Отчёт по лабораторной работе №7

Управление журналами событий в системе

Щемелев Илья Владимирович

Содержание

Список иллюстраций

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`.

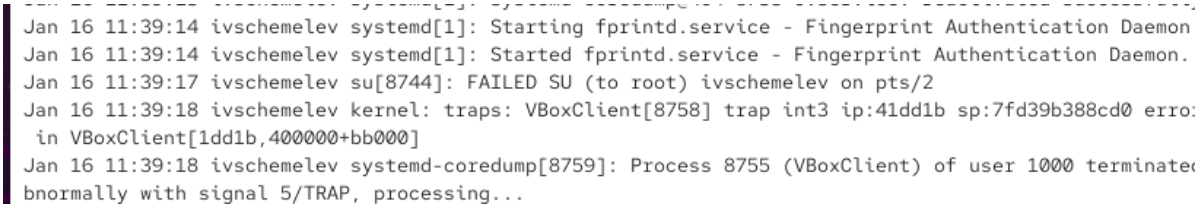

Рис. 2.1: Ошибка аутентификации при выполнении su

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.

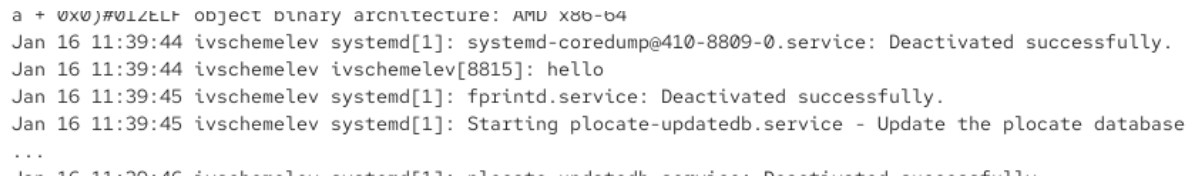

Рис. 2.2: Сообщение, добавленное в системный журнал

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 ro
ot(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 ivsc
hemelev(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 ivsc
hemelev(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 ivsc
hemelev(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 ro
ot(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 ivsc
hemelev(uid=1000)
Jan 16 11:37:54 ivschemelev su[8450]: pam_unix(su:session): session opened for user root(uid=0) by ivsc
hemelev(uid=1000)
Jan 16 11:37:58 ivschemelev su[8514]: pam_unix(su:session): session opened for user root(uid=0) by ivsc
hemelev(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=ivscheme
lev 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 ui
d=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

6. 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-1.6.3-21.el10.x86_64
  apr-util-lmdb-1.6.3-21.el10.x86_64               apr-util-openssl-1.6.3-21.el10.x86_64
  httpd-2.4.63-4.el10_1.3.x86_64                   httpd-core-2.4.63-4.el10_1.3.x86_64
  httpd-filesystem-2.4.63-4.el10_1.3.noarch        httpd-tools-2.4.63-4.el10_1.3.x86_64
  mod_http2-2.0.29-3.el10.x86_64                   mod_lua-2.4.63-4.el10_1.3.x86_64
  rocky-logos-httpd-100.4-7.el10.noarch

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

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@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# 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 f
rom mod_heartmonitor
[Fri Jan 16 11:41:30.299657 2026] [systemd:notice] [pid 9381:tid 9381] SELinux policy enabled; httpd ru
nning 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/h
ttpd -D FOREGROUND'
^C
root@ivschemelev:/home/ivschemelev#
```

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`.

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`.

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`.

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.

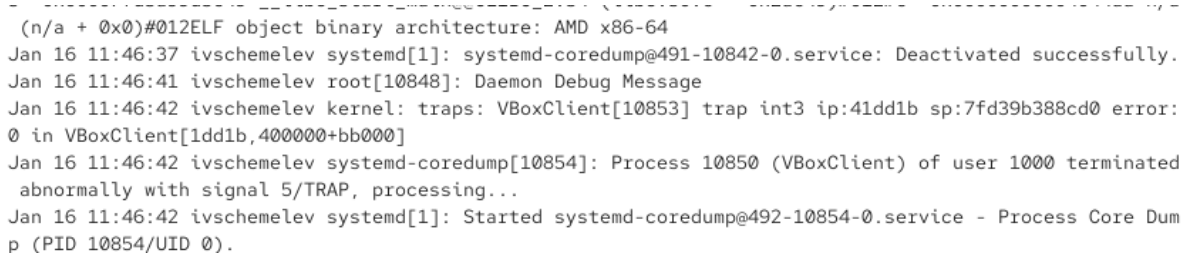

Рис. 2.9: Журнал ошибок

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.

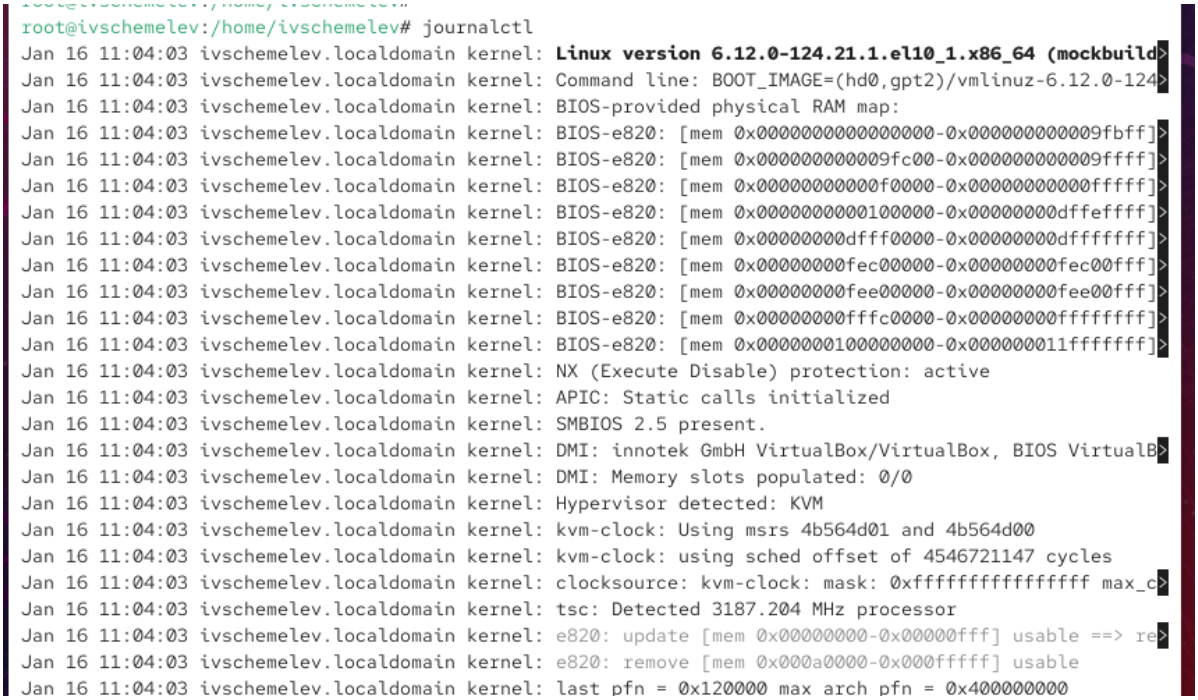

Рис. 3.1: Просмотр журнала с момента загрузки системы

2. Выполнен просмотр содержимого журнала без использования встроенного пейджера.

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

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.

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.

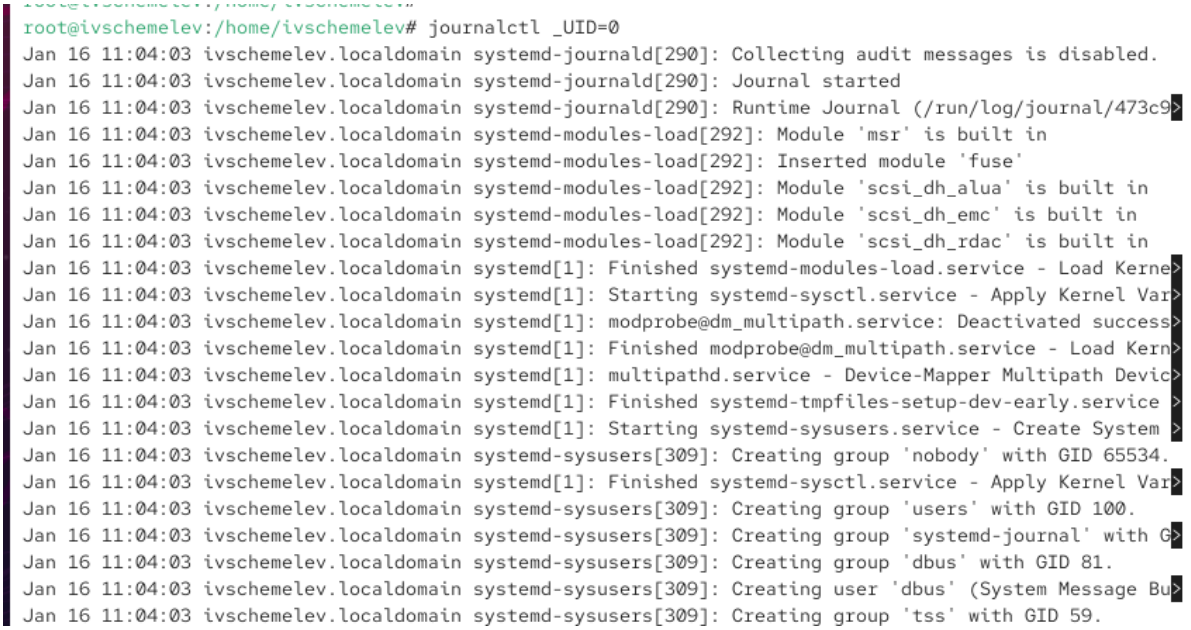

Рис. 3.5: События пользователя UID 0

6. Выполнен вывод последних 20 строк журнала.

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

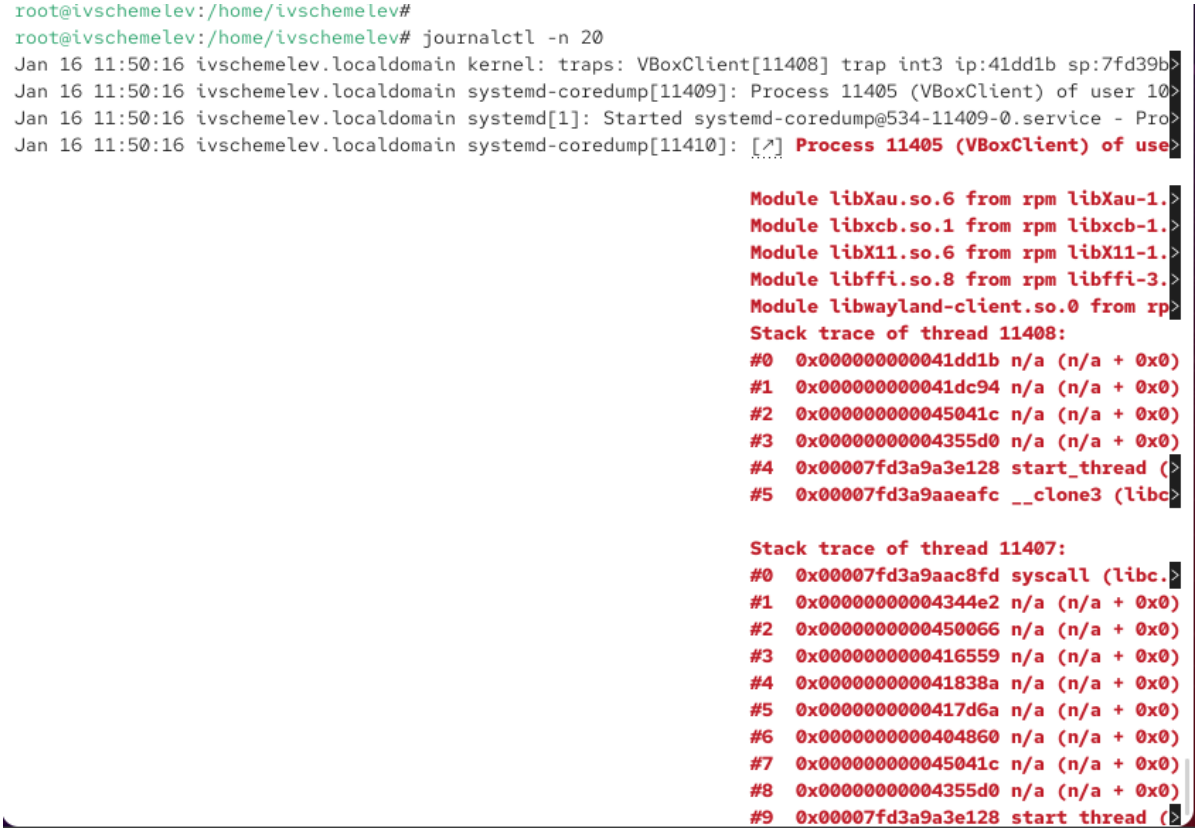

Рис. 3.6: Последние 20 записей системного журнала

7. Выполнена фильтрация журнала по уровню приоритета ошибок. Отображены сообщения с критическими и ошибочными состояниями, включая проблемы драйверов, графической подсистемы и служб пользователя.

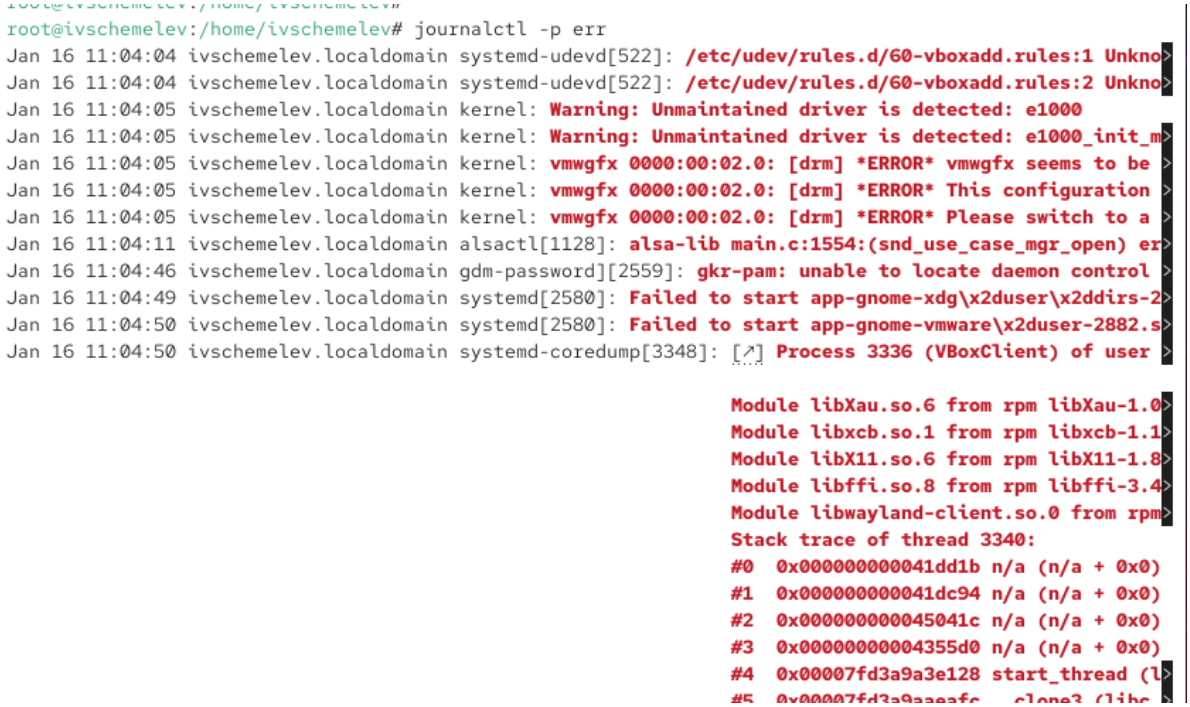

Рис. 3.7: Сообщения с приоритетом ошибок

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

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

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.

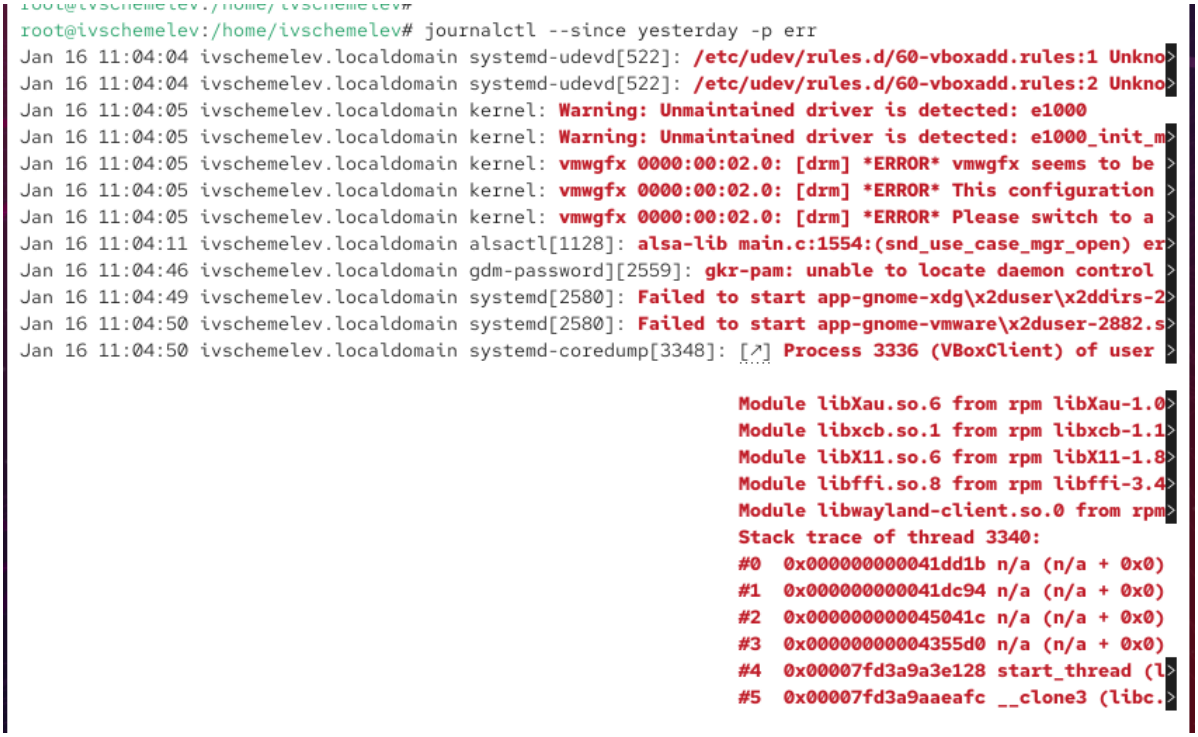

Рис. 3.9: Ошибки, зафиксированные со вчерашнего дня

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.

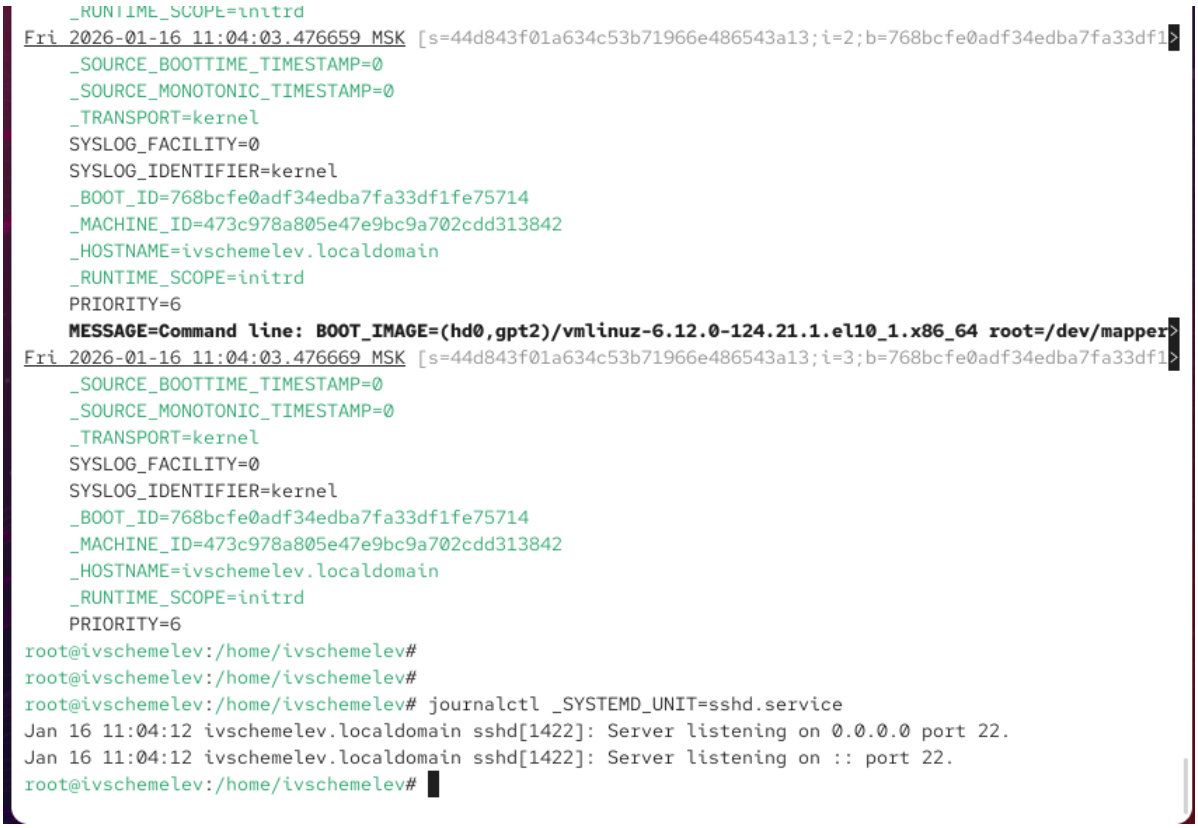

Рис. 3.10: Детальный вывод журнала в формате verbose

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 journald 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-journald 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 0x0000000000000000-0x000000000009fbff]>
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]>
```

Рис. 3.11: Проверка постоянного журнала journald

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 перечитывания 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.