Отчёт по лабораторной работе №7

Управление журналами событий в системе

Шаханеоядж Хаоладар

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

2 Выполнение

2.1 Мониторинг журнала системных событий в реальном времени

1. В трёх вкладках терминала были получены права администратора с помощью команды **su -**.
   Это позволило выполнять команды от имени суперпользователя во всех сессиях.

2. На второй вкладке терминала был запущен мониторинг системных событий в реальном времени с помощью команды **tail -f /var/log/messages**.
   В результате на экране стали отображаться новые записи журнала, появляющиеся в процессе работы системы.

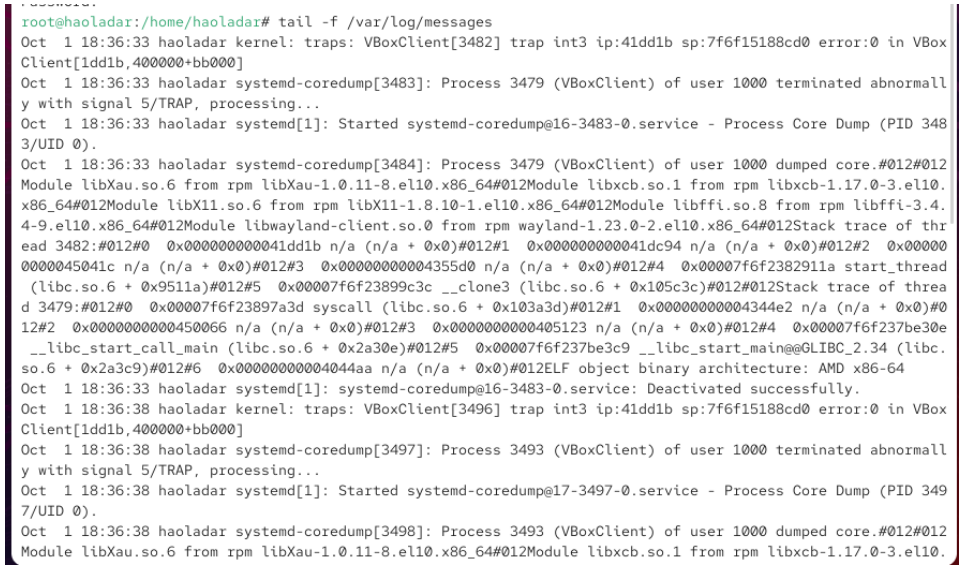

Рис. 2.1: Мониторинг системных событий в реальном времени

3. В третьей вкладке терминала была выполнена попытка получить права администратора с помощью команды **su**, но с введением неверного пароля. В окне мониторинга появилось сообщение об ошибке аутентификации: **FAILED SU (to root) haoladar on pts/2**.

   Это событие также было зафиксировано в файле **/var/log/messages**.

Рис. 2.2: Ошибка при попытке входа с неверным паролем

4. Далее в третьей вкладке от имени пользователя была выполнена команда **logger hello**.

   После этого в окне мониторинга появилось сообщение **hello**, подтверждающее запись пользовательского события в системный журнал.

Рис. 2.3: Сообщение logger hello в системном журнале

5. Мониторинг журнала **/var/log/messages** был завершён с помощью сочетания клавиш **Ctrl + C**.

   Затем был запущен просмотр последних 20 строк файла журнала безопасности командой **tail -n 20 /var/log/secure**.

   В результате отобразились сообщения о сессиях входа и ошибке аутентификации при вводе неправильного пароля команды **su**.

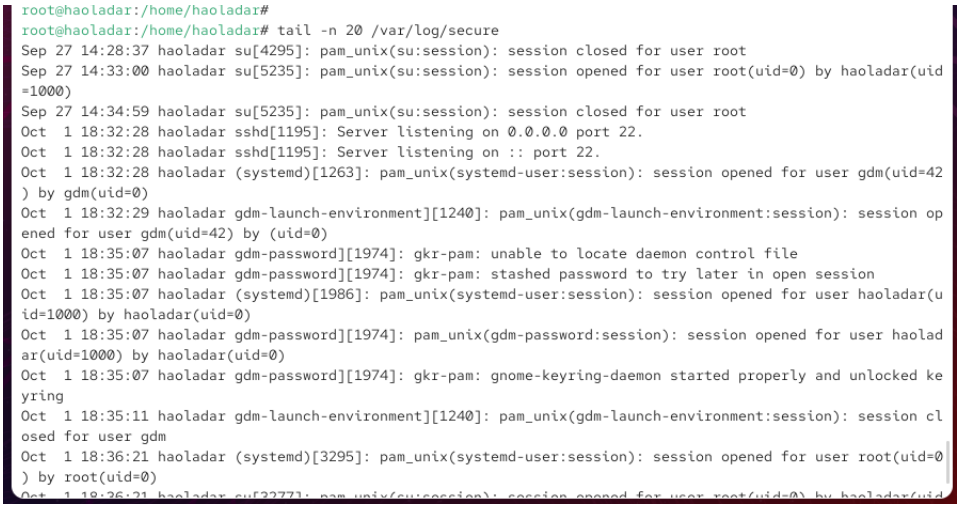

Рис. 2.4: Журнал безопасности /var/log/secure

3 Выполнение

3.1 Изменение правил rsyslog.conf

1. В первой вкладке терминала был установлен веб-сервер **Apache (httpd)** с помощью команды **dnf -y install httpd**.
   После завершения установки служба была запущена и добавлена в автозагрузку командами **systemctl start httpd** и **systemctl enable httpd**.

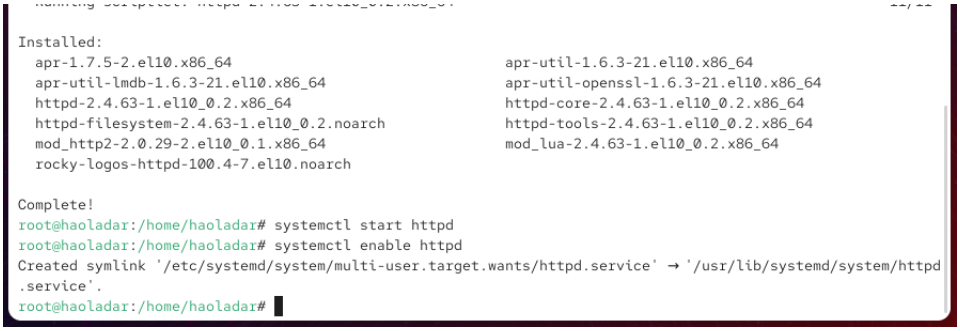

Рис. 3.1: Установка и запуск службы httpd

2. Во второй вкладке был открыт журнал ошибок веб-службы с помощью команды **tail -f /var/log/httpd/error_log**.
   На экране отобразились сообщения о запуске и настройке Apache, включая строки о включении SELinux, активации suEXEC и конфигурации модуля **mpm_event**.

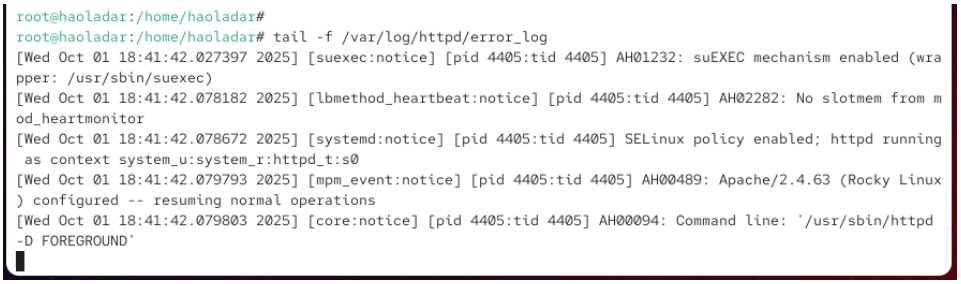

Рис. 3.2: Журнал ошибок Apache

3. В третьей вкладке был отредактирован конфигурационный файл **/etc/httpd/conf/httpd.conf**,
   в конец которого добавлена строка **ErrorLog syslog:local1**.
   Эта настройка перенаправляет сообщения об ошибках веб-сервера в системный журнал через объект **local1**.

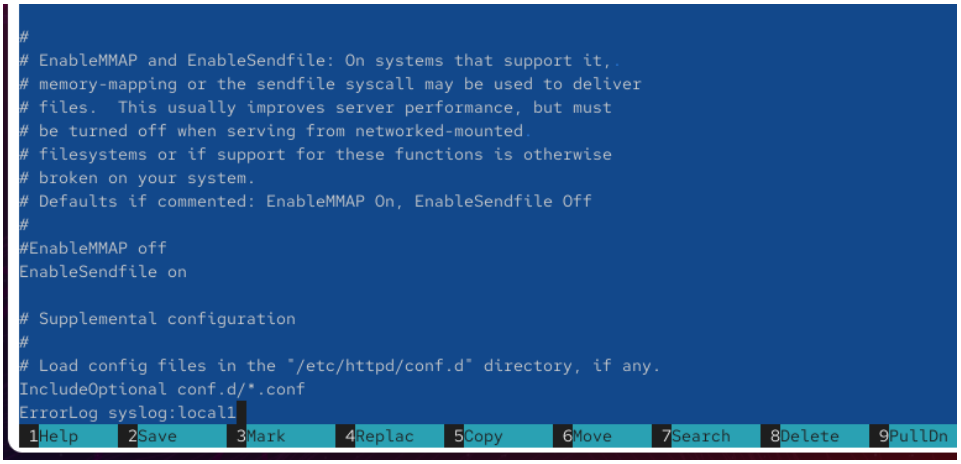

Рис. 3.3: Добавление строки ErrorLog syslog:local1 в конфигурацию httpd

4. В каталоге **/etc/rsyslog.d** был создан новый файл **httpd.conf** с правилом перенаправления сообщений от объекта **local1** в отдельный лог-файл **/var/log/httpd-error.log**:
   local1.* -/var/log/httpd-error.log.
   Это позволяет сохранять ошибки веб-службы в отдельном файле.

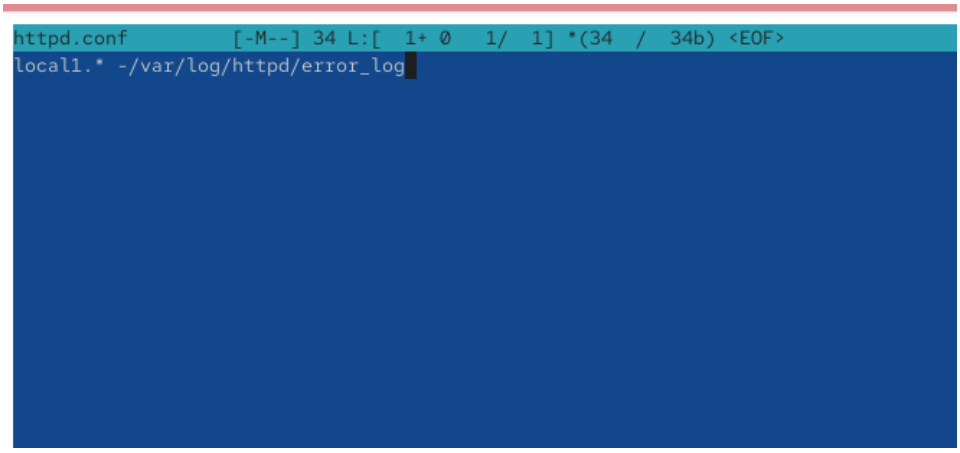

Рис. 3.4: Создание файла конфигурации rsyslog для httpd

5. После добавления правил конфигурации службы **rsyslog** и **httpd** были перезапущены командами
   systemctl restart rsyslog.service и **systemctl restart httpd**.
   Теперь все ошибки веб-службы записываются через **rsyslog** в файл **/var/log/httpd-error.log**.

6. В каталоге **/etc/rsyslog.d** был также создан дополнительный файл **debug.conf** для регистрации отладочных сообщений.
   В нём добавлена строка ***.debug /var/log/messages-debug**,
   что позволяет сохранять все отладочные сообщения в отдельный лог-файл.

Рис. 3.5: Создание файла debug.conf для регистрации отладочных сообщений

7. После перезапуска службы **rsyslog** в терминале был запущен мониторинг нового журнала с помощью команды **tail -f /var/log/messages-debug**.
   Далее от имени суперпользователя было отправлено отладочное сообщение:

logger -p daemon.debug “Daemon Debug Message”.

Сообщение успешно появилось в журнале, что подтверждает корректную настройку регистрации событий.

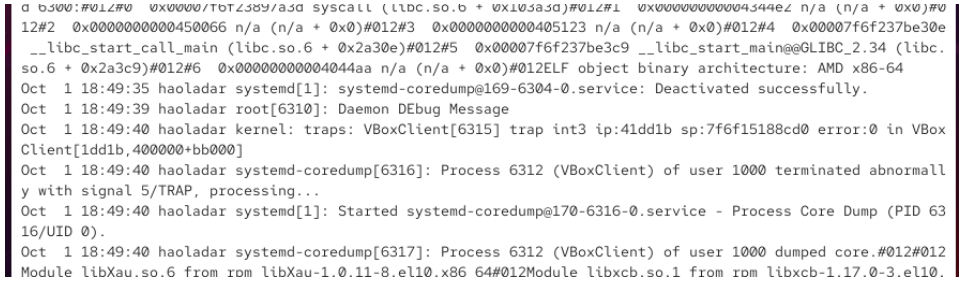

Рис. 3.6: Отображение отладочного сообщения в системном журнале

3.2 Использование journalctl

1. Во второй вкладке терминала был выполнен просмотр системного журнала с момента последнего запуска системы с помощью команды **journalctl**.
   На экране отобразились сообщения ядра и системных служб, включая данные о версии ядра, параметрах загрузки, BIOS и виртуальной среде.

Рис. 3.7: Просмотр системного журнала с момента последней загрузки

2. Для получения подробных сообщений без использования постраничного

вывода была выполнена команда **journalctl –no-pager**, которая вывела весь журнал в непрерывном виде.

Рис. 3.8: Просмотр возможных параметров фильтрации журнала

3. Режим реального времени включался командой **journalctl -f**, что позволило наблюдать новые системные события по мере их появления.
   Для выхода использовалось сочетание клавиш **Ctrl + C**.

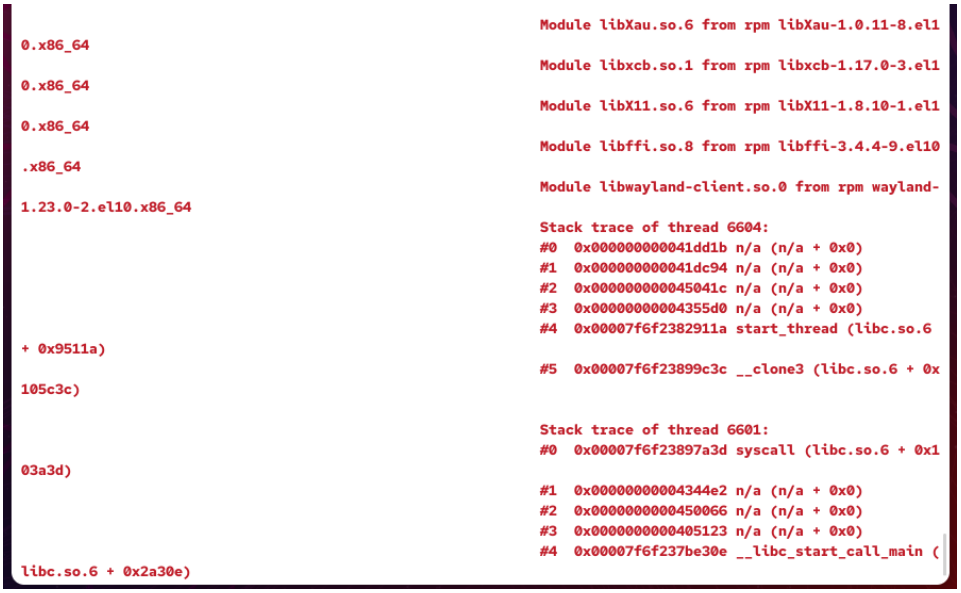

Рис. 3.9: Просмотр возможных параметров фильтрации журнала

4. Для ознакомления с параметрами фильтрации журнала была введена команда **journalctl** с двойным нажатием клавиши **Tab**,
   после чего на экран был выведен перечень всех доступных полей фильтрации: `_UID`, `_PID`, `_SYSTEMD_UNIT`, `_COMM` и другие.

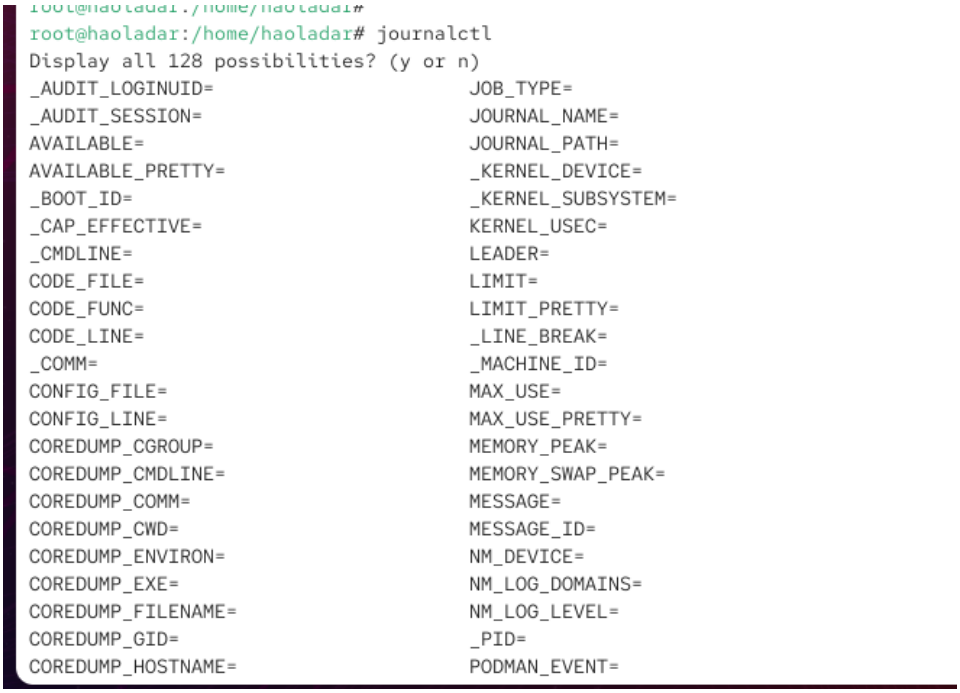

Рис. 3.10: Просмотр возможных параметров фильтрации журнала

5. С помощью команды **journalctl _UID=0** были отображены события, относящиеся к пользователю с идентификатором **UID 0 (root)**.

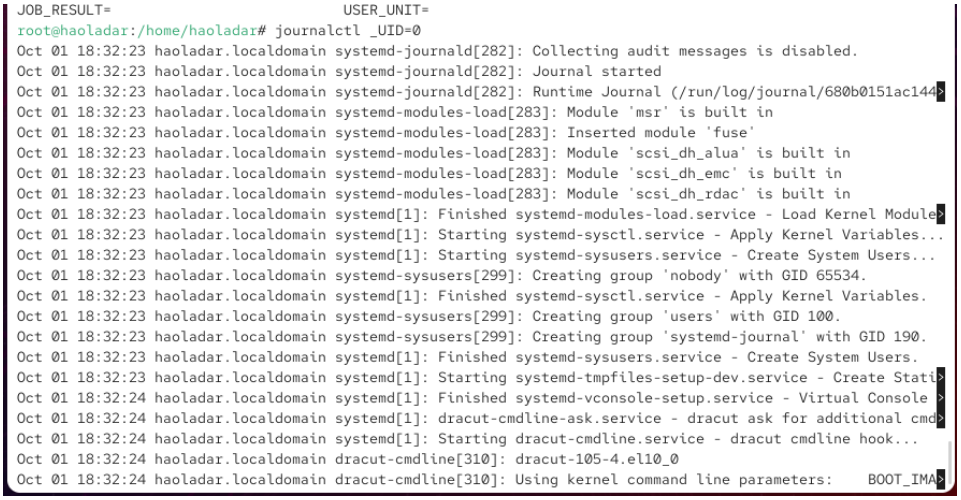

Рис. 3.11: Отображение событий, связанных с пользователем root

6. Для просмотра последних двадцати строк системного журнала использовалась команда **journalctl -n 20**,
   которая вывела актуальные системные события, включая сообщения о работе ядра и процессах.

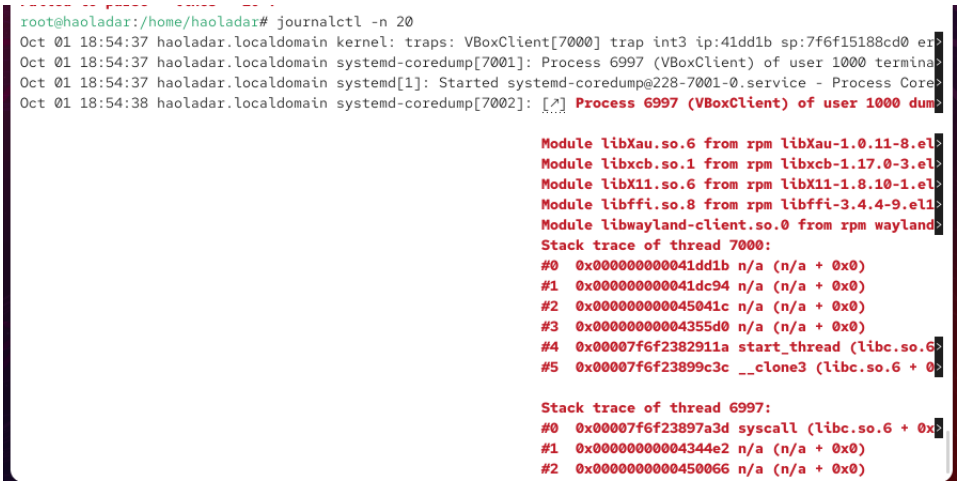

Рис. 3.12: Просмотр последних 20 строк журнала

7. Для отображения только сообщений об ошибках была введена команда **journalctl -p err**,
   которая вывела ошибки, зарегистрированные различными службами, включая **vmwgfx**, **alsa**, **gdm-password** и **systemd**.

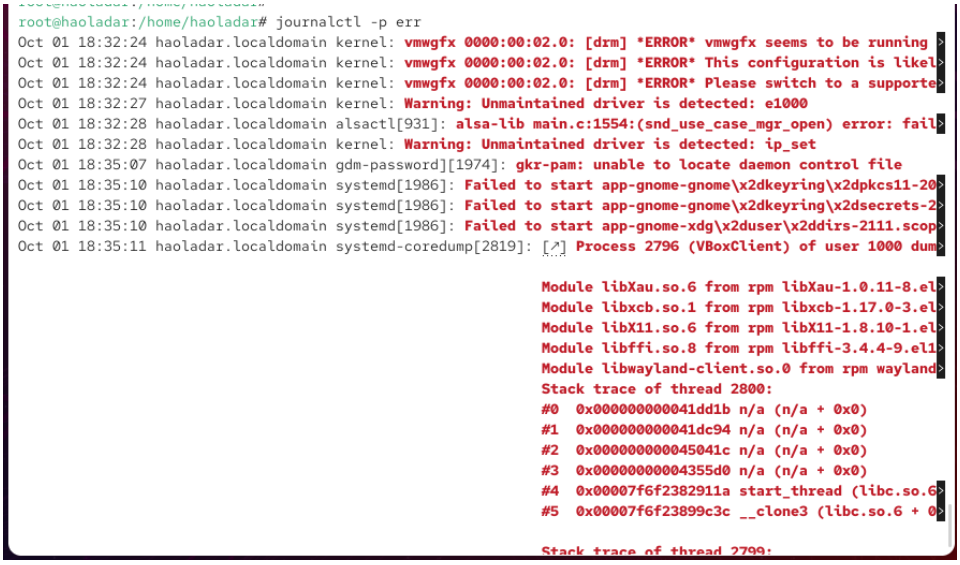

Рис. 3.13: Просмотр сообщений уровня ошибок

8. Для вывода всех сообщений со вчерашнего дня использовалась команда **journalctl –since yesterday**.

   В журнале отобразились все события, начиная с момента последней загрузки системы.

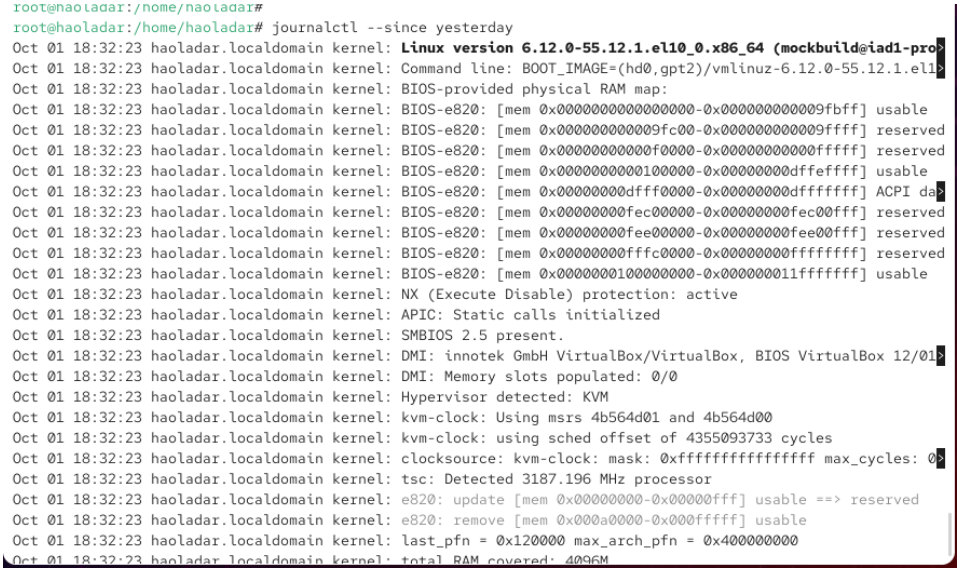

Рис. 3.14: Просмотр сообщений со вчерашнего дня

9. Для фильтрации сообщений уровня ошибок, зафиксированных со вчераш-

него дня, применена команда **journalctl –since yesterday -p err**.

На экране появились только сообщения с приоритетом «error» за заданный период.

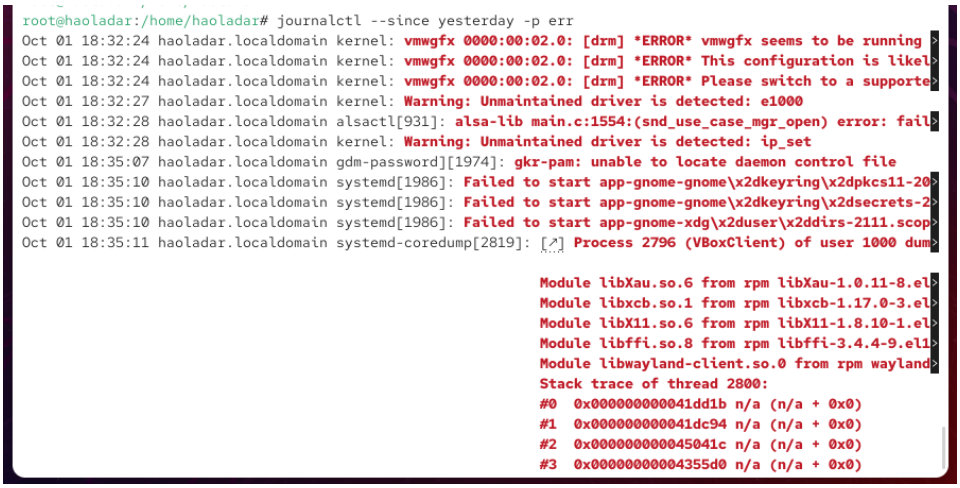

Рис. 3.15: Просмотр сообщений об ошибках со вчерашнего дня

10. Для детализированного вывода информации о записях журнала была использована команда **journalctl -o verbose**,

    которая показала дополнительные поля: идентификаторы процессов, время загрузки, имена модулей и приоритет сообщений.

11. Для анализа работы службы **sshd** была введена команда **journalctl _SYSTEMD_UNIT=sshd.service**.

    В результате отобразились сообщения о запуске службы SSH и активации прослушивания порта 22 на всех интерфейсах.

Рис. 3.16: Просмотр журнала службы SSH

3.3 Постоянный журнал journald

1. По умолчанию служба **systemd-journald** хранит свои журналы во временном каталоге **/run/log/journal**,
   поэтому записи теряются после перезагрузки системы.
   Для обеспечения постоянного хранения логов был создан каталог **/var/log/journal** командой
   mkdir -p /var/log/journal.

2. Далее были установлены корректные права доступа, позволяющие службе journald записывать данные в данный каталог:

   - **chown root:systemd-journal /var/log/journal** — назначает владельцем каталог root и группу systemd-journal;

   - **chmod 2755 /var/log/journal** — задаёт права доступа, обеспечивающие корректную работу службы при записи логов.

3. После изменения параметров доступа служба journald была уведомлена о необходимости обновить конфигурацию

без полной перезагрузки системы с помощью команды **killall -USR1 systemd-journald**.

4. Для проверки работоспособности постоянного хранения логов была выполнена команда **journalctl -b**,
   которая вывела сообщения системного журнала, начиная с момента последней загрузки.
   В выводе отображается информация о версии ядра, загрузочных параметрах и аппаратной конфигурации.

Рис. 3.17: Настройка постоянного хранения системного журнала journald

4 Контрольные вопросы

1. Какой файл используется для настройки rsyslogd?
   Основной файл конфигурации службы — **/etc/rsyslog.conf**.
   Дополнительные файлы с расширением **.conf** могут находиться в каталоге **/etc/rsyslog.d/**.

2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?
   Сообщения, относящиеся к аутентификации пользователей, хранятся в файле **/var/log/secure**.

3. Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?
   По умолчанию ротация логов выполняется **еженедельно**, что задаётся в файле **/etc/logrotate.conf** директивой `weekly`.

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

5. Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?
   Для просмотра журнала в реальном времени 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?
   Команда имеет вид:
   journalctl _PID=1 –since “09:00” –until “15:00”

7. Какая команда позволяет вам видеть сообщения journald после последней перезагрузки системы?
   Для этого используется команда:
   journalctl -b

8. Какая процедура позволяет сделать журнал journald постоянным?

   - Создать каталог **/var/log/journal** командой **mkdir -p /var/log/journal**

   - Назначить права и владельца:
     chown root:systemd-journal /var/log/journal
     chmod 2755 /var/log/journal

   - Применить изменения командой **killall -USR1 systemd-journald**
     После этого журнал **journald** станет постоянным и будет сохраняться между перезагрузками системы.

5 Заключение

В ходе работы освоены приёмы администрирования системных журналов в Linux.
Настроено постоянное хранение логов **journald**, изучены методы фильтрации и просмотра сообщений с помощью **journalctl** и **rsyslog**, а также способы регистрации и анализа системных событий в реальном времени.