ehatamov.localdomain kernel: gran_size: 64K chunk_size: 1G num_reg: 3 lose cover RAM: 0G
Oct 02 17:02:27 ehatamov.localdomain kernel: MTRR map: 6 entries (3 fixed + 3 variable; max 35), built from 16 variable MTRRs
Oct 02 17:02:27 ehatamov.localdomain kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
Oct 02 17:02:27 ehatamov.localdomain kernel: e820: update [mem 0x00000000-0xffffffff] usable ==> reserved
Oct 02 17:02:27 ehatamov.localdomain kernel: last_pfn = 0xc0000 max_arch_pfn = 0x400000000
Oct 02 17:02:27 ehatamov.localdomain kernel: found SMP mp-table at [mem 0x00000600-0x000006ff]

```

Рис. 2.11: Просмотр системного журнала с момента загрузки системы

- Для демонстрации сообщений без постраничного просмотра использовалась команда `journalctl -no-pager`.

В этом режиме весь вывод отображался сразу в окне терминала без ожидания действий пользователя.

```

#2 0x000000000045041c n/a (n/a + 0x0)
#3 0x00000000004355d0 n/a (n/a + 0x0)
#4 0x00007fdaed5f211a start_thread (libc.so.6 + 0x9511a)
#5 0x00007fdaed662c3c __clone3 (libc.so.6 + 0x105c3c)

Stack trace of thread 6238:
#0 0x00007fdaed660a3d syscall (libc.so.6 + 0x103a3d)
#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 0x00007fdaed5f211a start_thread (libc.so.6 + 0x9511a)
#7 0x00007fdaed662c3c __clone3 (libc.so.6 + 0x105c3c)

Stack trace of thread 6239:
#0 0x00007fdaed660a3d syscall (libc.so.6 + 0x103a3d)
#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 0x00007fdaed5f211a start_thread (libc.so.6 + 0x9511a)
#10 0x00007fdaed662c3c __clone3 (libc.so.6 + 0x105c3c)

Stack trace of thread 6237:
#0 0x00007fdaed660a3d syscall (libc.so.6 + 0x103a3d)
#1 0x00000000004344e2 n/a (n/a + 0x0)
#2 0x0000000000450066 n/a (n/a + 0x0)
#3 0x0000000000405123 n/a (n/a + 0x0)
#4 0x00007fdaed58730e __libc_start_call_main (libc.so.6 + 0x2a30e)
#5 0x00007fdaed5873c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a
3c9)

```

Рис. 2.12: Просмотр системного журнала

3. Далее был включён режим просмотра журнала в реальном времени с помощью `journalctl -f`.

Система отображала новые записи по мере их поступления. Выход из режима был выполнен сочетанием клавиш `Ctrl + C`.

```
Oct 02 17:16:07 ehatamov.localdomain systemd[1]: systemd-coredump@158-6287-0.service: Deactivated successfully.
Oct 02 17:16:12 ehatamov.localdomain kernel: traps: VBoxClient[6296] trap int3 ip:41dd1b sp:7fdadef4fcd0 error:0 in VBoxClient[1dd1b,400000+bb000]
Oct 02 17:16:12 ehatamov.localdomain systemd-coredump[6297]: Process 6293 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Oct 02 17:16:12 ehatamov.localdomain systemd[1]: Started systemd-coredump@158-6297-0.service - Process Core Dump (PID 6297/UID 0).
Oct 02 17:16:12 ehatamov.localdomain systemd-coredump[6298]: [?] Process 6293 (VBoxClient) of user 1000 dumped core.

                                ELF object binary architecture: AMD x86-64

                                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-1.23.0-2.el10.x86_64
                                Stack trace of thread 6296:
                                #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  0x00007fdaed5f211a start_thread (libc.so.6 + 0x9511a)
                                #5  0x00007fdaed662c3c __clone3 (libc.so.6 + 0x105c3c)

                                Stack trace of thread 6293:
                                #0  0x00007fdaed660a3d 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  0x00007fdaed58730e __libc_start_call_main (libc.so.6 + 0x2a30e)
                                #5  0x00007fdaed5873c9 __libc_start_main@@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)

                                #6  0x0000000004044aa n/a (n/a + 0x0)
                                ELF object binary architecture: AMD x86-64

Oct 02 17:16:12 ehatamov.localdomain systemd[1]: systemd-coredump@158-6297-0.service: Deactivated successfully.
```

Рис. 2.13: Просмотр системного журнала

4. Для изучения параметров фильтрации командой `journalctl` дважды была нажата клавиша `Tab`.

Терминал вывел список доступных фильтров, позволяющих отбирать события по различным полям — времени, пользователю, типу службы и другим параметрам.

```

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

```

Рис. 2.14: Просмотр доступных параметров фильтрации journalctl

- Для анализа событий, связанных с пользователем root, использовалась команда `journalctl _UID=0`.

В выводе отобразились записи, связанные с действиями суперпользователя и служб, запущенных от имени root.

```

root@ehatamov:/home/ehatamov# journalctl _UID=0
Oct 02 17:02:27 ehatamov.localdomain systemd-journald[282]: Collecting audit messages is disabled.
Oct 02 17:02:27 ehatamov.localdomain systemd-journald[282]: Journal started
Oct 02 17:02:27 ehatamov.localdomain systemd-journald[282]: Runtime Journal (/run/log/journal/b47de17405e044edba8d1cda0fbff070) is
Oct 02 17:02:27 ehatamov.localdomain systemd-modules-load[283]: Module 'msr' is built in
Oct 02 17:02:27 ehatamov.localdomain systemd-modules-load[283]: Inserted module 'fuse'
Oct 02 17:02:27 ehatamov.localdomain systemd-modules-load[283]: Module 'scsi_dh_alua' is built in
Oct 02 17:02:27 ehatamov.localdomain systemd-modules-load[283]: Module 'scsi_dh_emc' is built in
Oct 02 17:02:27 ehatamov.localdomain systemd-modules-load[283]: Module 'scsi_dh_rdac' is built in
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev-early.service - Create Static Device Nodes in
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Starting systemd-sysusers.service - Create System Users...
Oct 02 17:02:27 ehatamov.localdomain systemd-sysusers[298]: Creating group 'nobody' with GID 65534.
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variables.
Oct 02 17:02:27 ehatamov.localdomain systemd-sysusers[298]: Creating group 'users' with GID 100.
Oct 02 17:02:27 ehatamov.localdomain systemd-sysusers[298]: Creating group 'systemd-journal' with GID 190.
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Finished systemd-sysusers.service - Create System Users.
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create Static Device Nodes in /dev.
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Finished systemd-vconsole-setup.service - Virtual Console Setup.
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: dracut-cmdline-ask.service - dracut ask for additional cmdline parameters was ski
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Starting dracut-cmdline.service - dracut cmdline hook...
Oct 02 17:02:27 ehatamov.localdomain dracut-cmdline[308]: dracut-105-4.el10_0
Oct 02 17:02:27 ehatamov.localdomain dracut-cmdline[308]: Using kernel command line parameters: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Finished dracut-cmdline.service - dracut cmdline hook.
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Starting dracut-pre-udev.service - dracut pre-udev hook...
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Finished dracut-pre-udev.service - dracut pre-udev hook.
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Starting systemd-udev.service - Rule-based Manager for Device Events and Files...
Oct 02 17:02:27 ehatamov.localdomain systemd-udev[408]: Using default interface naming scheme 'rhel-10.0'.
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Started systemd-udev.service - Rule-based Manager for Device Events and Files.
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: dracut-pre-trigger.service - dracut pre-trigger hook was skipped because no trigg

```

Рис. 2.15: Просмотр событий для пользователя root (UID 0)

- Для вывода последних двадцати строк журнала была выполнена команда `journalctl -n 20`.

В результате были показаны свежие записи системных событий, включая ошибки и отчёты ядра.

```
root@ehatamov:/home/ehatamov# journalctl -n 20
Oct 02 17:19:51 ehatamov.localdomain kernel: traps: VBoxClient[6747] trap int3 {p:41dd1b sp:7fdadef4fcd0 error:0 in VBoxClient[1dc
Oct 02 17:19:51 ehatamov.localdomain systemd-coredump[6748]: Process 6744 (VBoxClient) of user 1000 terminated abnormally with sig
Oct 02 17:19:51 ehatamov.localdomain systemd[1]: Started systemd-coredump@201-6748-0.service - Process Core Dump (PID 6748/UID 0).
Oct 02 17:19:51 ehatamov.localdomain systemd-coredump[6749]: [?] Process 6744 (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-1.23.0-2.el10.x86_64
                                Stack trace of thread 6747:
                                #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 0x00007fdaed5f211a start_thread (libc.so.6 + 0x9511a)
                                #5 0x00007fdaed662c3c __clone3 (libc.so.6 + 0x105c3c)

                                Stack trace of thread 6744:
                                #0 0x00007fdaed660a3d syscall (libc.so.6 + 0x103a3d)
                                #1 0x00000000004344e2 n/a (n/a + 0x0)
                                #2 0x0000000000450066 n/a (n/a + 0x0)
                                #3 0x0000000000405123 n/a (n/a + 0x0)
                                #4 0x00007fdaed58730e __libc_start_call_main (libc.so.6 + 0x2a30e)
                                #5 0x00007fdaed5873c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a30e)
                                #6 0x00000000004044aa n/a (n/a + 0x0)
                                ELF object binary architecture: AMD x86-64
Oct 02 17:19:51 ehatamov.localdomain systemd[1]: systemd-coredump@201-6748-0.service: Deactivated successfully.
Oct 02 17:19:56 ehatamov.localdomain kernel: traps: VBoxClient[6770] trap int3 {p:41dd1b sp:7fdadef4fcd0 error:0 in VBoxClient[1dc
Oct 02 17:19:56 ehatamov.localdomain systemd-coredump[6771]: Process 6767 (VBoxClient) of user 1000 terminated abnormally with sig
Oct 02 17:19:56 ehatamov.localdomain systemd[1]: Started systemd-coredump@201-6771-0.service - Process Core Dump (PID 6771/UID 0).
```

Рис. 2.16: Просмотр последних строк системного журнала

7. Для отображения только сообщений об ошибках применялась команда `journalctl -p err`.

В результате вывелись сообщения уровня “error”, включая ошибки графического адаптера и сбой процессов VBoxClient.


```

root@ehatamov:/home/ehatamov# journalctl -p err
Oct 02 17:02:27 ehatamov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] "ERROR" vmwgfx seems to be running on an unsupported hyper
Oct 02 17:02:27 ehatamov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] "ERROR" This configuration is likely broken.
Oct 02 17:02:27 ehatamov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] "ERROR" Please switch to a supported graphics device to av
Oct 02 17:02:31 ehatamov.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Oct 02 17:02:32 ehatamov.localdomain alsactl[929]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import hw:0 use c
Oct 02 17:02:32 ehatamov.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Oct 02 17:02:38 ehatamov.localdomain gdm-password[1962]: gkr-pam: unable to locate daemon control file
Oct 02 17:02:43 ehatamov.localdomain systemd[1992]: Failed to start app-gnome-user\x2ddirs\x2dupdate\x2dgtk-2285.scope - Applicati
Oct 02 17:02:44 ehatamov.localdomain systemd-coredump[2818]: [?] Process 2793 (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-1.23.0-2.el10.x86_64
                                     Stack trace of thread 2802:
                                     #0 0x000000000041dd1b n/a (n/a + 0x0)
                                     #1 0x0000000000041dc94 n/a (n/a + 0x0)
                                     #2 0x0000000000045041c n/a (n/a + 0x0)
                                     #3 0x000000000004355d0 n/a (n/a + 0x0)
                                     #4 0x00007fdaed5f211a start_thread (libc.so.6 + 0x9511a)
                                     #5 0x00007fdaed662c3c __clone3 (libc.so.6 + 0x105c3c)

                                     Stack trace of thread 2793:
                                     #0 0x00007fdaed660a3d syscall (libc.so.6 + 0x103a3d)
                                     #1 0x000000000004344e2 n/a (n/a + 0x0)
                                     #2 0x00000000000450066 n/a (n/a + 0x0)
                                     #3 0x00000000000405123 n/a (n/a + 0x0)
                                     #4 0x00007fdaed58730e __libc_start_call_main (libc.so.6 + 0x2a30e)
                                     #5 0x00007fdaed5873c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)
                                     #6 0x000000000004044aa n/a (n/a + 0x0)
                                     ELF object binary architecture: AMD x86-64
Oct 02 17:02:49 ehatamov.localdomain systemd-coredump[2964]: [?] Process 2959 (VBoxClient) of user 1000 dumped core.

                                     Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64

```

Рис. 2.17: Вывод сообщений уровня ошибок

8. Для выборки сообщений за определённый период времени была использована команда `journalctl –since yesterday`.

В журнале отобразились все события, зафиксированные со вчерашнего дня.

9. Для фильтрации только ошибок за этот же период применялась команда `journalctl –since yesterday -p err`.

Отобразились сообщения, зарегистрированные со вчерашнего дня и имеющие уровень ошибки, включая сбои и предупреждения.

```

root@ehatamov:~# /home/ehatamov# journalctl --since yesterday -p err
Oct 02 17:02:27 ehatamov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] "ERROR" vmwgfx seems to be running on an unsupported hyper
Oct 02 17:02:27 ehatamov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] "ERROR" This configuration is likely broken.
Oct 02 17:02:27 ehatamov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] "ERROR" Please switch to a supported graphics device to av
Oct 02 17:02:31 ehatamov.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Oct 02 17:02:32 ehatamov.localdomain alsactl[929]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import hw0 use c
Oct 02 17:02:32 ehatamov.localdomain kernel: Warning: Unmaintained driver is detected: lp_set
Oct 02 17:02:38 ehatamov.localdomain gdm-password[1962]: gkr-pam: unable to locate daemon control file
Oct 02 17:02:43 ehatamov.localdomain systemd[1992]: Failed to start app-gnome-userx2ddirx\x2dupdate\x2dgtk-2285.scope - Applicati
Oct 02 17:02:44 ehatamov.localdomain systemd-coredump[2818]: [?] Process 2793 (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-1.23.0-2.el10.x86_64

Stack trace of thread 2802:
#0 0x000000000041ddb1 n/a (n/a + 0x0)
#1 0x0000000000041dc94 n/a (n/a + 0x0)
#2 0x0000000000045041c n/a (n/a + 0x0)
#3 0x000000000004355d0 n/a (n/a + 0x0)
#4 0x00007fdaed5f211a start_thread (libc.so.6 + 0x9511a)
#5 0x00007fdaed662c3c __clone3 (libc.so.6 + 0x105c3c)

Stack trace of thread 2793:
#0 0x00007fdaed660a3d syscall (libc.so.6 + 0x103a3d)
#1 0x000000000004344e2 n/a (n/a + 0x0)
#2 0x00000000000450066 n/a (n/a + 0x0)
#3 0x00000000000405123 n/a (n/a + 0x0)
#4 0x00007fdaed58730e __libc_start_call_main (libc.so.6 + 0x2a30e)
#5 0x00007fdaed5873c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2
#6 0x000000000004044a4 n/a (n/a + 0x0)

```

Рис. 2.18: Фильтрация сообщений об ошибках со вчерашнего дня

10. Для вывода подробной информации о событиях использовался параметр `-o verbose`, который позволяет просматривать расширенные метаданные каждой записи — идентификаторы процессов, временные метки и параметры системы.

```

    _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 ro resume=UUID=
Thu 2025-10-02 17:02:27.119572 MSK [s=62adc7143cd64534ad4588804ca2f38f;i=3;b=c71cb5a218d24eeffb5d0864fcdaa404b;m=1daa01;t=6402d6f68
    _SOURCE_MONOTONIC_TIMESTAMP=0
    _TRANSPORT=kernel
    SYSLOG_FACILITY=0
    SYSLOG_IDENTIFIER=kernel
    _BOOT_ID=c71cb5a218d24eeffb5d0864fcdaa404b
    _MACHINE_ID=b47de17405e044edba8d1cda0fbff070
    _HOSTNAME=ehatamov.localdomain
    _RUNTIME_SCOPE=initrd
    PRIORITY=6
    MESSAGE=BIOS-provided physical RAM map:
Thu 2025-10-02 17:02:27.119575 MSK [s=62adc7143cd64534ad4588804ca2f38f;i=4;b=c71cb5a218d24eeffb5d0864fcdaa404b;m=1daa05;t=6402d6f68
    _SOURCE_BOOTTIME_TIMESTAMP=0
    root@ehatamov:/home/ehatamov# journalctl -s systemd_unit=sshd.service
Oct 02 17:02:32 ehatamov.localdomain (sshd)[1196]: sshd.service: Referenced but unset environment variable evaluates to an empty s
Oct 02 17:02:32 ehatamov.localdomain sshd[1196]: Server listening on 0.0.0.0 port 22.
Oct 02 17:02:32 ehatamov.localdomain sshd[1196]: Server listening on :: port 22.
lines 1-3/3 (END)

```

Рис. 2.19: Просмотр подробной информации о событиях с параметром verbose

11. Для анализа работы службы sshd была выполнена команда journalctl -u sshd.service.

В результате отображались записи, связанные с запуском и работой SSH-сервера, включая сообщения о прослушивании порта 22.

2.4 Постоянный журнал journald

1. В терминале были получены права администратора для выполнения системных операций.
2. Был создан каталог для хранения постоянного журнала systemd:
`/var/log/journal`
Этот каталог используется для записи системных событий на диск, обеспечивая их сохранение даже после перезагрузки системы.
3. Для корректной работы службы journald были изменены права доступа к каталогу:
владельцем назначен root, а группой — systemd-journal.
Также были установлены права 2755, что разрешает доступ на чтение и запись процессам, связанным с journald.
4. Для применения изменений была отправлена команда `killall -USR1 systemd-journald`, сигнализирующая службе journald о необходимости обновления конфигурации без полной перезагрузки системы.
5. После выполнения настроек журнал systemd стал постоянным.
Для проверки отображения сообщений с момента последней перезагрузки использовалась команда `journalctl -b`.
В выводе отобразились системные записи ядра, параметры запуска и аппаратная информация.

```

root@ehatamov:/home/ehatamov# mkdir -p /var/log/journal
root@ehatamov:/home/ehatamov# chown root:systemd-journal /var/log/journal/
root@ehatamov:/home/ehatamov# chmod 2755 /var/log/journal/
root@ehatamov:/home/ehatamov# killall -USR1 systemd-journald
root@ehatamov:/home/ehatamov# journalctl -b
Oct 02 17:02:27 ehatamov.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rock)
Oct 02 17:02:27 ehatamov.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_64 root=/dev/mas
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-provided physical RAM map:
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] usable
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x000000000dffff0000-0x000000000dffffffffff] ACPI data
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x000000000fec000000-0x000000000fec00ffff] reserved
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x000000000fee000000-0x000000000fee00ffff] reserved
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x000000000fffc00000-0x000000000fffffffff] reserved
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x000000001000000000-0x0000000011ffffffff] usable
Oct 02 17:02:27 ehatamov.localdomain kernel: NX (Execute Disable) protection: active
Oct 02 17:02:27 ehatamov.localdomain kernel: APIC: Static calls initialized
Oct 02 17:02:27 ehatamov.localdomain kernel: SMBIOS 2.5 present.
Oct 02 17:02:27 ehatamov.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 02 17:02:27 ehatamov.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 02 17:02:27 ehatamov.localdomain kernel: Hypervisor detected: KVM
Oct 02 17:02:27 ehatamov.localdomain kernel: kvm-clock: Using msrc 4b564d01 and 4b564d00
Oct 02 17:02:27 ehatamov.localdomain kernel: kvm-clock: using sched offset of 4082479414 cycles
Oct 02 17:02:27 ehatamov.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_
Oct 02 17:02:27 ehatamov.localdomain kernel: tsc: Detected 3187.196 MHz processor
Oct 02 17:02:27 ehatamov.localdomain kernel: e820: update [mem 0x00000000-0x000000ffff] usable ==> reserved
Oct 02 17:02:27 ehatamov.localdomain kernel: e820: remove [mem 0x000a0000-0x0000ffff] usable
Oct 02 17:02:27 ehatamov.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 02 17:02:27 ehatamov.localdomain kernel: total RAM covered: 4096M
Oct 02 17:02:27 ehatamov.localdomain kernel: Found optimal setting for mtrr clean up
Oct 02 17:02:27 ehatamov.localdomain kernel: gran_size: 64K chunk_size: 1G num_reg: 3 lose cover RAM: 0G

```

Рис. 2.20: Настройка постоянного хранения журнала journald

3 Контрольные вопросы

1. Какой файл используется для настройки rsyslogd?

- Основной конфигурационный файл — `/etc/rsyslog.conf`.
- Дополнительные правила могут храниться в отдельных файлах в каталоге `/etc/rsyslog.d/`.

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

- Сообщения, связанные с аутентификацией, хранятся в файле `/var/log/secure`.

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

- По умолчанию ротация логов выполняется **еженедельно (weekly)**, а старые файлы обычно сохраняются до **4 недель**.
- Эти параметры задаются в файле `/etc/logrotate.conf`.

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

- Необходимо добавить строку:

`*.info /var/log/messages.info`

- Это правило направляет все сообщения уровня **info** и выше в отдельный лог-файл.

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

- Для просмотра сообщений в реальном времени используется команда:

```
journalctl -f
```

- Аналог команды `tail -f` для системного журнала.

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

- Для выборки сообщений по идентификатору процесса и времени используется команда:

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

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

- Для вывода сообщений, относящихся к текущему сеансу загрузки, используется команда:

```
journalctl -b
```

8. Какая процедура позволяет сделать журнал `journald` постоянным?

- Чтобы сделать журнал `systemd` постоянным, необходимо:

1. Создать каталог `/var/log/journal`.

2. Установить права доступа:

```
chown root:systemd-journal /var/log/journal
```

```
chmod 2755 /var/log/journal
```

3. Применить изменения без перезагрузки:

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

После этого логи `journald` будут сохраняться на диск и не теряться после перезагрузки.

4 Заключение

В ходе выполнения работы были изучены принципы функционирования системных журналов в Linux, а также механизмы их ведения и анализа с помощью служб **rsyslog** и **systemd-journald**.

Были рассмотрены способы настройки файлов конфигурации, перенаправления сообщений по уровням приоритета, создания собственных логов для приложений и организации постоянного хранения записей.

Кроме того, была освоена работа с утилитой **journalctl**, включая применение фильтров, просмотр сообщений в реальном времени и анализ событий по конкретным параметрам.