Отчёт по лабораторной работе №7

Управление журналами событий в системе

Лабси Мохаммед

Содержание

# 1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

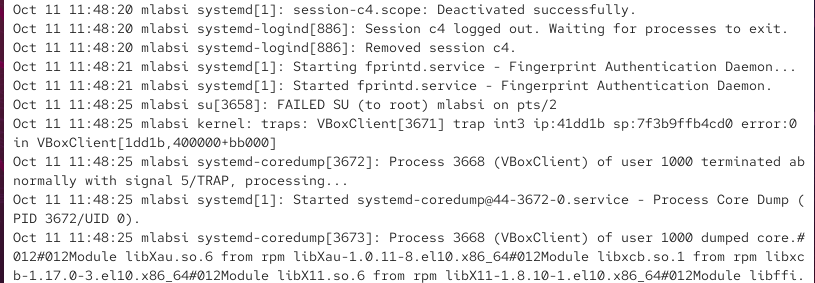
# 2 Ход выполнения

## 2.1 Мониторинг журнала системных событий в реальном времени

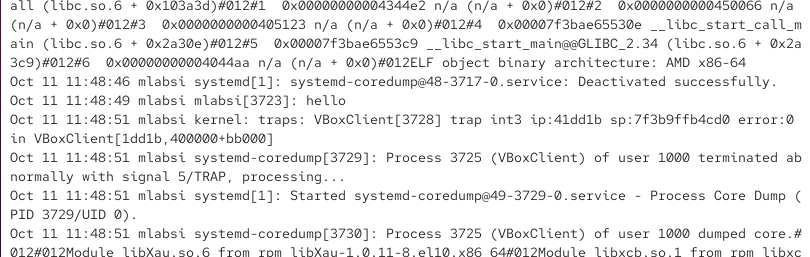
1. Во всех трёх вкладках терминала получены права администратора с помощью команды **su -**.
2. Во второй вкладке запущен мониторинг системных сообщений в реальном времени с помощью команды **tail -f /var/log/messages**.  
   На экране отображаются системные события, включая сообщения ядра и службы systemd.

* 
* Рис. 1: Мониторинг системных событий в реальном времени

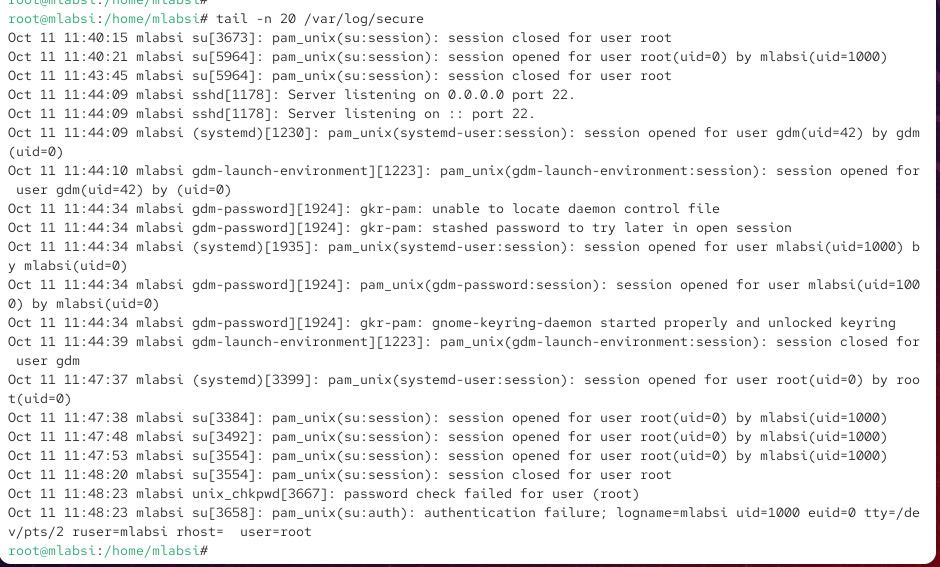
1. В третьей вкладке пользователь вышел из режима администратора (сочетанием **Ctrl + D**) и повторно попытался получить привилегии **root**, введя неверный пароль.  
   В журнале зафиксирована ошибка: **FAILED SU (to root) mlabsi on pts/2**.

* 
* Рис. 2: Ошибка авторизации при вводе неправильного пароля root

1. Из-под учётной записи пользователя введена команда **logger hello**.  
   В окне с мониторингом (вкладка 2) появилось сообщение, записанное также в файл **/var/log/messages**.

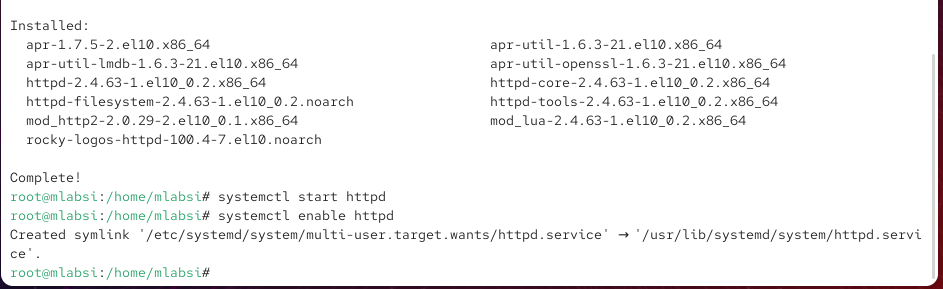
* 
* Рис. 3: Отображение пользовательского сообщения logger в системном журнале

1. После завершения трассировки комбинацией **Ctrl + C** был просмотрен журнал сообщений безопасности с помощью **tail -n 20 /var/log/secure**.  
   В логе отображены записи о попытках авторизации и ошибках при вводе пароля для root.

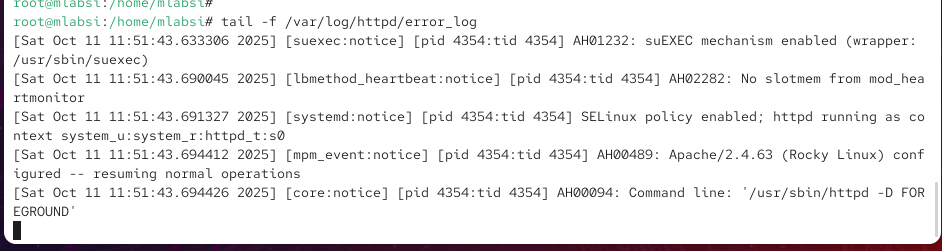
* 
* Рис. 4: Просмотр журнала /var/log/secure с записями об ошибках авторизации

## 2.2 Изменение правил rsyslog.conf

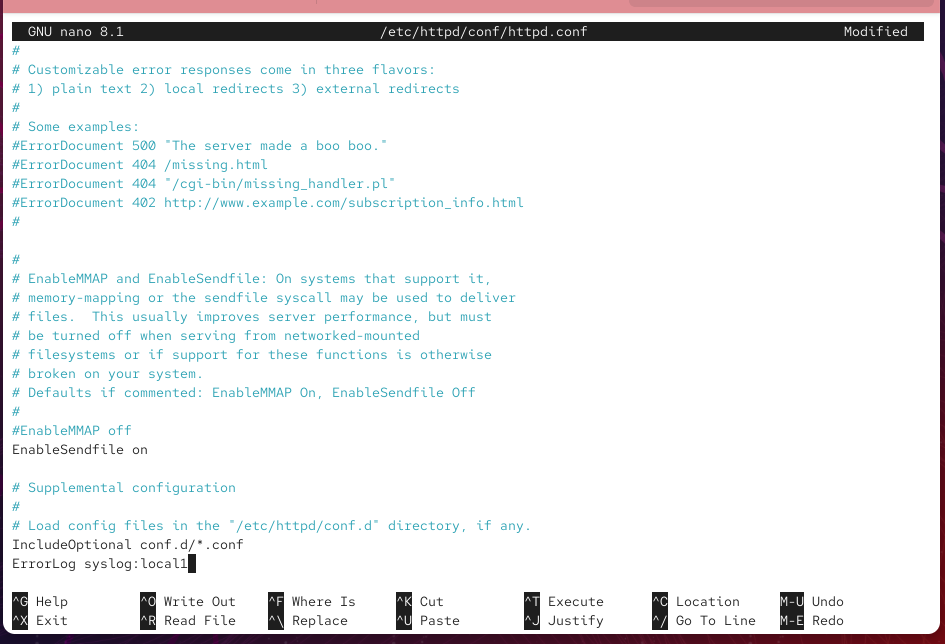
1. Установлен веб-сервер Apache. После завершения установки служба **httpd** была запущена и добавлена в автозагрузку при помощи команд **systemctl start httpd** и **systemctl enable httpd**.

* 
* Рис. 5: Установка и запуск службы Apache HTTPD

1. Во второй вкладке выполнен просмотр ошибок веб-сервера в реальном времени с помощью **tail -f /var/log/httpd/error\_log**.  
   В выводе отображаются уведомления об инициализации Apache и успешном запуске.

* 
* Рис. 6: Мониторинг журнала ошибок Apache в режиме реального времени

1. В файле **/etc/httpd/conf/httpd.conf** добавлена строка **ErrorLog syslog:local1**, что обеспечивает передачу сообщений веб-сервера в систему **syslog**.

* 
* Рис. 7: Добавление перенаправления логов в syslog в конфигурации Apache

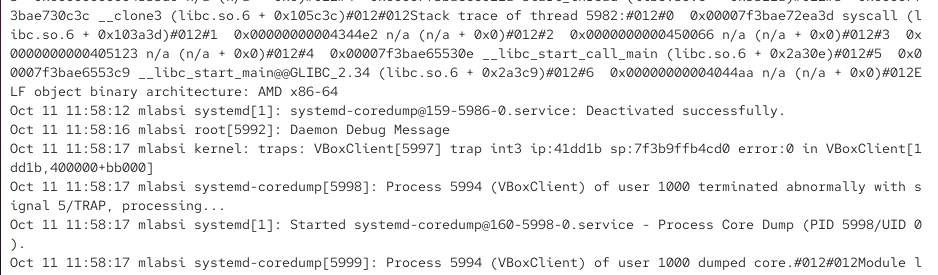
1. В каталоге **/etc/rsyslog.d** создан файл **httpd.conf**, в который добавлена строка **local1.\* -/var/log/httpd-error.log**.  
   Это правило перенаправляет все сообщения уровня **local1** в отдельный лог-файл **/var/log/httpd-error.log**.

* 
* Рис. 8: Создание файла конфигурации для логов Apache в rsyslog

1. В той же директории создан файл **debug.conf**, содержащий строку **\*.debug /var/log/messages-debug**, позволяющую сохранять отладочные сообщения в отдельный лог-файл.

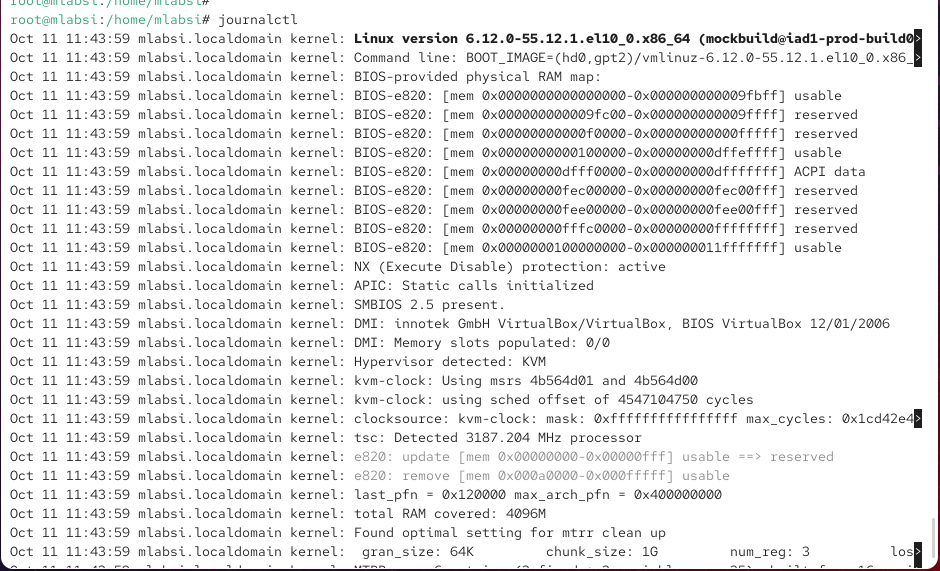
* 
* Рис. 9: Создание конфигурационного файла debug.conf для отладочных сообщений

1. После перезапуска служб **rsyslog** и **httpd** выполнена проверка перенаправления логов при помощи команды **logger -p daemon.debug “Daemon Debug Message”**.  
   В терминале с мониторингом (**tail -f /var/log/messages-debug**) появилось сообщение, подтверждающее корректную работу перенаправления отладочных событий.

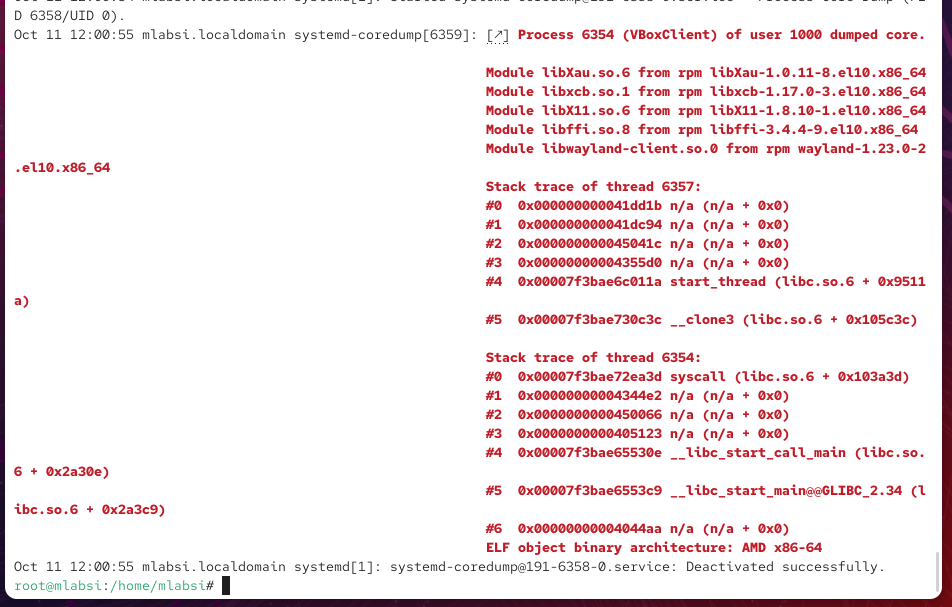
* 
* Рис. 10: Результат записи отладочного сообщения в лог /var/log/messages-debug

## 2.3 Использование journalctl

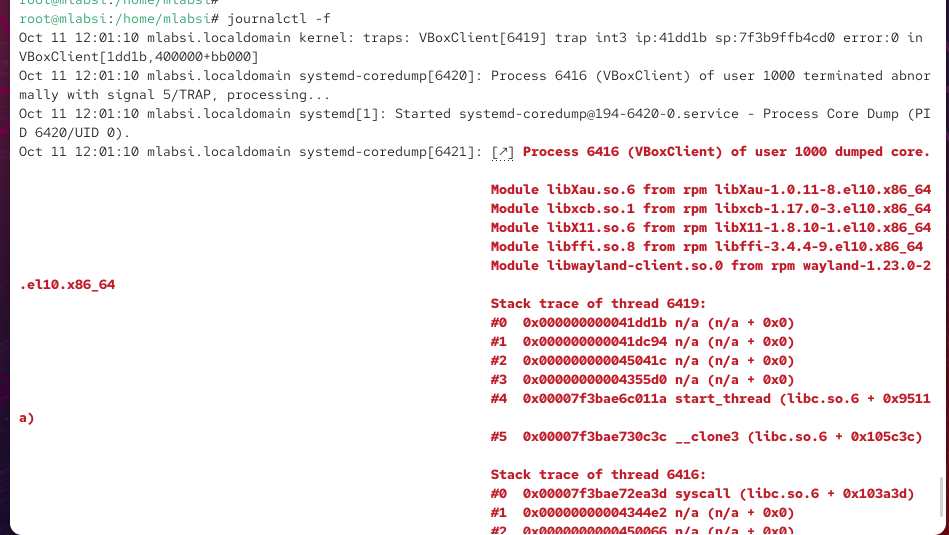
1. Во второй вкладке терминала было выполнено отображение системного журнала с момента последнего запуска системы с помощью команды **journalctl**.  
   В выводе отобразились записи о загрузке ядра и инициализации компонентов системы.

* 
* Рис. 11: Просмотр журнала с момента последнего запуска системы

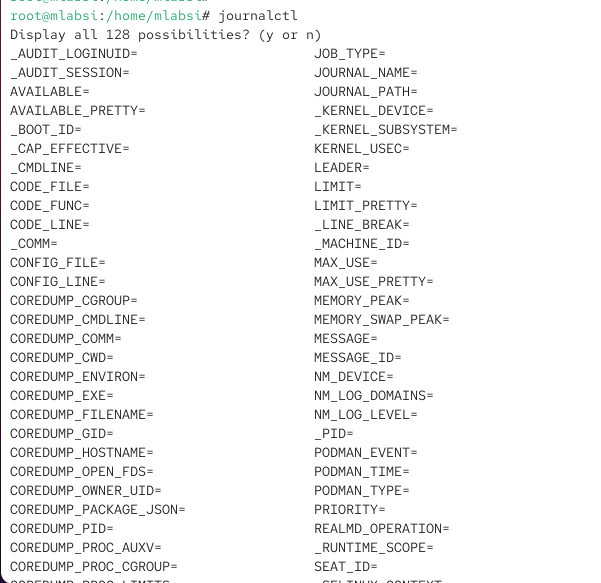
1. Для просмотра содержимого журнала без использования постраничного вывода была применена команда **journalctl –no-pager**, что позволило вывести весь журнал сразу на экран.
2. Включён режим просмотра событий в реальном времени при помощи **journalctl -f**.  
   На экране отображались текущие системные сообщения и диагностическая информация о работе процессов.

* 
* Рис. 12: Мониторинг системных событий в реальном времени через journalctl

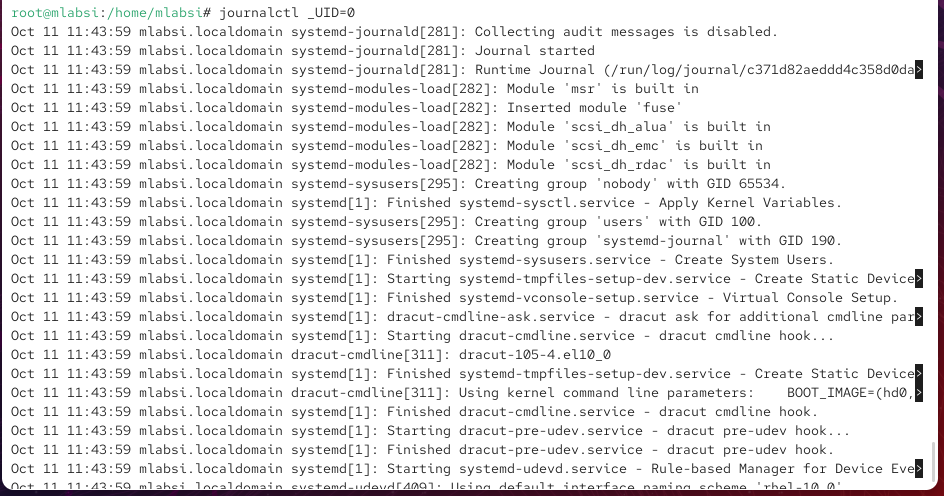
1. Для отображения доступных параметров фильтрации журнала выполнен вызов **journalctl** с двойным нажатием клавиши **Tab**, после чего показан список возможных фильтров и переменных.

* 
* Рис. 13: Отображение доступных параметров фильтрации в journalctl

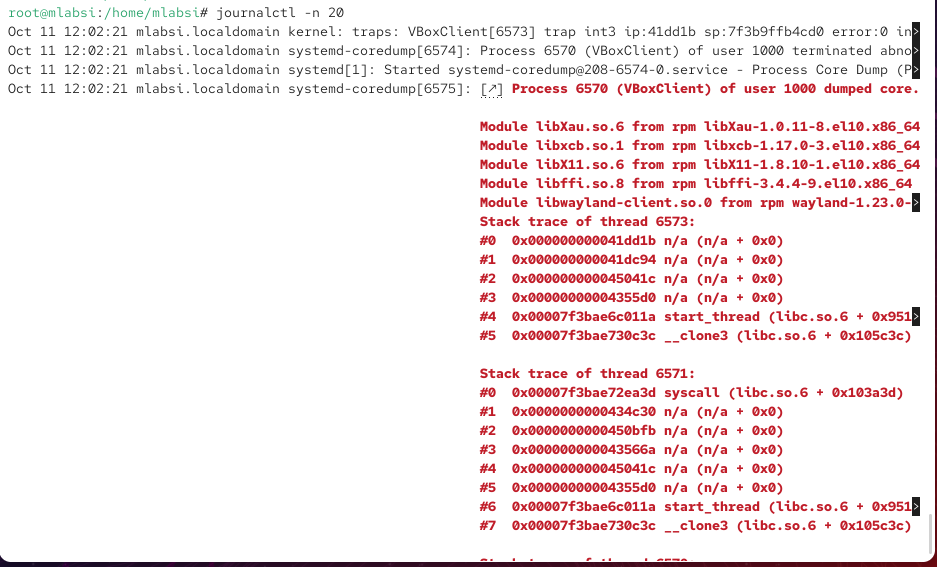
1. Для вывода сообщений, созданных пользователем с идентификатором **UID 0**, применена команда \*\*journalctl \_UID=0\*\*.  
   В результате показаны записи, относящиеся к действиям пользователя root.

* 
* Рис. 14: Фильтрация сообщений по UID 0

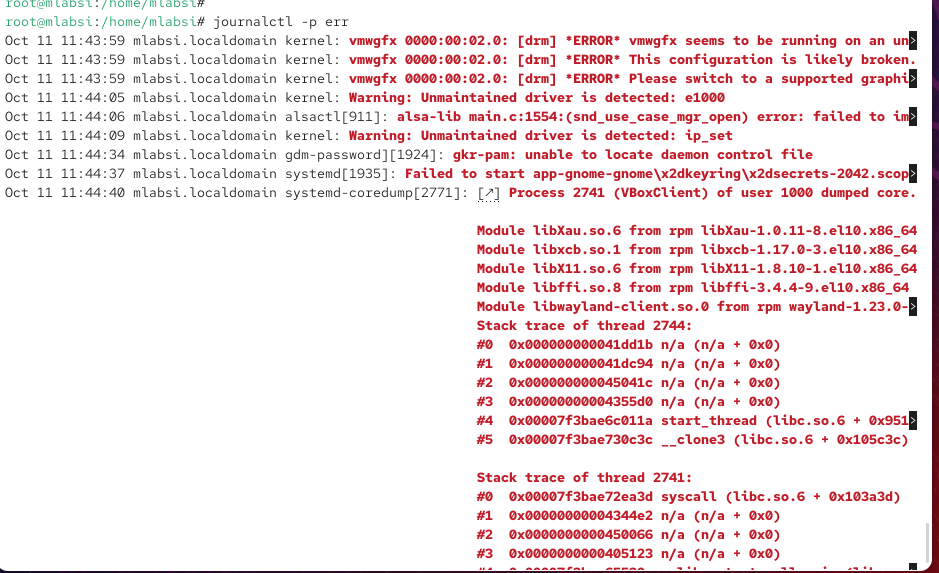
1. Для отображения последних двадцати строк журнала использована команда **journalctl -n 20**.  
   В выводе были зафиксированы сообщения о работе процессов VBoxClient и системных дампах памяти.

* 
* Рис. 15: Просмотр последних 20 строк журнала

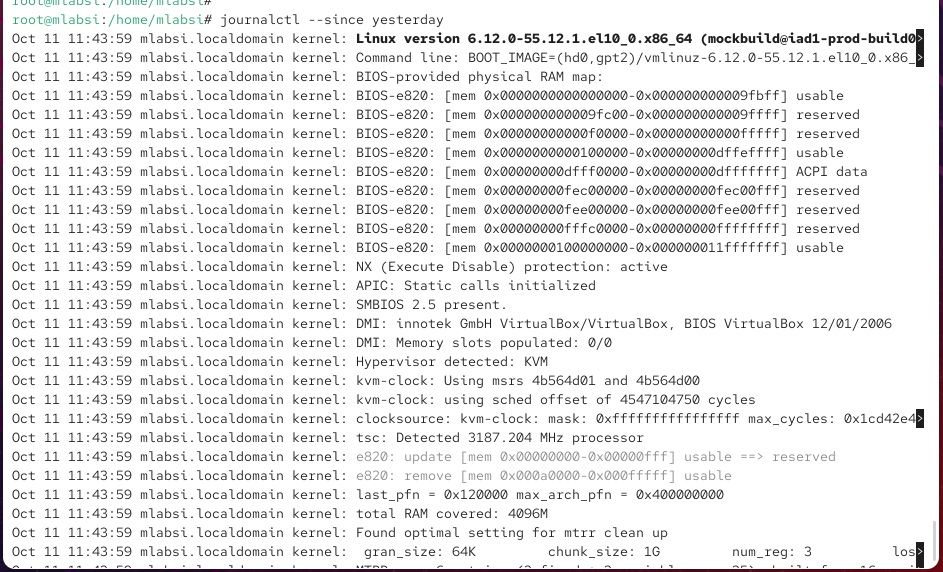
1. Для анализа только сообщений об ошибках введена команда **journalctl -p err**.  
   В списке отобразились предупреждения и ошибки ядра, включая проблемы с видеодрайвером, а также сбои пользовательских процессов.

* 
* Рис. 16: Просмотр сообщений уровня ошибки в системном журнале

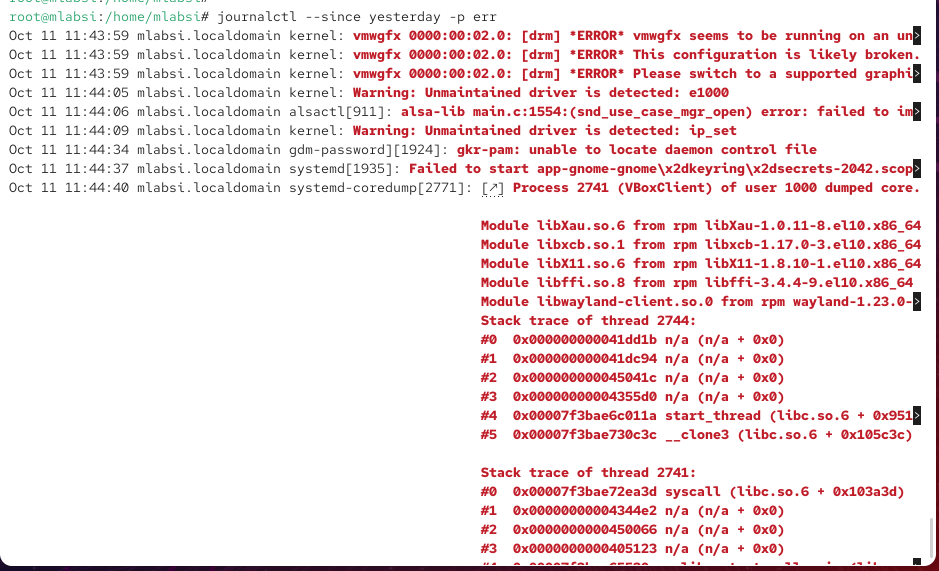
1. Для отображения записей, сделанных со вчерашнего дня, применена команда **journalctl –since yesterday**.  
   На экране показаны системные сообщения, начиная с момента загрузки операционной системы за предыдущие сутки.

* 
* Рис. 17: Просмотр системных сообщений со вчерашнего дня

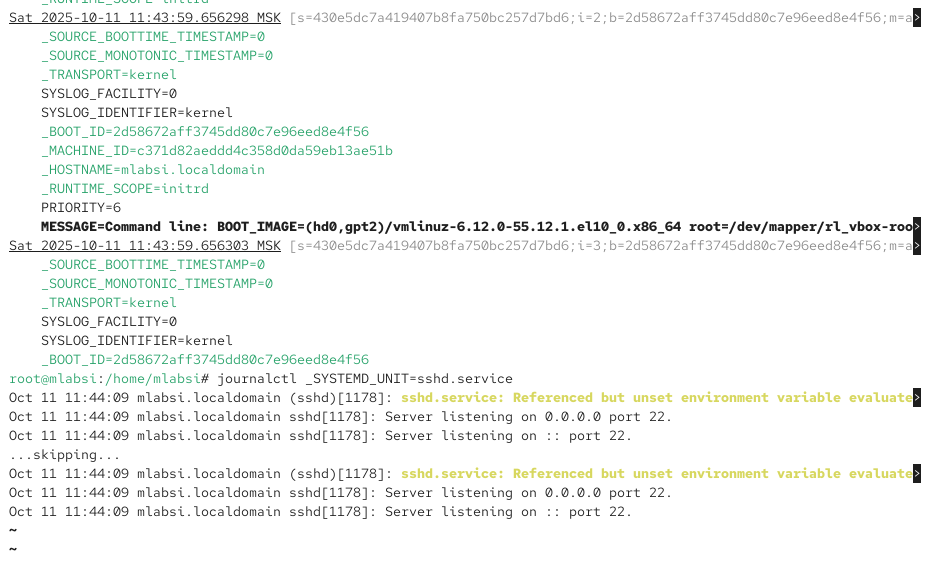
1. Для отображения сообщений уровня ошибки, зафиксированных со вчерашнего дня, использована команда **journalctl –since yesterday -p err**.  
   Выведены ошибки драйвера виртуализации, звуковой подсистемы и службы gnome-keyring.

* 
* Рис. 18: Просмотр сообщений уровня ошибки со вчерашнего дня

1. Для получения детальной информации о записях применена команда **journalctl -o verbose**.  
   В выводе содержатся расширенные метаданные каждой записи, включая идентификаторы, временные метки и источник сообщений.

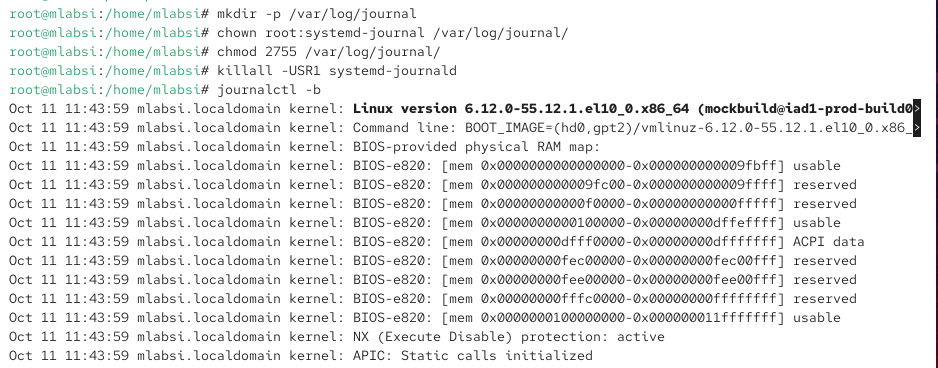
* 
* Рис. 19: Детальный вывод системного журнала в режиме verbose

1. Для анализа журнала службы SSH выполнена команда \*\*journalctl \_SYSTEMD\_UNIT=sshd.service\*\*.  
   В результате показаны события, связанные с запуском службы SSH и активацией сетевых портов.

* 
* Рис. 20: Просмотр журнала службы SSH

## 2.4 Постоянный журнал journald

1. Получены права администратора и создан каталог для хранения постоянного журнала с помощью команды **mkdir -p /var/log/journal**.  
   Это позволяет системе сохранять логи не только в оперативной памяти, но и на постоянном носителе.
2. Изменены права доступа к каталогу **/var/log/journal**, чтобы служба **systemd-journald** имела возможность записывать в него данные.  
   Для этого выполнены команды **chown root:systemd-journal /var/log/journal** и **chmod 2755 /var/log/journal**.
3. Для применения изменений перезапуск службы был осуществлён сигналом **killall -USR1 systemd-journald**, что позволило обновить конфигурацию без полной перезагрузки системы.
4. После этого просмотрен журнал сообщений с момента последнего запуска операционной системы при помощи **journalctl -b**.  
   В выводе отобразилась информация о версии ядра, инициализации BIOS и загрузке системных компонентов.

* 
* Рис. 21: Настройка постоянного журнала journald и просмотр системных сообщений после перезапуска службы

# 3 Контрольные вопросы

1. **Какой файл используется для настройки rsyslogd?**  
   Для настройки службы **rsyslogd** используется файл **/etc/rsyslog.conf**.  
   В нём задаются основные параметры работы демона и подключаются дополнительные конфигурационные файлы из каталога **/etc/rsyslog.d/**.
2. **В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?**  
   Сообщения, относящиеся к аутентификации и авторизации пользователей, записываются в файл **/var/log/secure**.
3. **Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?**  
   По умолчанию ротация файлов журналов осуществляется один раз в **неделю** с помощью службы **logrotate**.
4. **Какую строку следует добавить в конфигурацию для записи всех сообщений с приоритетом info в файл /var/log/messages.info?**  
   Для этого в конфигурационный файл необходимо добавить строку:  
   **\*.info /var/log/messages.info**
5. **Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?**  
   Для просмотра сообщений в режиме реального времени используется команда **journalctl -f**.  
   Она аналогична по действию команде **tail -f** для текстовых логов.
6. **Какая команда позволяет вам видеть все сообщения журнала, которые были написаны для PID 1 между 9:00 и 15:00?**  
   Сообщения для процесса с PID 1 за указанный промежуток времени можно просмотреть с помощью команды:  
   \*\*journalctl \_PID=1 –since “09:00” –until “15:00”\*\*
7. **Какая команда позволяет вам видеть сообщения journald после последней перезагрузки системы?**  
   Для просмотра сообщений, записанных после последнего запуска системы, используется команда **journalctl -b**.
8. **Какая процедура позволяет сделать журнал journald постоянным?**  
   Чтобы сделать журнал **journald** постоянным, необходимо:
   * создать каталог **/var/log/journal**;
   * изменить права доступа к нему (**chown root:systemd-journal /var/log/journal**, **chmod 2755 /var/log/journal**);
   * обновить конфигурацию с помощью команды **killall -USR1 systemd-journald**.  
     После этого логи будут сохраняться даже после перезагрузки системы.

# 4 Вывод

В ходе работы были изучены принципы ведения и фильтрации системных журналов с помощью rsyslog и journald, а также настроено их постоянное хранение и просмотр в реальном времени.