Отчёт по лабораторной работе №7

Управление журналами событий в системе

Турсунов Мухамметназар

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 суперпользователя с помощью команды **su -**.
   Это позволило выполнять административные действия и получать доступ к системным логам.

2. Во второй вкладке запущен мониторинг системных событий в реальном времени с помощью команды **tail -f /var/log/messages**.
   Команда отображает новые строки, добавляемые в журнал сообщений, что удобно для наблюдения за активностью системы в реальном времени.

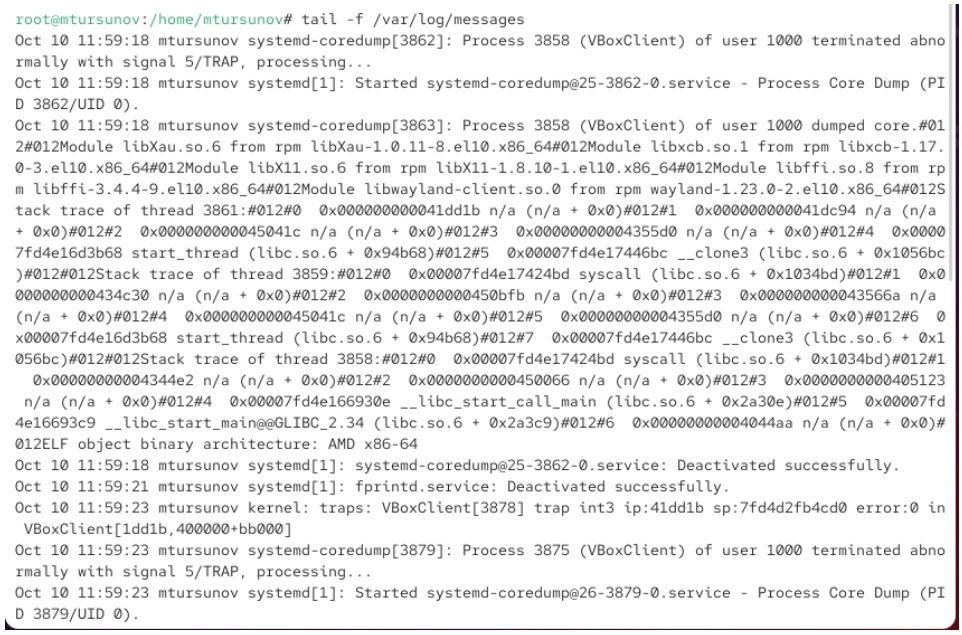

Рис. 2.1: Мониторинг системных событий через tail -f /var/log/messages

На экране фиксируются сообщения, связанные с процессами **VBoxClient**, сопровождающиеся ошибками и дампами памяти (core dump).
Это свидетельствует о сбоях в работе клиентских процессов VirtualBox.

3. В третьей вкладке произведён выход из режима суперпользователя с помощью **Ctrl + D**,
затем выполнена попытка повторного входа с использованием команды **su -**, при этом был введён неправильный пароль.
Во второй вкладке с активным мониторингом отобразилось сообщение об ошибке авторизации:
FAILED SU (to root) mtursunov on pts/2.

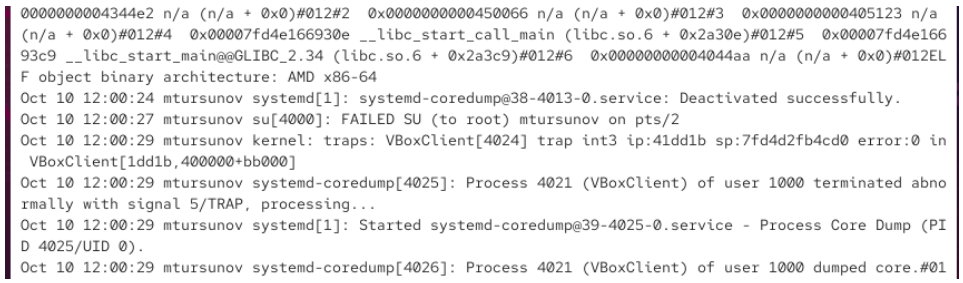

Рис. 2.2: Ошибка авторизации при попытке su -

4. Далее в пользовательской оболочке выполнена команда **logger hello**.

   Она предназначена для записи произвольных сообщений в системный журнал.

   После выполнения во второй вкладке с мониторингом появилось сообщение с текстом **hello**,

   подтверждающее успешную запись в файл **/var/log/messages**.

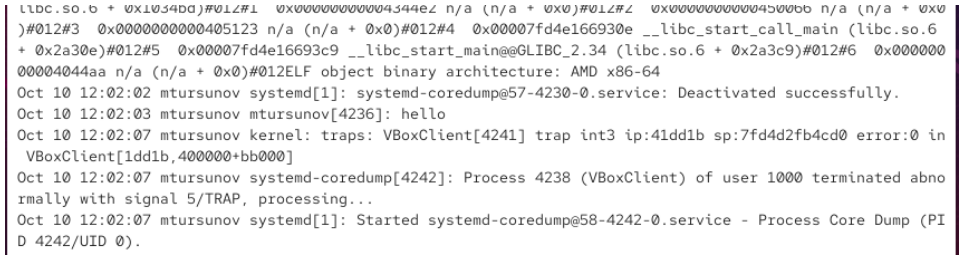

Рис. 2.3: Результат работы команды logger hello

5. После завершения наблюдения за системными событиями процесс мониторинга был остановлен сочетанием **Ctrl + C**.

   Затем выполнен просмотр последних двадцати строк журнала безопасности с помощью команды **tail -n 20 /var/log/secure**.

   В выводе зафиксированы события входа в систему, в том числе успешные и неудачные попытки авторизации через **su**, **sshd** и **gdm**.

   Также видны записи о неудачных попытках ввода пароля при повышении привилегий пользователя **mtursunov**.

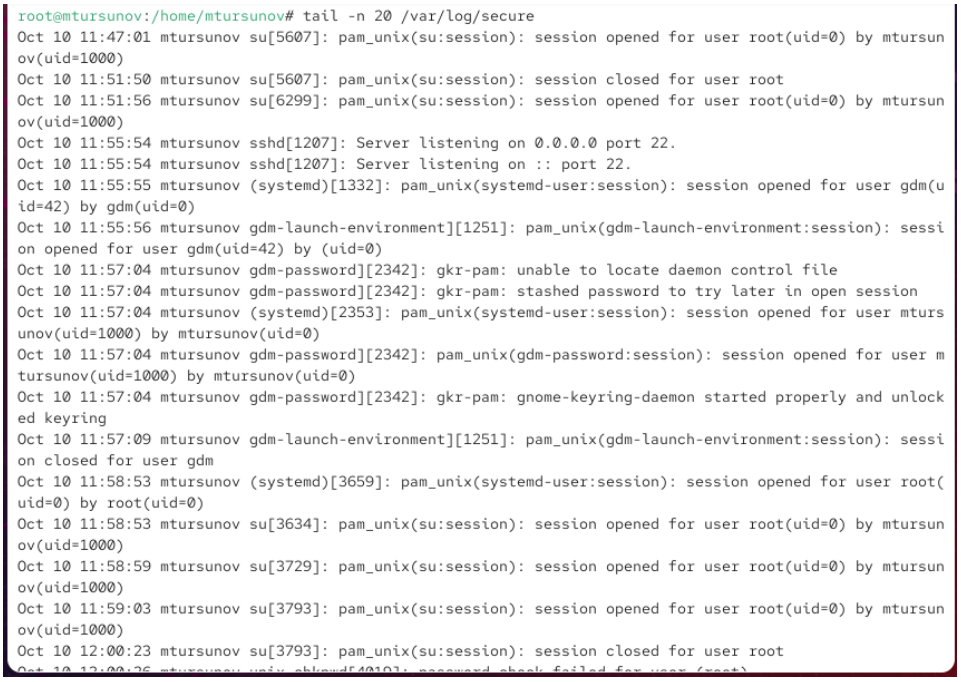

Рис. 2.4: Вывод файла /var/log/secure

2.2 Изменение правил rsyslog.conf

1. В первой вкладке терминала был установлен и запущен веб-сервер Apache. Для этого выполнены команды установки и запуска службы **httpd**, а также её автоматического запуска при загрузке системы.

2. После установки веб-службы выполнено наблюдение за журналом ошибок Apache:
   tail -f /var/log/httpd/error_log.
   В выводе фиксировались стандартные служебные сообщения о запуске и настройке Apache, включая уведомления SELinux и конфигурацию модулей.

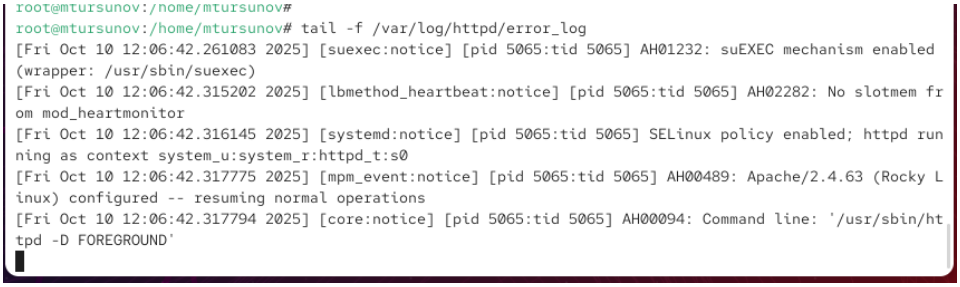

Рис. 2.5: Мониторинг журнала ошибок Apache

3. В конфигурационном файле **/etc/httpd/conf/httpd.conf** была добавлена строка:

   ErrorLog syslog:local1.

   Эта запись перенаправляет сообщения об ошибках веб-сервера в системный журнал, используя объект **local1**, предназначенный для пользовательских приложений.

Рис. 2.6: Изменение конфигурации httpd.conf

4. В каталоге **/etc/rsyslog.d** был создан новый файл **httpd.conf**, в который до-

бавлена строка:

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

Таким образом, все сообщения, поступающие в объект **local1**, будут записываться в отдельный лог-файл **/var/log/httpd-error.log**.

Рис. 2.7: Создание правила для перенаправления логов Apache

5. После изменения конфигураций службы журналирования и веб-сервера выполнена их перезагрузка:

   systemctl restart rsyslog.service и **systemctl restart httpd**.

   Это позволило применить новые параметры без перезагрузки системы.

Рис. 2.8: Перезапуск служб rsyslog и httpd

6. Для регистрации отладочных сообщений был создан дополнительный файл **debug.conf** в каталоге **/etc/rsyslog.d**.

   В него добавлена строка ***.debug /var/log/messages-debug**, направляющая

все сообщения с уровнем debug в отдельный журнал **/var/log/messages-debug**.

7. После перезапуска службы rsyslog был запущен мониторинг этого файла командой **tail -f /var/log/messages-debug**.
   Затем в другой вкладке терминала была выполнена команда **logger -p daemon.debug “Daemon Debug Message”**,
   которая отправила тестовое отладочное сообщение в системный журнал.

   В окне мониторинга отображается переданное сообщение, что подтверждает корректную настройку фильтрации и маршрутизации логов.

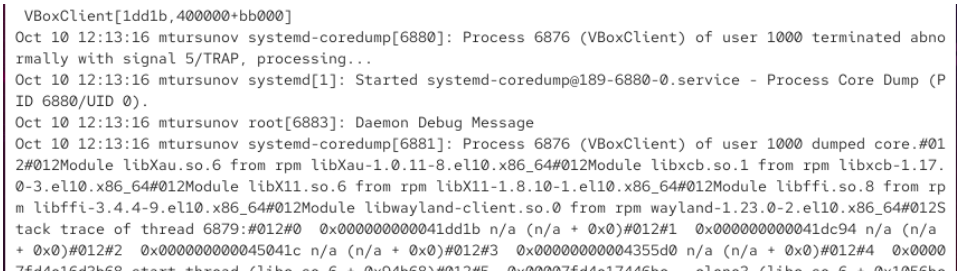

Рис. 2.9: Результат регистрации отладочного сообщения через logger

2.3 Использование journalctl

1. Во второй вкладке терминала был запущен просмотр системного журнала с момента последней загрузки системы с помощью команды **journalctl**.
   На экране отобразились записи ядра Linux, включая сведения о версии, параметрах загрузки, структуре памяти и активности BIOS.
   Управление просмотром осуществлялось клавишами **Enter** (построчно), **пробел** (постранично) и **q** (выход).

Рис. 2.10: Просмотр системного журнала с момента загрузки

2. Для получения журналов без использования пейджера применена команда **journalctl –no-pager**,
   что позволило вывести все записи сразу, без постраничной навигации.

3. Команда **journalctl -f** запустила отображение событий в реальном времени, аналогично действию утилиты `tail -f` для обычных логов.
   После появления новых сообщений (например, об ошибках VBoxClient) информация сразу же выводилась в консоль.
   Прекращение режима выполнено с помощью **Ctrl + C**.

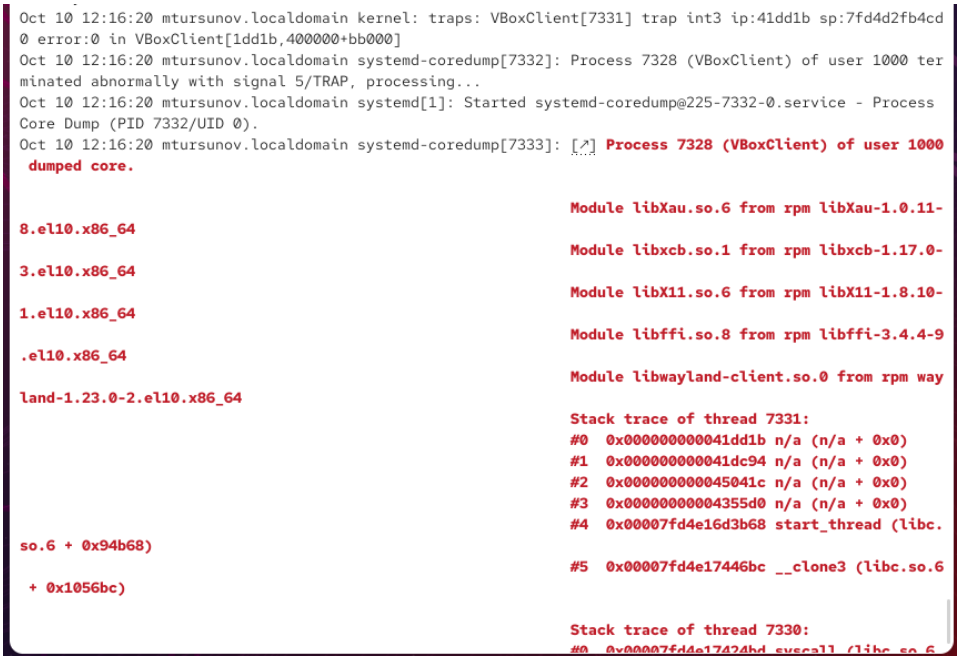

Рис. 2.11: Просмотр журнала в реальном времени

4. При двойном нажатии клавиши **Tab** после ввода команды **journalctl** был выведен список доступных параметров для фильтрации.
   Это позволило увидеть все возможные поля фильтрации, такие как `_UID`, `_SYSTEMD_UNIT`, `_EXE`, `_PID` и другие.

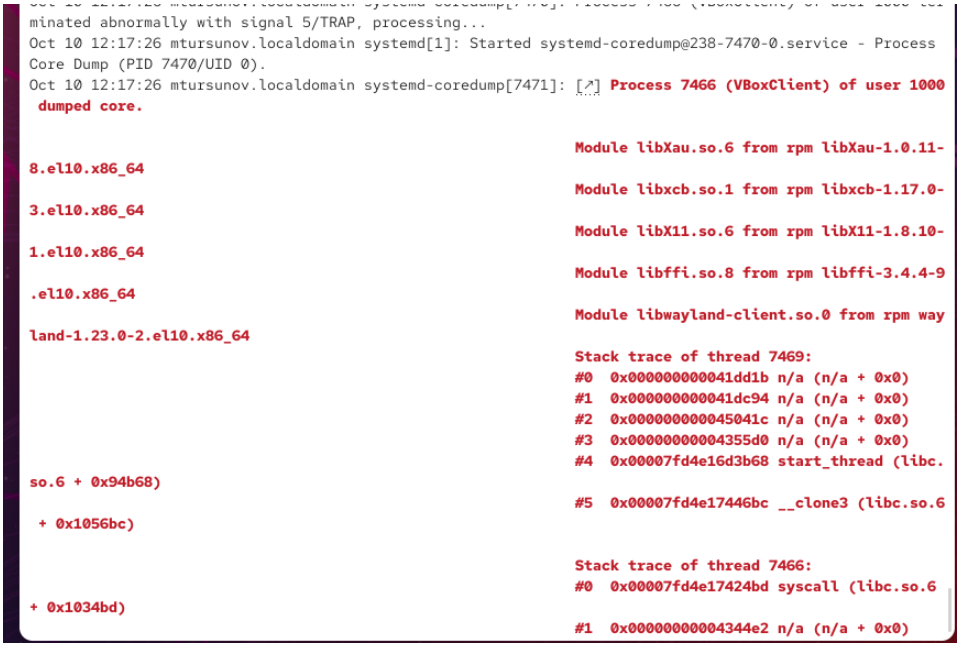

Рис. 2.12: Отображение параметров фильтрации journalctl

5. Для отображения записей, созданных пользователем с идентификатором UID 0 (root), была использована команда **journalctl _UID=0**.

   В результате выведены системные события, инициированные пользователем root во время запуска служб и модулей.

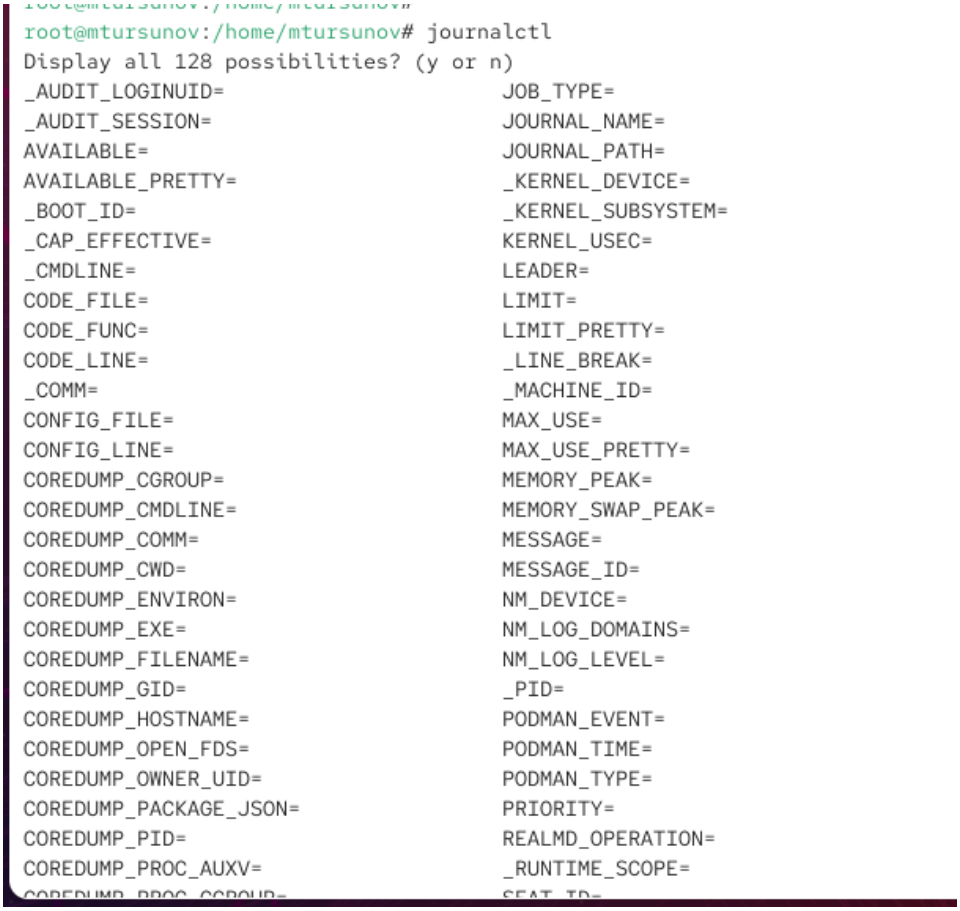

Рис. 2.13: Вывод записей для UID 0

6. Команда **journalctl -n 20** отобразила последние двадцать строк журнала. В них зафиксированы сообщения ядра и службы systemd, включая сведения о процессах и ошибках приложений.

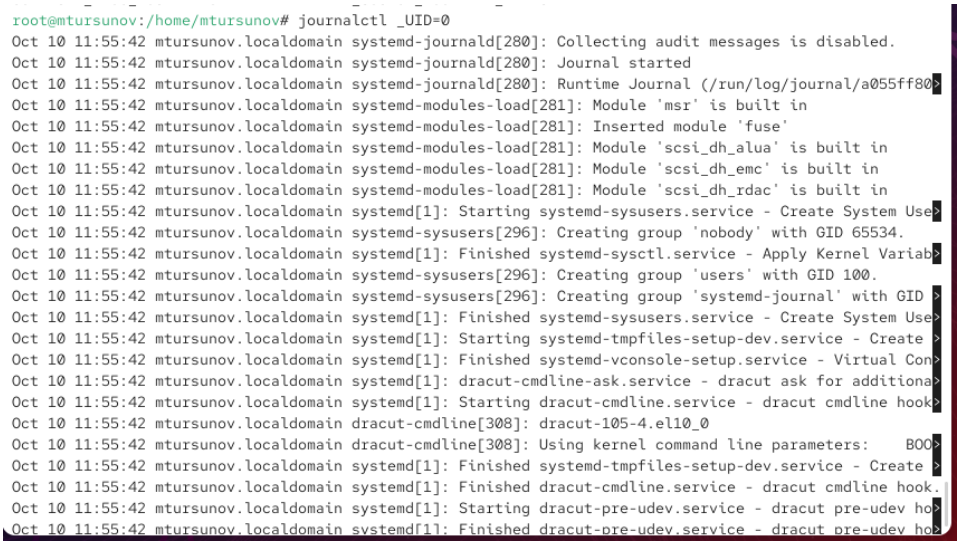

Рис. 2.14: Отображение последних 20 строк журнала

7. Для вывода только сообщений с уровнем приоритета “ошибка” использовалась команда **journalctl -p err**.

   На экран были выведены критические сообщения ядра и системных служб, включая ошибки видеодрайвера `vmwgfx` и библиотеки `alsa-lib`.

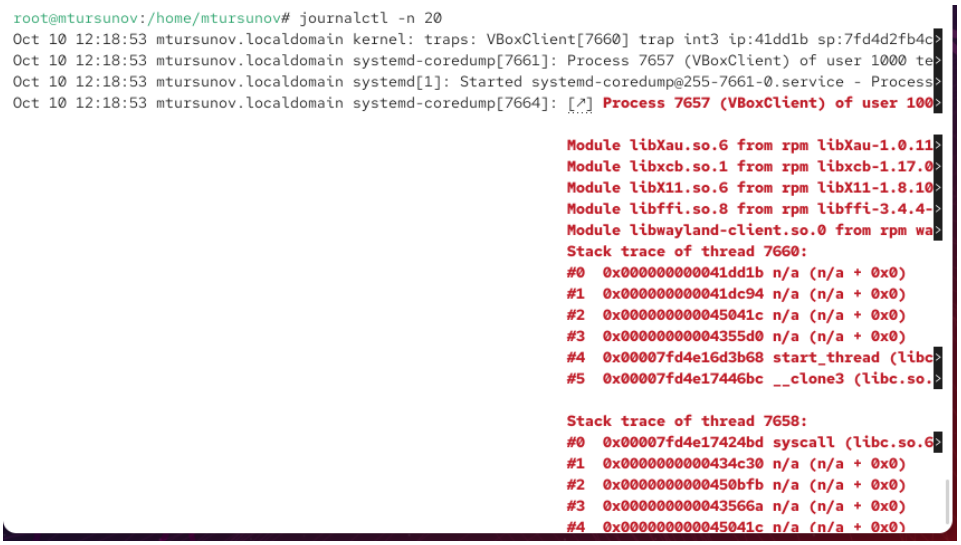

Рис. 2.15: Просмотр сообщений об ошибках

8. Для анализа событий, произошедших со вчерашнего дня, применена команда **journalctl –since yesterday**,

которая вывела все сообщения, начиная с предыдущих суток.

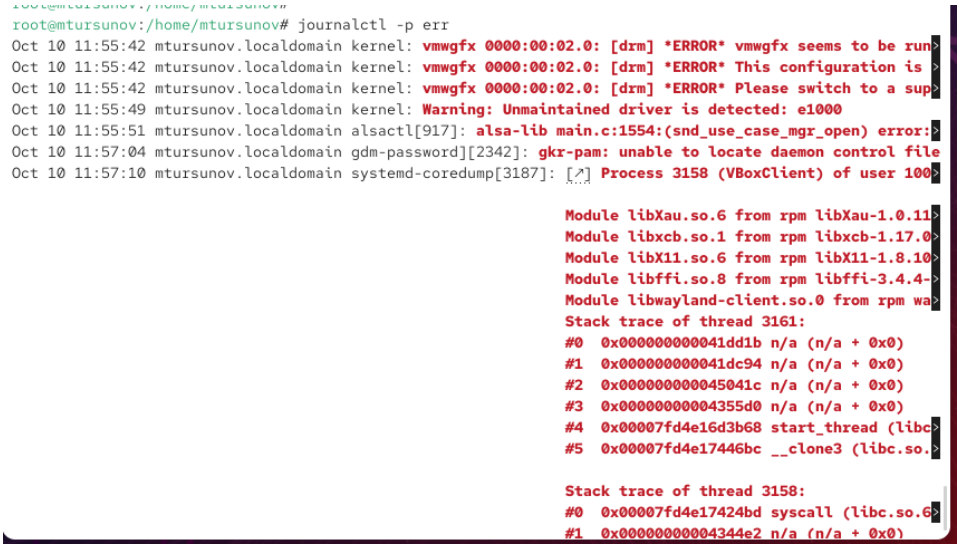

Рис. 2.16: Просмотр журнала с фильтром по времени

9. Команда **journalctl –since yesterday -p err** отобразила только сообщения об ошибках, зафиксированные со вчерашнего дня.
   Среди них присутствовали системные ошибки, предупреждения драйверов и сбои процессов VBoxClient.

Рис. 2.17: Просмотр ошибок со вчерашнего дня

10. Для получения расширенной информации о каждом событии была использована команда **journalctl -o verbose**.

    В этом режиме журнал отображает полные метаданные записей: дату, источник, уровень приоритета, идентификатор процесса, контекст и сообщение.

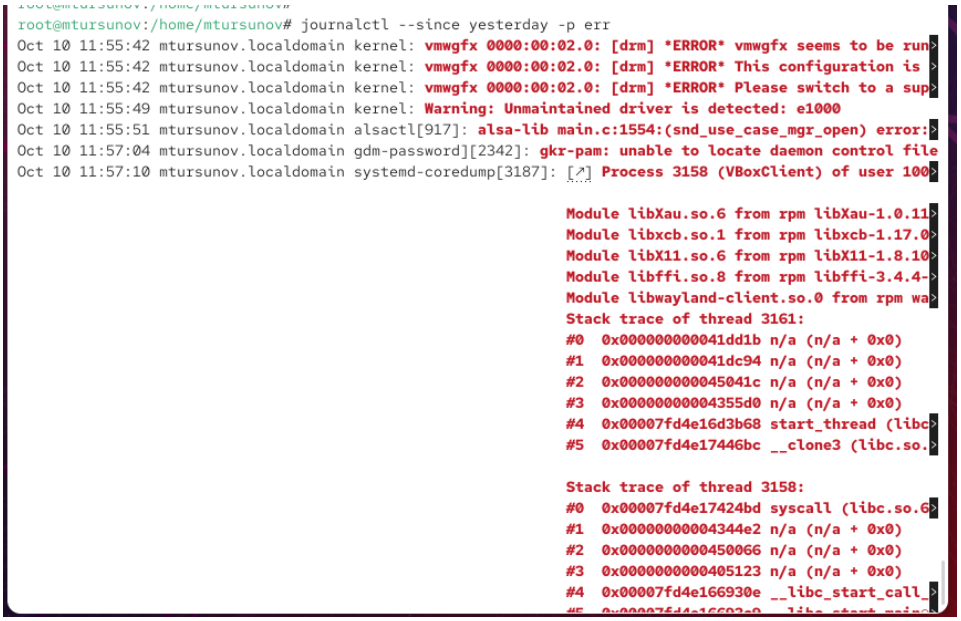

Рис. 2.18: Режим подробного вывода verbose

11. Для просмотра дополнительной информации о модуле SSHD использовалась команда **journalctl _SYSTEMD_UNIT=sshd.service**.

    В результате были показаны сообщения, связанные с запуском службы sshd, включая прослушивание портов и предупреждения окружения.

Рис. 2.19: Просмотр событий службы SSHD

2.4 Постоянный журнал journald

1. Для начала был получен доступ с правами суперпользователя.
   Это необходимо, так как изменение параметров системного журнала требует административных прав.

2. Создан каталог **/var/log/journal**, предназначенный для хранения постоянных записей журнала.
   Каталог создаётся с помощью команды **mkdir -p /var/log/journal**, которая создаёт директорию, если она отсутствует, включая промежуточные пути.

3. Для корректной работы службы **systemd-journald** настроены права доступа к каталогу:

   - командой **chown root:systemd-journal /var/log/journal** назначена владельцем группа *systemd-journal*,

   - командой **chmod 2755 /var/log/journal** заданы права доступа, позволяющие записи и чтение журналов службой journald.

4. Чтобы применить изменения без перезагрузки системы, была выполнена команда

   killall -USR1 systemd-journald, которая посылает процессу journald сигнал на перезапуск с перечитыванием конфигурации.

5. После этого журнал **systemd-journald** стал постоянным — все новые сообщения теперь сохраняются в каталоге **/var/log/journal** и не теряются после перезагрузки.

   Проверка осуществлена командой **journalctl -b**, которая выводит сообщения с момента последней загрузки системы.

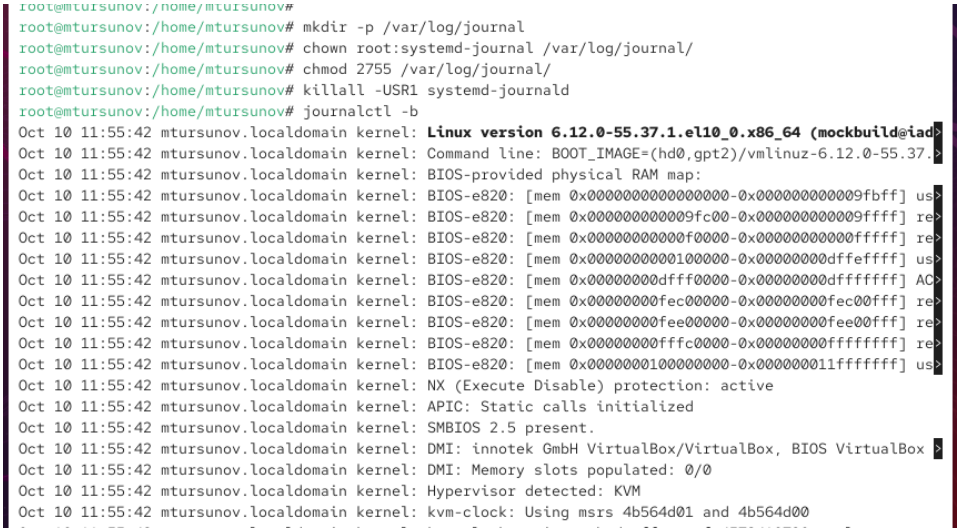

Рис. 2.20: Настройка постоянного журнала journald

3 Контрольные вопросы

1. **Какой файл используется для настройки rsyslogd?**
   /etc/rsyslog.conf
   а также дополнительные файлы конфигурации, расположенные в каталоге **/etc/rsyslog.d/**

2. **В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?**
   /var/log/secure

3. **Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?**
   По умолчанию ротация файлов журналов выполняется **еженедельно (weekly)** — один раз в неделю, согласно настройкам файла **/etc/logrotate.conf**.

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

5. **Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?**
   journalctl -f
   или для системных логов, управляемых rsyslog:
   tail -f /var/log/messages

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?**

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

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

   3. Отправить сигнал службе journald для применения изменений:
      killall -USR1 systemd-journald
      После этого журнал journald становится постоянным и сохраняется после перезагрузки.

4 Заключение

В ходе выполнения работы были изучены принципы и механизмы регистрации системных событий в Linux с использованием служб **rsyslog** и **systemd-journald**. Были выполнены практические действия по настройке журналов, фильтрации сообщений, перенаправлению логов веб-службы Apache, а также организации отдельного файла для отладочной информации.

Освоены приёмы работы с утилитой **journalctl**, включая поиск, фильтрацию, просмотр сообщений за определённые периоды и в режиме реального времени.