Отчёт по лабораторной работе №7

Управление журналами событий в системе

Яковлева Дарья Сергеевна

Содержание

# 1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

# 2 Выполнение лабораторной работы

## 2.1 Мониторинг журнала системных событий в реальном времени

Запускаю три вкладки терминала и получаю полномочия администратора с помощью su -.

Во второй вкладке запускаю мониторинг системных событий командой tail -f /var/log/messages.

В третьей вкладке возвращаюсь к учётной записи пользователя (Ctrl + D) и пробую получить права администратора, но ввожу неправильный пароль. В окне мониторинга фиксируется сообщение об ошибке (см. рис. fig. 1).

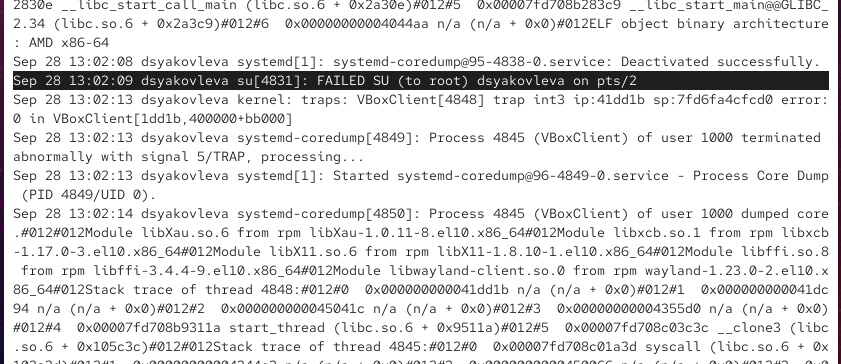


Рис. 1: Ошибка аутентификации при su

Затем в третьей вкладке из оболочки пользователя выполняю команду logger hello.

Во второй вкладке вижу появившееся сообщение в журнале (см. рис. fig. 2).

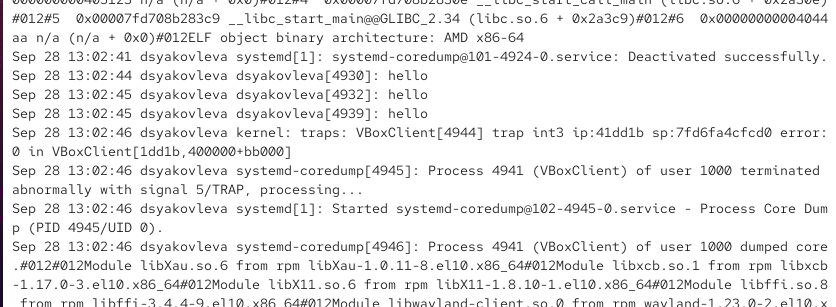


Рис. 2: Сообщение logger hello

После этого останавливаю мониторинг (Ctrl + C) и запускаю просмотр последних 20 строк журнала безопасности командой tail -n 20 /var/log/secure.

На экране отображаются сообщения, зафиксированные при ошибках аутентификации и вводе неверного пароля для su (см. рис. fig. 3).

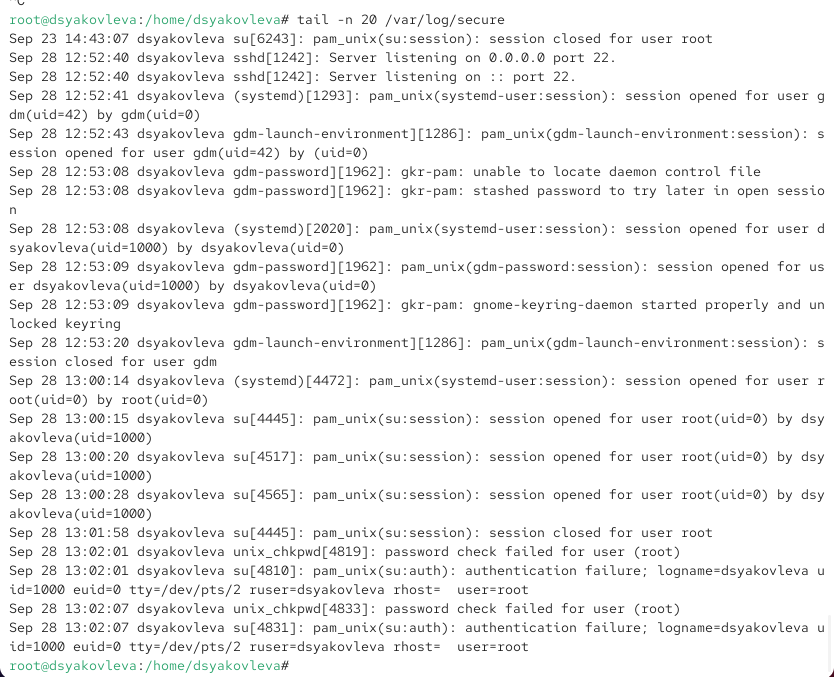


Рис. 3: Просмотр последних строк /var/log/secure

## 2.2 Изменение правил rsyslog.conf

Устанавливаю веб-сервер Apache. После завершения установки запускаю и добавляю службу в автозагрузку с помощью команд systemctl start httpd и systemctl enable httpd (см. рис. fig. 4).

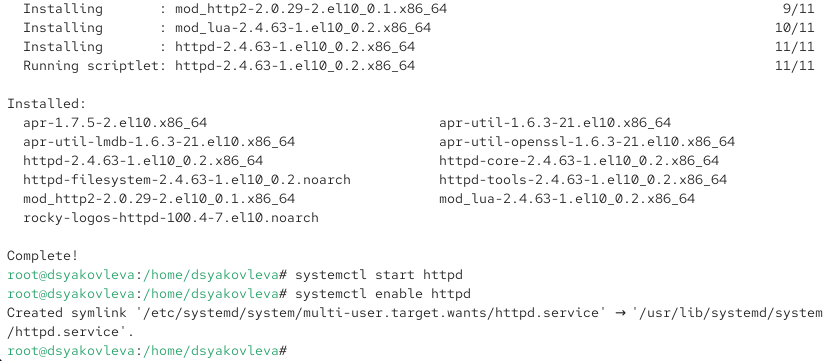


Рис. 4: Установка и запуск Apache

Во второй вкладке просматриваю журнал сообщений об ошибках веб-службы при помощи tail -f /var/log/httpd/error\_log (см. рис. fig. 5).

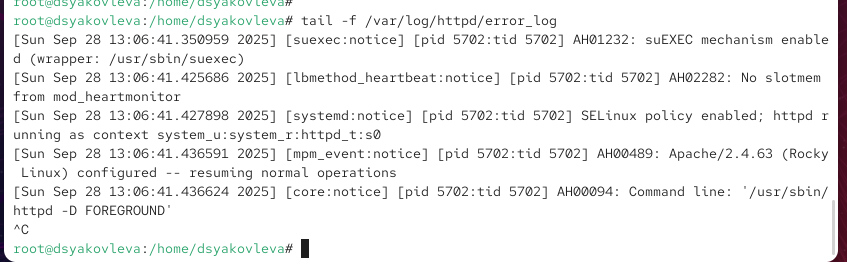


Рис. 5: Просмотр error\_log Apache

В конфигурационном файле /etc/httpd/conf/httpd.conf добавляю строку ErrorLog syslog:local1 (см. рис. fig. 6).



Рис. 6: Настройка ErrorLog в httpd.conf

Затем в каталоге /etc/rsyslog.d создаю файл httpd.conf и прописываю правило local1.\* -/var/log/httpd-error.log (см. рис. fig. 7).

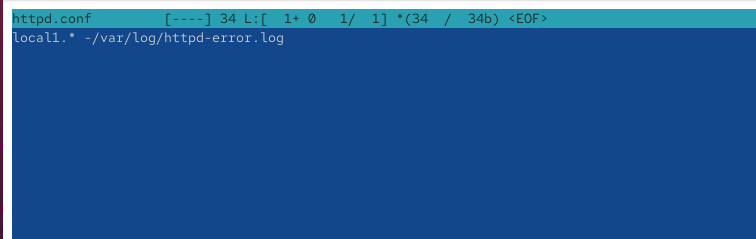


Рис. 7: Создание правила для httpd в rsyslog

После перезапуска служб rsyslog и httpd все ошибки веб-сервера начинают записываться в файл /var/log/httpd-error.log.

Далее создаю отдельный файл debug.conf в каталоге /etc/rsyslog.d и добавляю правило \*.debug /var/log/messages-debug, которое перенаправляет все отладочные сообщения в отдельный лог-файл (см. рис. fig. 8).

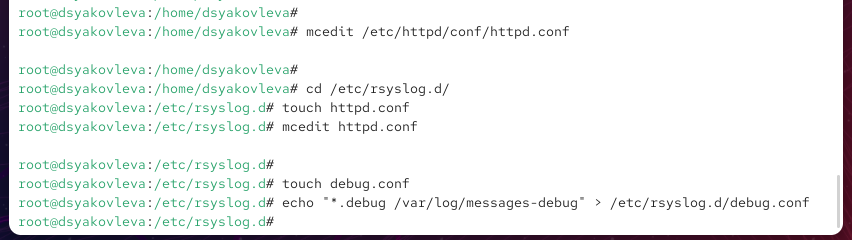


Рис. 8: Создание debug.conf

Во второй вкладке запускаю мониторинг отладочной информации с помощью tail -f /var/log/messages-debug. В третьей вкладке ввожу команду logger -p daemon.debug "Daemon Debug Message". В окне мониторинга отображается сообщение (см. рис. fig. 9).

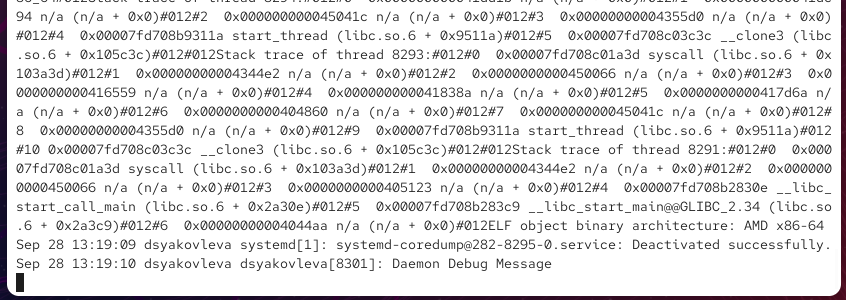


Рис. 9: Сообщение Daemon Debug Message

## 2.3 Использование journalctl

Во второй вкладке терминала просматриваю содержимое журнала событий с момента последнего запуска системы с помощью команды journalctl. Отображаются сообщения ядра и служб (см. рис. fig. 10).

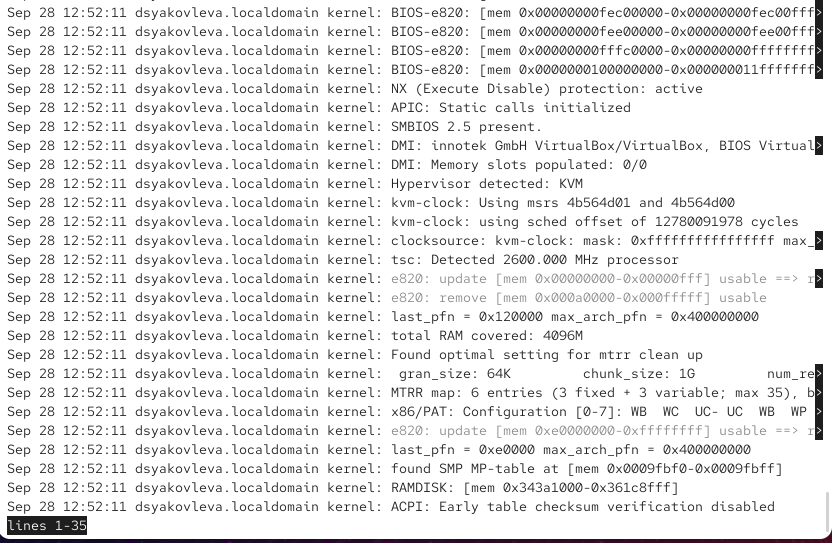


Рис. 10: Просмотр журнала journalctl

Запускаю просмотр журнала без использования пейджера с помощью опции --no-pager. Сообщения выводятся в обычном потоке терминала (см. рис. fig. 11).



Рис. 11: Вывод без пейджера

Использую режим просмотра журнала в реальном времени с параметром -f. Система отображает новые записи сразу после их появления (см. рис. fig. 12).

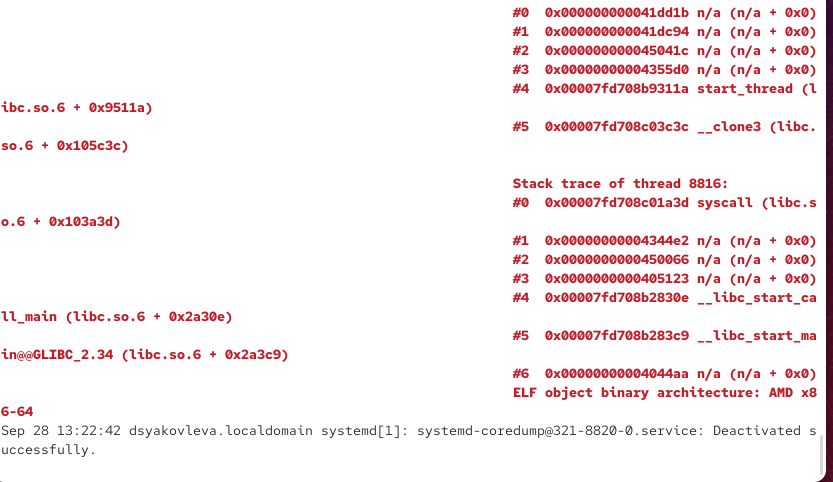


Рис. 12: Режим реального времени

Для изучения доступных параметров фильтрации ввожу команду journalctl и дважды нажимаю Tab. Отображается список возможных ключей фильтрации (см. рис. fig. 13).

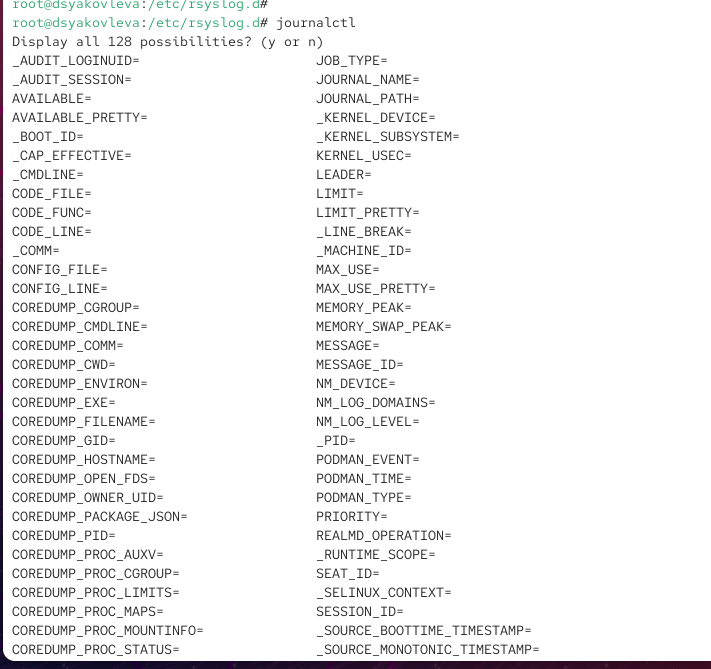


Рис. 13: Фильтрация журнала

Просматриваю события, относящиеся к пользователю с UID 0, при помощи команды journalctl \_UID=0 (см. рис. fig. 14).

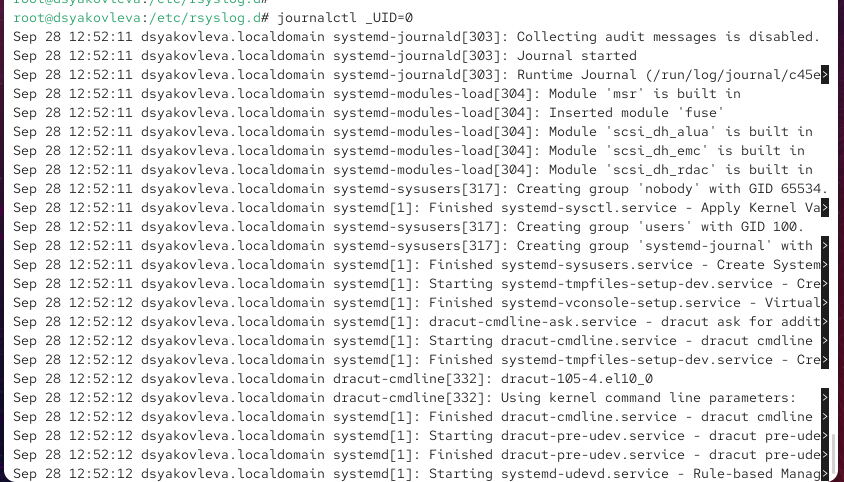


Рис. 14: Просмотр событий UID=0

Для вывода последних 20 строк журнала использую параметр -n 20. Вижу записи, относящиеся к ошибкам приложений (см. рис. fig. 15).

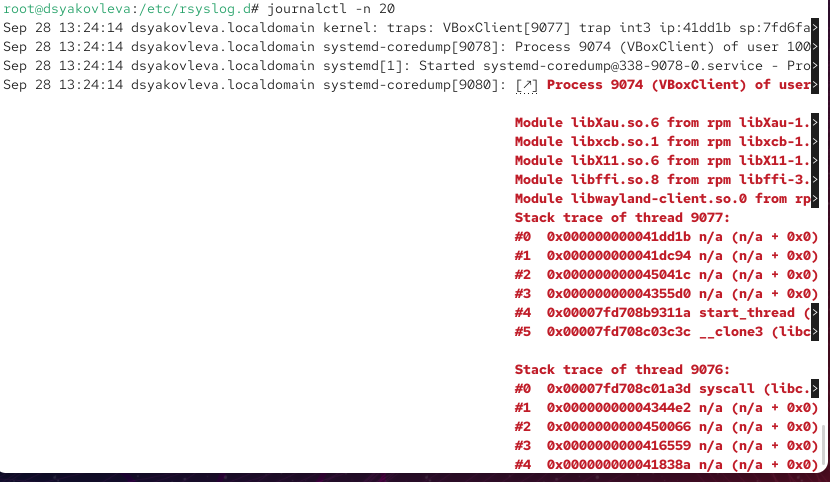


Рис. 15: Последние 20 строк журнала

Отображаю только сообщения об ошибках с помощью параметра -p err. В выводе фиксируются ошибки драйверов и служб (см. рис. fig. 16).

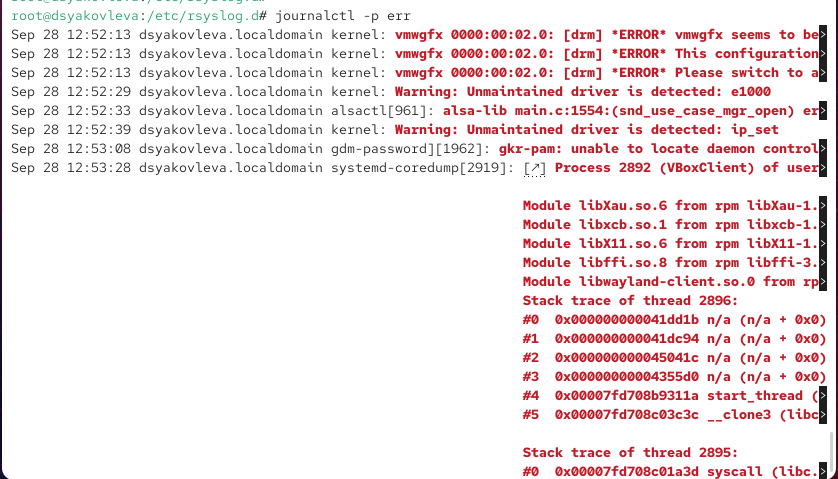


Рис. 16: Фильтрация по ошибкам

Для анализа журнала за определённый период использую параметр --since yesterday. На экране появляются все записи, начиная со вчерашнего дня (см. рис. fig. 17).

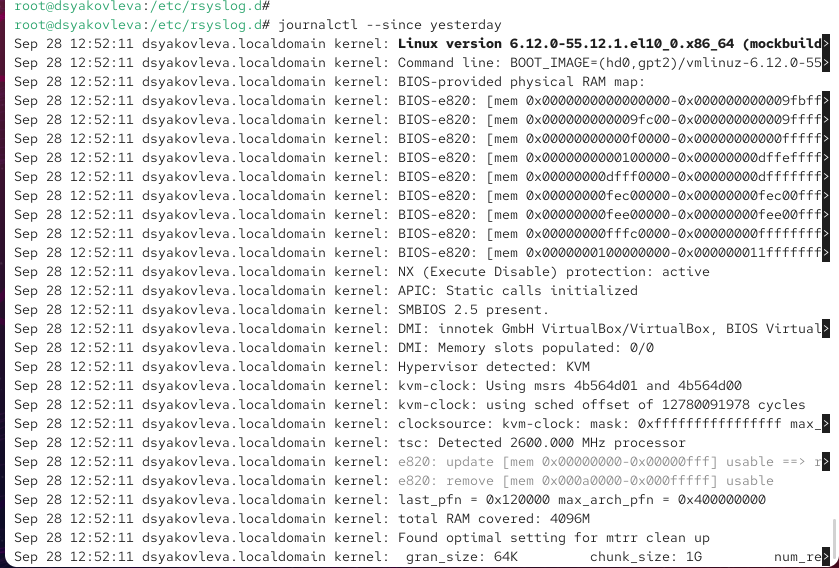


Рис. 17: Сообщения со вчерашнего дня

Затем применяю комбинацию параметров --since yesterday -p err, чтобы показать только ошибки со вчерашнего дня (см. рис. fig. 18).

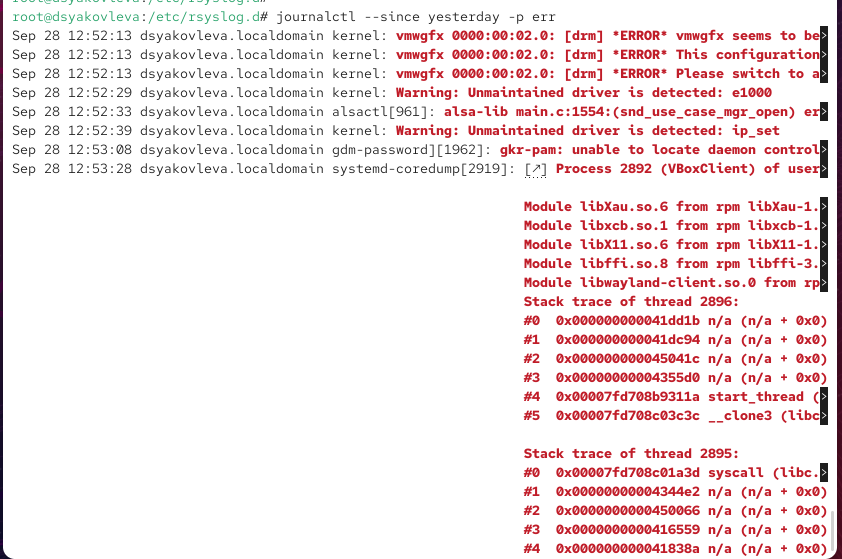


Рис. 18: Ошибки со вчерашнего дня

Для получения детальной информации использую параметр -o verbose. Сообщения журнала выводятся с дополнительными полями, включая идентификатор хоста и параметры ядра (см. рис. fig. 19).

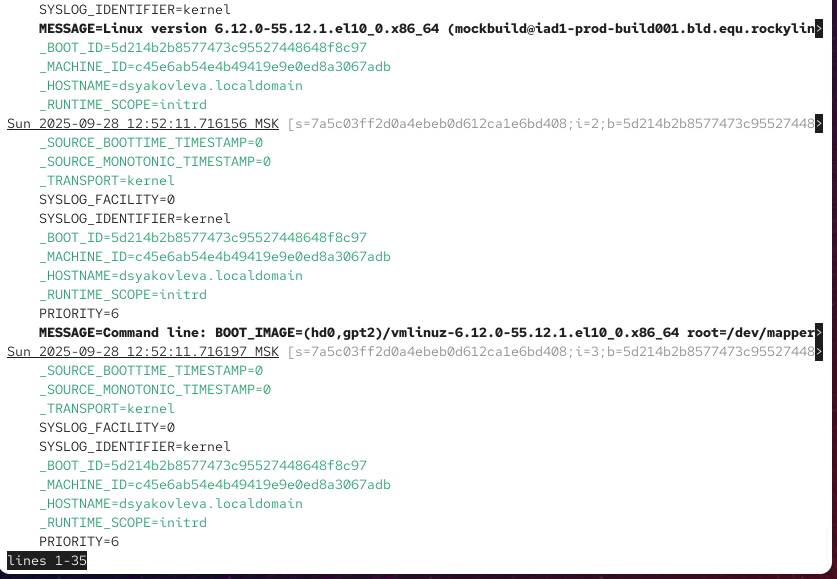


Рис. 19: Подробный вывод verbose

Для просмотра дополнительной информации о модуле sshd использую команду journalctl \_SYSTEMD\_UNIT=sshd.service. Отображаются записи о запуске сервера и его прослушивании порта 22 (см. рис. fig. 20).

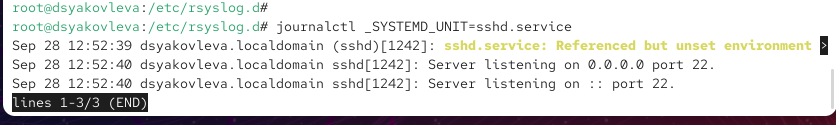


Рис. 20: Просмотр журнала sshd

## 2.4 Постоянный журнал journald

По умолчанию journald хранит сообщения во временном каталоге /run/log/journal, и они теряются после перезагрузки системы. Чтобы сделать журнал постоянным, создаю каталог /var/log/journal и задаю ему необходимые права доступа (см. рис. fig. 21).

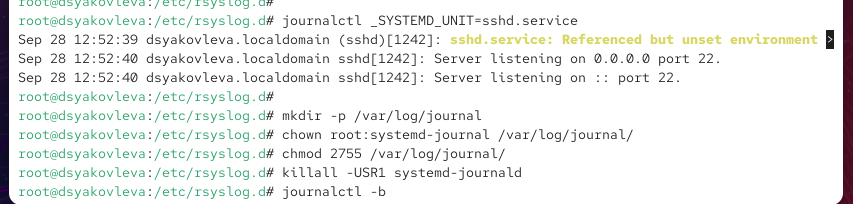


Рис. 21: Создание каталога для journald

После этого посылаю сигнал USR1 процессу systemd-journald, чтобы он принял изменения без перезагрузки (см. рис. fig. 22).

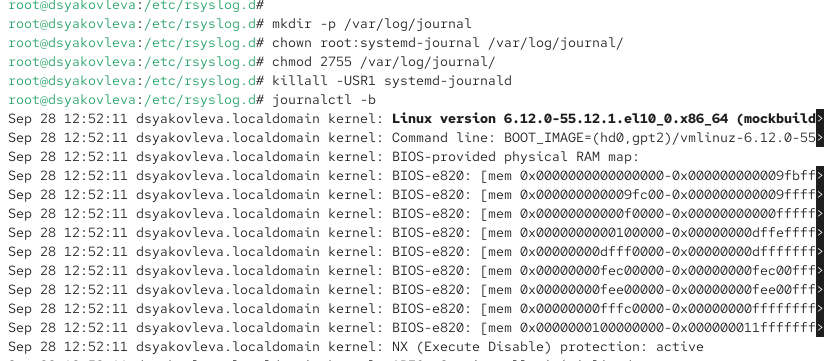


Рис. 22: Активация постоянного хранения журнала

Теперь журнал становится постоянным, и для просмотра сообщений с момента последней перезагрузки использую команду journalctl -b. В выводе отображаются сообщения ядра и системных служб после старта системы.

# 3 Контрольные вопросы

1. **Какой файл используется для настройки rsyslogd?**  
   Основной файл конфигурации — /etc/rsyslog.conf. Дополнительные правила можно хранить 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 файлов журналов происходит раз в неделю, а старые файлы хранятся в течение 4 недель. За это отвечает служба logrotate.
4. **Какую строку следует добавить в конфигурацию для записи всех сообщений с приоритетом info в файл /var/log/messages.info?**  
   Нужно добавить строку: \*.info /var/log/messages.info
5. **Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?**  
   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?**  
   Для этого используется команда journalctl -b.
8. **Какая процедура позволяет сделать журнал journald постоянным?**

* Создать каталог /var/log/journal.
* Задать ему владельца и группу: chown root:systemd-journal /var/log/journal.
* Установить права: chmod 2755 /var/log/journal.
* Отправить сигнал USR1 процессу systemd-journald или перезагрузить систему.  
  После этого журнал будет храниться постоянно.

# 4 Заключение

В ходе лабораторной работы были приобретены навыки мониторинга системных журналов и настройки регистрации событий в Linux: использование tail для просмотра логов в реальном времени, настройка правил rsyslog, работа с logger, исследование журналов при помощи journalctl, а также организация постоянного хранения журналов с помощью journald.