Отчёт о лабораторной работе

Лабораторная работа 7. Управление журналами операционной системы

Баранов Никита Дмитриевич

Содержание

# 1. Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

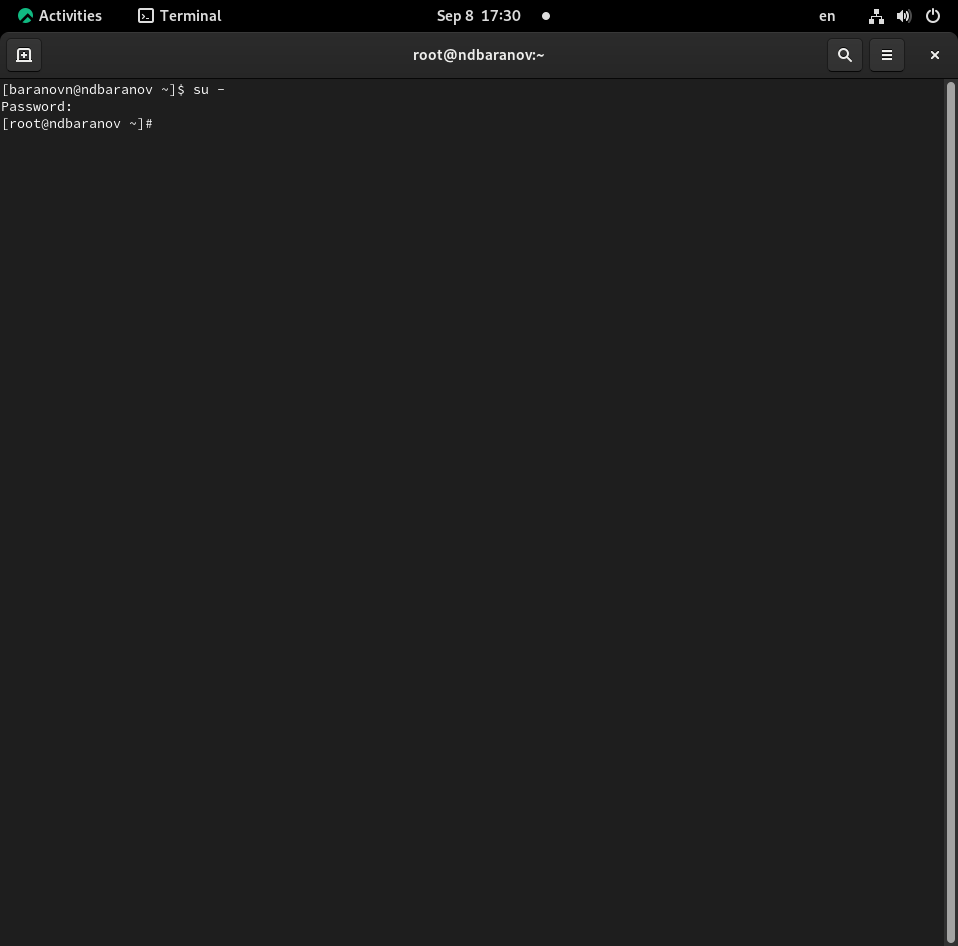
# 2. Задание

1. Продемонстрируйте навыки работы с журналом мониторинга событий в реальном времени (см. раздел 7.4.1).
2. Продемонстрируйте навыки создания и настройки отдельного файла конфигурации мониторинга отслеживания событий веб-службы (см. раздел 7.4.2).
3. Продемонстрируйте навыки работы с journalctl (см. раздел 7.4.3).
4. Продемонстрируйте навыки работы с journald (см. раздел 7.4.4).

# 3. Выполнение лабораторной работы

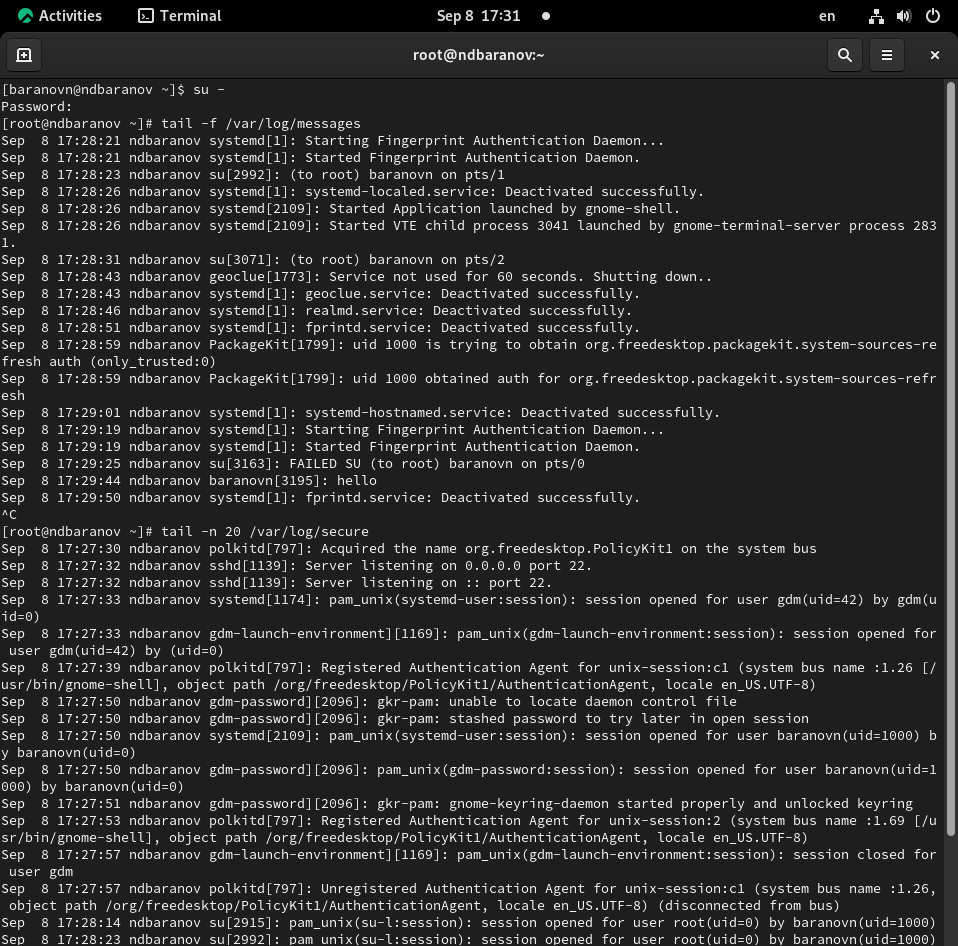
## 3.1 Мониторинг системных событий

Запускаем три вкладки терминала и получаем полномочия администратора (рис. [**fig:001?**]).



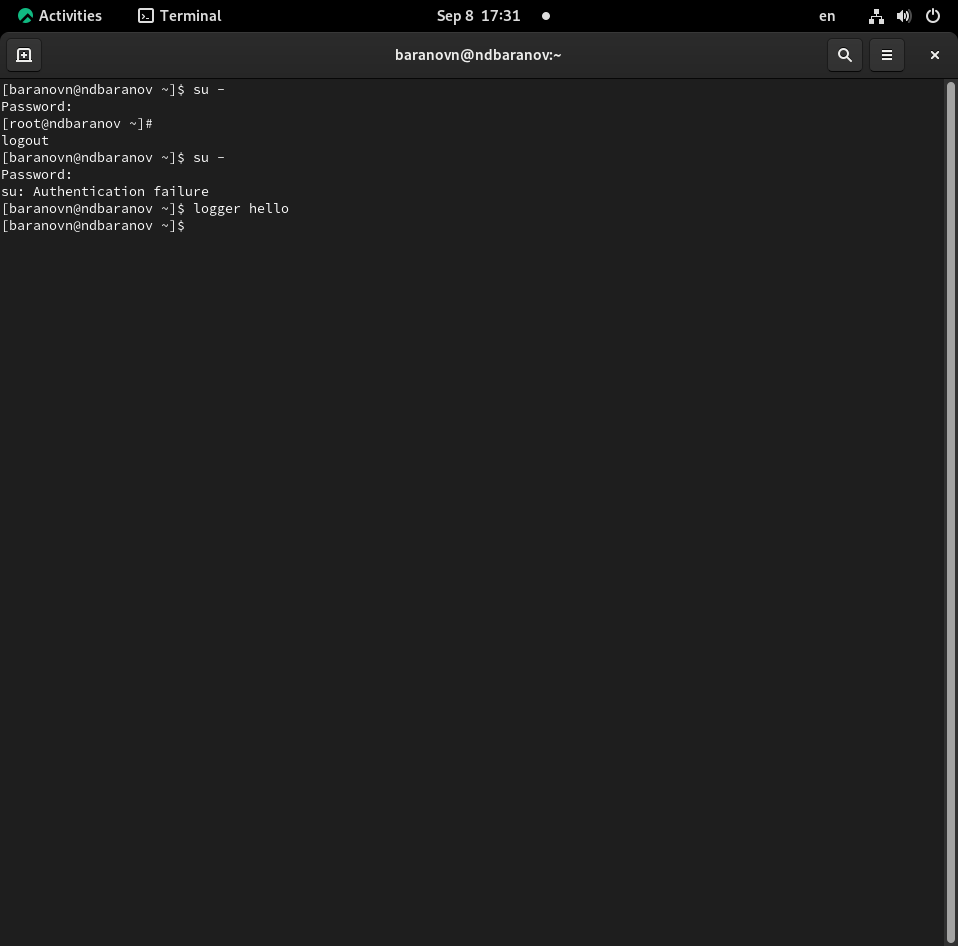
Получение прав администратора

На второй вкладке запускаем мониторинг системных событий в реальном времени (рис. [**fig:002?**]).



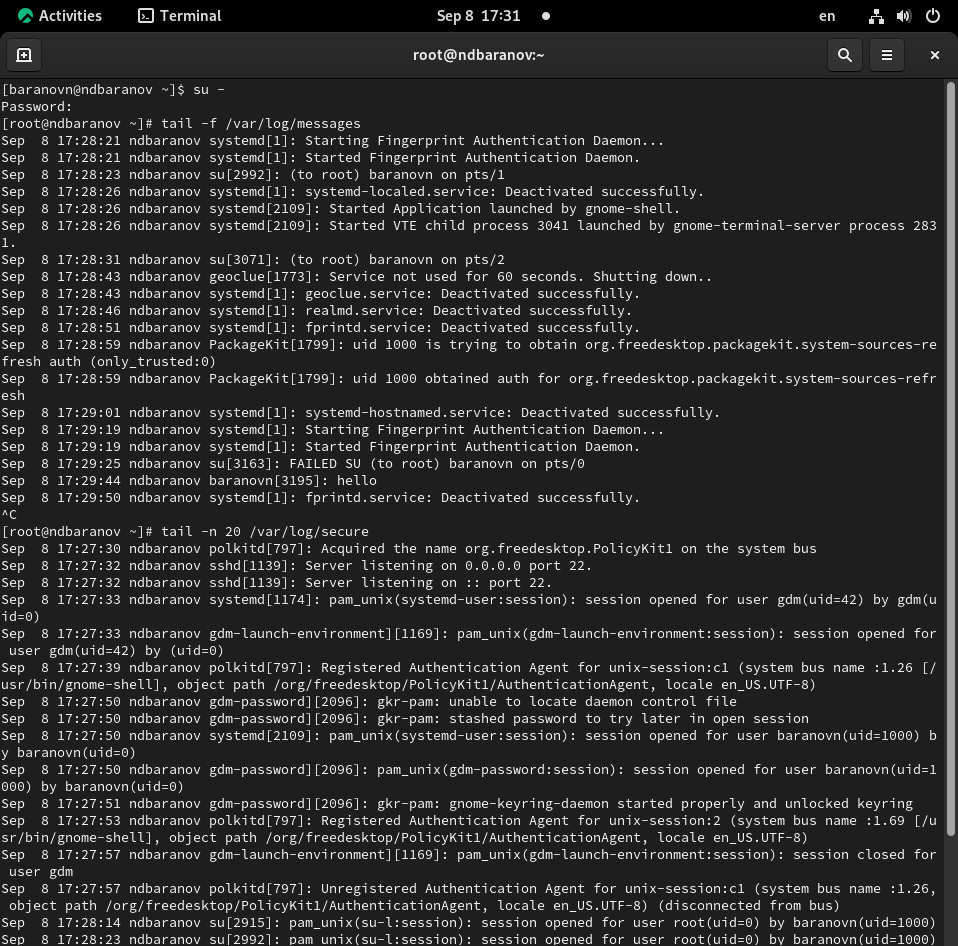
Мониторинг /var/log/messages

В третьей вкладке пытаемся получить полномочия администратора с неправильным паролем и видим сообщение об ошибке в логах (рис. [**fig:003?**]).



Неудачная попытка su и использование logger

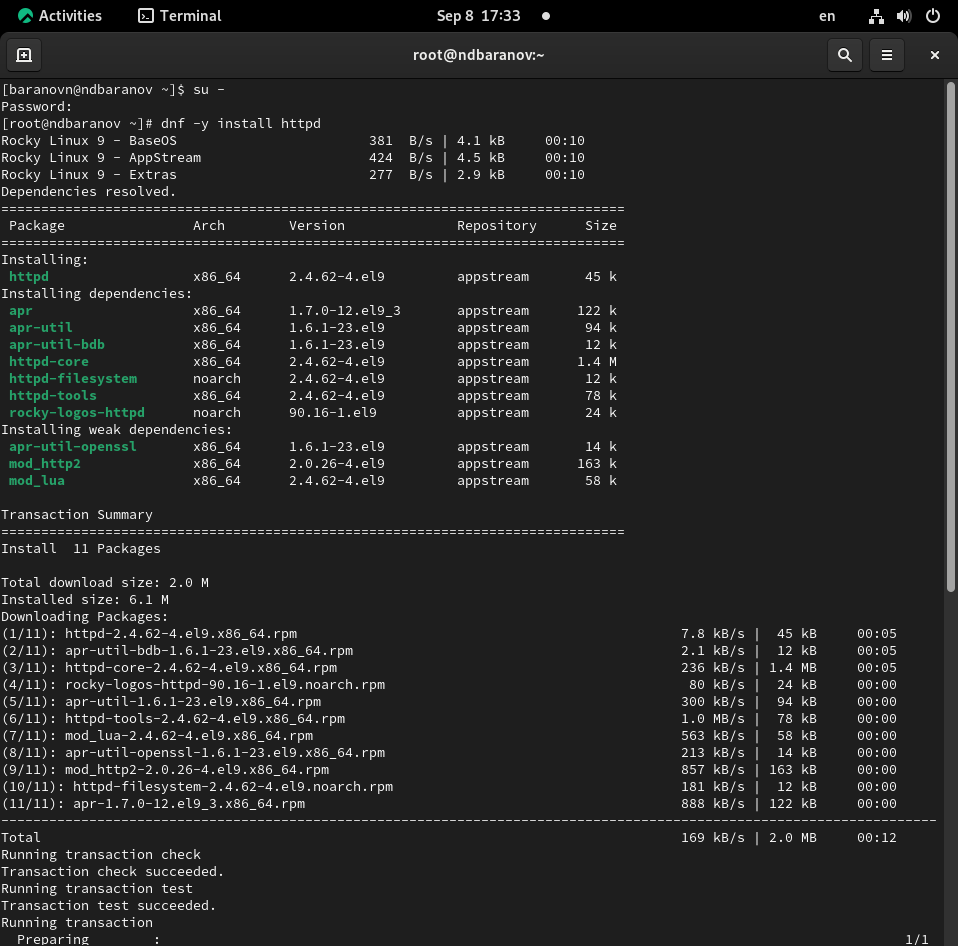
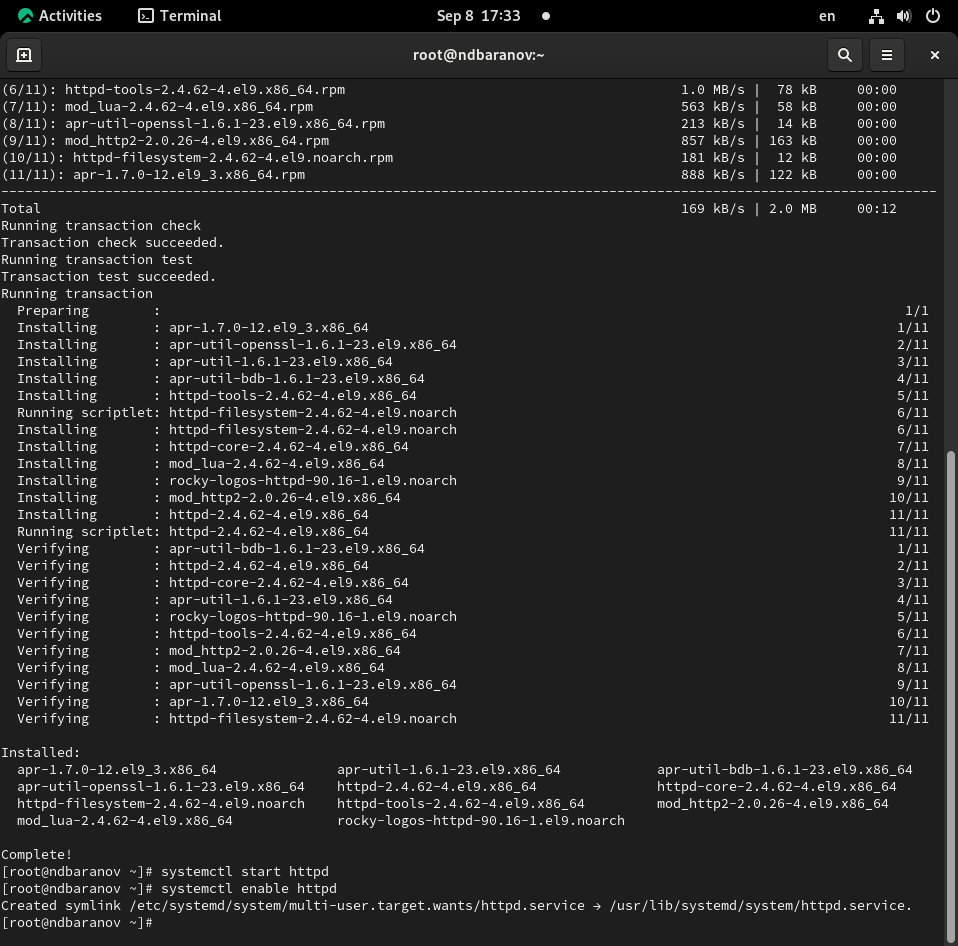
Просматриваем сообщения безопасности в /var/log/secure (рис. [**fig:002?**]).



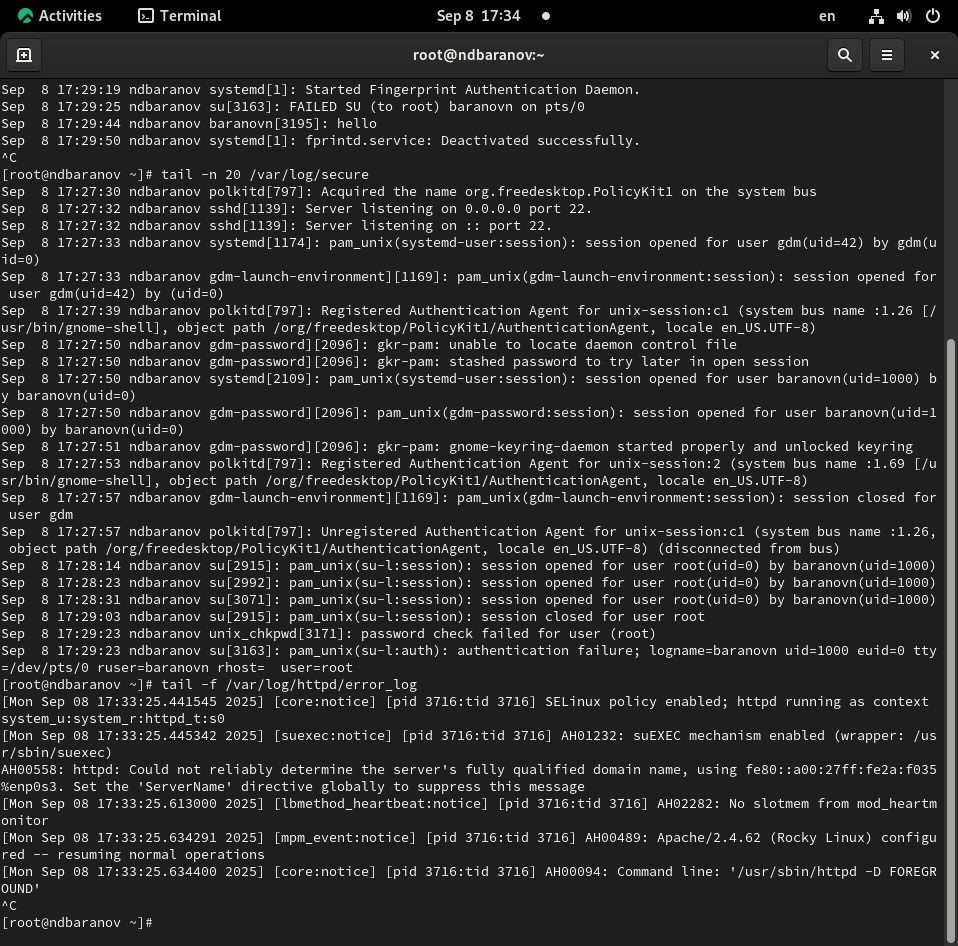
Просмотр логов безопасности

## 3.2 Настройка регистрации сообщений веб-службы

Устанавливаем и запускаем Apache HTTP server (рис. [**fig:004?**], [**fig:005?**]).

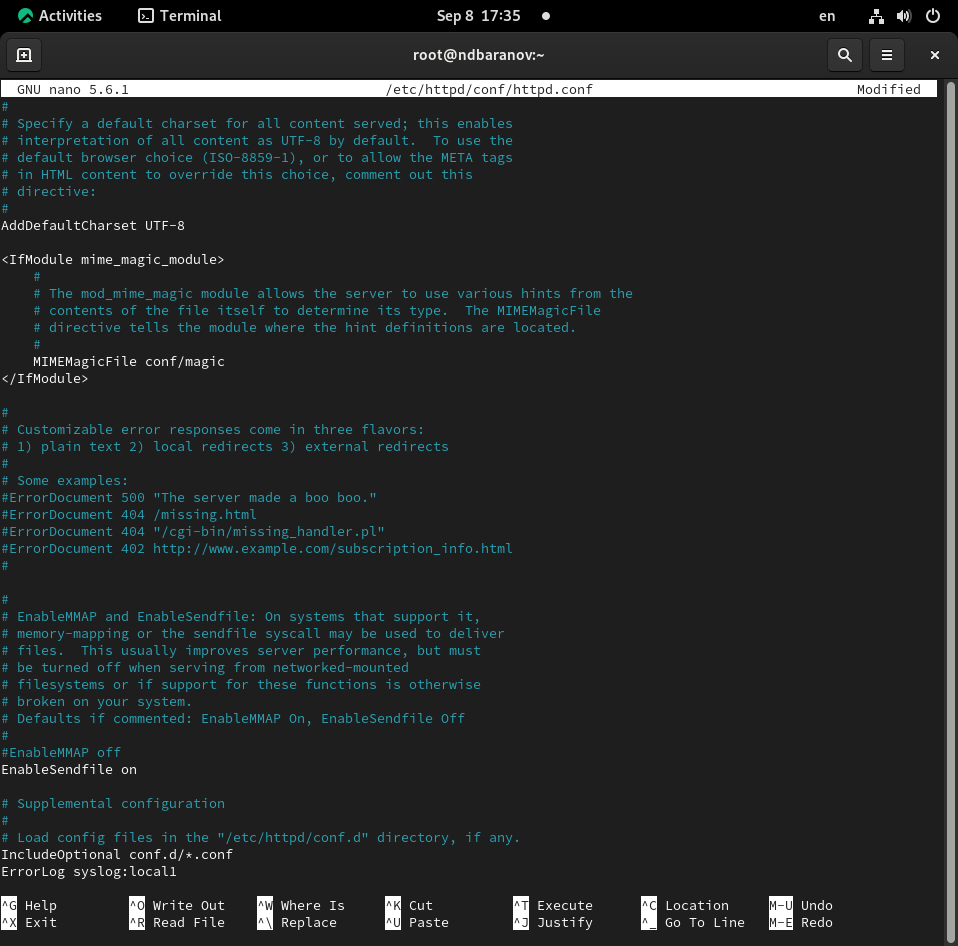
 

Просматриваем журнал ошибок веб-службы (рис. [**fig:006?**]).



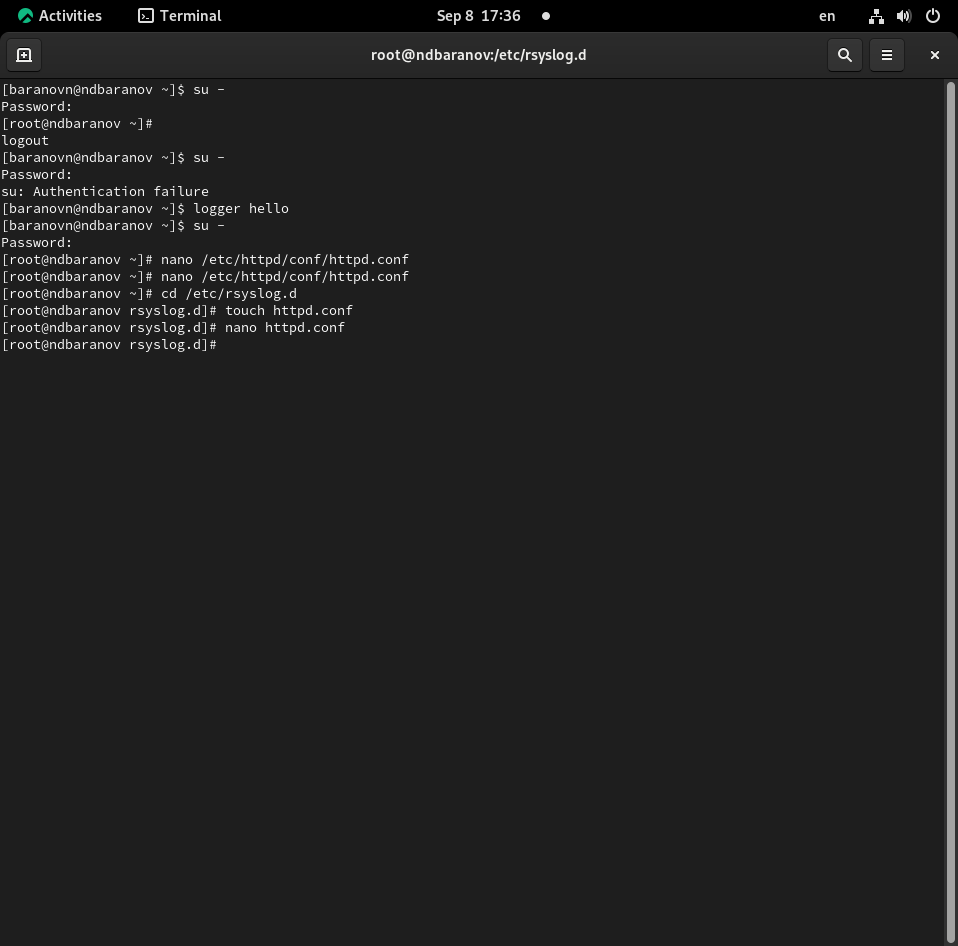
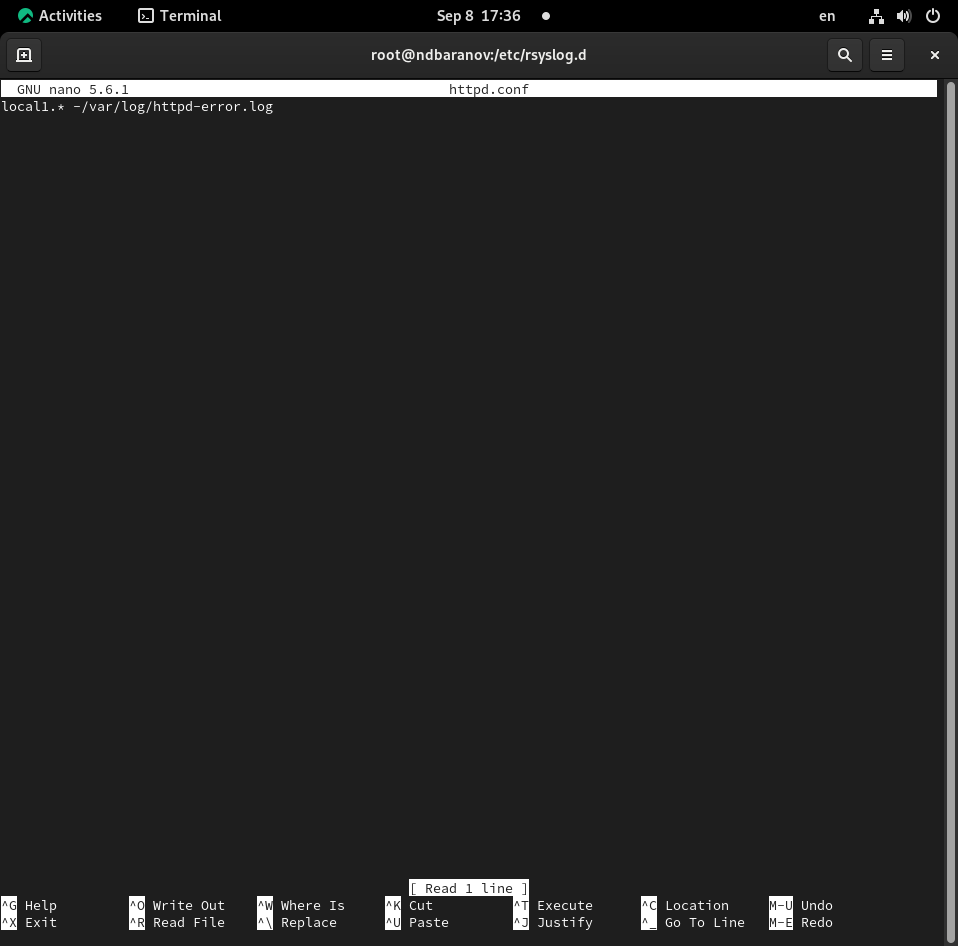
Просмотр error\_log Apache

Настраиваем Apache для использования syslog, добавляя строку в конфигурационный файл (рис. [**fig:007?**]).

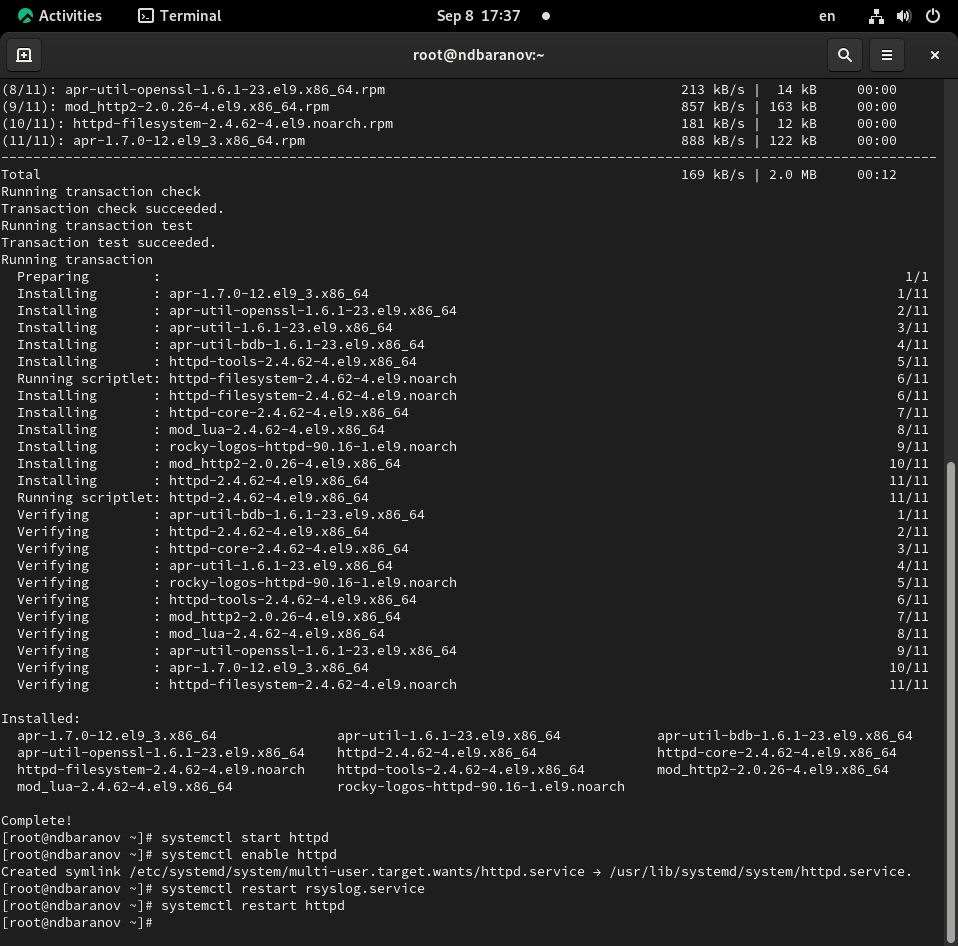


Настройка ErrorLog в httpd.conf

Создаем файл конфигурации для rsyslog и настраиваем перенаправление логов (рис. [**fig:008?**], [**fig:009?**]).

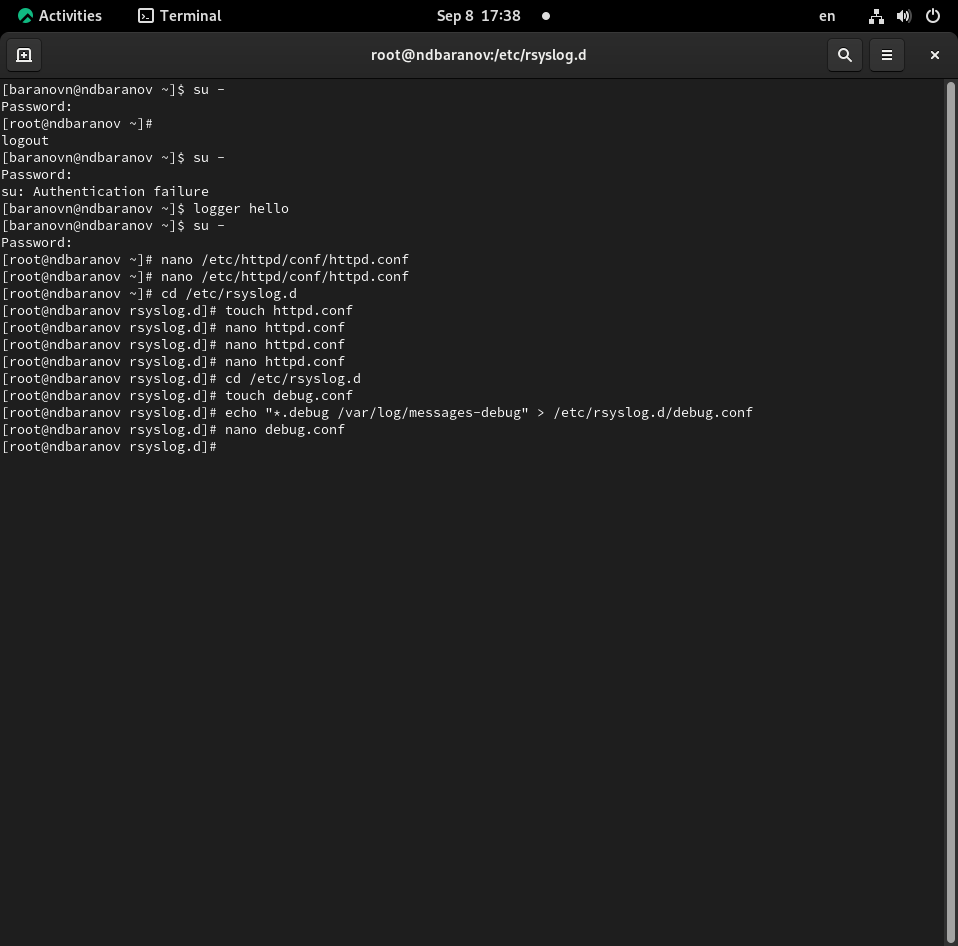
Перезапускаем службы и проверяем работу (рис. [**fig:010?**]).



Перезапуск служб

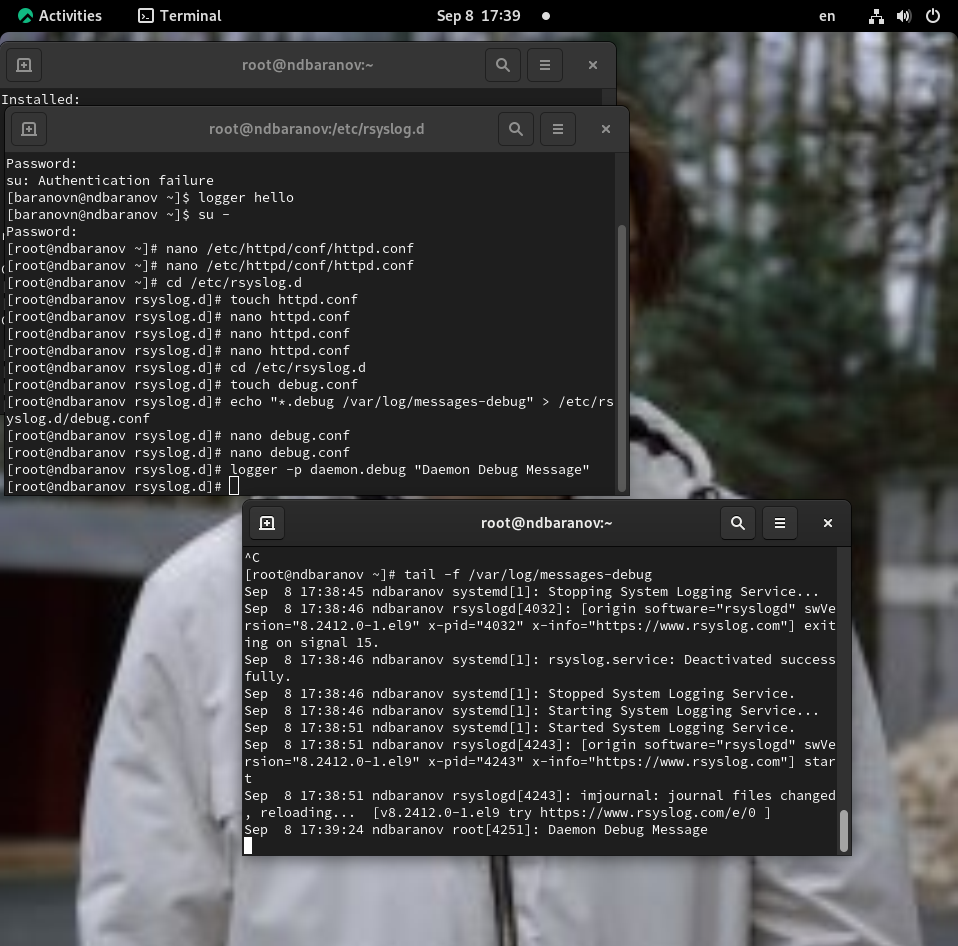
## 3.3 Настройка мониторинга отладочной информации

Создаем конфигурационный файл для отладочных сообщений (рис. [**fig:011?**]).



Создание debug.conf

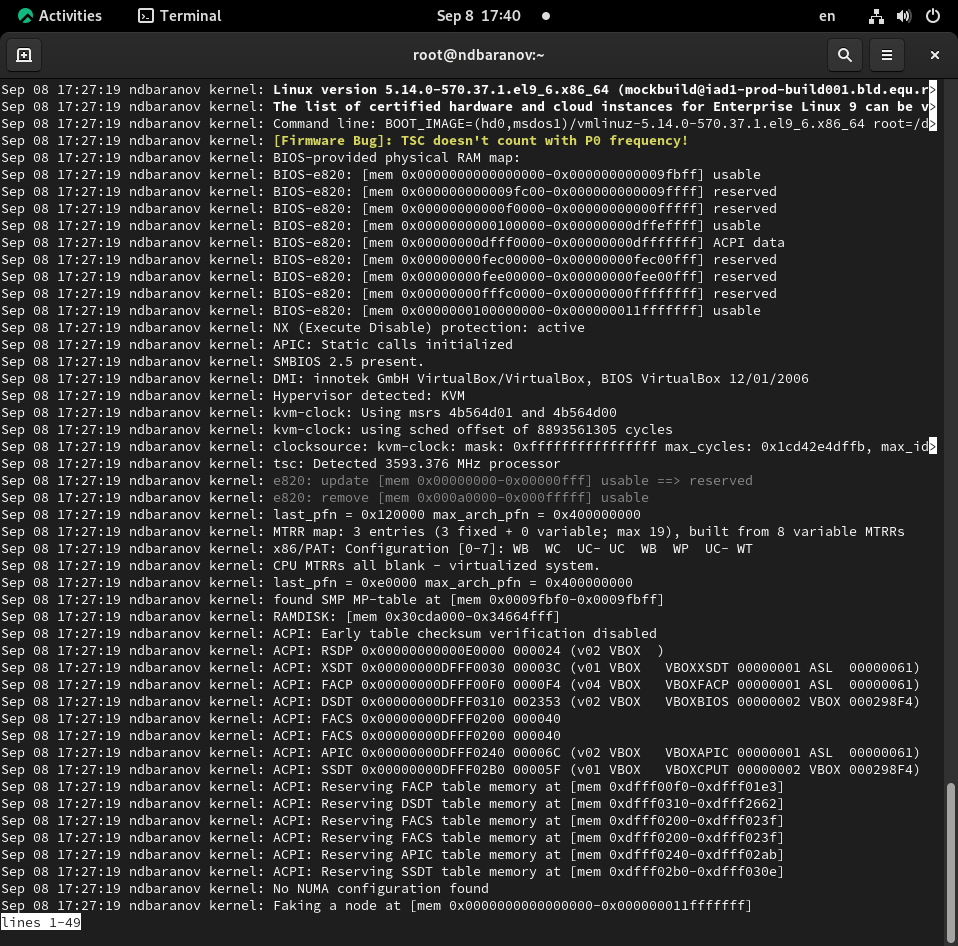
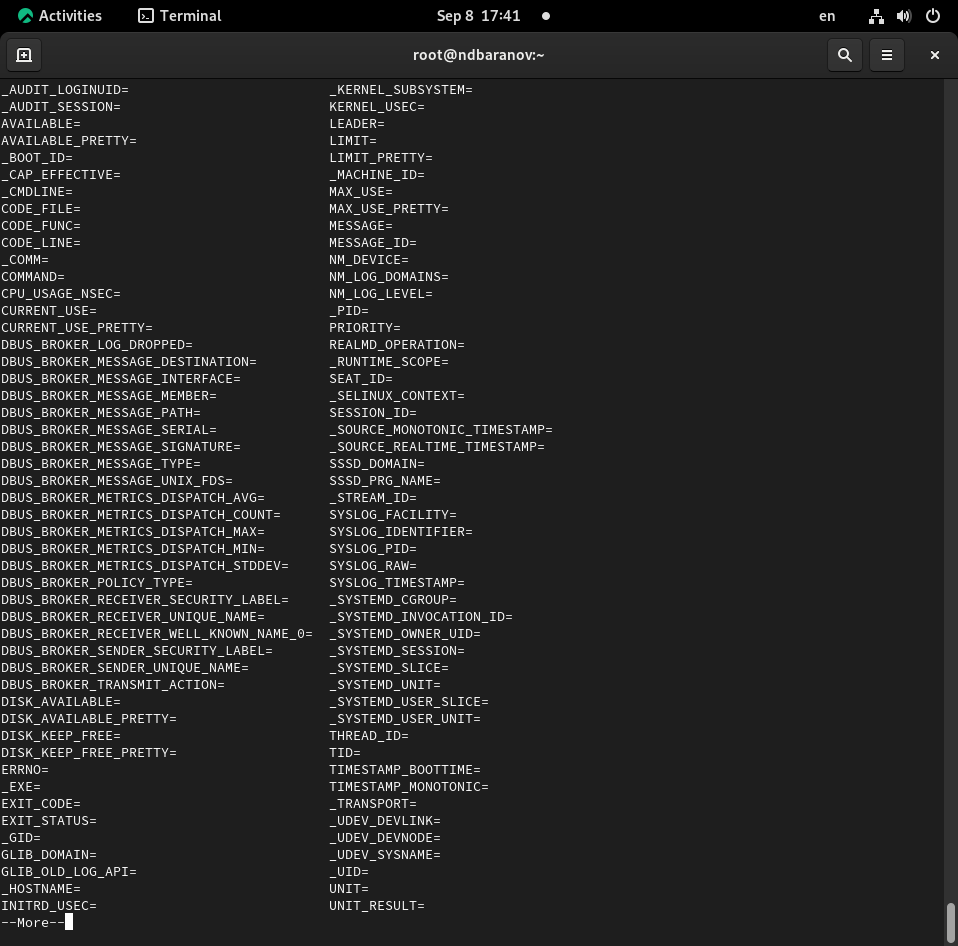
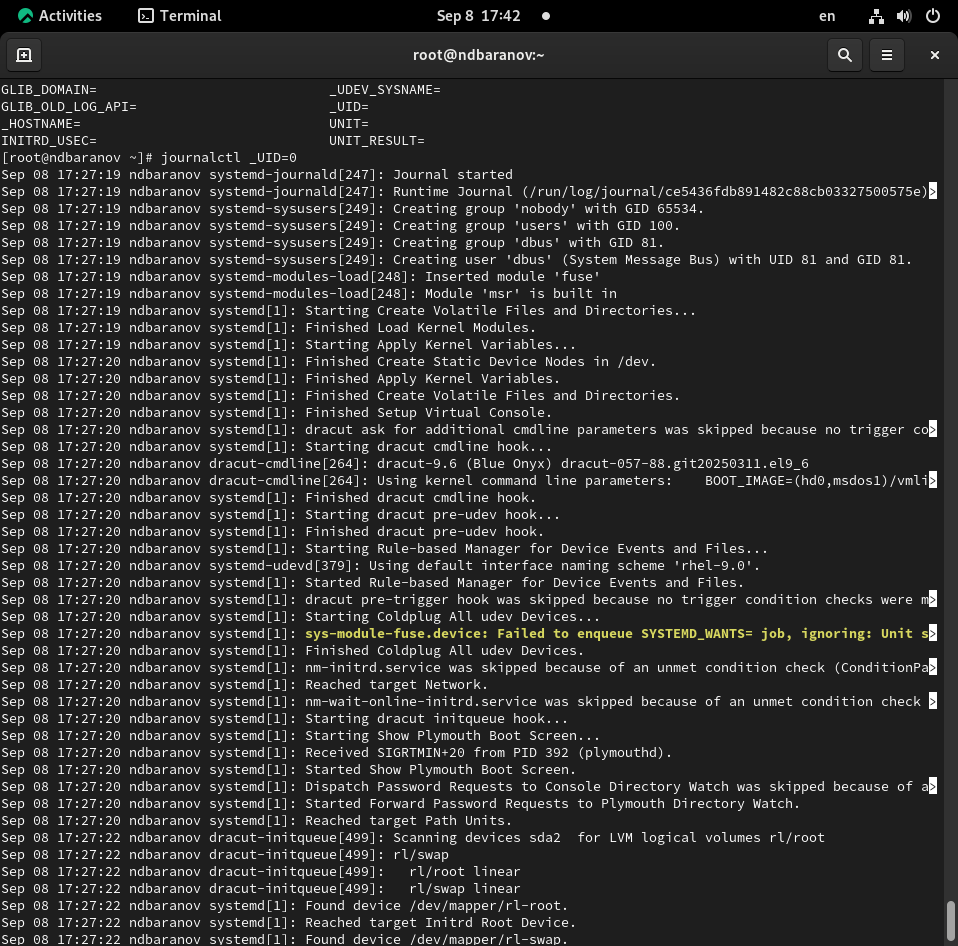
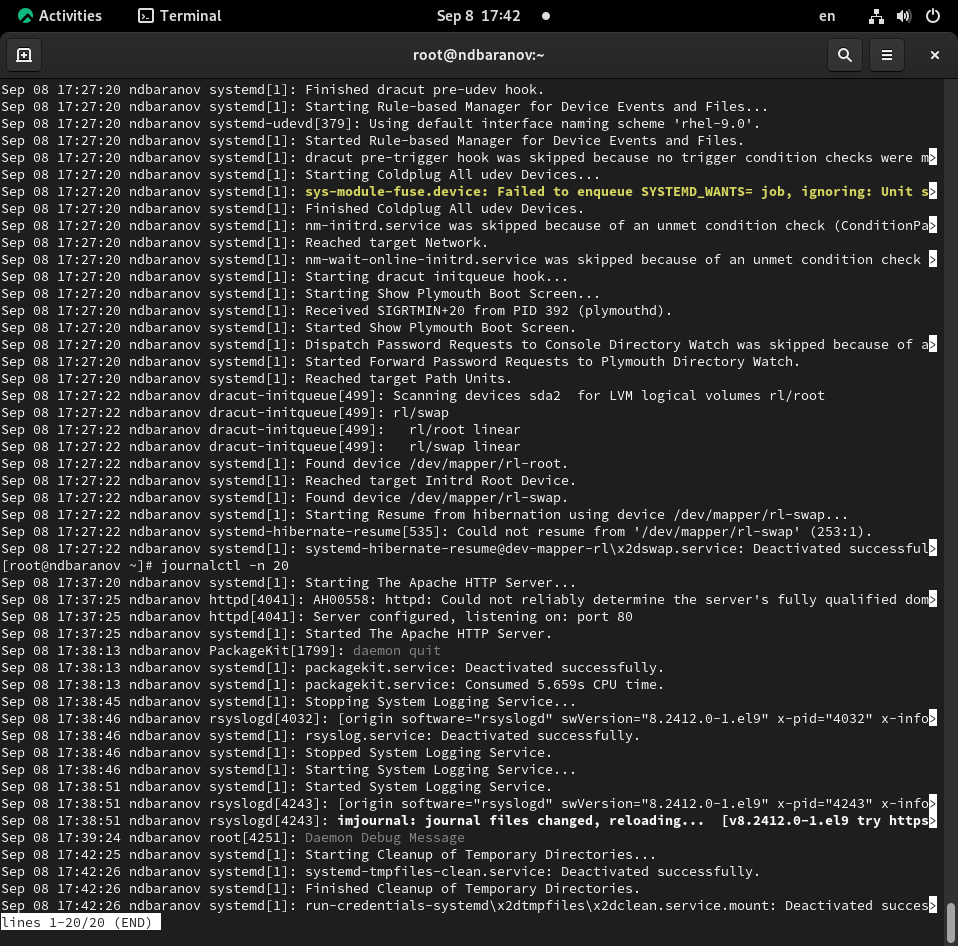
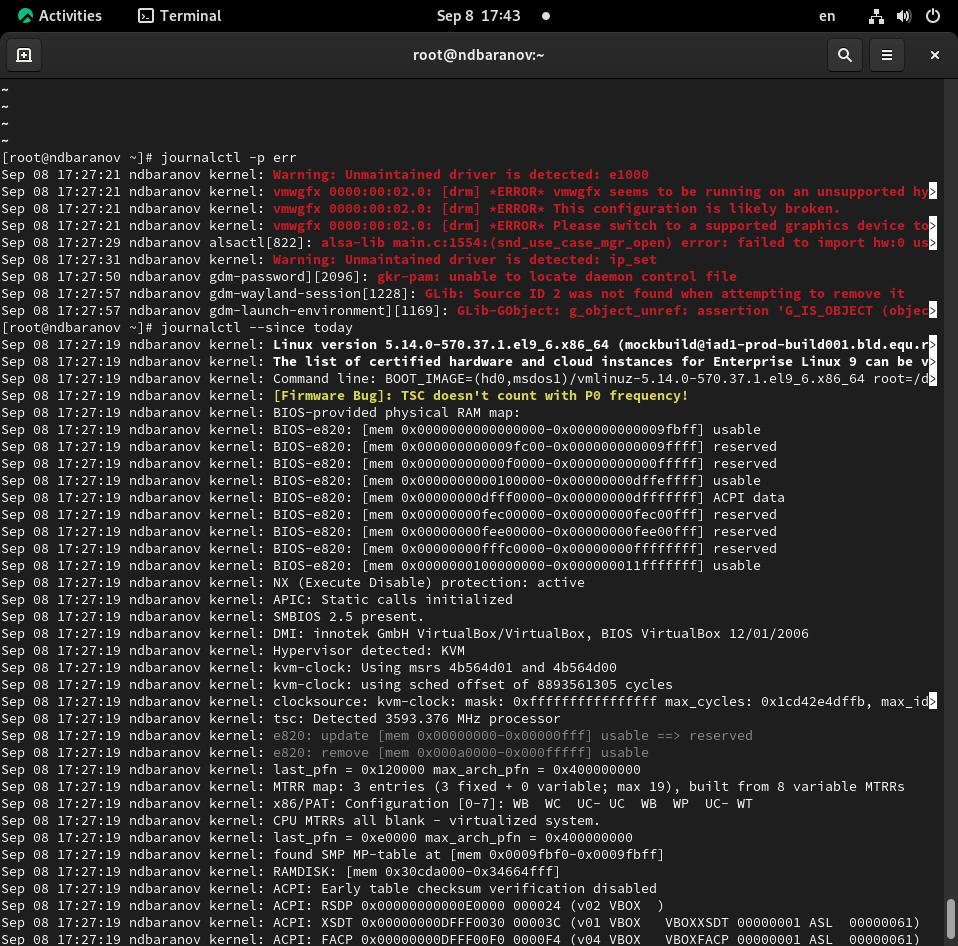
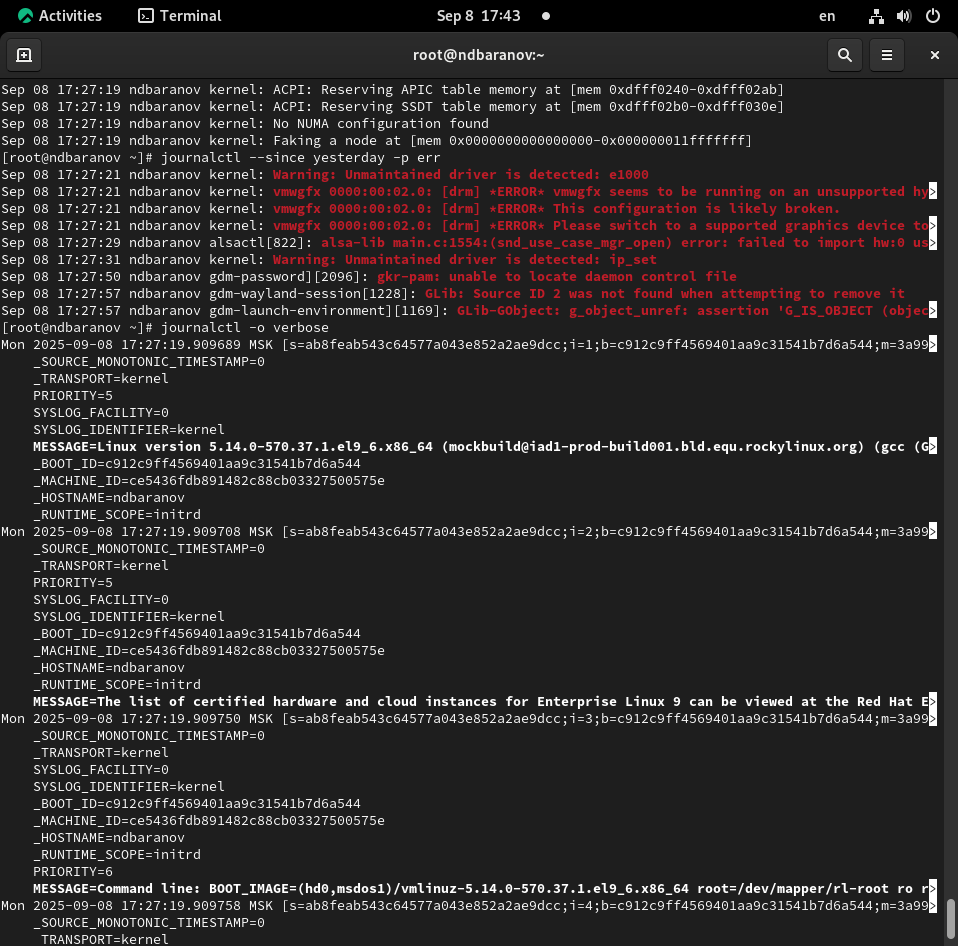
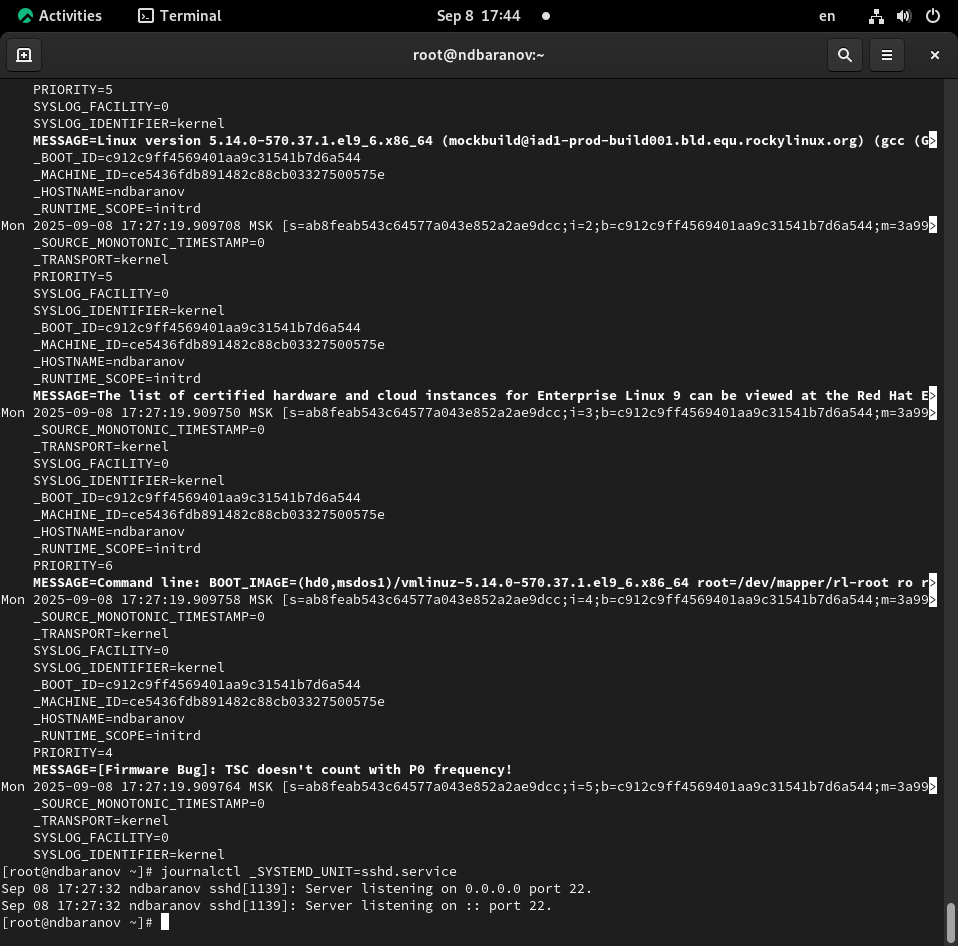
Перезапускаем rsyslog и тестируем отправку отладочного сообщения (рис. [**fig:012?**]).



Тестирование отладочных сообщений

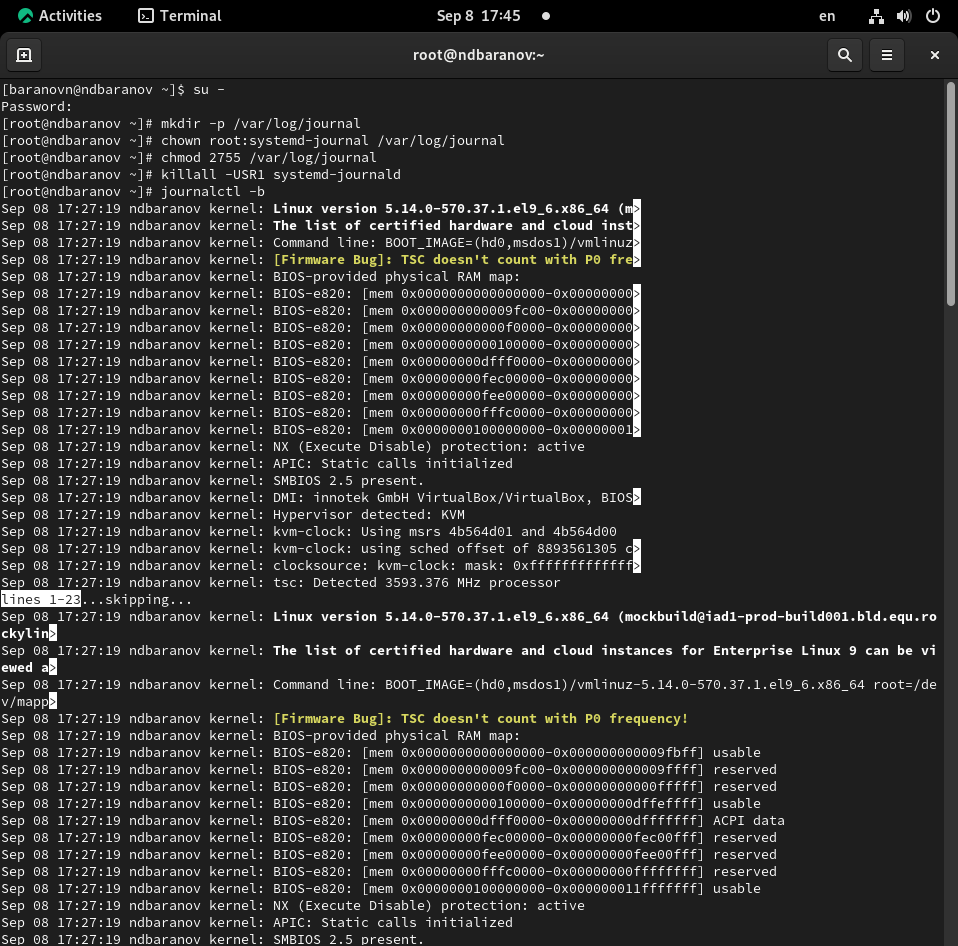
## 3.4 Работа с journalctl

Просматриваем различные варианты использования journalctl (рис. [**fig:013?**], [**fig:014?**], [**fig:015?**], [**fig:016?**], [**fig:017?**], [**fig:018?**], [**fig:019?**]).

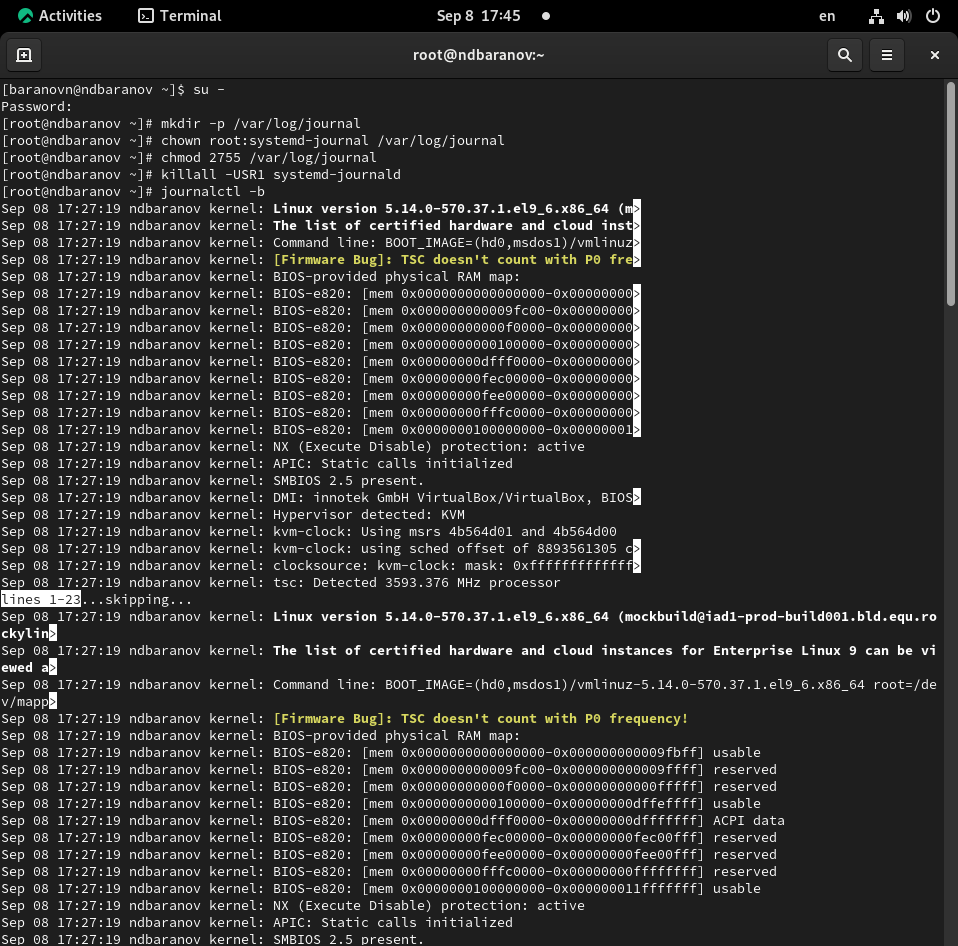
## 3.5 Настройка постоянного хранения журналов systemd

Создаем каталог для постоянного хранения журналов и настраиваем права доступа (рис. [**fig:020?**]).



Настройка постоянного хранения журналов

Применяем изменения и проверяем журнал с момента последней загрузки системы (рис. [**fig:020?**]).



Проверка журнала после настройки

# 4. Выводы

В ходе лабораторной работы были получены навыки работы с системными журналами операционной системы. Настроена регистрация сообщений веб-службы Apache через syslog, созданы правила для мониторинга отладочной информации и освоена работа с утилитой journalctl для просмотра и анализа журналов systemd. Также была выполнена настройка постоянного хранения журналов systemd в каталоге /var/log/journal, что позволяет сохранять записи журнала между перезагрузками системы.

# Список литературы