Отчёт по лабораторной работе №7

Управление журналами событий в системе

Максат Хемраев

Содержание

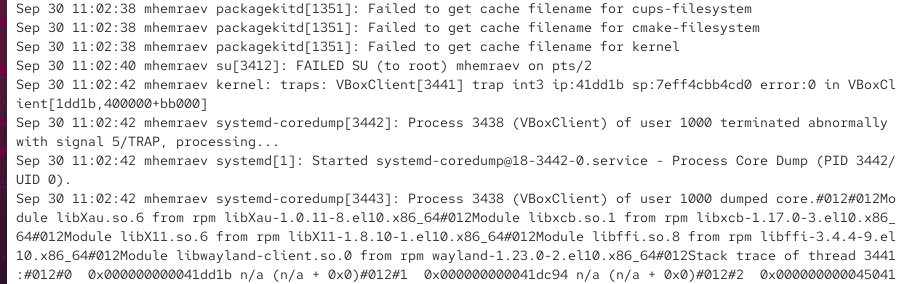
# 1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

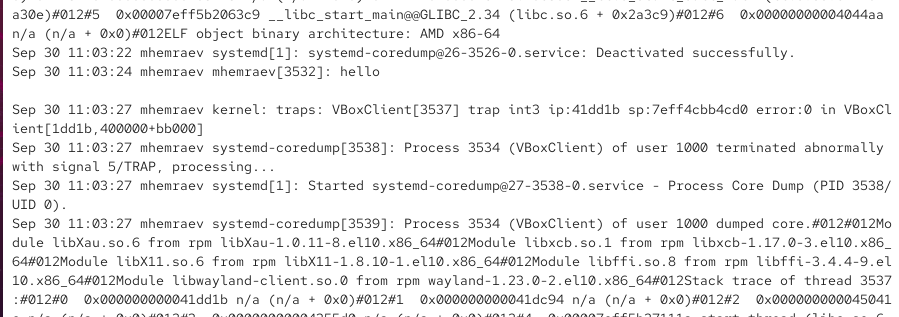
# 2 Отчёт по выполнению работы

## 2.1 Мониторинг журнала системных событий в реальном времени

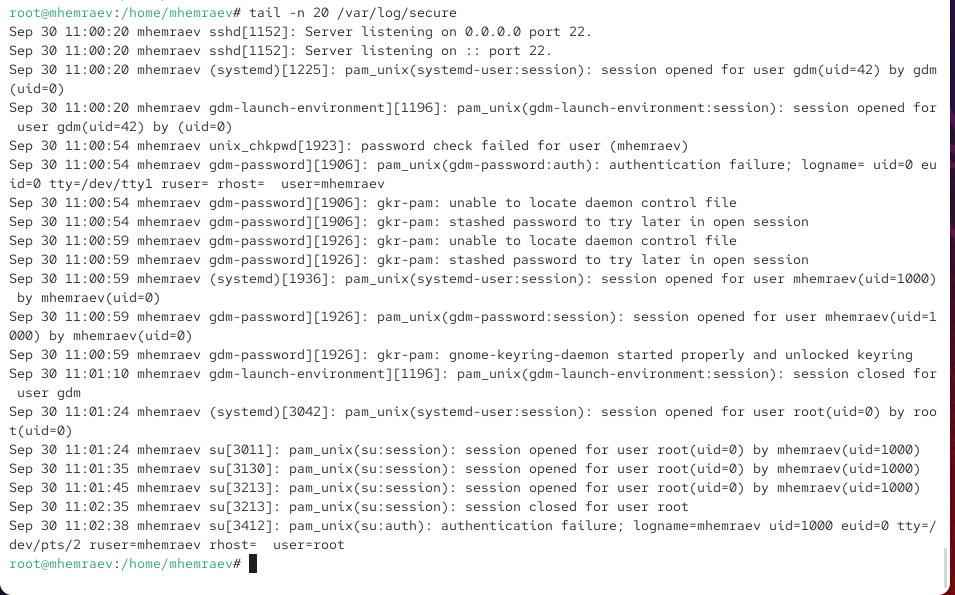
1. В трёх вкладках терминала были получены полномочия администратора с помощью команды su -.
2. Во второй вкладке терминала был запущен мониторинг системных сообщений в реальном времени.  
   Это позволило отслеживать любые события, которые фиксируются в файле журнала: tail -f /var/log/messages.

* 
* Рис. 1: Мониторинг системных сообщений

1. В третьей вкладке терминала была выполнена попытка перехода к суперпользователю с заведомо неверным паролем.  
   В результате в окне с мониторингом отобразилось сообщение об ошибке авторизации:  
   «FAILED SU (to root) mhemraev on pts/2».

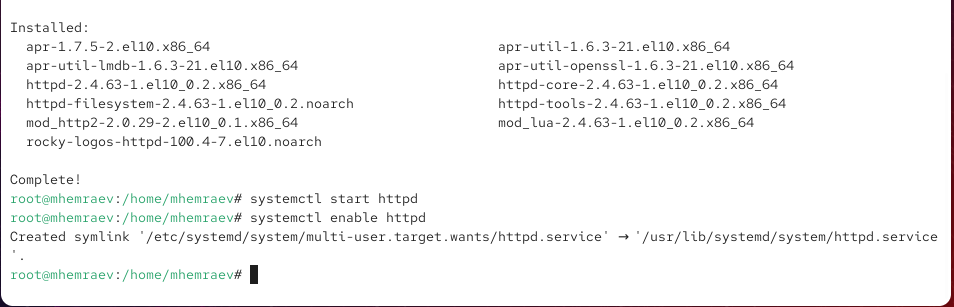
* 
* Рис. 2: Ошибка аутентификации при su

1. Затем, находясь под учётной записью обычного пользователя, была выполнена команда logger hello.  
   Сообщение hello отобразилось в окне мониторинга и одновременно было записано в файл /var/log/messages.
2. После этого мониторинг сообщений /var/log/messages был остановлен сочетанием клавиш **Ctrl + C**.  
   Далее был выполнен анализ журнала безопасности с помощью просмотра последних строк файла /var/log/secure:  
   tail -n 20 /var/log/secure.

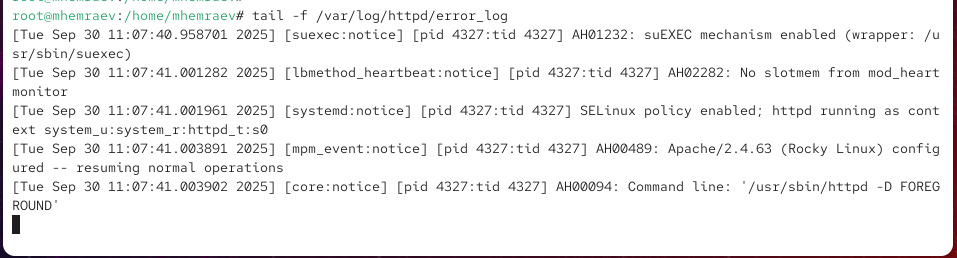
* На экране отобразились записи, связанные с неудачными попытками авторизации и действиями с полномочиями суперпользователя.
* 
* Рис. 3: Проверка журнала /var/log/secure

## 2.2 Изменение правил rsyslog.conf

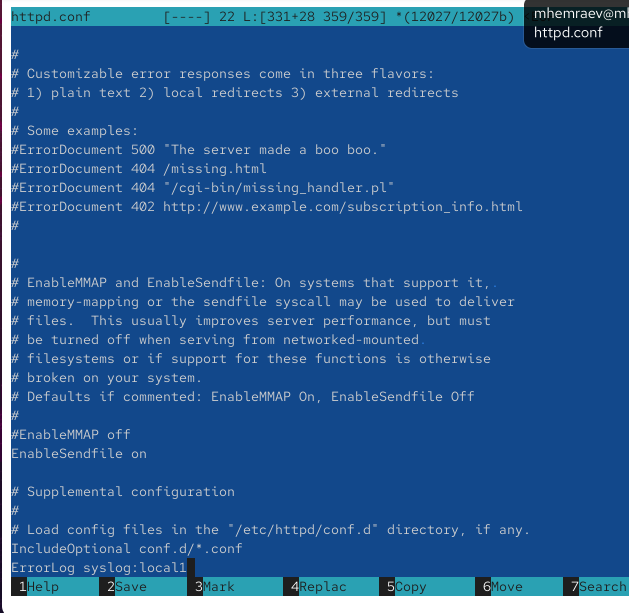
1. В первой вкладке терминала была выполнена установка веб-сервера Apache.  
   После завершения установки служба httpd была запущена и добавлена в автозагрузку.

* 
* Рис. 4: Установка и запуск Apache

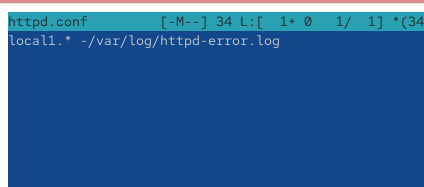
1. Во второй вкладке терминала был просмотрен журнал ошибок веб-службы с помощью трассировки файла /var/log/httpd/error\_log.  
   На экране отобразились сообщения о запуске и настройке httpd.

* 
* Рис. 5: Просмотр журнала ошибок Apache

1. В третьей вкладке терминала был открыт конфигурационный файл /etc/httpd/conf/httpd.conf.  
   В его конец была добавлена строка ErrorLog syslog:local1, что перенаправило регистрацию ошибок веб-сервера через syslog.

* 
* Рис. 6: Редактирование httpd.conf

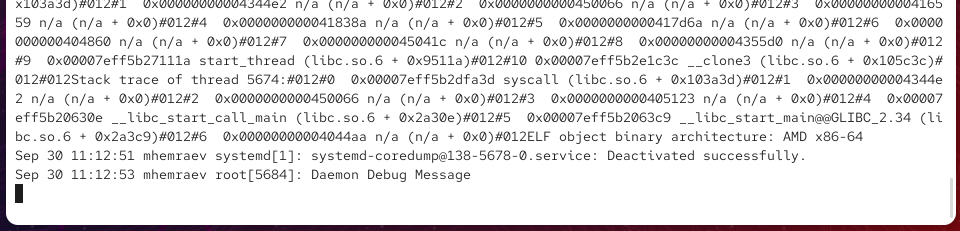
1. В каталоге /etc/rsyslog.d был создан файл httpd.conf.  
   В нём прописано правило local1.\* -/var/log/httpd-error.log, которое направляет все сообщения объекта **local1** в отдельный файл журнала ошибок Apache.

* 
* Рис. 7: Создание файла httpd.conf для rsyslog

1. В первой вкладке терминала были перезапущены службы **rsyslog** и **httpd** для применения новых правил.  
   После этого сообщения об ошибках веб-сервера стали записываться в файл /var/log/httpd-error.log.
2. В каталоге /etc/rsyslog.d был также создан файл debug.conf.  
   В нём прописано правило \*.debug /var/log/messages-debug, что позволяет перенаправлять все отладочные сообщения в отдельный лог.

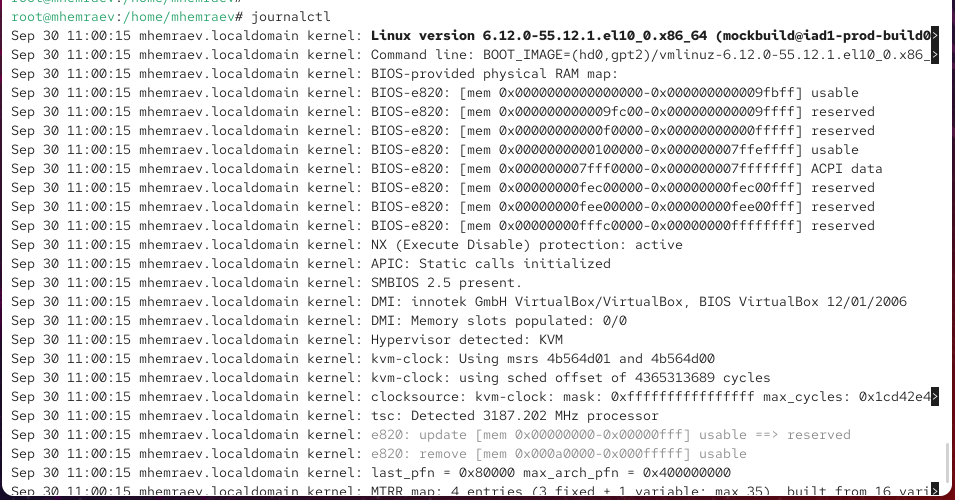
* 
* Рис. 8: Создание правила для отладки

1. После перезапуска службы rsyslog был включён мониторинг отладочных сообщений с помощью команды tail -f /var/log/messages-debug.
2. В третьей вкладке терминала была отправлена отладочная запись:  
   logger -p daemon.debug "Daemon Debug Message".  
   Сообщение успешно появилось в журнале /var/log/messages-debug, что подтверждает корректность настроек.

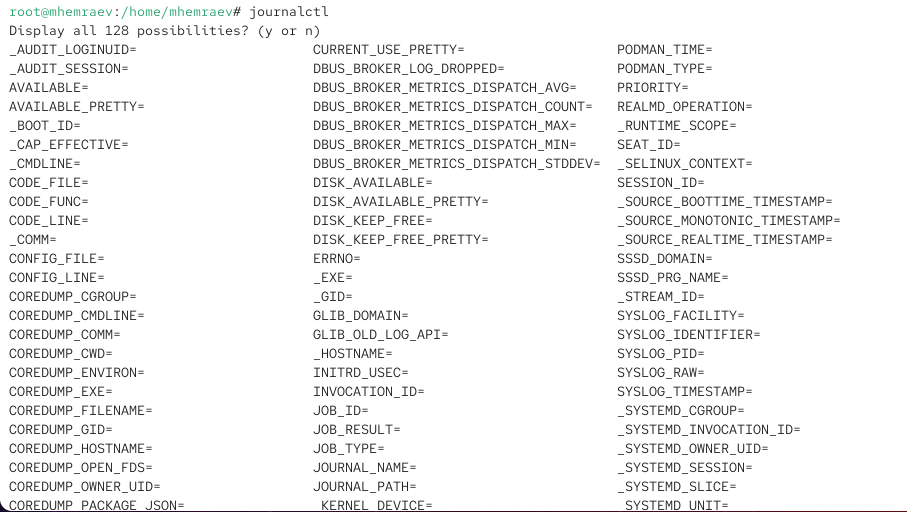
* 
* Рис. 9: Проверка отладочного сообщения

## 2.3 Использование journalctl

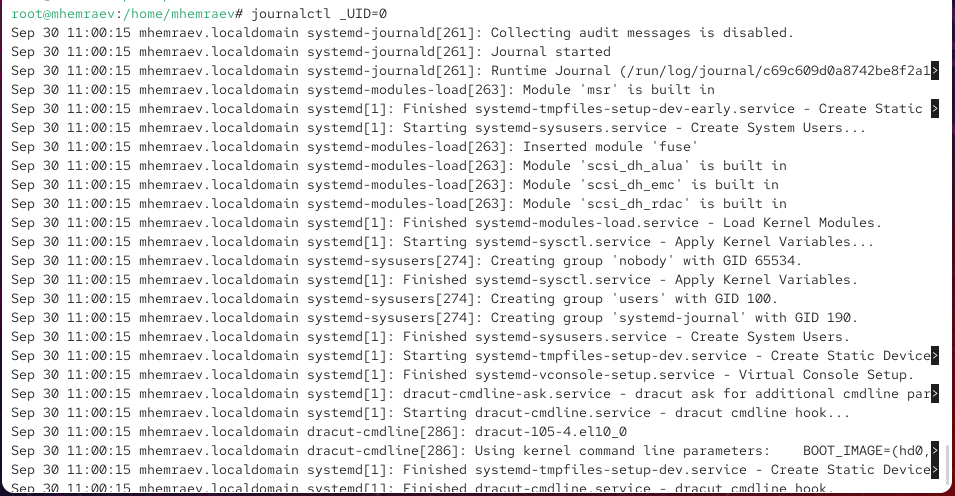
1. Во второй вкладке терминала был просмотрен журнал с событиями, начиная с момента последней загрузки системы.  
   Для перемещения использовались клавиши Enter (построчно) и пробел (постранично), выход осуществлялся клавишей q.

* 
* Рис. 10: Просмотр журнала systemd

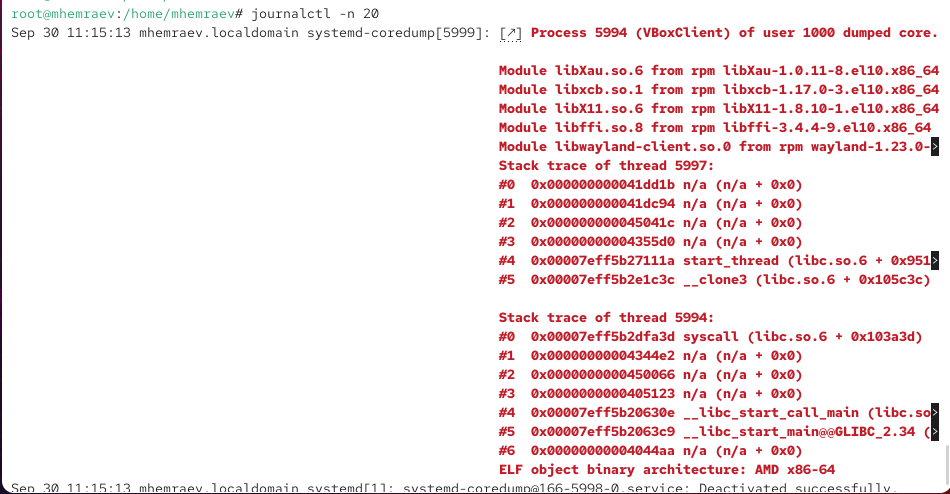
1. Журнал был выведен в консоль без применения постраничного пейджера.  
   Это позволило отобразить все записи сплошным списком: journalctl --no-pager.
2. Для наблюдения за событиями в реальном времени был активирован режим: journalctl -f.  
   Прерывание вывода выполнялось комбинацией **Ctrl + C**.
3. Для изучения доступных параметров фильтрации журнала была введена команда journalctl и дважды нажата клавиша **Tab**, что показало список из 128 возможных атрибутов.

* 
* Рис. 11: Фильтрация по параметрам

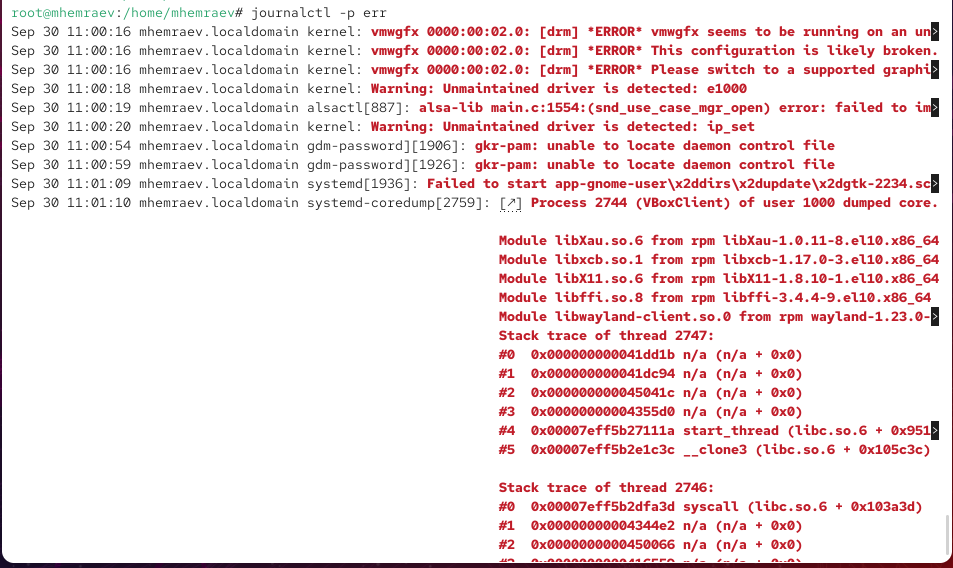
1. Далее был выполнен просмотр событий только для **UID 0** (суперпользователь).

* 
* Рис. 12: Фильтрация по UID 0

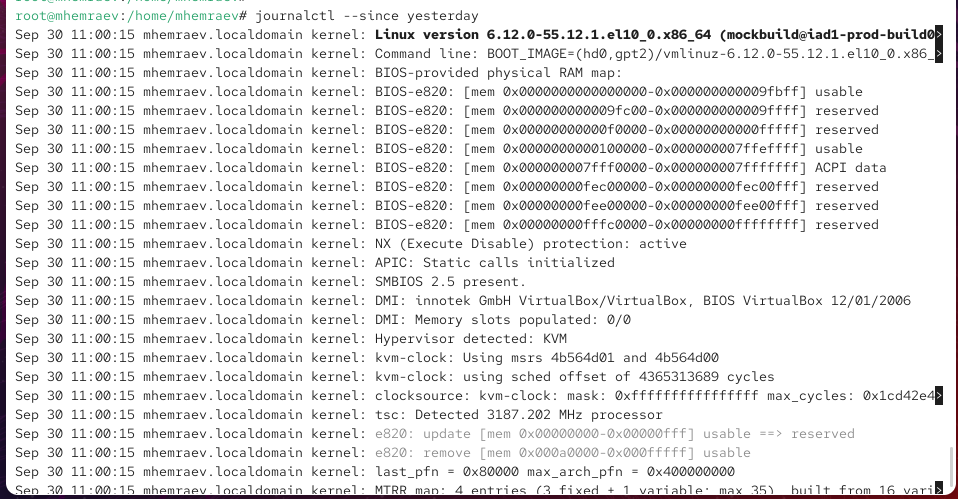
1. Для отображения последних строк журнала была использована команда: journalctl -n 20.

* 
* Рис. 13: Последние 20 строк журнала

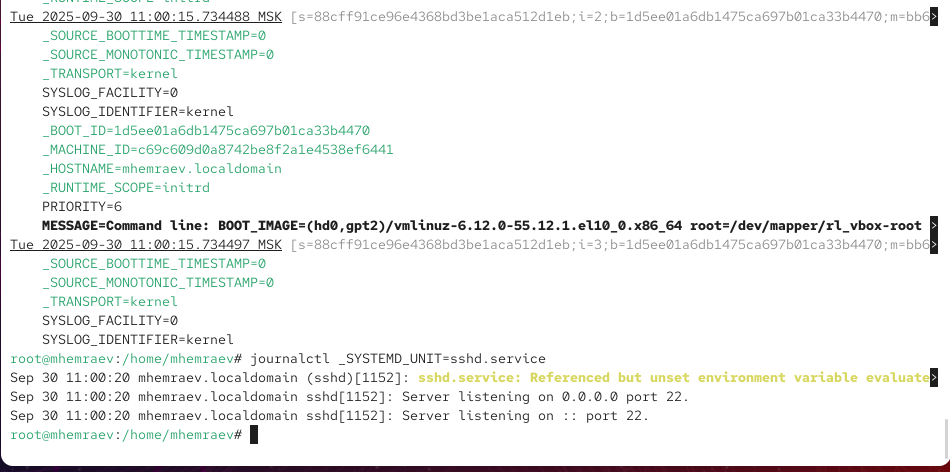
1. Для просмотра исключительно сообщений об ошибках был применён фильтр по приоритету: journalctl -p err.

* 
* Рис. 14: Ошибки в журнале

1. Для анализа сообщений за определённый период времени была использована опция --since.  
   Были просмотрены все события начиная со вчерашнего дня: journalctl --since yesterday.

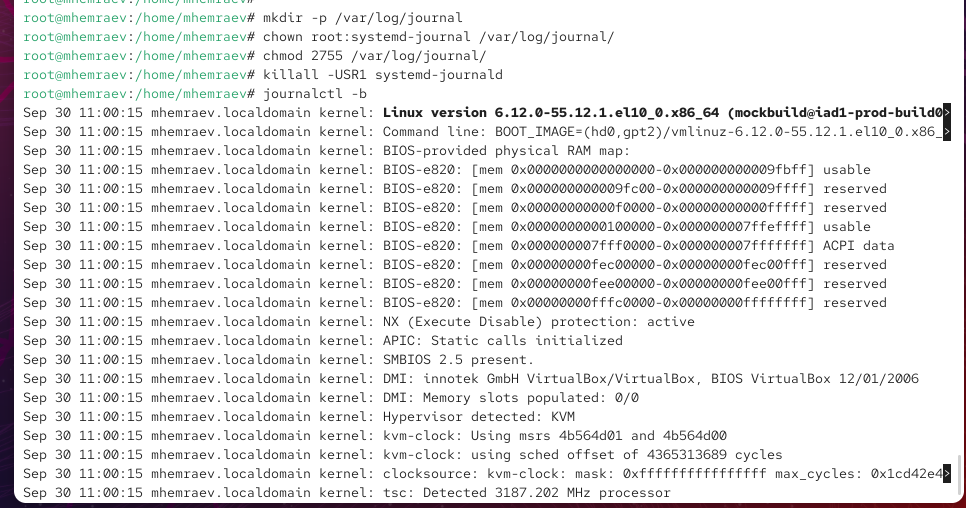
* 
* Рис. 15: Сообщения со вчерашнего дня

1. Для получения сообщений с уровнем ошибки начиная со вчерашнего дня использовалась команда:  
   journalctl --since yesterday -p err.
2. Для получения детальной информации о событиях был использован вывод в расширенном формате:  
   journalctl -o verbose.
3. Для изучения информации о модуле sshd были просмотрены соответствующие записи:  
   journalctl \_SYSTEMD\_UNIT=sshd.service.

* 
* Рис. 16: Просмотр событий для sshd

## 2.4 Постоянный журнал journald

1. В терминале были получены полномочия администратора.
2. Для хранения записей журнала был создан каталог /var/log/journal.
3. Были скорректированы права доступа к каталогу, чтобы служба **systemd-journald** могла записывать данные:
   * назначен владелец и группа root:systemd-journal;
   * установлены права доступа 2755.
4. Для применения изменений служба **systemd-journald** была уведомлена сигналом:  
   killall -USR1 systemd-journald.  
   После этого служба начала вести постоянный журнал.
5. Для проверки работы был выполнен просмотр записей текущей загрузки с помощью команды:  
   journalctl -b.  
   На экране отобразились системные сообщения, начиная с последнего запуска.

* 
* Рис. 17: Просмотр журнала текущей загрузки

# 3 Контрольные вопросы

### 3.0.1 1. Какой файл используется для настройки rsyslogd?

* Основной файл конфигурации: /etc/rsyslog.conf
* Дополнительные файлы: каталог /etc/rsyslog.d/

### 3.0.2 2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?

* Сообщения об аутентификации хранятся в /var/log/secure

### 3.0.3 3. Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?

* По умолчанию ротация выполняется еженедельно
* Настройки определяются в /etc/logrotate.conf

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

* В конфигурации следует прописать правило: \*.info /var/log/messages.info

### 3.0.5 5. Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?

* Для rsyslog используется команда tail -f /var/log/messages
* Для journald — команда journalctl -f

### 3.0.6 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”

### 3.0.7 7. Какая команда позволяет вам видеть сообщения journald после последней перезагрузки системы?

* journalctl -b

### 3.0.8 8. Какая процедура позволяет сделать журнал journald постоянным?

* Создать каталог /var/log/journal
* Назначить владельца root:systemd-journal
* Установить права доступа 2755
* Перезапустить journald сигналом USR1
* После этого записи журнала сохраняются постоянно

# 4 Заключение

В ходе работы были изучены основы журналирования в Linux, рассмотрены методы настройки службы rsyslog и systemd-journald, а также способы фильтрации и просмотра системных сообщений. Получены навыки создания постоянного журнала и применения правил для разделения логов по уровням важности.