Отчёт по лабораторной работе №7

Управление журналами событий в системе

Анастасия Мазуркевич

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

Для начала в трёх вкладках терминала были получены полномочия администратора с помощью команды **su -**.

Во второй вкладке был запущен мониторинг системных событий в реальном времени: **tail -f /var/log/messages**.

В логе фиксировались события, связанные с работой сервисов, ядра и пользователями. В частности, при работе виртуальной машины VirtualBox неоднократно появлялись ошибки клиента **VBoxClient**, сопровождаемые дампами памяти.

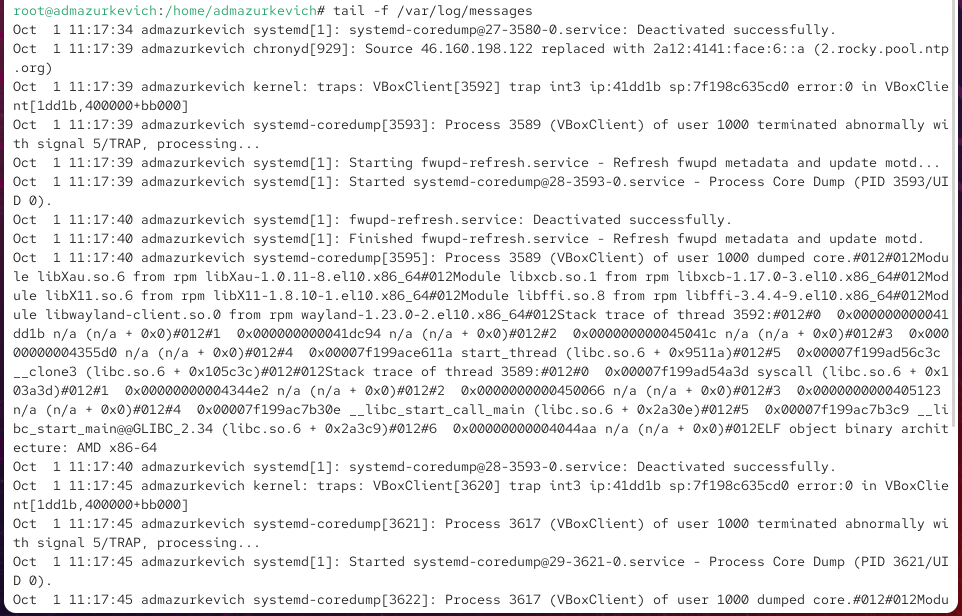


Рис. 1: Мониторинг системных сообщений

В третьей вкладке, после возврата к своей учётной записи, была предпринята попытка получить права администратора через **su**, но пароль был введён неверно.  
Во второй вкладке с мониторингом это зафиксировалось сообщением: **FAILED SU (to root) admazurkevich on pts/2**.

А также сопровождалось формированием дампа памяти для завершившегося процесса.

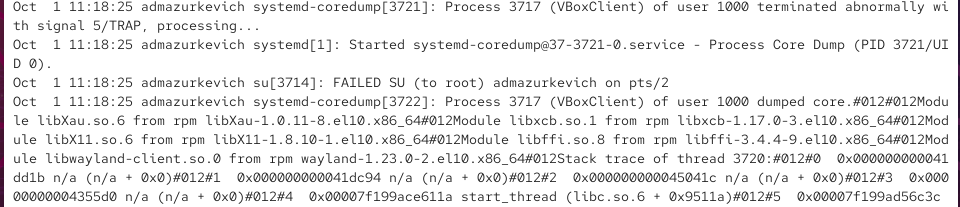


Рис. 2: Сообщение об ошибке аутентификации

Под учётной записью пользователя была выполнена команда **logger hello**.

Событие сразу же появилось в окне мониторинга и было записано в файл **/var/log/messages**.  
Таким образом, через logger можно добавлять произвольные заметки в системные логи.

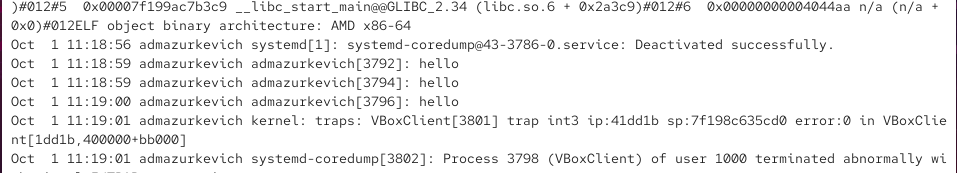


Рис. 3: Сообщение logger hello в журнале

После остановки мониторинга (**Ctrl + C**) был просмотрен файл с сообщениями безопасности — вывод последних 20 строк: **tail -n 20 /var/log/secure**.

В журнале зафиксированы успешные и неуспешные попытки входа в систему, а также ошибки авторизации при вводе неправильного пароля для root. Здесь отразились все действия, связанные с командами **su** и проверками пароля.

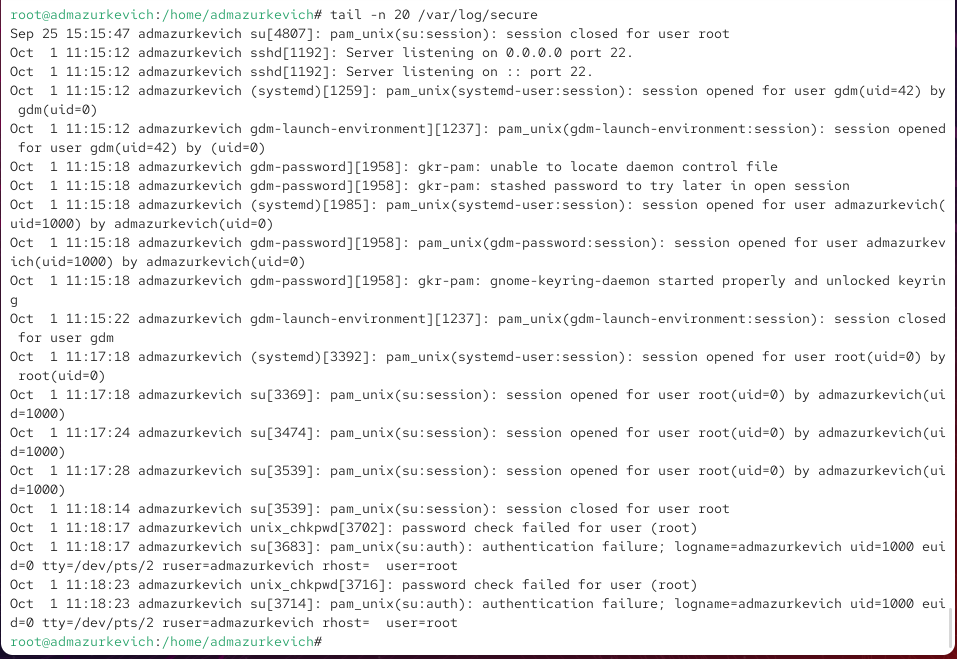


Рис. 4: Фрагмент журнала secure

## 2.2 Изменение правил rsyslog.conf

В первой вкладке терминала была выполнена установка пакета Apache:  
**dnf -y install httpd**

После завершения процесса веб-служба была запущена и добавлена в автозагрузку:

* **systemctl start httpd**
* **systemctl enable httpd**

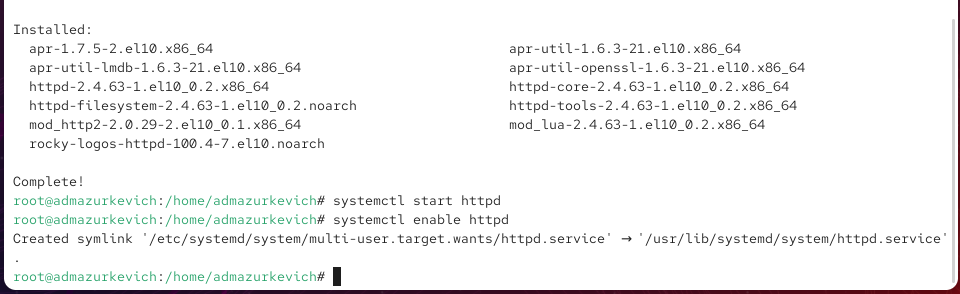


Рис. 5: Установка и запуск Apache

Во второй вкладке терминала был запущен просмотр сообщений об ошибках веб-сервера в реальном времени:

**tail -f /var/log/httpd/error\_log**

Здесь фиксировались события запуска Apache, активация SELinux-политики и переход службы в рабочий режим.

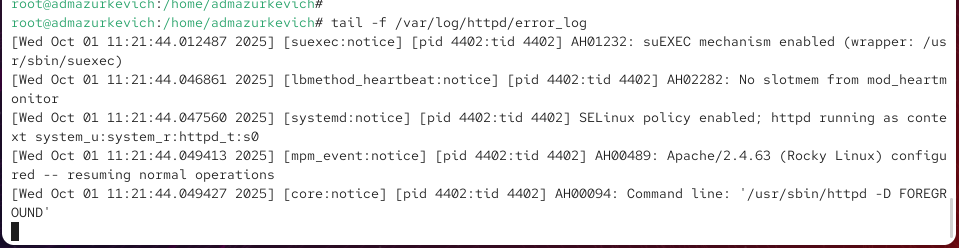


Рис. 6: Журнал ошибок Apache

В конфигурационный файл **/etc/httpd/conf/httpd.conf** была добавлена строка:

**ErrorLog syslog:local1**

Это позволило отправлять ошибки Apache в системный журнал через объект **local1**.

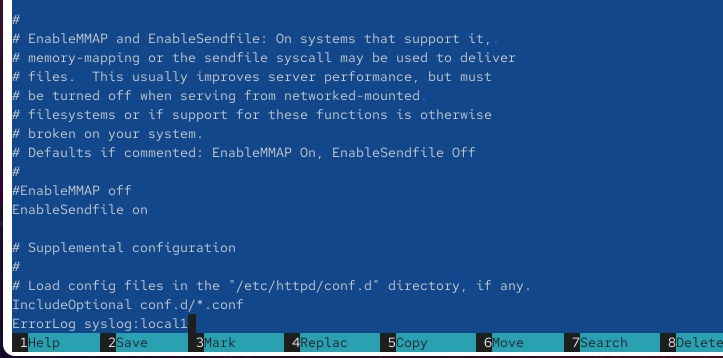


Рис. 7: Добавление правила ErrorLog в httpd.conf

В каталоге **/etc/rsyslog.d** был создан файл **httpd.conf**, в который добавлено правило:

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

Таким образом, все сообщения от Apache через **local1** стали фиксироваться в отдельном файле **/var/log/httpd-error.log**.

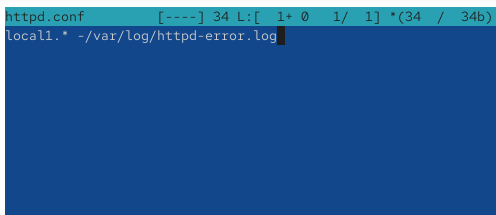


Рис. 8: Создание правила для логов Apache в rsyslog

После этого были перезапущены службы:

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

В том же каталоге **/etc/rsyslog.d** был создан новый файл **debug.conf**, куда добавлено правило:

**\*.debug /var/log/messages-debug**

Таким образом, все отладочные сообщения перенаправляются в отдельный лог-файл.

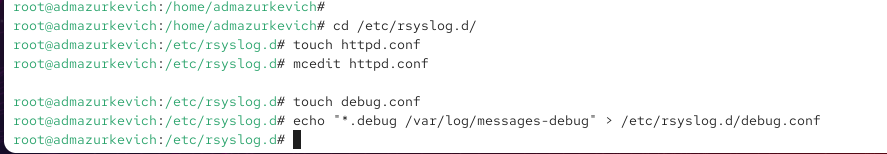


Рис. 9: Создание конфигурации debug.conf

Во второй вкладке был запущен мониторинг файла **/var/log/messages-debug** командой:

**tail -f /var/log/messages-debug**

Затем в третьей вкладке было выполнено:

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

В мониторинге появилось сообщение отладки, что подтвердило успешную настройку.

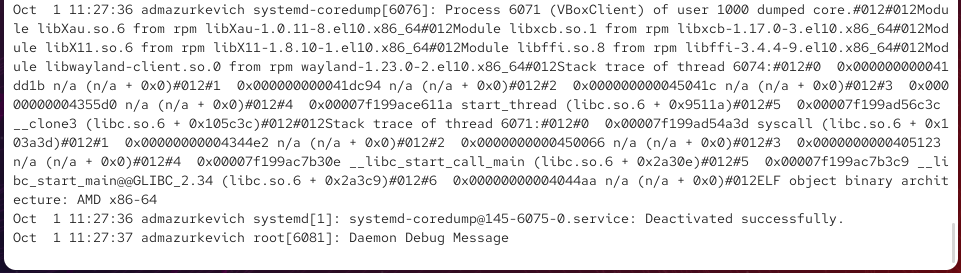


Рис. 10: Сообщение отладки в журнале

## 2.3 Использование journalctl

Для просмотра журнала с момента загрузки системы была использована команда:  
**journalctl**

Отображаются все события ядра и сервисов, начиная с инициализации оборудования и запуска служб.

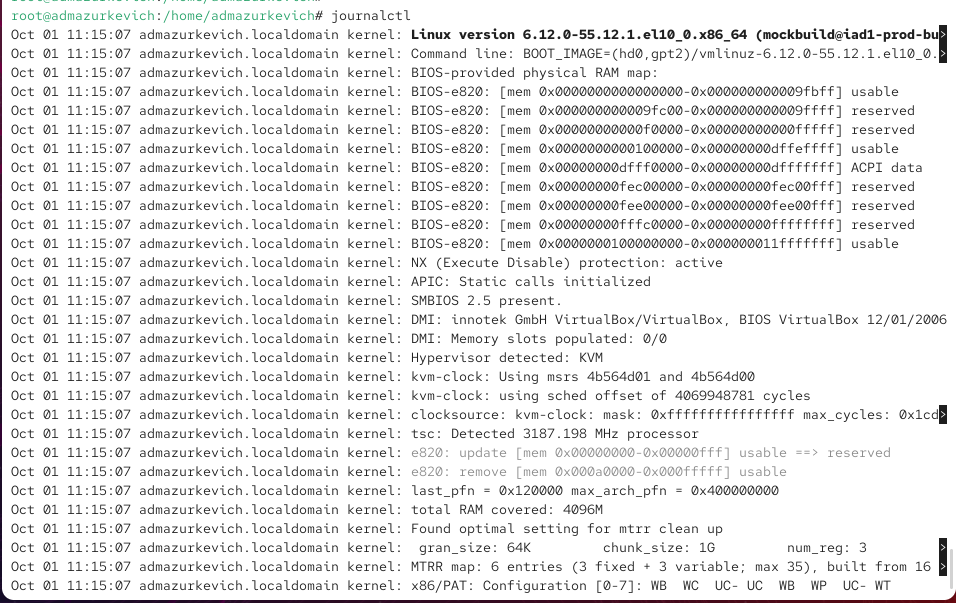


Рис. 11: Просмотр системного журнала

Чтобы вывести содержимое журнала без использования постраничного просмотра, была выполнена команда:  
**journalctl –no-pager**

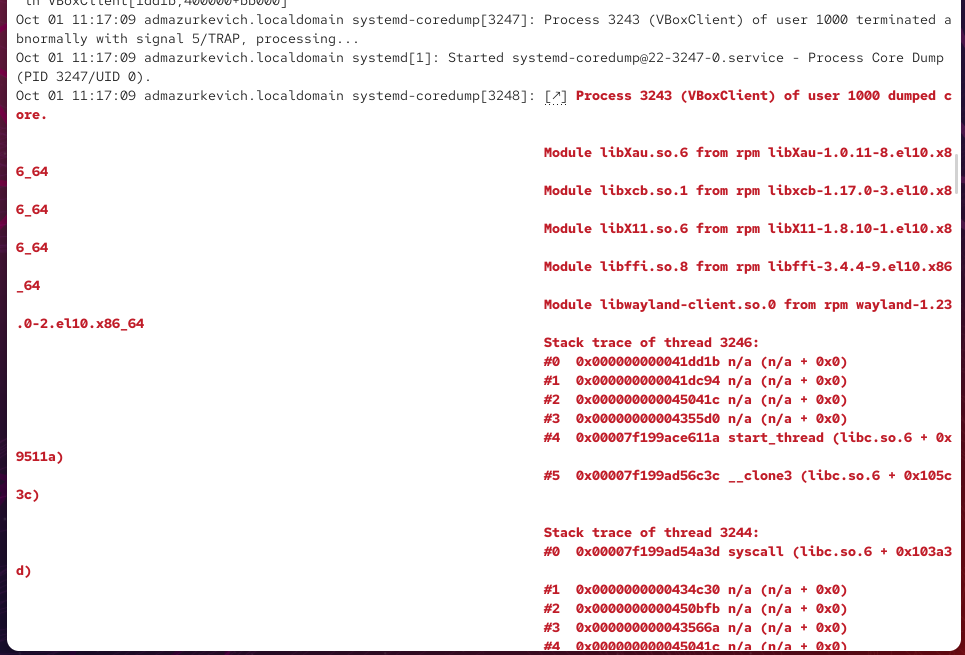


Рис. 12: Просмотр системного журнала

Для анализа новых сообщений в режиме онлайн применялась команда:  
**journalctl -f**

Мониторинг можно прервать сочетанием клавиш **Ctrl + C**.

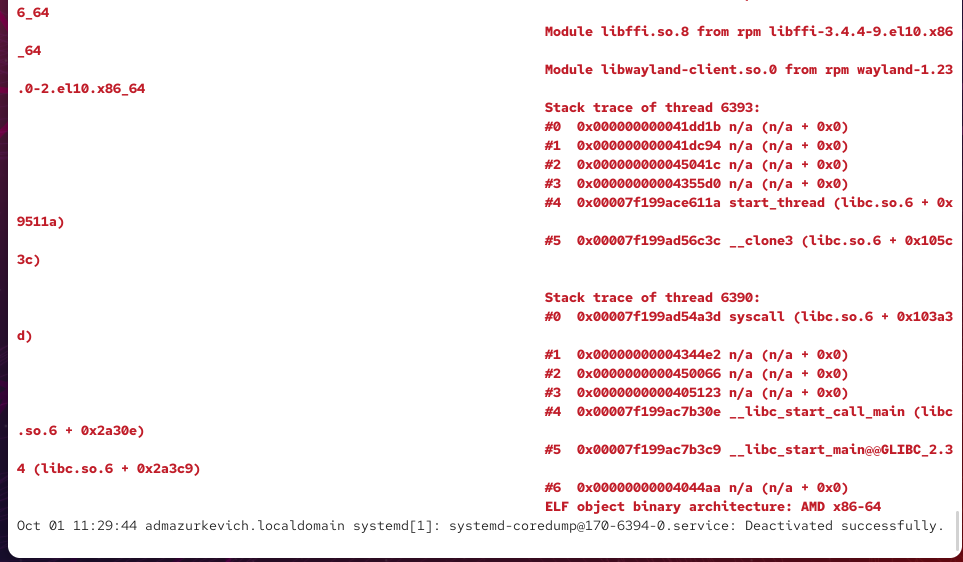


Рис. 13: Режим просмотра журнала в реальном времени

После ввода команды **journalctl** и двойного нажатия клавиши **Tab** отобразился список доступных параметров фильтрации: по UID, PID, системным полям и сервисам.

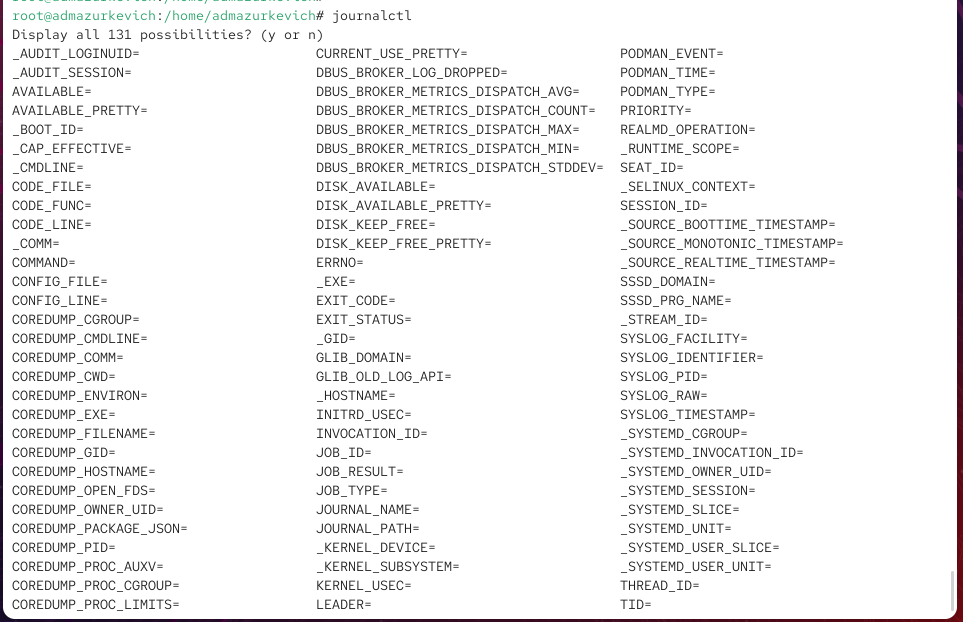


Рис. 14: Фильтрация журнала по параметрам

Для вывода записей, связанных с пользователем root, была применена команда:  
\*\*journalctl \_UID=0\*\*

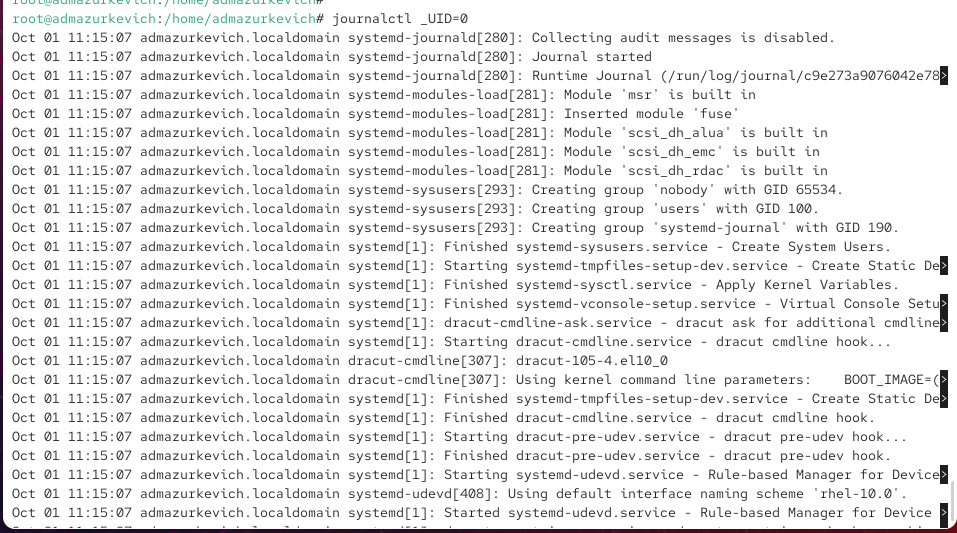


Рис. 15: Журнал для UID 0

Команда **journalctl -n 20** вывела последние 20 строк системного журнала.

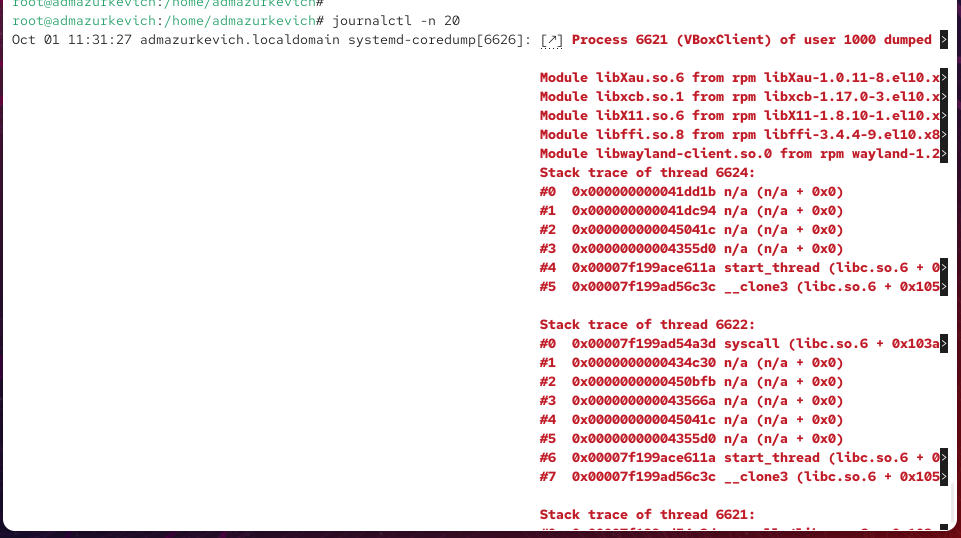


Рис. 16: Вывод последних строк журнала

С помощью команды:  
**journalctl -p err**

были отображены только записи уровня ошибки. Здесь фиксируются проблемы с драйверами, службами и падения приложений.

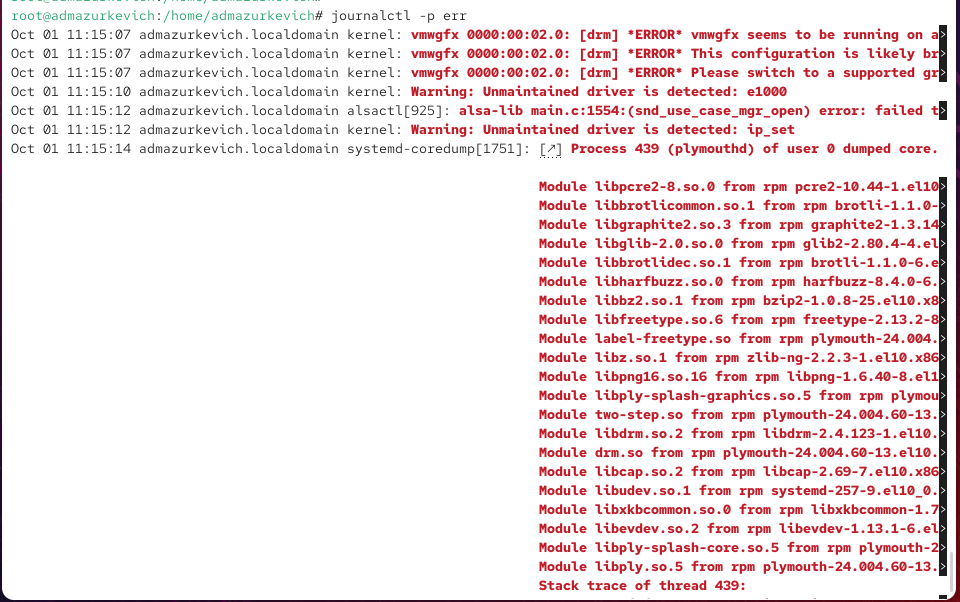


Рис. 17: Сообщения уровня ошибки

Для анализа сообщений со вчерашнего дня была выполнена команда:  
**journalctl –since yesterday**

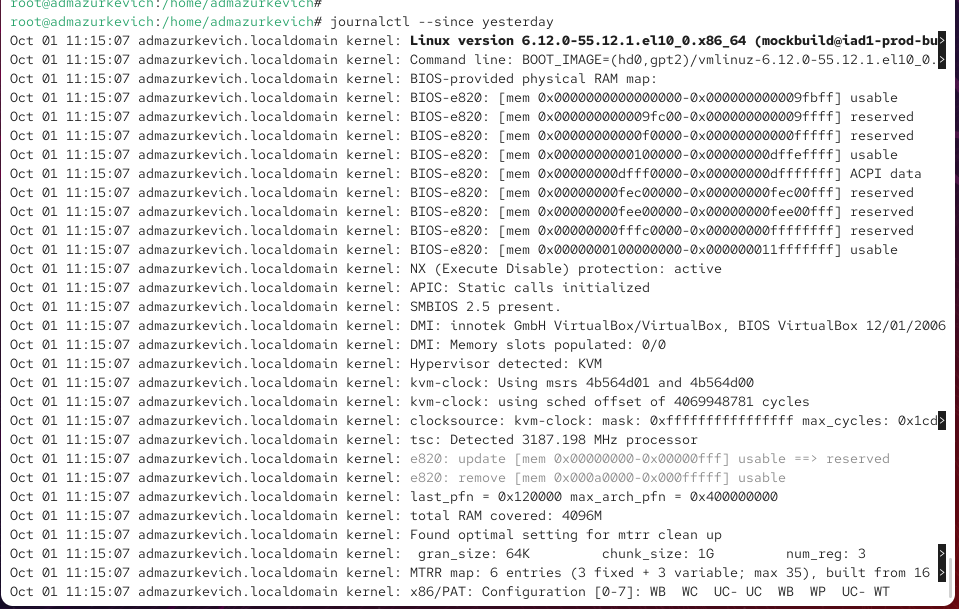


Рис. 18: Сообщения со вчерашнего дня

Для просмотра только ошибок со вчерашнего дня использовалась команда:  
**journalctl –since yesterday -p err**

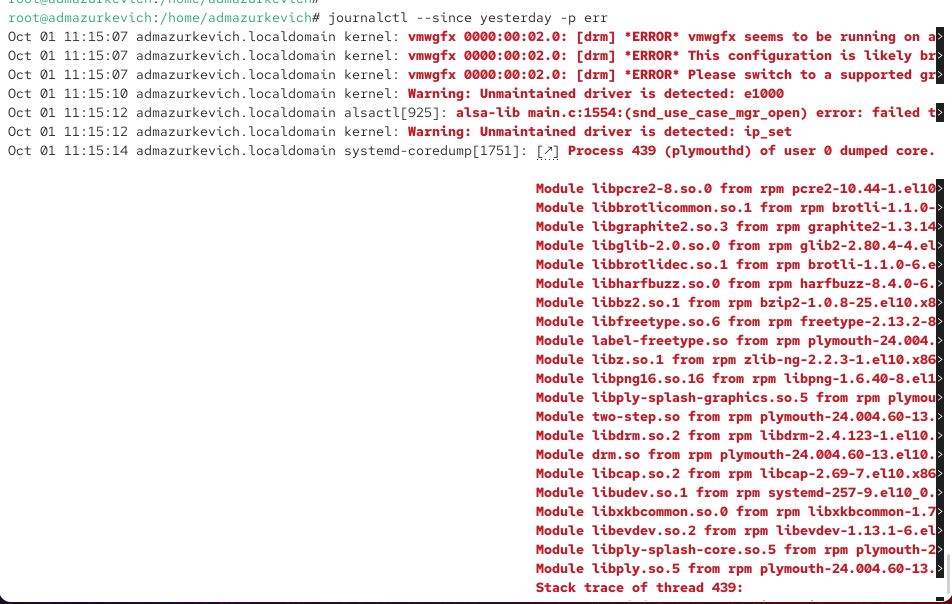


Рис. 19: Ошибки со вчерашнего дня

Для получения расширенной информации по каждому событию была использована команда:  
**journalctl -o verbose**

В выводе указываются дополнительные параметры: идентификатор загрузки, имя хоста, приоритет события, источник и другие метаданные.

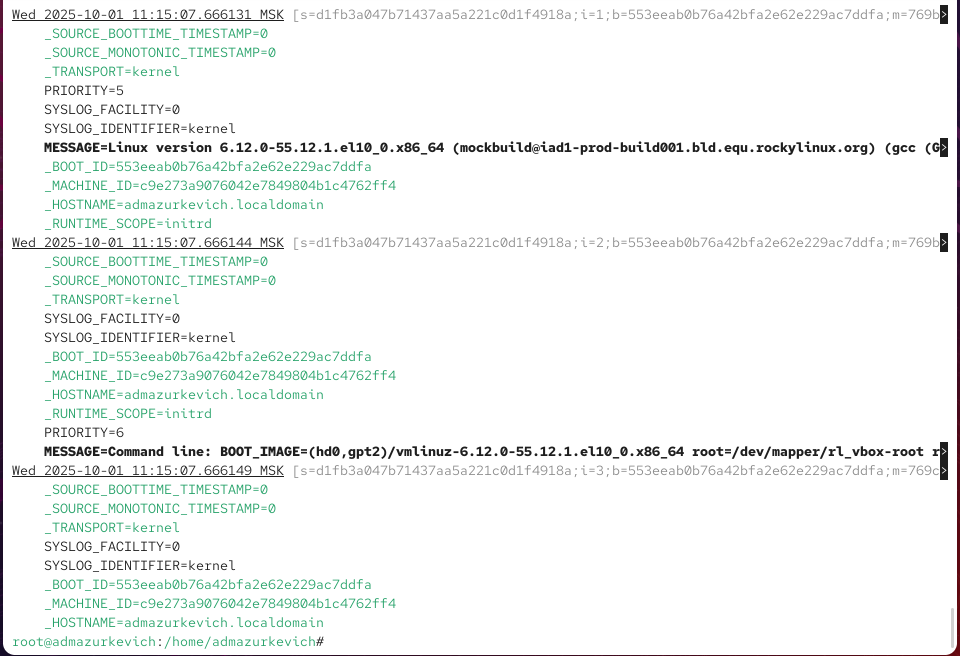


Рис. 20: Детализированный вывод журнала

Для анализа работы службы **sshd** была использована команда:  
\*\*journalctl \_SYSTEMD\_UNIT=sshd.service\*\*

В выводе отобразились события, связанные с запуском и работой SSH-сервера: сообщения об окружении и прослушивание порта 22 (как IPv4, так и IPv6).

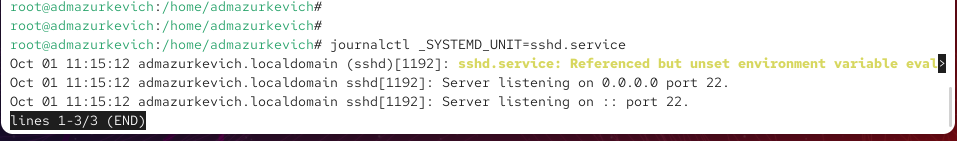


Рис. 21: Журнал работы SSHD

## 2.4 Создание каталога для хранения журналов

Для организации хранения журналов был создан каталог **/var/log/journal**, в который затем перенаправлены данные systemd-journald.

Выполненные действия:  
- создание каталога: **mkdir -p /var/log/journal**  
- назначение прав доступа: **chmod 2755 /var/log/journal**  
- перезапуск службы systemd-journald сигналом: **killall -USR1 systemd-journald**

После этого команда **journalctl -b** показала системные сообщения с момента последней загрузки ядра.

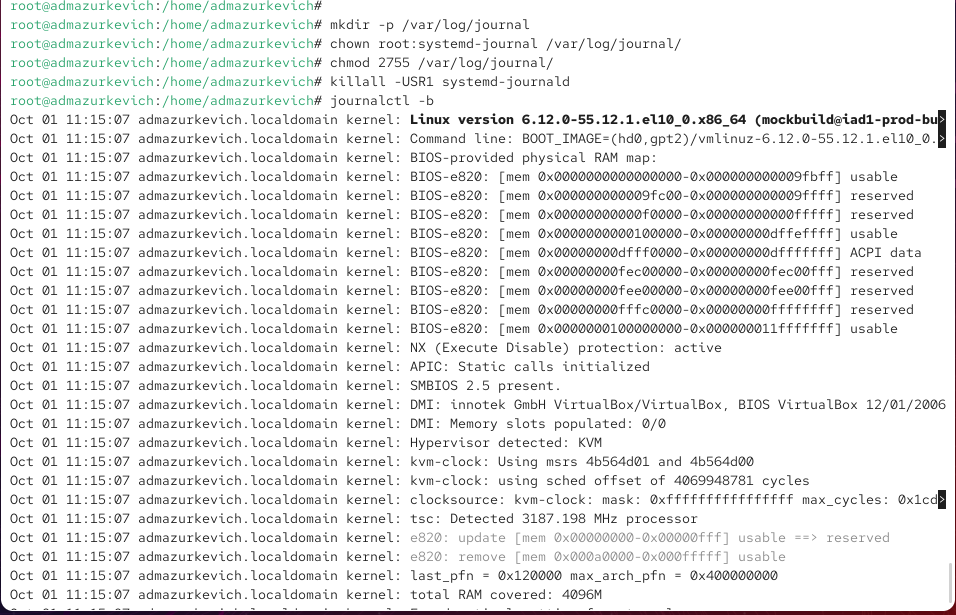


Рис. 22: Перенос журналов и вывод сообщений загрузки

# 3 Контрольные вопросы

**1. Какой файл используется для настройки rsyslogd?**  
Основной конфигурационный файл — /etc/rsyslog.conf.  
Дополнительно правила могут храниться в каталоге /etc/rsyslog.d/.

**2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?**  
Сообщения об аутентификации фиксируются в файле /var/log/secure.

**3. Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?**  
По умолчанию ротация выполняется раз в неделю с использованием утилиты logrotate.

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

**5. Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?**  
Для этого 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?**  
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?**  
Необходимо создать каталог для хранения журналов и назначить ему права:  
- mkdir -p /var/log/journal  
- chmod 2755 /var/log/journal  
- перезапустить службу: systemctl restart systemd-journald

После этого журнал будет сохраняться в постоянном виде даже после перезагрузки системы.

# 4 Заключение

В ходе лабораторной работы были изучены основы управления системными журналами в Linux с использованием **rsyslog** и **systemd-journald**.  
Была проведена настройка перенаправления сообщений веб-сервера Apache в отдельные файлы, реализовано хранение отладочной информации, а также рассмотрены способы фильтрации и просмотра логов через journalctl.