

Отчёт по лабораторной работе №7

Управление журналами событий в системе

Щемелев Илья Владимирович

Содержание

1	Цель работы	5
2	Ход выполнения	6
2.1	Мониторинг журнала системных событий в реальном времени . .	6
2.2	Изменение правил rsyslog и настройка журналирования веб-службы	8
3	Ход выполнения	13
3.1	Использование journalctl для анализа системного журнала	13
3.2	Настройка постоянного журнала journald	23
4	Контрольные вопросы	25
5	Заключение	27

Список иллюстраций

2.1	Ошибка аутентификации при выполнении su	7
2.2	Сообщение, добавленное в системный журнал	7
2.3	Просмотр журнала безопасности	8
2.4	Установка и запуск Apache	9
2.5	Журнал ошибок Apache	9
2.6	Редактирование конфигурационного файла httpd.conf	10
2.7	Настройка rsyslog для Apache	11
2.8	Файл конфигурации	11
2.9	Журнал ошибок	12
3.1	Просмотр журнала с момента загрузки системы	14
3.2	Просмотр журнала без пейджера	15
3.3	Мониторинг журнала в реальном времени	16
3.4	Список параметров фильтрации journalctl	17
3.5	События пользователя UID 0	18
3.6	Последние 20 записей системного журнала	19
3.7	Сообщения с приоритетом ошибок	20
3.8	Сообщения журнала со вчерашнего дня	21
3.9	Ошибки, зафиксированные со вчерашнего дня	22
3.10	Детальный вывод журнала в формате verbose	23
3.11	Проверка постоянного журнала journald	24

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

1. Для выполнения задания было открыто три вкладки терминала.
В каждой вкладке получены полномочия администратора.
Успешное получение прав суперпользователя подтверждается изменением приглашения командной строки на `root@`.
2. Во второй вкладке терминала запущен мониторинг системных сообщений в реальном времени путём отслеживания файла журнала `/var/log/messages`.
Данный режим позволяет в реальном времени наблюдать все события, регистрируемые системой.
3. В третьей вкладке выполнен выход из режима суперпользователя и предпринята попытка повторного получения административных прав с вводом неверного пароля.
В результате аутентификация завершилась неудачно.
Во второй вкладке терминала было зафиксировано сообщение вида `FAILED SU (to root)`, которое также сохранилось в файле `/var/log/messages`.

```

Jan 16 11:39:14 ivschemelev systemd[1]: Starting fprintd.service - Fingerprint Authentication Daemon
Jan 16 11:39:14 ivschemelev systemd[1]: Started fprintd.service - Fingerprint Authentication Daemon.
Jan 16 11:39:17 ivschemelev su[8744]: FAILED SU (to root) ivschemelev on pts/2
Jan 16 11:39:18 ivschemelev kernel: traps: VBoxClient[8758] trap int3 ip:41dd1b sp:7fd39b388cd0 error:
in VBoxClient[1dd1b,400000+bb000]
Jan 16 11:39:18 ivschemelev systemd-coredump[8759]: Process 8755 (VBoxClient) of user 1000 terminated
abnormally with signal 5/TRAP, processing...

```

Рис. 2.1: Ошибка аутентификации при выполнении su

4. В третьей вкладке терминала из-под учётной записи обычного пользователя сгенерировано пользовательское сообщение журнала.

Во второй вкладке терминала отобразилось соответствующее сообщение, подтверждающее его запись в системный журнал.

```

a + 0x0) #01ZELT object binary architecture: AMD x86-b4
Jan 16 11:39:44 ivschemelev systemd[1]: systemd-coredump@410-8809-0.service: Deactivated successfully.
Jan 16 11:39:44 ivschemelev ivschemelev[8815]: hello
Jan 16 11:39:45 ivschemelev systemd[1]: fprintd.service: Deactivated successfully.
Jan 16 11:39:45 ivschemelev systemd[1]: Starting plocate-updatedb.service - Update the plocate database
...
Jan 16 11:39:46 ivschemelev systemd[1]: plocate-updatedb.service: Deactivated successfully.

```

Рис. 2.2: Сообщение, добавленное в системный журнал

5. Мониторинг системных сообщений в реальном времени был остановлен.

После этого выполнен просмотр последних 20 строк журнала безопасности /var/log/secure.

В журнале отображены записи, относящиеся к ранее выполненным неудачным попыткам аутентификации при использовании команды su.

```

root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# tail -n 20 /var/log/secure
Jan 16 11:09:07 ivschemelev (systemd)[4230]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)
Jan 16 11:09:07 ivschemelev su[4205]: pam_unix(su:session): session opened for user root(uid=0) by ivschemelev(uid=1000)
Jan 16 11:15:22 ivschemelev su[4205]: pam_unix(su:session): session closed for user root
Jan 16 11:17:13 ivschemelev su[5461]: pam_unix(su:session): session opened for user root(uid=0) by ivschemelev(uid=1000)
Jan 16 11:24:43 ivschemelev su[5461]: pam_unix(su:session): session closed for user root
Jan 16 11:24:51 ivschemelev su[6503]: pam_unix(su:session): session opened for user root(uid=0) by ivschemelev(uid=1000)
Jan 16 11:36:10 ivschemelev gdm-password[8007]: gkr-pam: unlocked login keyring
Jan 16 11:36:12 ivschemelev su[6503]: pam_unix(su:session): session closed for user root
Jan 16 11:37:47 ivschemelev (systemd)[8360]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)
Jan 16 11:37:48 ivschemelev su[8335]: pam_unix(su:session): session opened for user root(uid=0) by ivschemelev(uid=1000)
Jan 16 11:37:54 ivschemelev su[8450]: pam_unix(su:session): session opened for user root(uid=0) by ivschemelev(uid=1000)
Jan 16 11:37:58 ivschemelev su[8514]: pam_unix(su:session): session opened for user root(uid=0) by ivschemelev(uid=1000)
Jan 16 11:38:24 ivschemelev su[8514]: pam_unix(su:session): session closed for user root
Jan 16 11:38:30 ivschemelev unix_chkpwd[8644]: password check failed for user (ivschemelev)
Jan 16 11:38:30 ivschemelev sudo[8632]: pam_unix(sudo-i:auth): authentication failure; logname=ivschemelev uid=1000 euid=0 tty=/dev/pts/2 ruser=ivschemelev rhost= user=ivschemelev
Jan 16 11:38:33 ivschemelev unix_chkpwd[8656]: password check failed for user (ivschemelev)
Jan 16 11:38:36 ivschemelev unix_chkpwd[8658]: password check failed for user (ivschemelev)
Jan 16 11:38:37 ivschemelev sudo[8632]: ivschemelev : 3 incorrect password attempts ; TTY=pts/2 ; PWD=/root ; USER=root ; COMMAND=/bin/bash
Jan 16 11:39:15 ivschemelev unix_chkpwd[8753]: password check failed for user (root)
Jan 16 11:39:15 ivschemelev su[8744]: pam_unix(su:auth): authentication failure; logname=ivschemelev uid=1000 euid=0 tty=/dev/pts/2 ruser=ivschemelev rhost= user=root
root@ivschemelev:/home/ivschemelev#

```

Рис. 2.3: Просмотр журнала безопасности

2.2 Изменение правил rsyslog и настройка журналирования веб-службы

- В первой вкладке терминала произведена установка веб-сервера Apache HTTP Server.

После завершения установки веб-служба была запущена и добавлена в автозагрузку системы.


```

Installed:
  apr-1.7.5-2.el10.x86_64
  apr-util-lmdb-1.6.3-21.el10.x86_64
  httpd-2.4.63-4.el10_1.3.x86_64
  httpd-filesystem-2.4.63-4.el10_1.3.noarch
  mod_http2-2.0.29-3.el10.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-2.4.63-4.el10_1.3.x86_64
  httpd-tools-2.4.63-4.el10_1.3.x86_64
  mod_lua-2.4.63-4.el10_1.3.x86_64

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

```

Рис. 2.4: Установка и запуск Apache

7. Во второй вкладке терминала выполнен просмотр журнала ошибок веб-службы, расположенного в каталоге `/var/log/httpd`.

В журнале зафиксированы сообщения о запуске Apache, загрузке модулей и применении политики SELinux.

```

root@ivschemelov:/home/ivschemelov#
root@ivschemelov:/home/ivschemelov# tail -f /var/log/httpd/error_log
[Fri Jan 16 11:41:30.271293 2026] [suexec:notice] [pid 9381:tid 9381] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri Jan 16 11:41:30.299133 2026] [lbmethod_heartbeat:notice] [pid 9381:tid 9381] AH02282: No slotmem from mod_heartbeat
[Fri Jan 16 11:41:30.299657 2026] [systemd:notice] [pid 9381:tid 9381] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Fri Jan 16 11:41:30.302566 2026] [mpm_event:notice] [pid 9381:tid 9381] AH00489: Apache/2.4.63 (Rocky Linux) configured -- resuming normal operations
[Fri Jan 16 11:41:30.302576 2026] [core:notice] [pid 9381:tid 9381] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
^C
root@ivschemelov:/home/ivschemelov# █

```

Рис. 2.5: Журнал ошибок Apache

8. В третьей вкладке терминала открыт файл конфигурации веб-сервера `/etc/httpd/conf/httpd.conf`.

В конец файла добавлена директива, перенаправляющая журнал ошибок Apache в системный журнал syslog с использованием объекта `local1`.

```
GNU nano 8.1 /etc/httpd/conf/httpd.conf Modified
#
# MIMEMagicFile conf/magic
</IfModule>

#
# 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. 2.6: Редактирование конфигурационного файла httpd.conf

9. В каталоге /etc/rsyslog.d создан отдельный файл конфигурации для обработки сообщений веб-службы.

В нём задано правило, обеспечивающее запись всех сообщений объекта local1 в файл /var/log/httpd-error.log.

```
ivschemelev@ivschemelev:/home/ivsc| ivschemelev@ivschemelev:/  
GNU nano 8.1 httpd.conf  
local1.* -/var/log/httpd-error.log
```

Рис. 2.7: Настройка rsyslog для Apache

10. Для применения изменений выполнена перезагрузка службы системного журналирования и веб-службы Apache.

После этого все сообщения об ошибках веб-службы начали записываться в указанный файл журнала.

11. В каталоге `/etc/rsyslog.d` создан отдельный файл конфигурации для регистрации отладочных сообщений системы.

В файле задано правило, направляющее все сообщения уровня `debug` в файл `/var/log/messages-debug`.

```
root@ivschemelev:/home/ivschemelev#  
root@ivschemelev:/home/ivschemelev# nano /etc/httpd/conf/httpd.conf  
root@ivschemelev:/home/ivschemelev# cd /etc/rsyslog.d/  
root@ivschemelev:/etc/rsyslog.d# touch httpd.conf  
root@ivschemelev:/etc/rsyslog.d# nano httpd.conf  
root@ivschemelev:/etc/rsyslog.d# touch debug.conf  
root@ivschemelev:/etc/rsyslog.d# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf  
root@ivschemelev:/etc/rsyslog.d#  
root@ivschemelev:/etc/rsyslog.d# logger -p daemon.debug "Daemon Debug Message"  
root@ivschemelev:/etc/rsyslog.d#
```

Рис. 2.8: Файл конфигурации

12. Для применения новой конфигурации служба `rsyslog` была перезапущена.
13. Во второй вкладке терминала запущен мониторинг файла `/var/log/messages-debug` в реальном времени.

После генерации отладочного сообщения в журнале отобразилась соответствующая запись, что подтвердило корректность настроек.

```
(n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Jan 16 11:46:37 ivschemelev systemd[1]: systemd-coredump@491-10842-0.service: Deactivated successfully.
Jan 16 11:46:41 ivschemelev root[10848]: Daemon Debug Message
Jan 16 11:46:42 ivschemelev kernel: traps: VBoxClient[10853] trap int3 ip:41dd1b sp:7fd39b388cd0 error:
0 in VBoxClient[1dd1b,400000+bb000]
Jan 16 11:46:42 ivschemelev systemd-coredump[10854]: Process 10850 (VBoxClient) of user 1000 terminated
abnormally with signal 5/TRAP, processing...
Jan 16 11:46:42 ivschemelev systemd[1]: Started systemd-coredump@492-10854-0.service - Process Core Dump
(PID 10854/UID 0).
```

Рис. 2.9: Журнал ошибок

14. По завершении проверки мониторинг был остановлен.

3 Ход выполнения

3.1 Использование journalctl для анализа системного журнала

1. Во второй вкладке терминала выполнен просмотр журнала событий, зафиксированных с момента последнего запуска системы.
Отображены сообщения ядра Linux, инициализации оборудования, запуска systemd и системных служб.
Для навигации по журналу использовались построчный и постраничный режимы просмотра, выход из режима просмотра выполнен стандартным способом.

```

root@ivschemellev:/home/ivschemellev# journalctl
Jan 16 11:04:03 ivschemelev.localdomain kernel: Linux version 6.12.0-124.21.1.el10_1.x86_64 (mockbuild)
Jan 16 11:04:03 ivschemelev.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-124
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-provided physical RAM map:
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff]
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff]
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff]
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff]
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x000000000dfff0000-0x000000000dffffff]
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff]
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee0ffff]
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff]
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff]
Jan 16 11:04:03 ivschemelev.localdomain kernel: NX (Execute Disable) protection: active
Jan 16 11:04:03 ivschemelev.localdomain kernel: APIC: Static calls initialized
Jan 16 11:04:03 ivschemelev.localdomain kernel: SMBIOS 2.5 present.
Jan 16 11:04:03 ivschemelev.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualB
Jan 16 11:04:03 ivschemelev.localdomain kernel: DMI: Memory slots populated: 0/0
Jan 16 11:04:03 ivschemelev.localdomain kernel: Hypervisor detected: KVM
Jan 16 11:04:03 ivschemelev.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Jan 16 11:04:03 ivschemelev.localdomain kernel: kvm-clock: using sched offset of 4546721147 cycles
Jan 16 11:04:03 ivschemelev.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_c
Jan 16 11:04:03 ivschemelev.localdomain kernel: tsc: Detected 3187.204 MHz processor
Jan 16 11:04:03 ivschemelev.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> re
Jan 16 11:04:03 ivschemelev.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Jan 16 11:04:03 ivschemelev.localdomain kernel: last pfn = 0x120000 max arch pfn = 0x40000000

```

Рис. 3.1: Просмотр журнала с момента загрузки системы

2. Выполнен просмотр содержимого журнала без использования встроенного пейджера.

В результате все сообщения журнала были выведены непосредственно в терминал без возможности интерактивной прокрутки.

```
.10-1.el10.x86_64
.4-10.el10.x86_64
wayland-1.23.1-1.el10.x86_64

libc.so.6 + 0x95128)
so.6 + 0x105afc)

o.6 + 0x1038fd)

ll_main (libc.so.6 + 0x2a58e)
in@@GLIBC_2.34 (libc.so.6 + 0x2a649)

6-64
Jan 16 11:49:05 ivschemelev.localdomain systemd[1]: systemd-coredump@520-11194-0.service: Deactivated successfully.
root@ivschemellev:/home/ivschemellev#
```

```
Module libX11.so.6 from rpm libX11-1.8
Module libffi.so.8 from rpm libffi-3.4
Module libwayland-client.so.0 from rpm

Stack trace of thread 11193:
#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  0x00007fd3a9a3e128 start_thread (l
#5  0x00007fd3a9aaeafc __clone3 (libc.

Stack trace of thread 11190:
#0  0x00007fd3a9aac8fd syscall (libc.s
#1  0x00000000004344e2 n/a (n/a + 0x0)
#2  0x0000000000450066 n/a (n/a + 0x0)
#3  0x0000000000405123 n/a (n/a + 0x0)
#4  0x00007fd3a99d358e __libc_start_ca
#5  0x00007fd3a99d3649 __libc_start_ma
#6  0x00000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x8
```

Рис. 3.2: Просмотр журнала без пейджера

3. Запущен режим мониторинга журнала в реальном времени.

В процессе наблюдения отображались новые события, регистрируемые системой, включая сообщения служб и ядра.

После завершения наблюдения режим реального времени был остановлен.

```
libc.so.6 + 0x95128)
so.6 + 0x105afc)
o.6 + 0x1038fd)
ll_main (libc.so.6 + 0x2a58e)
in@@GLIBC_2.34 (libc.so.6 + 0x2a649)
6-64
Jan 16 11:49:25 ivschemelev.localdomain systemd[1]: systemd-coredump@524-11254-0.service: Deactivated successfully.
^C
root@ivschemellev:/home/ivschemellev#
```

```
#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 0x00007fd3a9a3e128 start_thread (l
#7 0x00007fd3a9aaeafc __clone3 (libc.

Stack trace of thread 11250:
#0 0x00007fd3a9aac8fd syscall (libc.s
#1 0x00000000004344e2 n/a (n/a + 0x0)
#2 0x0000000000450066 n/a (n/a + 0x0)
#3 0x0000000000405123 n/a (n/a + 0x0)
#4 0x00007fd3a99d358e __libc_start_ca
#5 0x00007fd3a99d3649 __libc_start_ma
#6 0x00000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x8
```

Рис. 3.3: Мониторинг журнала в реальном времени

4. Для изучения доступных параметров фильтрации журнала был инициирован режим автодополнения.

В результате отображён список возможных полей и атрибутов, по которым может быть выполнена выборка сообщений.


```

root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# journalctl
Display all 129 possibilities? (y or n)
_AUDIT_LOGINUID=          JOURNAL_NAME=
_AUDIT_SESSION=          JOURNAL_PATH=
AVAILABLE=               _KERNEL_DEVICE=
AVAILABLE_PRETTY=        _KERNEL_SUBSYSTEM=
_BOOT_ID=                KERNEL_USEC=
_CAP_EFFECTIVE=          LEADER=
_CMDLINE=                LIMIT=
CODE_FILE=               LIMIT_PRETTY=
CODE_FUNC=               _LINE_BREAK=
CODE_LINE=               _MACHINE_ID=
_COMM=                   MAX_USE=
CONFIG_FILE=             MAX_USE_PRETTY=
CONFIG_LINE=             MEMORY_PEAK=
COREDUMP_CGROUP=         MEMORY_SWAP_PEAK=
COREDUMP_CMDLINE=        MESSAGE=
COREDUMP_COMM=           MESSAGE_ID=
COREDUMP_CWD=            NM_DEVICE=
COREDUMP_ENVIRON=        NM_LOG_DOMAINS=
COREDUMP_EXE=            NM_LOG_LEVEL=
COREDUMP_FILENAME=       _PID=
COREDUMP_GID=            PODMAN_EVENT=
COREDUMP_HOSTNAME=       PODMAN_TIME=
COREDUMP_OPEN_FDS=       PODMAN_TYPE=
COREDUMP_OWNER_UID=      PRIORITY=
COREDUMP_PACKAGE_JSON=   REALMD_OPERATION=
COREDUMP_PID=             _RUNTIME_SCOPE=
COREDUMP_PROC_AUXV=      SEAT_ID=

```

Рис. 3.4: Список параметров фильтрации journalctl

5. Выполнен просмотр событий, относящихся к пользователю с идентификатором UID 0.

В журнале отображены сообщения, связанные с запуском системных служб и действиями, выполненными от имени суперпользователя.

```

root@ivschemelev:/home/ivschemelev# journalctl _UID=0
Jan 16 11:04:03 ivschemelev.localdomain systemd-journald[290]: Collecting audit messages is disabled.
Jan 16 11:04:03 ivschemelev.localdomain systemd-journald[290]: Journal started
Jan 16 11:04:03 ivschemelev.localdomain systemd-journald[290]: Runtime Journal (/run/log/journal/473c9>
Jan 16 11:04:03 ivschemelev.localdomain systemd-modules-load[292]: Module 'msr' is built in
Jan 16 11:04:03 ivschemelev.localdomain systemd-modules-load[292]: Inserted module 'fuse'
Jan 16 11:04:03 ivschemelev.localdomain systemd-modules-load[292]: Module 'scsi_dh_alua' is built in
Jan 16 11:04:03 ivschemelev.localdomain systemd-modules-load[292]: Module 'scsi_dh_emc' is built in
Jan 16 11:04:03 ivschemelev.localdomain systemd-modules-load[292]: Module 'scsi_dh_rdac' is built in
Jan 16 11:04:03 ivschemelev.localdomain systemd[1]: Finished systemd-modules-load.service - Load Kerne>
Jan 16 11:04:03 ivschemelev.localdomain systemd[1]: Starting systemd-sysctl.service - Apply Kernel Var>
Jan 16 11:04:03 ivschemelev.localdomain systemd[1]: modprobe@dm_multipath.service: Deactivated success>
Jan 16 11:04:03 ivschemelev.localdomain systemd[1]: Finished modprobe@dm_multipath.service - Load Kern>
Jan 16 11:04:03 ivschemelev.localdomain systemd[1]: multipathd.service - Device-Mapper Multipath Devic>
Jan 16 11:04:03 ivschemelev.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev-early.service >
Jan 16 11:04:03 ivschemelev.localdomain systemd[1]: Starting systemd-sysusers.service - Create System >
Jan 16 11:04:03 ivschemelev.localdomain systemd-sysusers[309]: Creating group 'nobody' with GID 65534.
Jan 16 11:04:03 ivschemelev.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Var>
Jan 16 11:04:03 ivschemelev.localdomain systemd-sysusers[309]: Creating group 'users' with GID 100.
Jan 16 11:04:03 ivschemelev.localdomain systemd-sysusers[309]: Creating group 'systemd-journal' with G>
Jan 16 11:04:03 ivschemelev.localdomain systemd-sysusers[309]: Creating group 'dbus' with GID 81.
Jan 16 11:04:03 ivschemelev.localdomain systemd-sysusers[309]: Creating user 'dbus' (System Message Bu>
Jan 16 11:04:03 ivschemelev.localdomain systemd-sysusers[309]: Creating group 'tss' with GID 59.

```

Рис. 3.5: События пользователя UID 0

6. Выполнен вывод последних 20 строк журнала.

В журнале зафиксированы события, связанные с работой графической подсистемы, модулей VirtualBox и обработкой аварийных завершений процессов.

```

root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# journalctl -n 20
Jan 16 11:50:16 ivschemelev.localdomain kernel: traps: VBoxClient[11408] trap int3 ip:41dd1b sp:7fd39b>
Jan 16 11:50:16 ivschemelev.localdomain systemd-coredump[11409]: Process 11405 (VBoxClient) of user 10>
Jan 16 11:50:16 ivschemelev.localdomain systemd[1]: Started systemd-coredump@534-11409-0.service - Pro>
Jan 16 11:50:16 ivschemelev.localdomain systemd-coredump[11410]: [?] Process 11405 (VBoxClient) of use>

Module libXau.so.6 from rpm libXau-1.>
Module libxcb.so.1 from rpm libxcb-1.>
Module libX11.so.6 from rpm libX11-1.>
Module libffi.so.8 from rpm libffi-3.>
Module libwayland-client.so.0 from rp>
Stack trace of thread 11408:
#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  0x00007fd3a9a3e128 start_thread (>
#5  0x00007fd3a9aaefc __clone3 (libc>

Stack trace of thread 11407:
#0  0x00007fd3a9aac8fd syscall (libc.>
#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  0x00007fd3a9a3e128 start thread (>

```

Рис. 3.6: Последние 20 записей системного журнала

7. Выполнена фильтрация журнала по уровню приоритета ошибок.

Отображены сообщения с критическими и ошибочными состояниями, включая проблемы драйверов, графической подсистемы и служб пользователя.

```

root@ivschemellev:/home/ivschemellev# journalctl -p err
Jan 16 11:04:04 ivschemelev.localdomain systemd-udevd[522]: /etc/udev/rules.d/60-vboxadd.rules:1 Unkn>
Jan 16 11:04:04 ivschemelev.localdomain systemd-udevd[522]: /etc/udev/rules.d/60-vboxadd.rules:2 Unkn>
Jan 16 11:04:05 ivschemelev.localdomain kernel: Warning: Unmaintained driver is detected: e1000>
Jan 16 11:04:05 ivschemelev.localdomain kernel: Warning: Unmaintained driver is detected: e1000_init_m>
Jan 16 11:04:05 ivschemelev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be >
Jan 16 11:04:05 ivschemelev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration >
Jan 16 11:04:05 ivschemelev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a >
Jan 16 11:04:11 ivschemelev.localdomain alsactl[1128]: alsa-lib main.c:1554:(snd_use_case_mgr_open) er>
Jan 16 11:04:46 ivschemelev.localdomain gdm-password[2559]: gkr-pam: unable to locate daemon control>
Jan 16 11:04:49 ivschemelev.localdomain systemd[2580]: Failed to start app-gnome-xdg\x2duser\x2ddirs-2>
Jan 16 11:04:50 ivschemelev.localdomain systemd[2580]: Failed to start app-gnome-vmware\x2duser-2882.s>
Jan 16 11:04:50 ivschemelev.localdomain systemd-coredump[3348]: [^] Process 3336 (VBoxClient) of user >

Module libXau.so.6 from rpm libXau-1.0>
Module libxcb.so.1 from rpm libxcb-1.1>
Module libX11.so.6 from rpm libX11-1.8>
Module libffi.so.8 from rpm libffi-3.4>
Module libwayland-client.so.0 from rpm>
Stack trace of thread 3340:
#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  0x00007fd3a9a3e128 start_thread (l>
#5  0x00007fd3a9a3e128 clone3 (libc>

```

Рис. 3.7: Сообщения с приоритетом ошибок

8. Выполнен просмотр сообщений журнала, зарегистрированных со вчерашнего дня.

В журнале представлены сообщения ядра, загрузки системы и инициализации аппаратных и программных компонентов.

```

root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# journalctl --since yesterday
Jan 16 11:04:03 ivschemelev.localdomain kernel: Linux version 6.12.0-124.21.1.el10_1.x86_64 (mockbuild)
Jan 16 11:04:03 ivschemelev.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-124
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-provided physical RAM map:
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x0000000000009fc00-0x000000000009ffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x0000000000dfff0000-0x0000000000dfffffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee0ffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x0000000010000000-0x0000000011fffffff]>
Jan 16 11:04:03 ivschemelev.localdomain kernel: NX (Execute Disable) protection: active
Jan 16 11:04:03 ivschemelev.localdomain kernel: APIC: Static calls initialized
Jan 16 11:04:03 ivschemelev.localdomain kernel: SMBIOS 2.5 present.
Jan 16 11:04:03 ivschemelev.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualB
Jan 16 11:04:03 ivschemelev.localdomain kernel: DMI: Memory slots populated: 0/0
Jan 16 11:04:03 ivschemelev.localdomain kernel: Hypervisor detected: KVM
Jan 16 11:04:03 ivschemelev.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Jan 16 11:04:03 ivschemelev.localdomain kernel: kvm-clock: using sched offset of 4546721147 cycles
Jan 16 11:04:03 ivschemelev.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_c
Jan 16 11:04:03 ivschemelev.localdomain kernel: tsc: Detected 3187.204 MHz processor
Jan 16 11:04:03 ivschemelev.localdomain kernel: e820: update from 0x00000000 0x000000005f5f mask 0x00000000

```

Рис. 3.8: Сообщения журнала со вчерашнего дня

9. Выполнен просмотр сообщений об ошибках, зафиксированных со вчерашнего дня.

В журнале отображены только записи с ошибочным уровнем приоритета за указанный временной интервал.

```

100@ivschemellev:/home/ivschemellev# journalctl --since yesterday -p err
Jan 16 11:04:04 ivschemelev.localdomain systemd-udevd[522]: /etc/udev/rules.d/60-vboxadd.rules:1 Unkn
Jan 16 11:04:04 ivschemelev.localdomain systemd-udevd[522]: /etc/udev/rules.d/60-vboxadd.rules:2 Unkn
Jan 16 11:04:05 ivschemelev.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Jan 16 11:04:05 ivschemelev.localdomain kernel: Warning: Unmaintained driver is detected: e1000_init_m
Jan 16 11:04:05 ivschemelev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be
Jan 16 11:04:05 ivschemelev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration
Jan 16 11:04:05 ivschemelev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a
Jan 16 11:04:11 ivschemelev.localdomain alsactl[1128]: alsa-lib main.c:1554:(snd_use_case_mgr_open) ex
Jan 16 11:04:46 ivschemelev.localdomain gdm-password[2559]: gkr-pam: unable to locate daemon control
Jan 16 11:04:49 ivschemelev.localdomain systemd[2580]: Failed to start app-gnome-xdg\x2duser\x2ddirs-2
Jan 16 11:04:50 ivschemelev.localdomain systemd[2580]: Failed to start app-gnome-vmware\x2duser-2882.s
Jan 16 11:04:50 ivschemelev.localdomain systemd-coredump[3348]: [?] Process 3336 (VBoxClient) of user

Module libXau.so.6 from rpm libXau-1.0
Module libxcb.so.1 from rpm libxcb-1.1
Module libX11.so.6 from rpm libX11-1.8
Module libffi.so.8 from rpm libffi-3.4
Module libwayland-client.so.0 from rpm
Stack trace of thread 3340:
#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 0x00007fd3a9a3e128 start_thread (l
#5 0x00007fd3a9aaefc clone3 (libc

```

Рис. 3.9: Ошибки, зафиксированные со вчерашнего дня

10. Выполнен вывод журнала в расширенном формате.

Отображена детальная информация о каждом событии, включая идентификаторы загрузки, временные метки, приоритеты, источники сообщений и дополнительные служебные поля.

```

_RUNTIME_SCOPE=initrd
Fri 2026-01-16 11:04:03.476659 MSK [s=44d843f01a634c53b71966e486543a13;i=2;b=768bcfe0adf34edba7fa33df1>
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=768bcfe0adf34edba7fa33df1fe75714
_MACHINE_ID=473c978a805e47e9bc9a702cdd313842
_HOSTNAME=ivschemev.localdomain
_RUNTIME_SCOPE=initrd
PRIORITY=6
MESSAGE=Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-124.21.1.el10_1.x86_64 root=/dev/mapper>
Fri 2026-01-16 11:04:03.476669 MSK [s=44d843f01a634c53b71966e486543a13;i=3;b=768bcfe0adf34edba7fa33df1>
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=768bcfe0adf34edba7fa33df1fe75714
_MACHINE_ID=473c978a805e47e9bc9a702cdd313842
_HOSTNAME=ivschemev.localdomain
_RUNTIME_SCOPE=initrd
PRIORITY=6
root@ivschemev:/home/ivschemev#
root@ivschemev:/home/ivschemev#
root@ivschemev:/home/ivschemev# journalctl _SYSTEMD_UNIT=sshd.service
Jan 16 11:04:12 ivschemev.localdomain sshd[1422]: Server listening on 0.0.0.0 port 22.
Jan 16 11:04:12 ivschemev.localdomain sshd[1422]: Server listening on :: port 22.
root@ivschemev:/home/ivschemev#

```

Рис. 3.10: Детальный вывод журнала в формате verbose

11. Выполнен просмотр сообщений, относящихся к службе SSH.

В журнале отображены записи о запуске демона, открытии сетевых портов и готовности службы к приёму подключений.

3.2 Настройка постоянного журнала journald

1. Для выполнения настройки был запущен терминал, после чего получены полномочия администратора.

Работа выполнялась от имени суперпользователя, что необходимо для изменения системных каталогов и параметров службы journald.

2. В файловой системе создан каталог /var/log/journal, предназначенный для постоянного хранения записей журнала systemd.

Использование данного каталога позволяет сохранять сообщения журнала на диске, а не только в оперативной памяти.

3. Для корректной работы службы `journal` были изменены права доступа и владелец каталога `/var/log/journal`.

Каталогу назначен владелец `root` и группа `systemd-journal`, а также установлен режим доступа, обеспечивающий запись журналов и корректное наследование прав.

4. Для применения внесённых изменений службе `systemd-journal` был отправлен сигнал перезагрузки конфигурации.

Данный способ позволяет активировать постоянное журналирование без полной перезагрузки операционной системы.

5. После выполнения настройки журнал `systemd` стал постоянным.

Для проверки корректности работы выполнен просмотр сообщений журнала с момента последней загрузки системы.

В журнале отображаются сообщения ядра Linux, параметры загрузки и события инициализации системы, что подтверждает успешное сохранение записей на диске.

```
root@ivschemelev:/home/ivschemelev#  
root@ivschemelev:/home/ivschemelev#  
root@ivschemelev:/home/ivschemelev# mkdir -p /var/log/journal  
root@ivschemelev:/home/ivschemelev# chown root:systemd-journal /var/log/journal/  
root@ivschemelev:/home/ivschemelev# chmod 2755 /var/log/journal/  
root@ivschemelev:/home/ivschemelev# killall -USR1 systemd-journald  
root@ivschemelev:/home/ivschemelev# journalctl -b  
Jan 16 11:04:03 ivschemelev.localdomain kernel: Linux version 6.12.0-124.21.1.el10_1.x86_64 (mockbuild>  
Jan 16 11:04:03 ivschemelev.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-124>  
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-provided physical RAM map:  
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbff]>  
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff]>  
Jan 16 11:04:03 ivschemelev.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff1>
```

Рис. 3.11: Проверка постоянного журнала `journal`

4 Контрольные вопросы

1. Для настройки службы rsyslogd используется основной конфигурационный файл **/etc/rsyslog.conf**.

Дополнительные правила и пользовательские настройки могут размещаться в отдельных конфигурационных файлах в каталоге **/etc/rsyslog.d/**, которые автоматически подключаются при запуске службы.

2. Сообщения rsyslogd, связанные с аутентификацией и авторизацией пользователей, записываются в файл журнала **/var/log/secure**.

В данном файле фиксируются события входа в систему, ошибки ввода пароля, использование команды su, а также работа служб аутентификации.

3. Если параметры ротации журналов не настраивались вручную, то ротация файлов журналов выполняется по умолчанию средствами **logrotate**.

В стандартной конфигурации ротация журналов производится **один раз в сутки** с хранением нескольких архивных копий лог-файлов.

4. Для записи всех сообщений с приоритетом **info** в файл **/var/log/messages.info** в конфигурации rsyslog необходимо добавить строку:

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

Данная директива указывает службе rsyslog записывать все сообщения уровня info и выше в указанный файл.

5. Для просмотра сообщений системного журнала в режиме реального времени используется команда:

```
journalctl -f
```

Данный режим позволяет наблюдать появление новых записей журнала по мере их регистрации системой.

6. Для просмотра всех сообщений журнала, записанных для процесса с идентификатором PID 1 в интервале времени с 9:00 до 15:00, используется команда:

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

В результате будут отображены только те записи журнала, которые соответствуют указанному процессу и временному диапазону.

7. Для просмотра сообщений journald после последней перезагрузки системы применяется команда:

```
journalctl -b
```

Она выводит все события текущего загрузочного сеанса операционной системы.

8. Для того чтобы сделать журнал journald постоянным, необходимо выполнить следующую процедуру:

- создать каталог **/var/log/journal**;
- назначить владельцем каталога пользователя root и группу systemd-journal;
- установить корректные права доступа для каталога;
- перезагрузить систему либо отправить службе systemd-journald сигнал пересчитывания конфигурации.

После выполнения данных действий записи журнала будут сохраняться на диске и сохраняться между перезагрузками системы.

5 Заключение

В ходе выполнения лабораторной работы были изучены механизмы ведения и анализа системных журналов в операционной системе Linux. Освоены приёмы мониторинга журналов в реальном времени, фильтрации сообщений по различным параметрам, а также настройки службы rsyslog для централизованной регистрации событий. Дополнительно выполнена настройка постоянного хранения журнала systemd-journald, что обеспечивает сохранность диагностической информации между перезагрузками системы и повышает удобство администрирования.