

Отчёт по лабораторной работе №7

Управление журналами событий в системе

Анастасия Мазуркевич

Содержание

1	Цель работы	5
2	Ход выполнения	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	Создание каталога для хранения журналов	16
3	Контрольные вопросы	18
4	Заключение	20

Список иллюстраций

2.1	Мониторинг системных сообщений	6
2.2	Сообщение об ошибке аутентификации	7
2.3	Сообщение logger hello в журнале	7
2.4	Фрагмент журнала secure	8
2.5	Установка и запуск Apache	8
2.6	Журнал ошибок Apache	9
2.7	Добавление правила ErrorLog в httpd.conf	9
2.8	Создание правила для логов Apache в rsyslog	10
2.9	Создание конфигурации debug.conf	10
2.10	Сообщение отладки в журнале	11
2.11	Просмотр системного журнала	11
2.12	Просмотр системного журнала	12
2.13	Режим просмотра журнала в реальном времени	12
2.14	Фильтрация журнала по параметрам	13
2.15	Журнал для UID 0	13
2.16	Вывод последних строк журнала	14
2.17	Сообщения уровня ошибки	14
2.18	Сообщения со вчерашнего дня	15
2.19	Ошибки со вчерашнего дня	15
2.20	Детализированный вывод журнала	16
2.21	Журнал работы SSHD	16
2.22	Перенос журналов и вывод сообщений загрузки	17

Список таблиц

1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

2 Ход выполнения

2.1 Мониторинг журнала системных событий в реальном времени

Для начала в трёх вкладках терминала были получены полномочия администратора с помощью команды **su -**.

Во второй вкладке был запущен мониторинг системных событий в реальном времени: **tail -f /var/log/messages**.

В логе фиксировались события, связанные с работой сервисов, ядра и пользователями. В частности, при работе виртуальной машины VirtualBox неоднократно появлялись ошибки клиента **VBoxClient**, сопровождаемые дампами памяти.

```
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:41ddb sp:7f198c635cd0 error:0 in VBoxClient[400000+bb000]
Oct 1 11:17:39 admazurkevich systemd-coredump[3593]: Process 3589 (VBoxClient) of user 1000 terminated abnormally with 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/UID 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#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 3592:#012#0 0x00000000000041dd n/a (n/a + 0x0)#012#1 0x00000000000041dc n/a (n/a + 0x0)#012#2 0x0000000000004504 n/a (n/a + 0x0)#012#3 0x0000000000004355 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 + 0x103a3d)#012#1 0x0000000000004344 n/a (n/a + 0x0)#012#2 0x0000000000004506 n/a (n/a + 0x0)#012#3 0x0000000000004051 n/a (n/a + 0x0)#012#4 0x00007f199ac7b30e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x00007f199ac7b3c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x0000000000004044 n/a (n/a + 0x0)#012ELF object binary architecture: 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:41ddb sp:7f198c635cd0 error:0 in VBoxClient[400000+bb000]
Oct 1 11:17:45 admazurkevich systemd-coredump[3621]: Process 3617 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Oct 1 11:17:45 admazurkevich systemd[1]: Started systemd-coredump@29-3621-0.service - Process Core Dump (PID 3621/UID 0).
Oct 1 11:17:45 admazurkevich systemd-coredump[3622]: Process 3617 (VBoxClient) of user 1000 dumped core.#012#012Modu
```

Рис. 2.1: Мониторинг системных сообщений

В третьей вкладке, после возврата к своей учётной записи, была предпринята попытка получить права администратора через **su**, но пароль был введён неверно.

Во второй вкладке с мониторингом это зафиксировалось сообщением: **FAILED SU (to root) admazurkevich on pts/2**.

А также сопровождалось формированием дампа памяти для завершившегося процесса.

```
Oct 1 11:18:25 admazurkevich systemd-coredump[3721]: Process 3717 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Oct 1 11:18:25 admazurkevich systemd[1]: Started systemd-coredump@37-3721-0.service - Process Core Dump (PID 3721/UID 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#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 3720:#012#0 0x00000000000041dd n/a (n/a + 0x0)#012#1 0x00000000000041dc n/a (n/a + 0x0)#012#2 0x0000000000004504 n/a (n/a + 0x0)#012#3 0x000000000000435d n/a (n/a + 0x0)#012#4 0x00007f199ace611a start_thread (libc.so.6 + 0x9511a)#012#5 0x00007f199ad56c3c
```

Рис. 2.2: Сообщение об ошибке аутентификации

Под учётной записью пользователя была выполнена команда **logger hello**.

Событие сразу же появилось в окне мониторинга и было записано в файл **/var/log/messages**.

Таким образом, через logger можно добавлять произвольные заметки в системные логи.

```
)#012#5 0x00007f199ac7b3c9 __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 1 11:18:56 admazurkevich systemd[1]: systemd-coredump@43-3786-0.service: Deactivated successfully.
Oct 1 11:18:59 admazurkevich admazurkevich[3792]: hello
Oct 1 11:18:59 admazurkevich admazurkevich[3794]: hello
Oct 1 11:19:00 admazurkevich admazurkevich[3796]: hello
Oct 1 11:19:01 admazurkevich kernel: traps: VBoxClient[3801] trap int3 ip:41ddb sp:7f198c635cd0 error:0 in VBoxClient[4000000000000000]
Oct 1 11:19:01 admazurkevich systemd-coredump[3802]: Process 3798 (VBoxClient) of user 1000 terminated abnormally with
```

Рис. 2.3: Сообщение logger hello в журнале

После остановки мониторинга (**Ctrl + C**) был просмотрен файл с сообщениями безопасности — вывод последних 20 строк: **tail -n 20 /var/log/secure**.

В журнале зафиксированы успешные и неуспешные попытки входа в систему, а также ошибки авторизации при вводе неправильного пароля для root. Здесь отразились все действия, связанные с командами **su** и проверками пароля.

```

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. 2.4: Фрагмент журнала secure

2.2 Изменение правил rsyslog.conf

В первой вкладке терминала была выполнена установка пакета Apache:

dnf -y install httpd

После завершения процесса веб-служба была запущена и добавлена в автоза-
грузку:

- **systemctl start httpd**
- **systemctl enable httpd**

```

Installed:
apr-1.7.5-2.el10.x86_64                                apr-util-1.6.3-21.el10.x86_64
apr-util-ldb-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
httpdfilesystem-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@admazurkevich:/home/admazurkevich# systemctl start httpd
root@admazurkevich:/home/admazurkevich# systemctl enable httpd
Created symlink '/etc/systemd/system/multi-user.target.wants/httpd.service' → '/usr/lib/systemd/system/httpd.service'.
root@admazurkevich:/home/admazurkevich#

```

Рис. 2.5: Установка и запуск Apache

Во второй вкладке терминала был запущен просмотр сообщений об ошибках веб-сервера в реальном времени:

tail -f /var/log/httpd/error_log

Здесь фиксировались события запуска Apache, активация SELinux-политики и переход службы в рабочий режим.

```
root@admazurkevich:/home/admazurkevich#  
root@admazurkevich:/home/admazurkevich# tail -f /var/log/httpd/error_log  
[Wed Oct 01 11:21:44.012487 2025] [suexec:notice] [pid 4402:tid 4402] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)  
[Wed Oct 01 11:21:44.046861 2025] [lbmethod_heartbeat:notice] [pid 4402:tid 4402] AH02282: No slotmem from mod_heartmonitor  
[Wed Oct 01 11:21:44.047560 2025] [systemd:notice] [pid 4402:tid 4402] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0  
[Wed Oct 01 11:21:44.049413 2025] [mpm_event:notice] [pid 4402:tid 4402] AH00489: Apache/2.4.63 (Rocky Linux) configured -- resuming normal operations  
[Wed Oct 01 11:21:44.049427 2025] [core:notice] [pid 4402:tid 4402] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 2.6: Журнал ошибок Apache

В конфигурационный файл **/etc/httpd/conf/httpd.conf** была добавлена строка:

ErrorLog syslog:local1

Это позволило отправлять ошибки Apache в системный журнал через объект **local1**.

```
#  
# 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 правила ErrorLog в httpd.conf

В каталоге **/etc/rsyslog.d** был создан файл **httpd.conf**, в который добавлено правило:

local1.* -/var/log/httpd-error.log

Таким образом, все сообщения от Apache через **local1** стали фиксироваться в отдельном файле **/var/log/httpd-error.log**.

```
httpd.conf [----] 34 L:[ 1+ 0 1/ 1] *(34 / 34b)
local1.* -/var/log/httpd-error.log
```

Рис. 2.8: Создание правила для логов Apache в rsyslog

После этого были перезапущены службы:

- **systemctl restart rsyslog.service**
- **systemctl restart httpd**

В том же каталоге **/etc/rsyslog.d** был создан новый файл **debug.conf**, куда добавлено правило:

***.debug /var/log/messages-debug**

Таким образом, все отладочные сообщения перенаправляются в отдельный лог-файл.

```
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. 2.9: Создание конфигурации debug.conf

Во второй вкладке был запущен мониторинг файла **/var/log/messages-debug** командой:

tail -f /var/log/messages-debug

Затем в третьей вкладке было выполнено:

logger -p daemon.debug "Daemon Debug Message"

В мониторинге появилось сообщение отладки, что подтвердило успешную настройку.

```
Oct 1 11:27:36 admazurkevich systemd-coredump[6076]: Process 6071 (VBoxClient) of user 1000 dumped core.#012#012Module
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 6074:#012#0 0x00000000000041
dd1b n/a (n/a + 0x0)#012#1 0x00000000000041dc94 n/a (n/a + 0x0)#012#2 0x00000000000045041c 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
__clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 6071:#012#0 0x00007f199ad54a3d syscall (libc.so.6 + 0x1
03a3d)#012#1 0x0000000000004344e2 n/a (n/a + 0x0)#012#2 0x000000000000450066 n/a (n/a + 0x0)#012#3 0x000000000000405123
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 0x0000000000004044aa n/a (n/a + 0x0)#012ELF object binary archit
ecture: AMD x86-64
Oct 1 11:27:36 admazurkevich systemd[1]: systemd-coredump@145-6075-0.service: Deactivated successfully.
Oct 1 11:27:37 admazurkevich root[6081]: Daemon Debug Message
```

Рис. 2.10: Сообщение отладки в журнале

2.3 Использование journalctl

Для просмотра журнала с момента загрузки системы была использована ко-
манда:

journalctl

Отображаются все события ядра и сервисов, начиная с инициализации оборудо-
вания и запуска служб.

```
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:siad1-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 0x0000000000000000-0x0000000000009fbfff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000009fc000-0x0000000000009fffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000009f0000-0x0000000000009fffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x00000000000000000-0x000000000000dfffff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x000000000000dffff000-0x000000000000dfffff] 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 0x00000000fffc0000-0x00000000fffc0fff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000010000000-0x0000000010000fff] 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 4009948781 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 0x00000000-0x000000ffff] usable ==> reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: e820: remove [mem 0x000000000-0x000000ffff] 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. 2.11: Просмотр системного журнала

Чтобы вывести содержимое журнала без использования постраничного про-
смотора, была выполнена команда:

journalctl -no-pager

```
Oct 01 11:17:09 admazurkevich.localdomain systemd-coredump[3247]: Process 3243 (VBoxClient) of user 1000 terminated a
bnormally with signal 5/TRAP, processing...
Oct 01 11:17:09 admazurkevich.localdomain systemd[1]: Started systemd-coredump@22-3247-0.service - Process Core Dump
(PID 3247/UID 0).
Oct 01 11:17:09 admazurkevich.localdomain systemd-coredump[3248]: [P] Process 3243 (VBoxClient) of user 1000 dumped c
ore.

6_64 Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x8
6_64 Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x8
6_64 Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x8
_64 Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86
.0-2.el10.x86_64 Module libwayland-client.so.0 from rpm wayland-1.23

Stack trace of thread 3246:
#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 0x00007f199ace611a start_thread (libc.so.6 + 0x
9511a)
3c) #5 0x00007f199ad56c3c __clone3 (libc.so.6 + 0x105c
d) Stack trace of thread 3244:
#0 0x00007f199ad54a3d syscall (libc.so.6 + 0x103a3
#1 0x000000000434c30 n/a (n/a + 0x0)
#2 0x000000000450bfb n/a (n/a + 0x0)
#3 0x00000000043566a n/a (n/a + 0x0)
#4 0x00000000045041c n/a (n/a + 0x0)
```

Рис. 2.12: Просмотр системного журнала

Для анализа новых сообщений в режиме онлайн применялась команда:

journalctl -f

Мониторинг можно прервать сочетанием клавиш **Ctrl + C**.

```
6_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 6393:
#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 0x00007f199ace611a start_thread (libc.so.6 + 0x
9511a)
3c) #5 0x00007f199ad56c3c __clone3 (libc.so.6 + 0x105c
d) Stack trace of thread 6390:
#0 0x00007f199ad54a3d syscall (libc.so.6 + 0x103a3
#1 0x0000000004344e2 n/a (n/a + 0x0)
#2 0x000000000450066 n/a (n/a + 0x0)
#3 0x000000000405123 n/a (n/a + 0x0)
#4 0x00007f199ac7b30e __libc_start_call_main (libc
.so.6 + 0x2a30e)
#5 0x00007f199ac7b3c9 __libc_start_main@@GLIBC_2.3
4 (libc.so.6 + 0x2a3c9)
#6 0x0000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x86-64
Oct 01 11:29:44 admazurkevich.localdomain systemd[1]: systemd-coredump@170-6394-0.service: Deactivated successfully.
```

Рис. 2.13: Режим просмотра журнала в реальном времени

После ввода команды **journalctl** и двойного нажатия клавиши **Tab** отобразился список доступных параметров фильтрации: по UID, PID, системным полям и сервисам.

```

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=
_CMD=                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_CMD=        GLIB_DOMAIN=          SYSLOG_IDENTIFIER=
COREDUMP_COMM=       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. 2.14: Фильтрация журнала по параметрам

Для вывода записей, связанных с пользователем root, была применена команда:

```
**journalctl _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/c9e273a9076042e78b
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_rdc' 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 Setup
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: dracut-cmdline-ask.service - dracut ask for additional cmdlines
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-udevdev.service - Rule-based Manager for Device
Oct 01 11:15:07 admazurkevich.localdomain systemd-udevdev[408]: Using default interface naming scheme 'rhel-10.0'.
Oct 01 11:15:07 admazurkevich.localdomain systemd[1]: Started systemd-udevdev.service - Rule-based Manager for Device

```

Рис. 2.15: Журнал для UID 0

Команда **journalctl -n 20** вывела последние 20 строк системного журнала.


```

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 0x0000000001000000-0x0000000000dfffff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x000000000dffff0000-0x000000000dfffff] ACPI data
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x000000000fec000000-0x000000000fec00ffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x000000000fee000000-0x000000000fee00ffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x000000000ffc000000-0x000000000ffc00ffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x000000001000000000-0x0000000011fffff] 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: 0xffffffffffffff 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 0x000000000-0x000000fff] usable ==> reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: e820: remove [mem 0x000a00000-0x0000ffff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: last_pfn = 0x1200000 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. 2.18: Сообщения со вчерашнего дня

Для просмотра только ошибок со вчерашнего дня использовалась команда:

journalctl –since yesterday -p err

```

root@admazurkevich:/home/admazurkevich# journalctl --since yesterday -p err
Oct 01 11:15:07 admazurkevich.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on a
Oct 01 11:15:07 admazurkevich.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely br
Oct 01 11:15:07 admazurkevich.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported gr
Oct 01 11:15:10 admazurkevich.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Oct 01 11:15:12 admazurkevich.localdomain alsactl[925]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to
Oct 01 11:15:12 admazurkevich.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Oct 01 11:15:14 admazurkevich.localdomain systemd-coredump[1751]: [?] Process 439 (plymouthd) of user 0 dumped core.

                               Module libcpre2-8.so.0 from rpm pcre2-10.44-1.el10
                               Module libbrotlicommon.so.1 from rpm brotli-1.1.0-5
                               Module libgraphite2.so.3 from rpm graphite2-1.3.14
                               Module libglib-2.0.so.0 from rpm glib2-2.80.4-4.el10
                               Module libbrotlidedc.so.1 from rpm brotli-1.1.0-6.el10
                               Module libharfbuzz.so.0 from rpm harfbuzz-8.4.0-6.el10
                               Module libbz2.so.1 from rpm bzip2-1.0.8-25.el10.x86_64
                               Module libfreetype.so.6 from rpm freetype-2.13.2-8.el10
                               Module label-freetype.so from rpm plymouth-24.004.60-13
                               Module libz.so.1 from rpm zlib-ng-2.2.3-1.el10.x86_64
                               Module libpng16.so.16 from rpm libpng-1.6.40-8.el10
                               Module libply-splash-graphics.so.5 from rpm plymouth-24.004.60-13
                               Module two-step.so from rpm plymouth-24.004.60-13
                               Module libdrm.so.2 from rpm libdrm-2.4.123-1.el10
                               Module drwm.so from rpm plymouth-24.004.60-13.el10
                               Module libcap.so.2 from rpm libcap-2.69-7.el10.x86_64
                               Module libudev.so.1 from rpm systemd-257-9.el10_0
                               Module libxkbcommon.so.0 from rpm libxkbcommon-1.7.0
                               Module libevdev.so.2 from rpm libevdev-1.13.1-6.el10
                               Module libply-splash-core.so.5 from rpm plymouth-24.004.60-13
                               Module libply.so.5 from rpm plymouth-24.004.60-13
                               Stack trace of thread 439:

```

Рис. 2.19: Ошибки со вчерашнего дня

Для получения расширенной информации по каждому событию была использована команда:

journalctl -o verbose

В выводе указываются дополнительные параметры: идентификатор загрузки, имя хоста, приоритет события, источник и другие метаданные.


```
Wed 2025-10-01 11:15:07.666131 MSK [s=d1fb3a047b71437aa5a221c0d1f4918a;i=1;b=553eeab0b76a42bfa2e62e229ac7ddfa;m=769b8]
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
PRIORITY=5
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
MESSAGE=Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (6
_BOOT_ID=553eeab0b76a42bfa2e62e229ac7ddfa
_MACHINE_ID=c9e273a9076042e7849804b1c4762ff4
_HOSTNAME=admazurkevich.localdomain
_RUNTIME_SCOPE=initrd
Wed 2025-10-01 11:15:07.666144 MSK [s=d1fb3a047b71437aa5a221c0d1f4918a;i=2;b=553eeab0b76a42bfa2e62e229ac7ddfa;m=769b8]
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=553eeab0b76a42bfa2e62e229ac7ddfa
_MACHINE_ID=c9e273a9076042e7849804b1c4762ff4
_HOSTNAME=admazurkevich.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/r1_vbox-root x
Wed 2025-10-01 11:15:07.666149 MSK [s=d1fb3a047b71437aa5a221c0d1f4918a;i=3;b=553eeab0b76a42bfa2e62e229ac7ddfa;m=769b8]
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=553eeab0b76a42bfa2e62e229ac7ddfa
_MACHINE_ID=c9e273a9076042e7849804b1c4762ff4
_HOSTNAME=admazurkevich.localdomain
root@admazurkevich:/home/admazurkevich#
```

Рис. 2.20: Детализированный вывод журнала

Для анализа работы службы **sshd** была использована команда:

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

В выводе отобразились события, связанные с запуском и работой SSH-сервера: сообщения об окружении и прослушивание порта 22 (как IPv4, так и IPv6).

```
root@admazurkevich:/home/admazurkevich#
root@admazurkevich:/home/admazurkevich#
root@admazurkevich:/home/admazurkevich# journalctl _SYSTEMD_UNIT=sshd.service
Oct 01 11:15:12 admazurkevich.localdomain (sshd)[1192]: sshd.service: Referenced but unset environment variable enva
Oct 01 11:15:12 admazurkevich.localdomain sshd[1192]: Server listening on 0.0.0.0 port 22.
Oct 01 11:15:12 admazurkevich.localdomain sshd[1192]: Server listening on :: port 22.
lines 1-3/3 (END)
```

Рис. 2.21: Журнал работы SSHD

2.4 Создание каталога для хранения журналов

Для организации хранения журналов был создан каталог **/var/log/journal**, в который затем перенаправлены данные systemd-journald.

Выполненные действия:

- создание каталога: **mkdir -p /var/log/journal**
- назначение прав доступа: **chmod 2755 /var/log/journal**
- перезапуск службы systemd-journald сигналом: **killall -USR1 systemd-journald**

После этого команда **journalctl -b** показала системные сообщения с момента последней загрузки ядра.

```
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 775 /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:siad1-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 0x000000000009f000-0x000000000000ffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] usable
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000dfff0000-0x0000000000dfffff] ACPI data
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000fee00000-0x0000000000fec00fff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000fee00000-0x0000000000fee00fff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x0000000000ffc00000-0x0000000000ffffff] reserved
Oct 01 11:15:07 admazurkevich.localdomain kernel: BIOS-e820: [mem 0x000000001000000000-0x0000000010ffffff] 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 msrc 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 0x0000a0000-0x0000ffff] 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. 2.22: Перенос журналов и вывод сообщений загрузки

3 Контрольные вопросы

1. Какой файл используется для настройки rsyslogd?

Основной конфигурационный файл — `/etc/rsyslog.conf`.

Дополнительно правила могут храниться в каталоге `/etc/rsyslog.d/`.

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

Сообщения об аутентификации фиксируются в файле `/var/log/secure`.

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

По умолчанию ротация выполняется раз в неделю с использованием утилиты `logrotate`.

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

Необходимо добавить правило: `*.info /var/log/messages.info`

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

Для этого используется команда:

```
journalctl -f
```

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"
```

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

```
journalctl -b
```

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

Необходимо создать каталог для хранения журналов и назначить ему права:

```
- mkdir -p /var/log/journal
```

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

```
- перезапустить службу: systemctl restart systemd-journald
```

После этого журнал будет сохраняться в постоянном виде даже после перезагрузки системы.

4 Заключение

В ходе лабораторной работы были изучены основы управления системными журналами в Linux с использованием **rsyslog** и **systemd-journald**.

Была проведена настройка перенаправления сообщений веб-сервера Apache в отдельные файлы, реализовано хранение отладочной информации, а также рассмотрены способы фильтрации и просмотра логов через `journalctl`.