Отчёт по лабораторной работе №7

Управление журналами событий в системе

Эзиз Хатамов

Содержание

# 1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

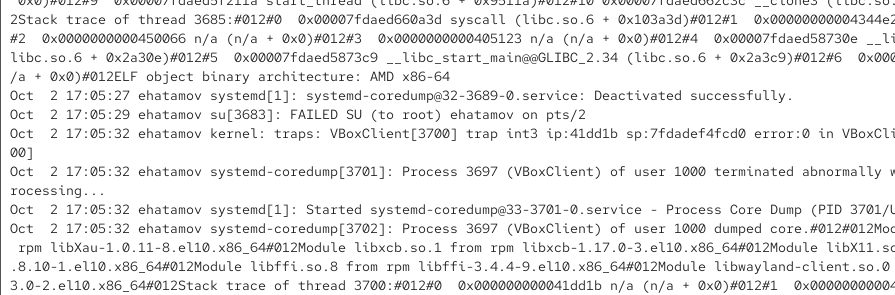
# 2 Отчёт по выполнению работы

## 2.1 Мониторинг журнала системных событий в реальном времени

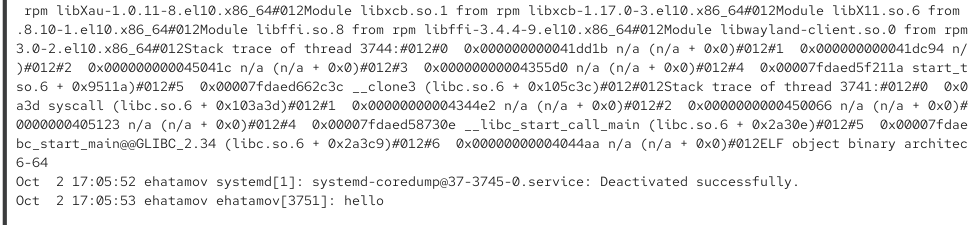
1. В трёх вкладках терминала были получены права администратора с помощью команды su -.  
   После успешного ввода пароля был осуществлён вход под пользователем root.
2. Во второй вкладке был запущен мониторинг системных событий в реальном времени с помощью команды tail -f /var/log/messages.  
   На экране начали отображаться текущие системные сообщения, включая информацию о работе служб и процессах пользователя.

* 
* Рис. 1: Мониторинг системных событий через tail -f /var/log/messages

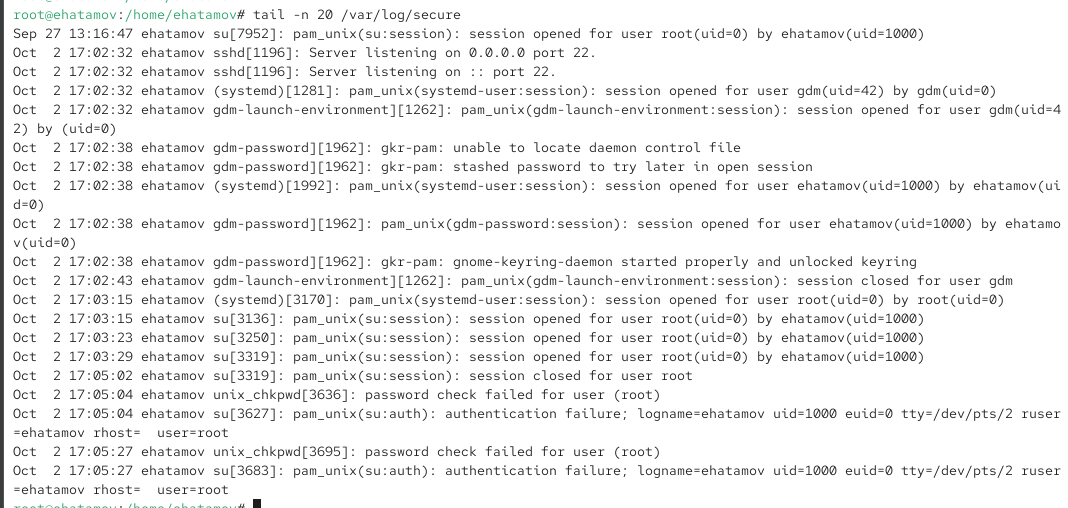
1. В третьей вкладке из оболочки пользователя была выполнена попытка получить права администратора с помощью команды su -, однако был введён неверный пароль.  
   В результате в окне мониторинга (во второй вкладке) отобразилось сообщение об ошибке:  
   FAILED SU (to root) ehatamov on pts/2  
   Это свидетельствует о неудачной попытке аутентификации при переходе в режим суперпользователя.

* 
* Рис. 2: Ошибка при попытке получить права root с неверным паролем

1. Затем пользователь ehatamov ввёл команду logger hello.  
   После выполнения этой команды в терминале с мониторингом появилось сообщение ehatamov: hello, что подтверждает успешную запись пользовательского сообщения в системный журнал.

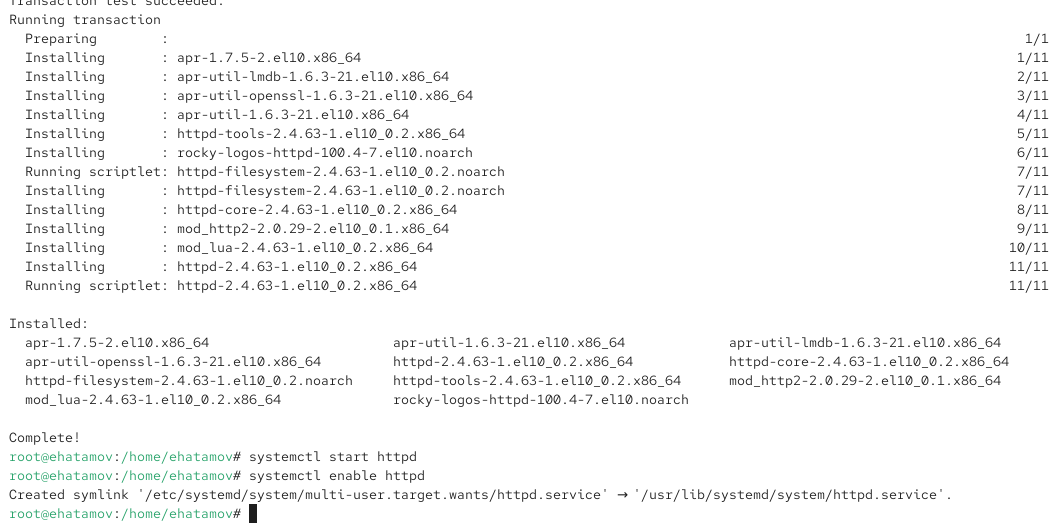
* 
* Рис. 3: Фиксация пользовательского сообщения в системном журнале через logger

1. Мониторинг системных сообщений был остановлен сочетанием клавиш Ctrl + C.  
   Затем для анализа журнала безопасности были выведены последние 20 строк файла /var/log/secure с помощью команды tail -n 20 /var/log/secure.  
   В результате отобразились записи, подтверждающие предыдущие действия — успешные и неудачные попытки входа, а также обращения к системным службам.

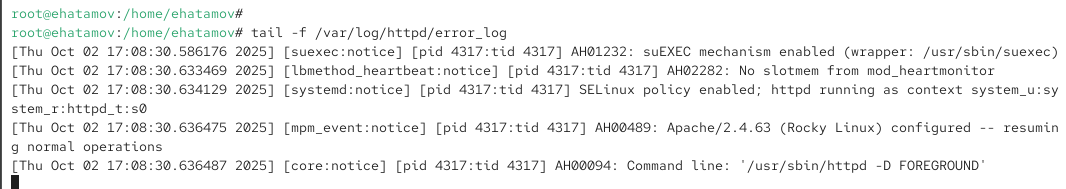
* 
* Рис. 4: Просмотр последних строк файла /var/log/secure

## 2.2 Изменение правил rsyslog.conf

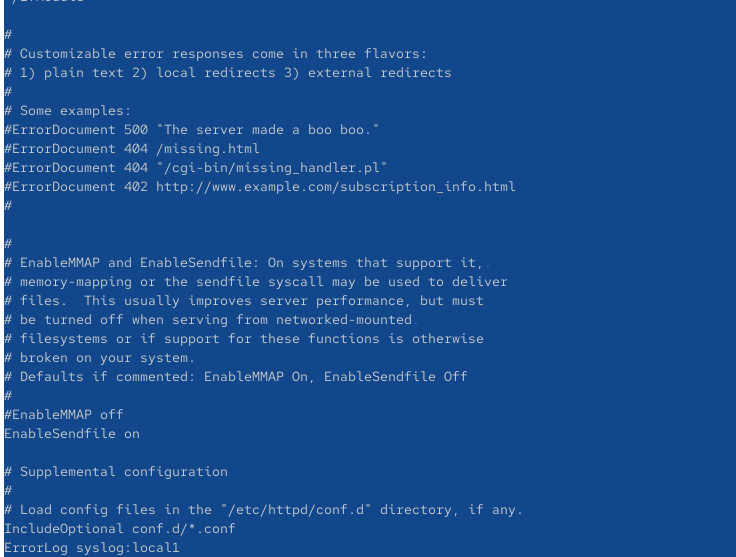
1. В первой вкладке терминала был установлен веб-сервер Apache с помощью команды dnf -y install httpd.  
   После завершения установки служба была запущена и добавлена в автозагрузку при помощи команд systemctl start httpd и systemctl enable httpd.  
   Успешное выполнение команд подтвердило корректную установку и активацию сервиса.

* 
* Рис. 5: Установка и запуск веб-сервера Apache

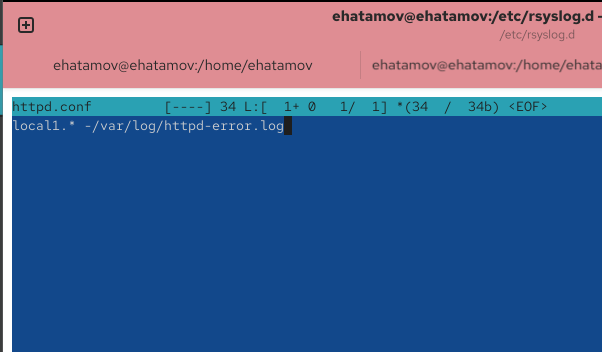
1. Во второй вкладке был запущен мониторинг журнала ошибок веб-службы Apache: tail -f /var/log/httpd/error\_log.  
   В журнале отобразились стандартные служебные сообщения о запуске Apache и активации модулей.

* 
* Рис. 6: Мониторинг журнала ошибок Apache

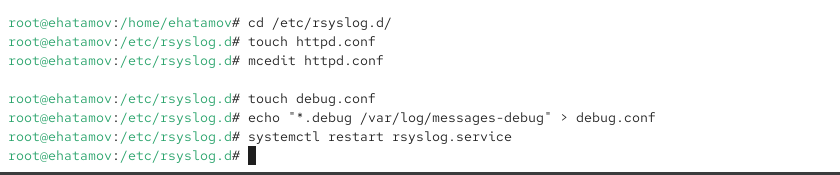
1. В третьей вкладке терминала в файле /etc/httpd/conf/httpd.conf была добавлена строка ErrorLog syslog:local1.  
   Это позволило перенаправить сообщения об ошибках веб-службы в системный журнал через механизм syslog.

* 
* Рис. 7: Добавление строки ErrorLog syslog:local1 в конфигурацию Apache

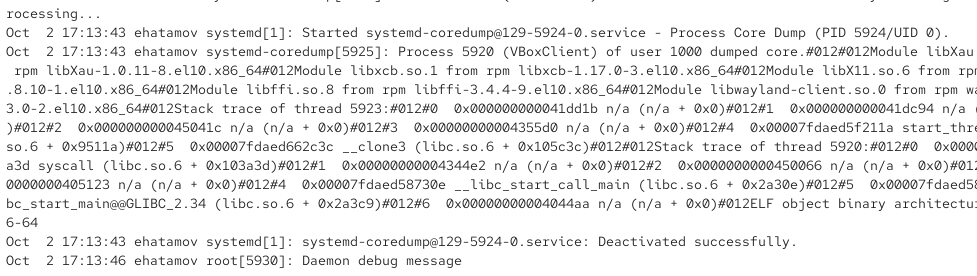
1. Для настройки приёма сообщений от Apache в каталоге /etc/rsyslog.d был создан новый файл конфигурации httpd.conf.  
   В него была добавлена строка local1.\* -/var/log/httpd-error.log, направляющая все сообщения категории local1 в отдельный лог-файл /var/log/httpd-error.log.

* 
* Рис. 8: Создание конфигурационного файла httpd.conf в /etc/rsyslog.d

1. После внесения изменений служба rsyslog была перезапущена с помощью команды systemctl restart rsyslog.service для применения новых настроек.
2. Далее был создан отдельный файл конфигурации debug.conf для мониторинга отладочной информации.  
   В этот файл была добавлена строка “\*.debug /var/log/messages-debug”, направляющая все сообщения уровня debug в файл /var/log/messages-debug.  
   После редактирования службы rsyslog была снова перезапущена.

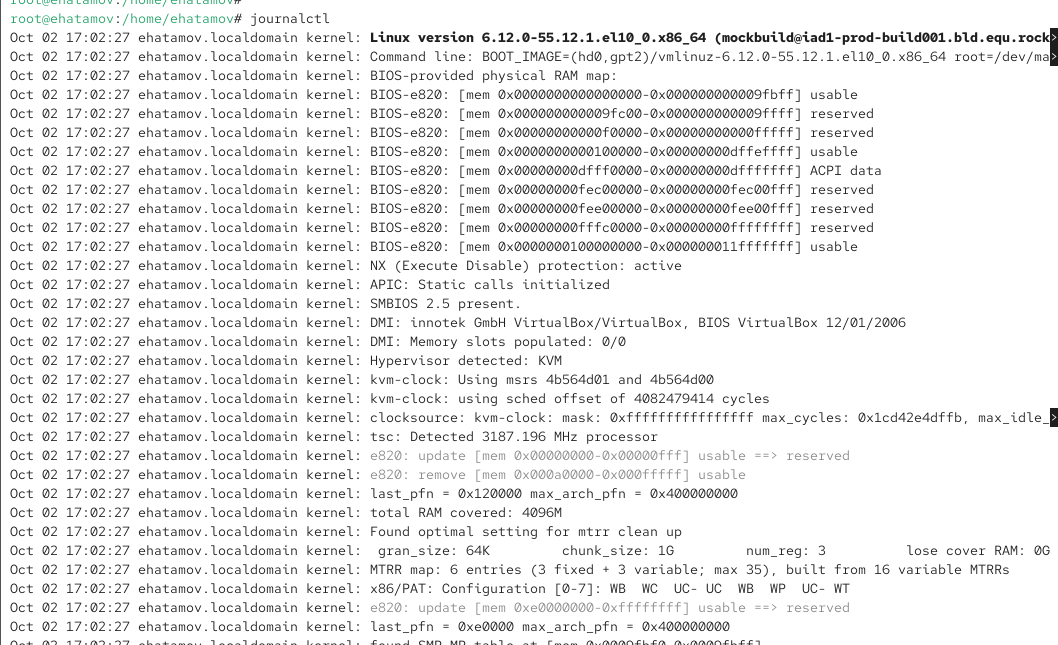
* 
* Рис. 9: Создание файлов конфигурации httpd.conf и debug.conf, настройка вывода сообщений уровня debug

1. Для проверки работы механизма логирования был запущен мониторинг отладочного журнала командой tail -f /var/log/messages-debug.  
   Затем было создано тестовое сообщение через команду logger -p daemon.debug “Daemon debug message”.  
   В окне мониторинга появилось сообщение от root, подтверждающее успешную запись события в отладочный лог.

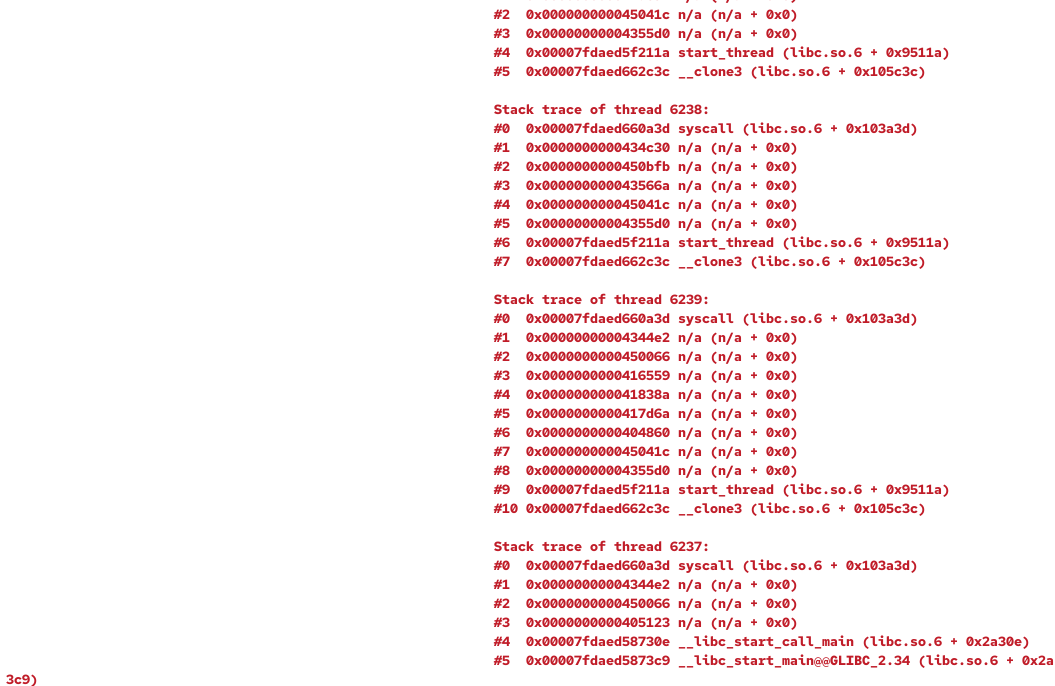
* 
* Рис. 10: Проверка работы отладочного логирования в messages-debug

## 2.3 Использование journalctl

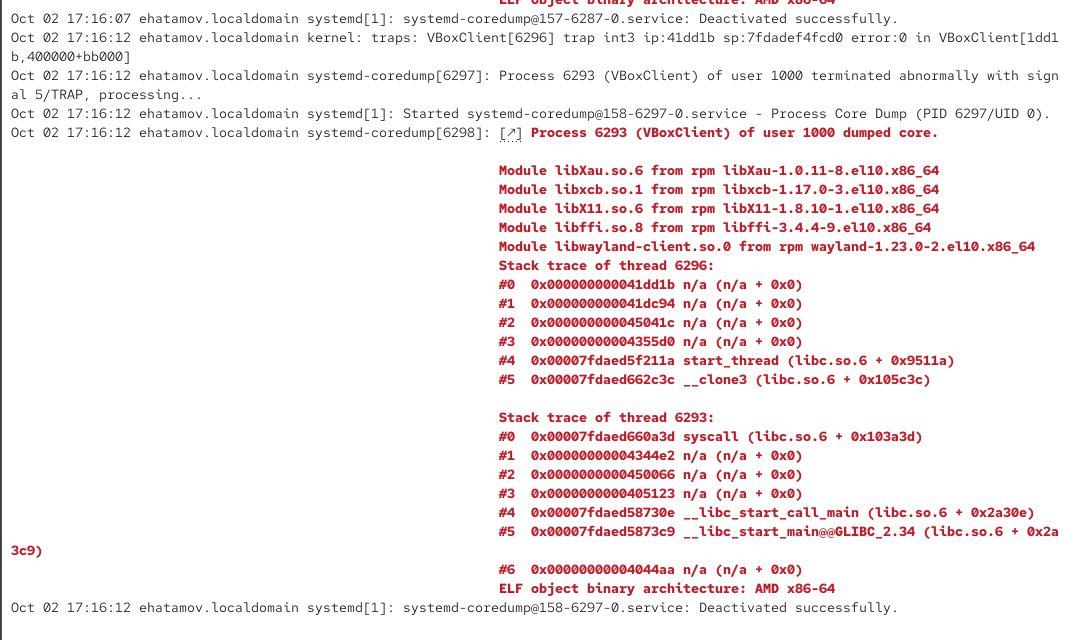
1. Во второй вкладке терминала было выполнено отображение содержимого системного журнала с момента последнего запуска системы с помощью команды journalctl.  
   В выводе отображались записи ядра и системных служб, включая данные о конфигурации виртуальной машины, аппаратных компонентах и запуске ядра.

* 
* Рис. 11: Просмотр системного журнала с момента загрузки системы

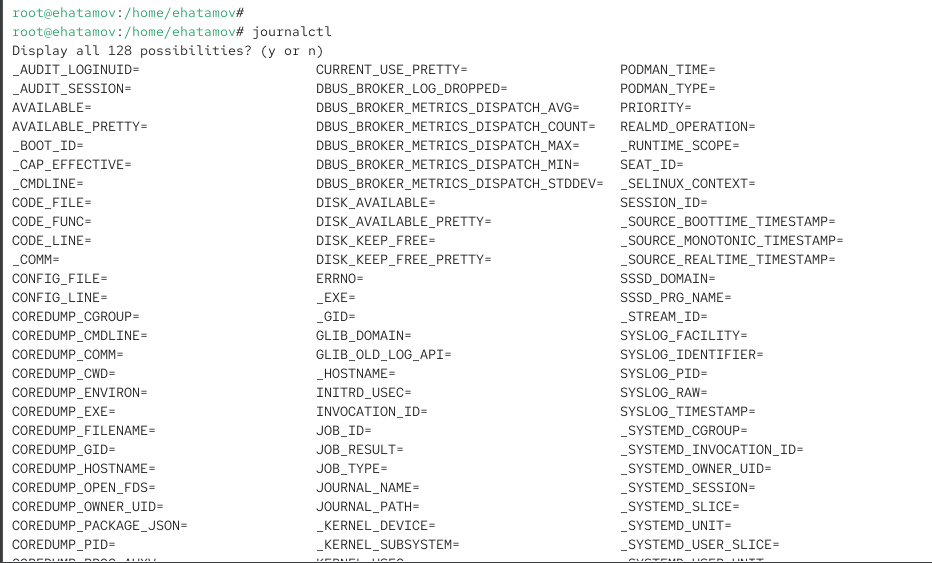
1. Для демонстрации сообщений без постраничного просмотра использовалась команда journalctl –no-pager.  
   В этом режиме весь вывод отображался сразу в окне терминала без ожидания действий пользователя.

* 
* Рис. 12: Просмотр системного журнала

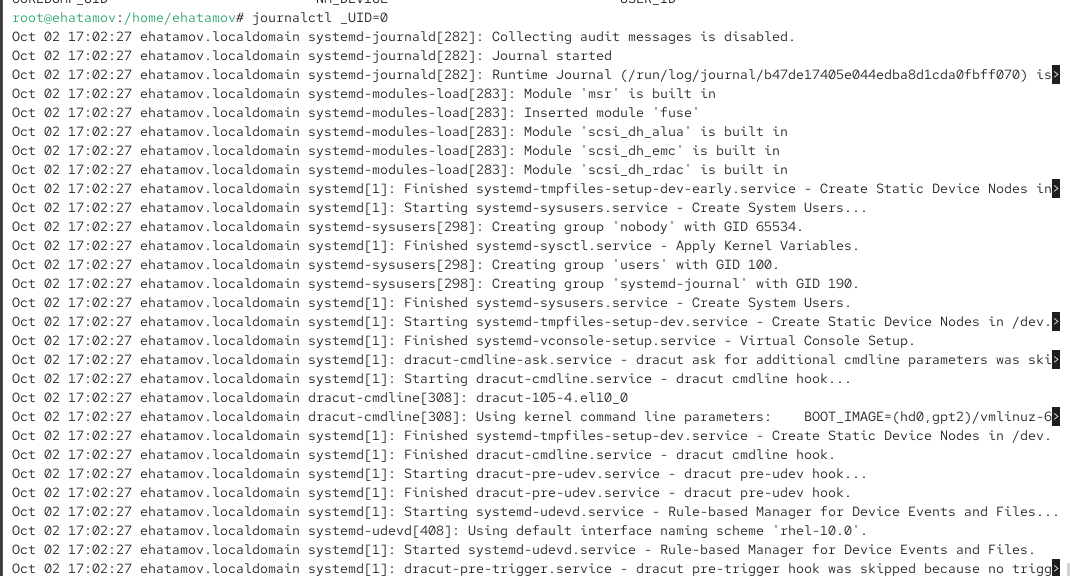
1. Далее был включён режим просмотра журнала в реальном времени с помощью journalctl -f.  
   Система отображала новые записи по мере их поступления. Выход из режима был выполнен сочетанием клавиш Ctrl + C.

* 
* Рис. 13: Просмотр системного журнала

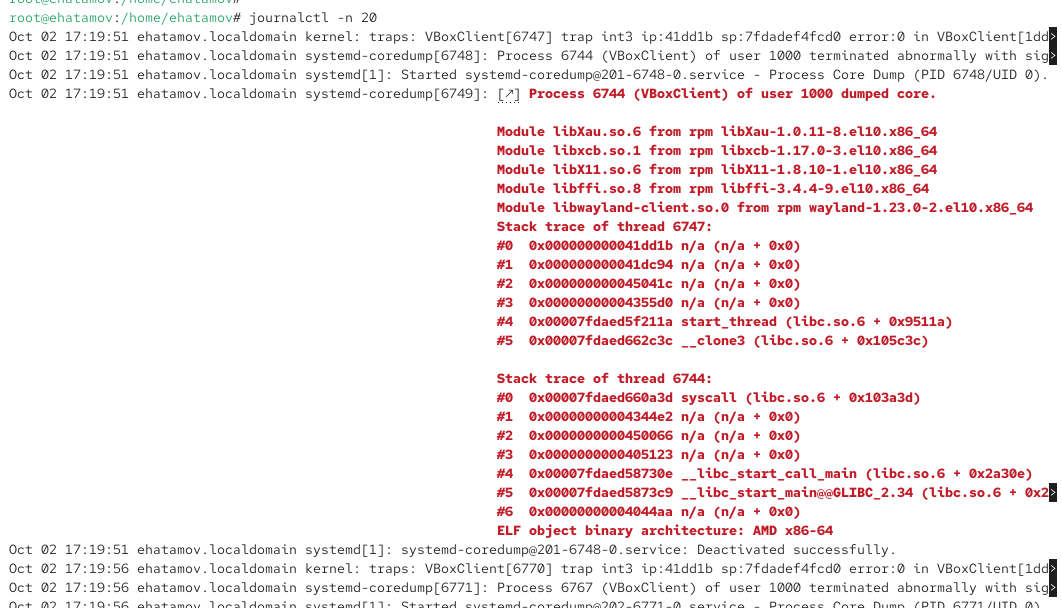
1. Для изучения параметров фильтрации командой journalctl дважды была нажата клавиша Tab.  
   Терминал вывел список доступных фильтров, позволяющих отбирать события по различным полям — времени, пользователю, типу службы и другим параметрам.

* 
* Рис. 14: Просмотр доступных параметров фильтрации journalctl

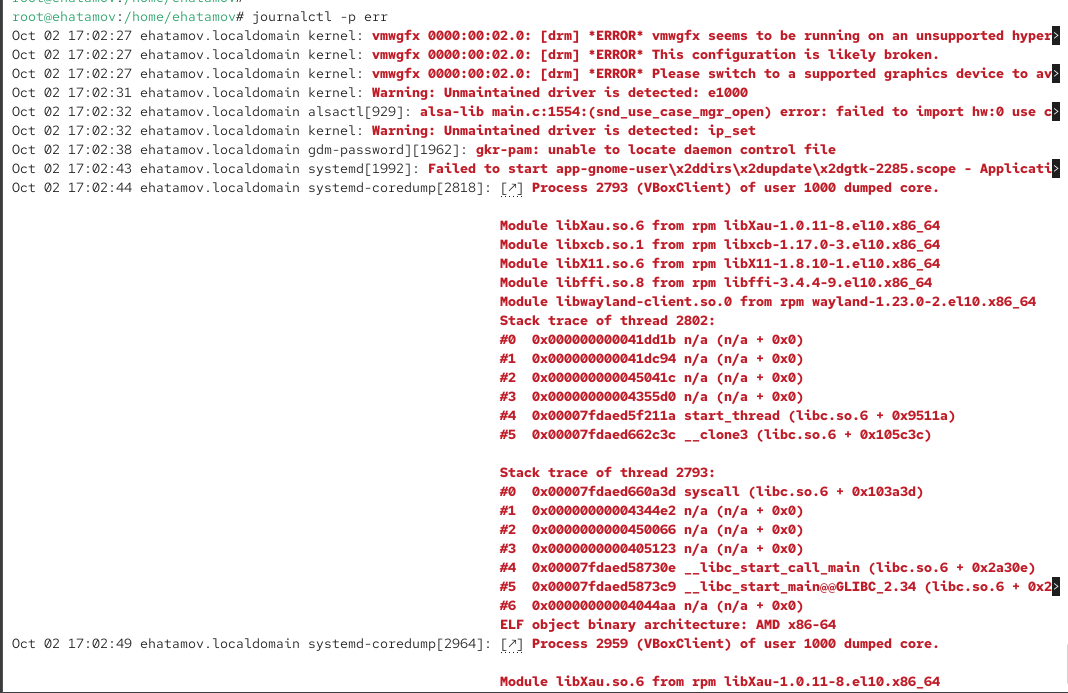
1. Для анализа событий, связанных с пользователем root, использовалась команда journalctl \_UID=0.  
   В выводе отобразились записи, связанные с действиями суперпользователя и служб, запущенных от имени root.

* 
* Рис. 15: Просмотр событий для пользователя root (UID 0)

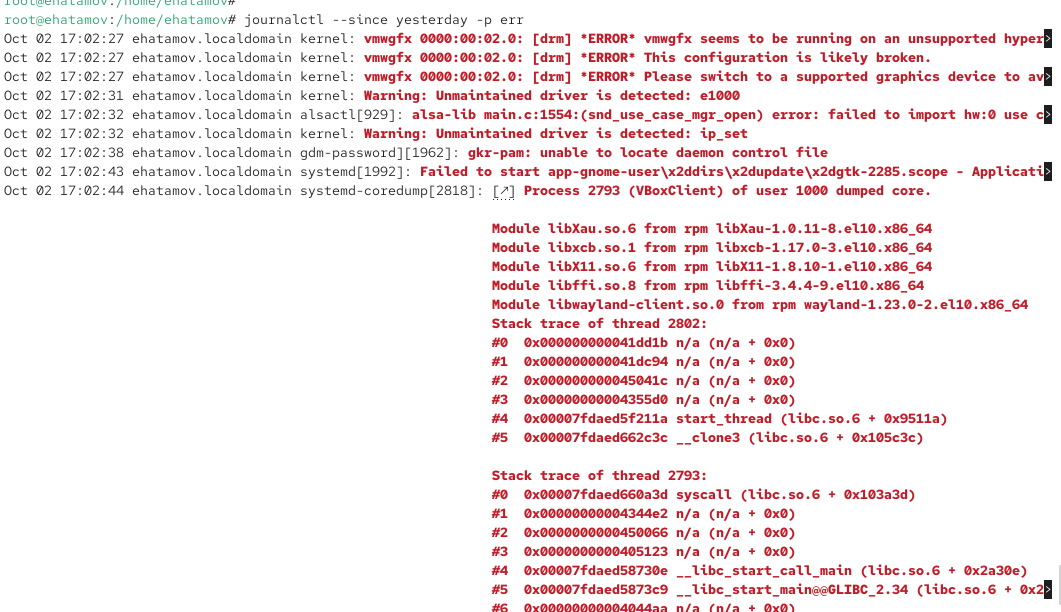
1. Для вывода последних двадцати строк журнала была выполнена команда journalctl -n 20.  
   В результате были показаны свежие записи системных событий, включая ошибки и отчёты ядра.

* 
* Рис. 16: Просмотр последних строк системного журнала

1. Для отображения только сообщений об ошибках применялась команда journalctl -p err.  
   В результате вывелись сообщения уровня “error”, включая ошибки графического адаптера и сбои процессов VBoxClient.

* 
* Рис. 17: Вывод сообщений уровня ошибок

1. Для выборки сообщений за определённый период времени была использована команда journalctl –since yesterday.  
   В журнале отобразились все события, зафиксированные со вчерашнего дня.
2. Для фильтрации только ошибок за этот же период применялась команда journalctl –since yesterday -p err.  
   Отобразились сообщения, зарегистрированные со вчерашнего дня и имеющие уровень ошибки, включая сбои и предупреждения.

* 
* Рис. 18: Фильтрация сообщений об ошибках со вчерашнего дня

1. Для вывода подробной информации о событиях использовался параметр -o verbose, который позволяет просматривать расширенные метаданные каждой записи — идентификаторы процессов, временные метки и параметры системы.

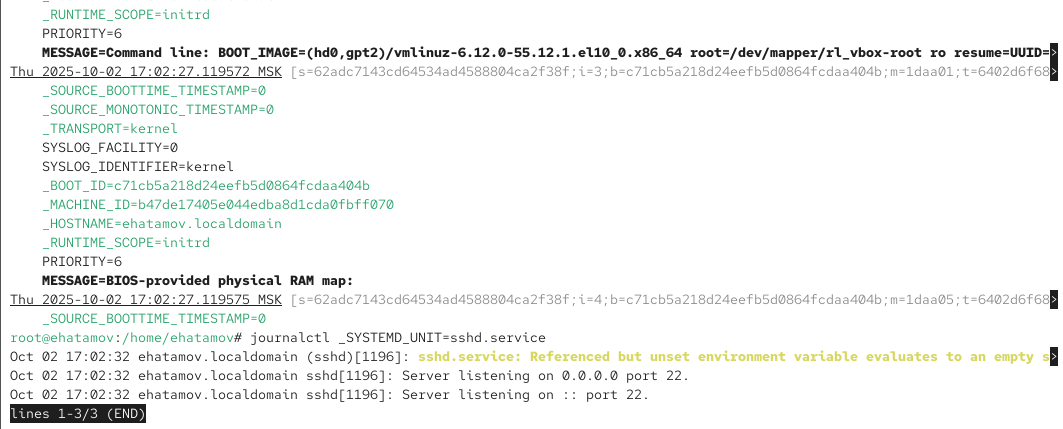
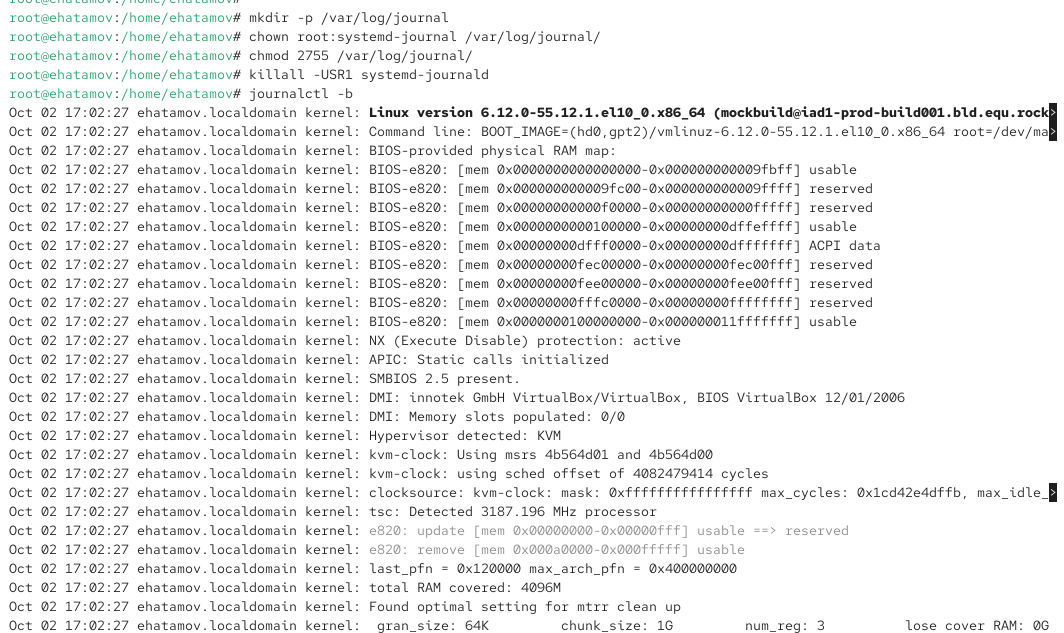


Рис. 19: Просмотр подробной информации о событиях с параметром verbose

1. Для анализа работы службы sshd была выполнена команда journalctl \_SYSTEMD\_UNIT=sshd.service.  
   В результате отображались записи, связанные с запуском и работой SSH-сервера, включая сообщения о прослушивании порта 22.

## 2.4 Постоянный журнал journald

1. В терминале были получены права администратора для выполнения системных операций.
2. Был создан каталог для хранения постоянного журнала systemd:  
   /var/log/journal  
   Этот каталог используется для записи системных событий на диск, обеспечивая их сохранение даже после перезагрузки системы.
3. Для корректной работы службы journald были изменены права доступа к каталогу:  
   владельцем назначен root, а группой — systemd-journal.  
   Также были установлены права 2755, что разрешает доступ на чтение и запись процессам, связанным с journald.
4. Для применения изменений была отправлена команда killall -USR1 systemd-journald, сигнализирующая службе journald о необходимости обновления конфигурации без полной перезагрузки системы.
5. После выполнения настроек журнал systemd стал постоянным.  
   Для проверки отображения сообщений с момента последней перезагрузки использовалась команда journalctl -b.  
   В выводе отобразились системные записи ядра, параметры запуска и аппаратная информация.

* 
* Рис. 20: Настройка постоянного хранения журнала journald

# 3 Контрольные вопросы

1. **Какой файл используется для настройки rsyslogd?**
   * Основной конфигурационный файл — /etc/rsyslog.conf.
   * Дополнительные правила могут храниться в отдельных файлах в каталоге /etc/rsyslog.d/.
2. **В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?**
   * Сообщения, связанные с аутентификацией, 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 (weekly)**, а старые файлы обычно сохраняются до **4 недель**.
   * Эти параметры задаются в файле /etc/logrotate.conf.
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
   * Это правило направляет все сообщения уровня **info** и выше в отдельный лог-файл.
5. **Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?**
   * Для просмотра сообщений в реальном времени используется команда:
   * journalctl -f
   * Аналог команды tail -f для системного журнала.
6. **Какая команда позволяет вам видеть все сообщения журнала, которые были написаны для PID 1 между 9:00 и 15:00?**
   * Для выборки сообщений по идентификатору процесса и времени используется команда:
   * journalctl \_PID=1 --since "09:00:00" --until "15:00:00"
7. **Какая команда позволяет вам видеть сообщения journald после последней перезагрузки системы?**
   * Для вывода сообщений, относящихся к текущему сеансу загрузки, используется команда:
   * journalctl -b
8. **Какая процедура позволяет сделать журнал journald постоянным?**
   * Чтобы сделать журнал systemd постоянным, необходимо:
     1. Создать каталог /var/log/journal.
     2. Установить права доступа:
     + chown root:systemd-journal /var/log/journal  
       chmod 2755 /var/log/journal
     1. Применить изменения без перезагрузки:
     + killall -USR1 systemd-journald
     + После этого логи journald будут сохраняться на диск и не теряться после перезагрузки.

# 4 Заключение

В ходе выполнения работы были изучены принципы функционирования системных журналов в Linux, а также механизмы их ведения и анализа с помощью служб **rsyslog** и **systemd-journald**.  
Были рассмотрены способы настройки файлов конфигурации, перенаправления сообщений по уровням приоритета, создания собственных логов для приложений и организации постоянного хранения записей.  
Кроме того, была освоена работа с утилитой **journalctl**, включая применение фильтров, просмотр сообщений в реальном времени и анализ событий по конкретным параметрам.