Лабораторная работа №6

Основы информационной безопасности

Кондрашова Анастасия Андреевна

Содержание

# 1 Цель работы

* Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1
* Проверить работу SELinx на практике совместно с веб-сервером Apache.

# 2 Выполнение лабораторной работы

1. С помощью команды getenforce убеждаемся, что SELinux работает в режиме enforcing, а с помощью комнды sestatus устанавливаем политику targeted

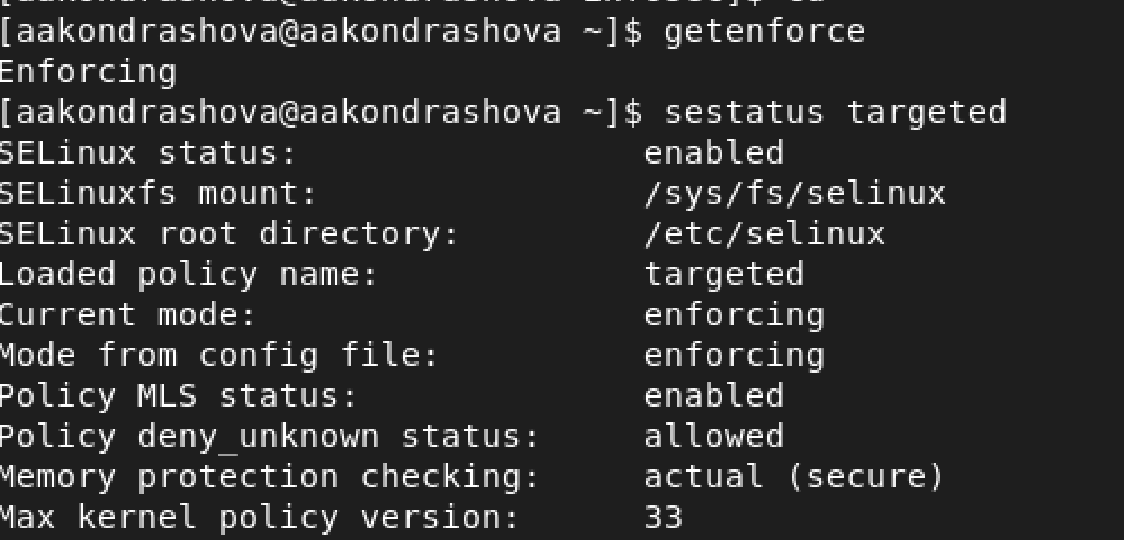


Рис. 1: Getenforce и sestatus

1. Убеждаемся, что сервер работает с помощью команды service httpd status

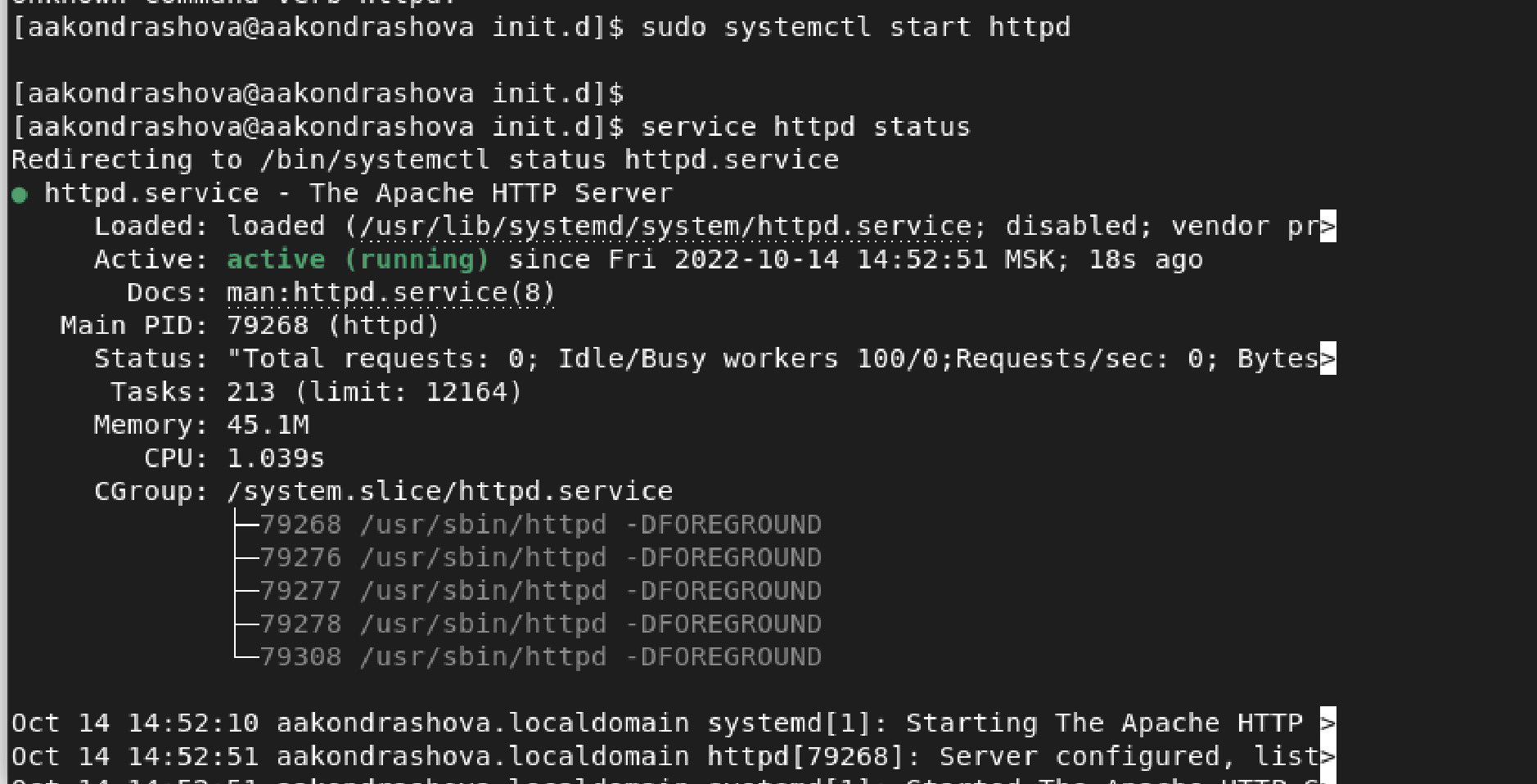


Рис. 2: Работа сервера

1. С помощью команды ps -eZ находим, что контекст безопасности Apache - httpd\_t

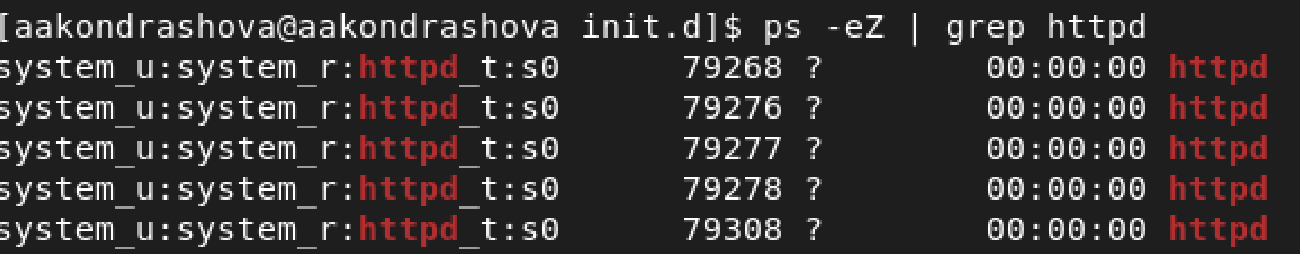


Рис. 3: Контекст безопасности

1. Смотрим текущее состояние переключателей командой sestatus -b httpd

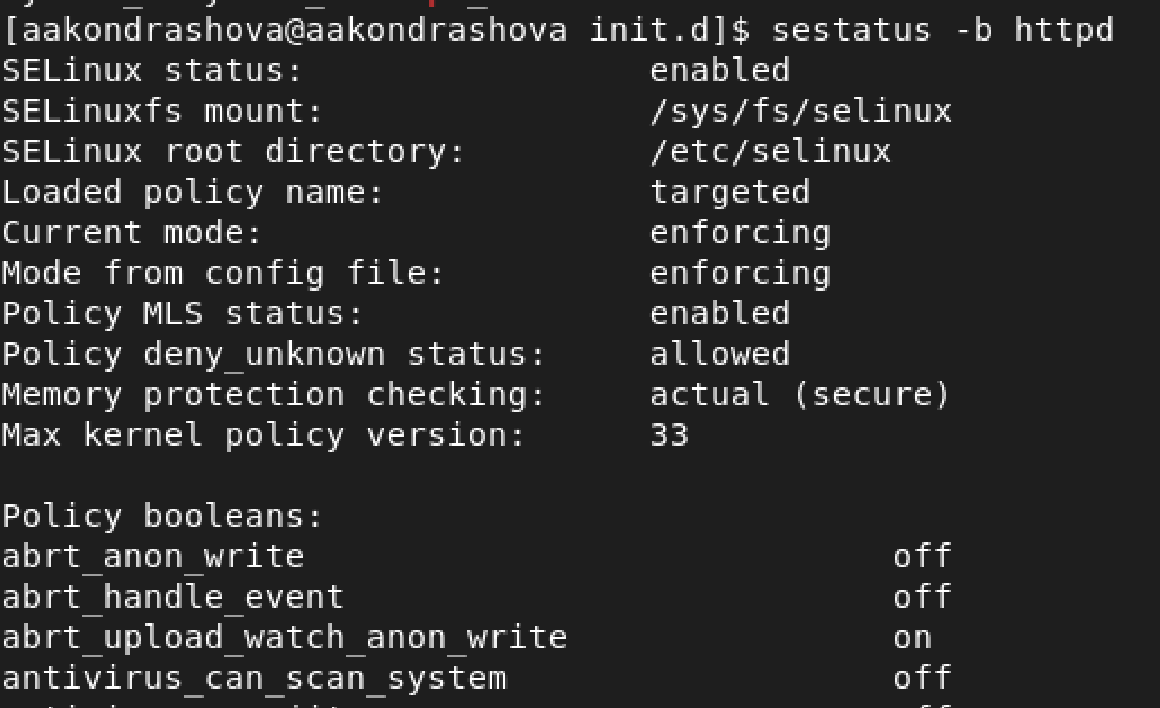


Рис. 4: Текущее состояние переключателей

1. Смотрим статистику по политике командой seinfo. Узнаём, что множество пользователей — 8, ролей — 14, типов — 5002

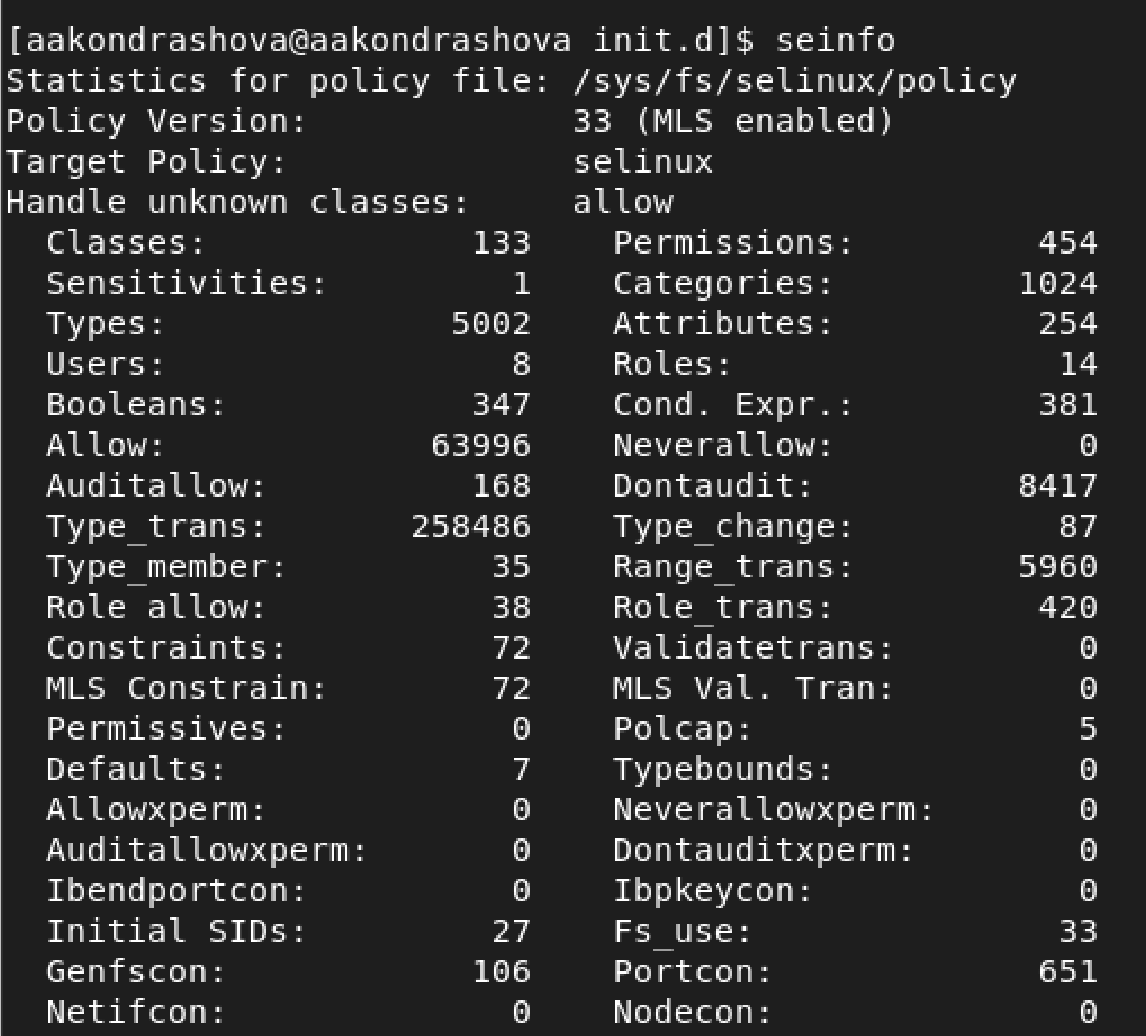


Рис. 5: Статистика по политике

1. Определяем тип файлов и круг пользователей с правой на создание и поддиректорий в директориях /var/www и /var/www/html командой ls -lZ

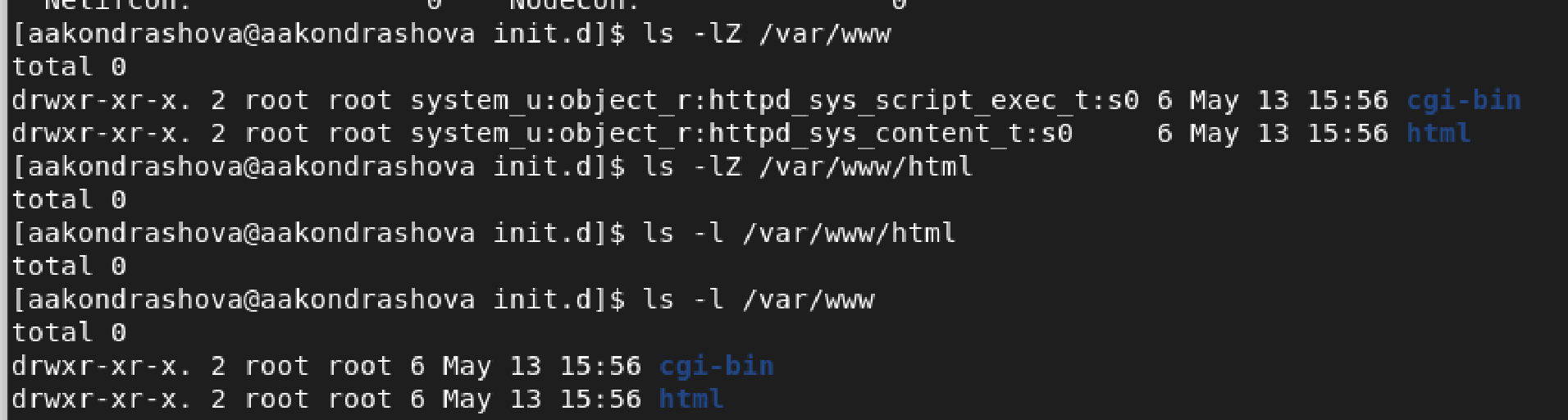


Рис. 6: тип файлов и круг пользователей

1. От имени суперпользователя создаём файл /var/www/html/test.html

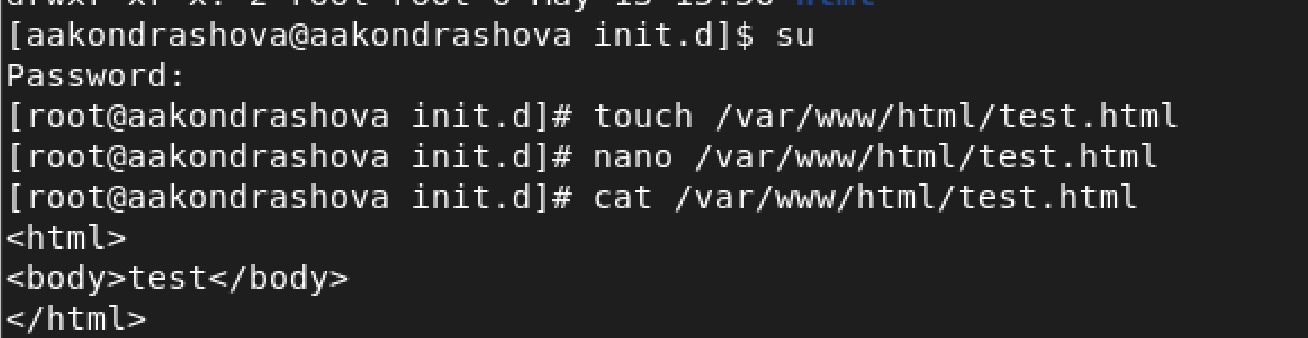


Рис. 7: Создание файла

1. Командой matchpathcon узнаём контекст файла test.html и директории /var/www/html — это httpd\_sys\_content\_t.

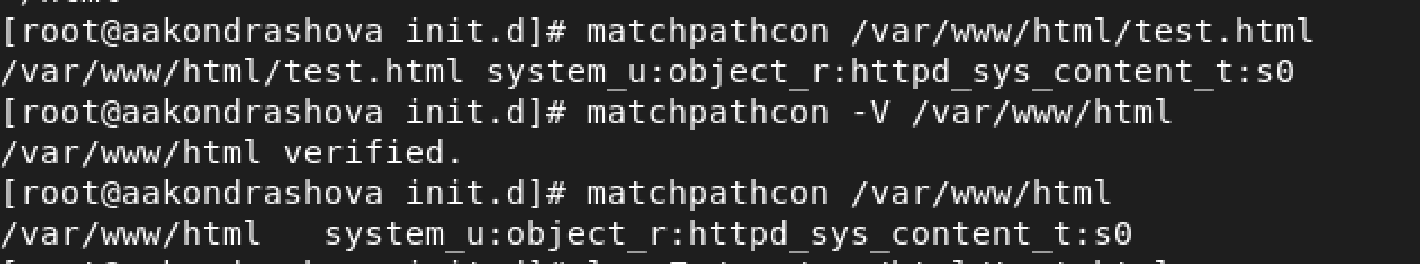


Рис. 8: Констекст файла

1. Обращаемся к файлу через ссылку в веб-браузере. Контент отображён корректно.

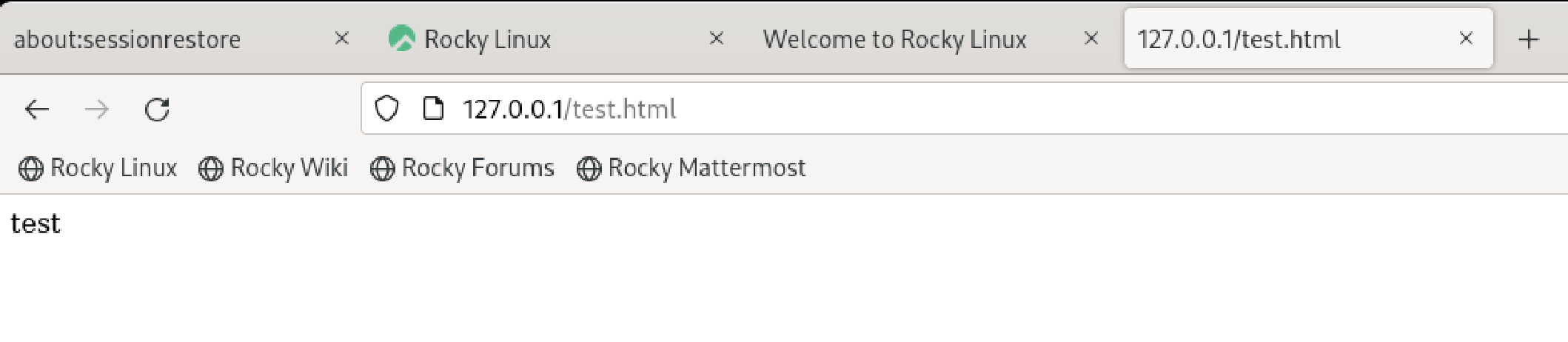


Рис. 9: Корректное отображение контента

1. Изучая справку man httpd\_selunix узнаём, что для httpd определены следующие контексты: httpd\_sys\_content\_t, httpd\_sys\_script\_exec\_t, httpd\_sys\_script\_ro\_t, httpd\_sys\_script\_rw\_t, httpd\_sys\_script\_ra\_t, httpd\_unconfined\_script\_exec\_t. Меняем контекст файла test.html командой chcon -t.

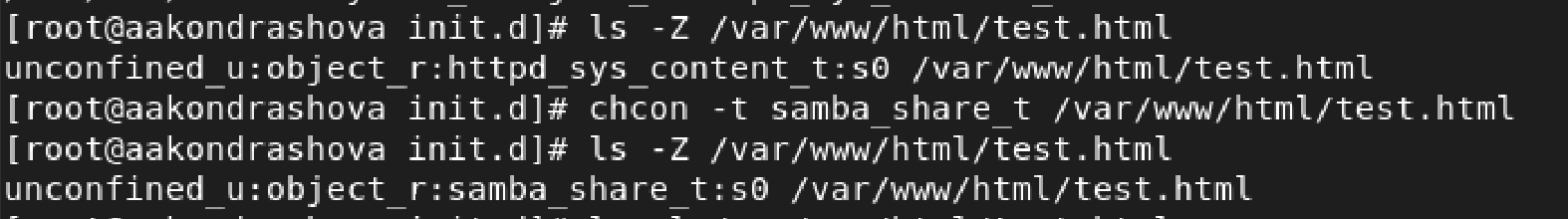


Рис. 10: Смена контекста

1. При повторной попытке открыть файл через веб-браузер получаем ошибку доступа.

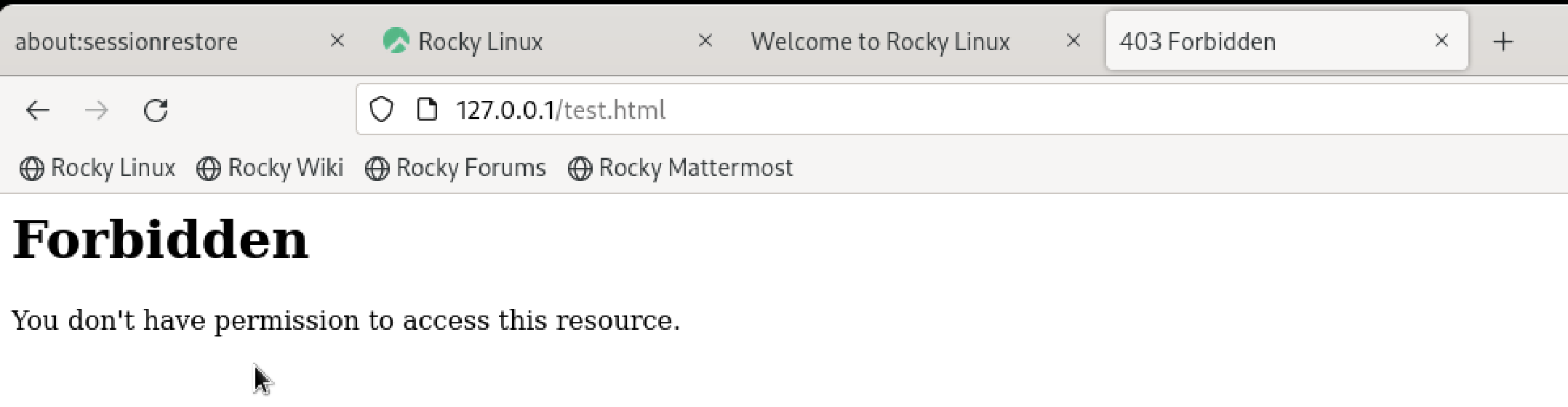


Рис. 11: Ошибка доступа

1. Убеждаемся, что файл доступен для чтения всем пользователям командой ls -l. Далее смотрим log-файлы веб-сервера Apache командой tail, где показаны ошибки.

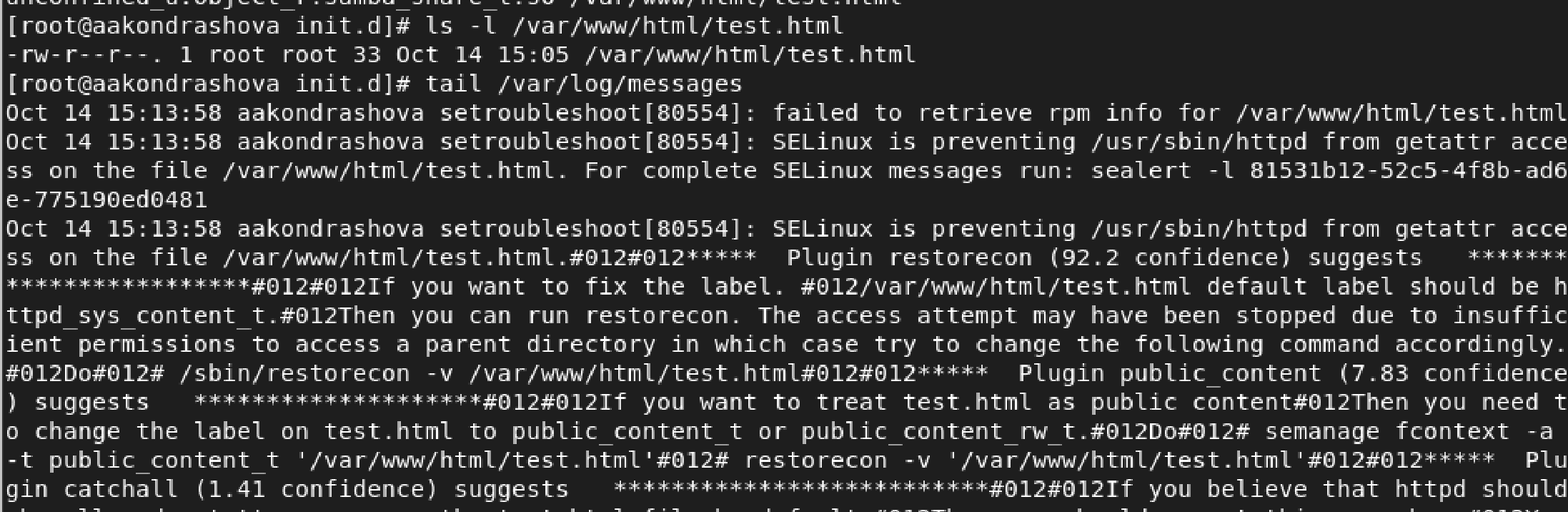


Рис. 12: Просмотр логов

1. Устанавливаем веб-сервер Apache на прослушивание TCP-порта 81, изменяя строку Listen в файле /etc/httpd/conf/httpd.conf.

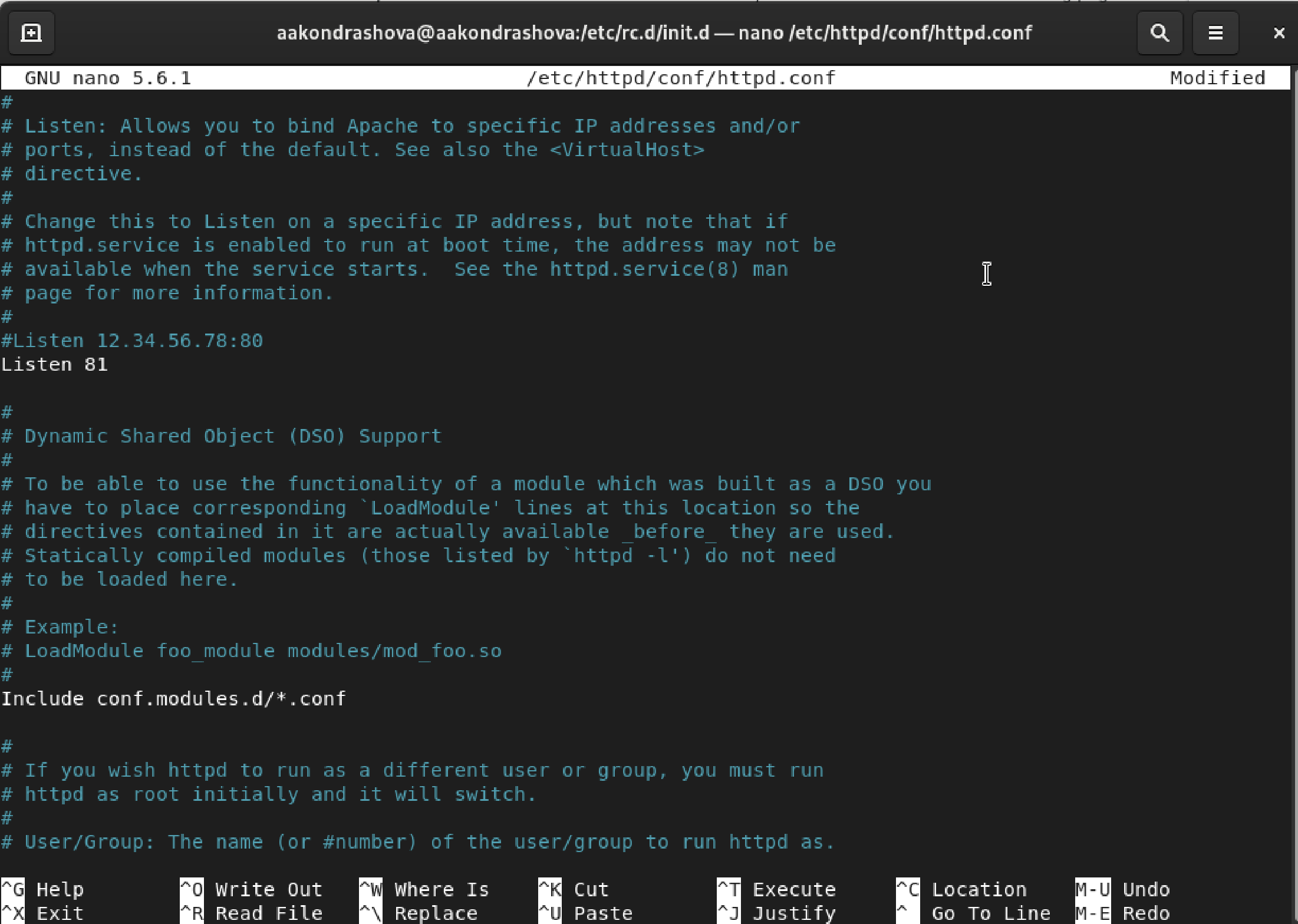


Рис. 13: Прослушивание 81 порта

1. Перезапускаем сервер и смотри данные log-файлов веб-сервера Apache.

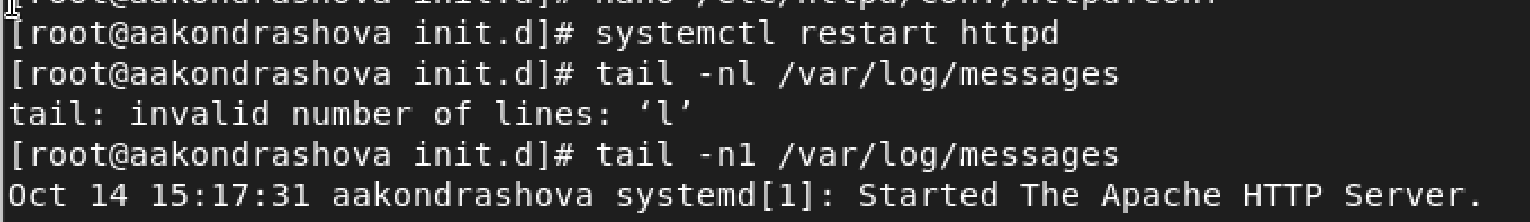


Рис. 14: Перезапуск сервера

1. Устанавлием для веб-сервера Apache порт TCP-81 и проверяем его наличие в списке портов командой semanage.

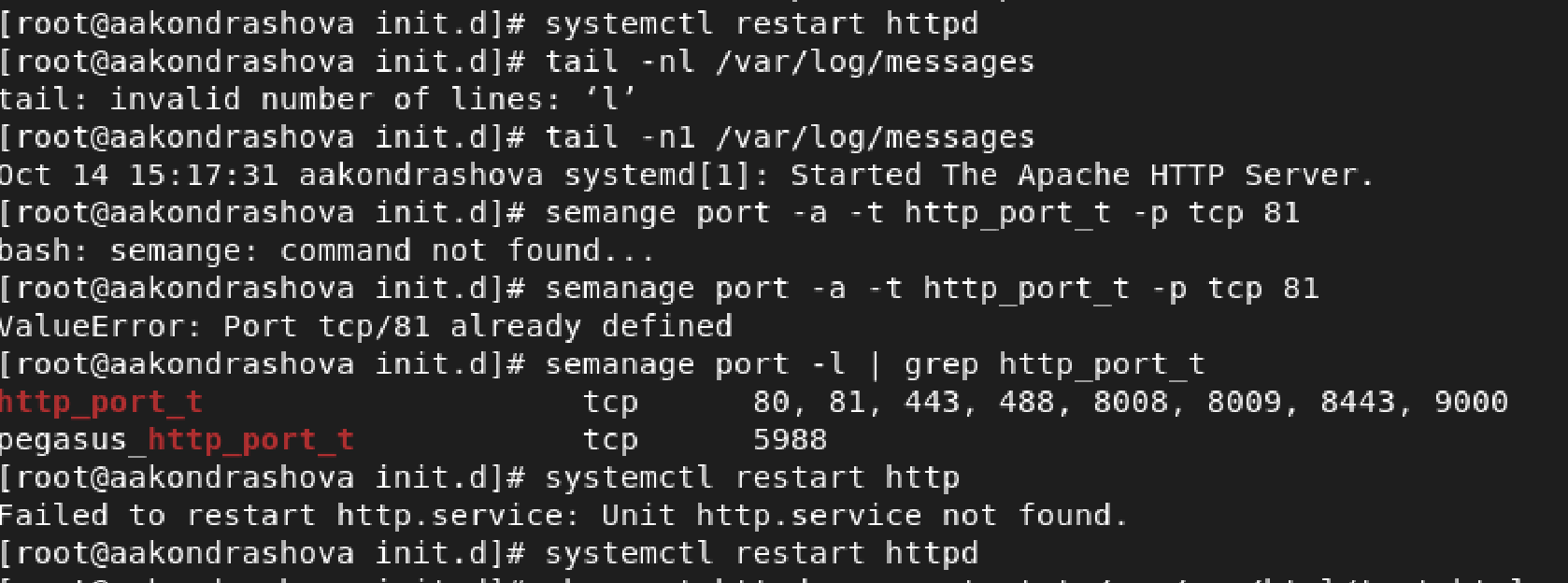


Рис. 15: Установка порта 81

1. Возвращаем файлу test.html контекст httpd\_sys\_content\_t и снова успешно просматриваем страницу в веб-браузере.

Рис. 16: Смена контекста 2

Рис. 16: Смена контекста 2

1. Возвращаем в конфигурационный файл прослушивание порта 80 и удаляем порт 81 из списка портов.

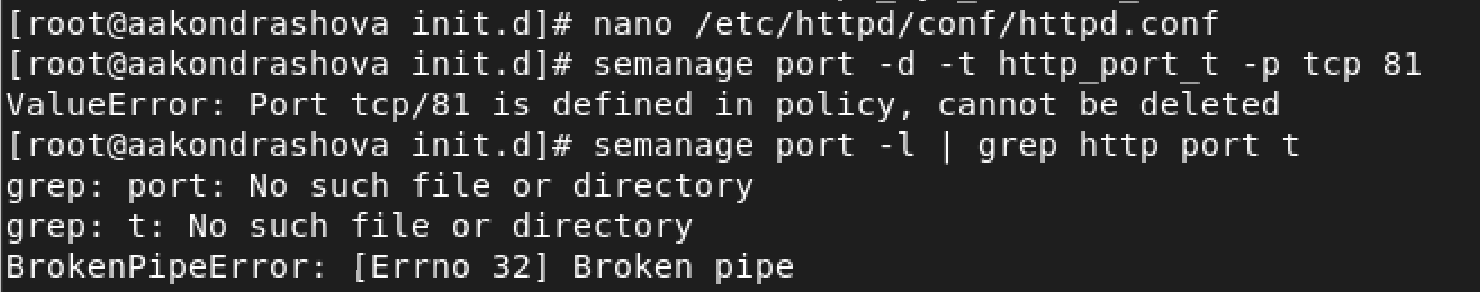


Рис. 17: Удаление 81 порта

1. Удаляем файл test.html.

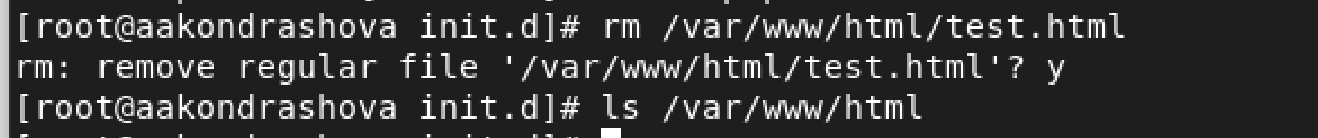


Рис. 18: Удаление файла

# 3 Выводы

Я получила основные навыки администрирования в OC Linux и проверила работу SELinux на практике совместно с веб-сервером Apache.