Лабораторная работа №6

Мандатное разграничение прав в Linux

Маслова Анастасия Сергеевна

Содержание

[1 Цель работы 1](#_Toc179625937)

[2 Выполнение лабораторной работы 1](#_Toc179625938)

[3 Вывод 8](#_Toc179625939)

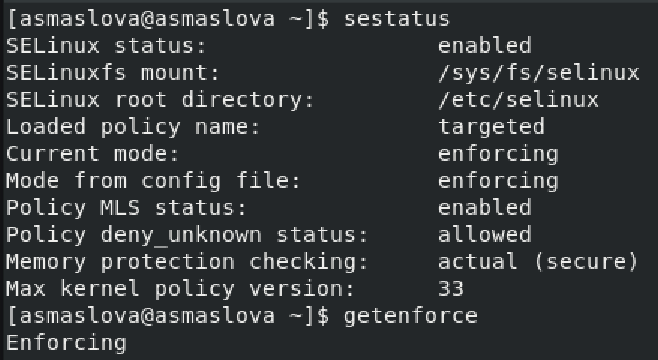
[Список литературы 8](#_Toc179625940)

# 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.

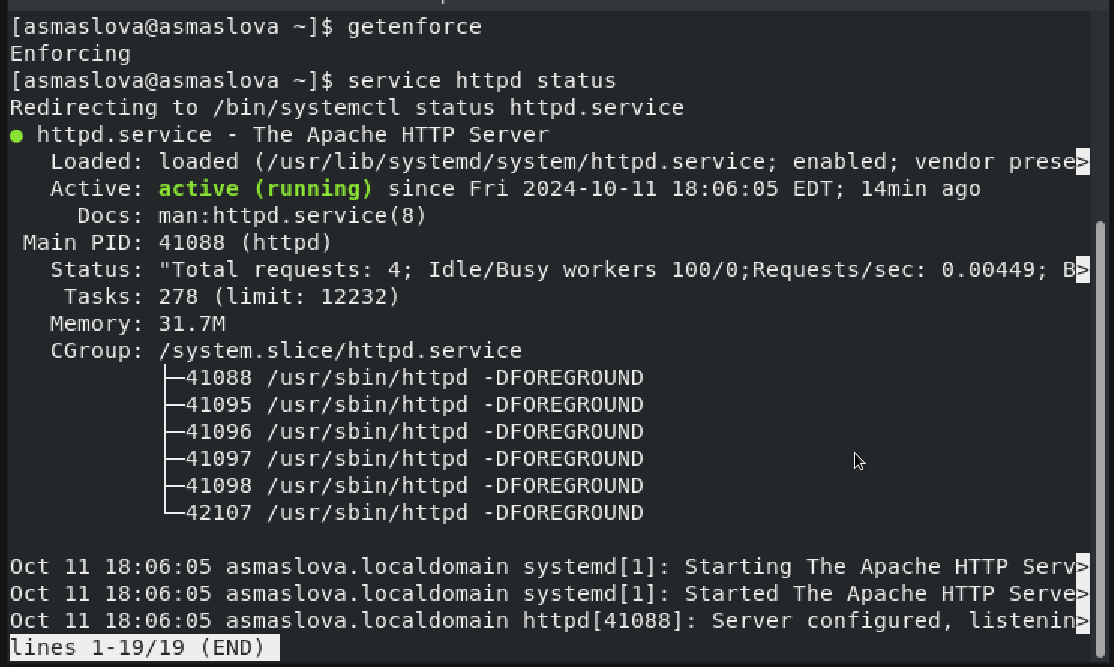
# 2 Выполнение лабораторной работы

1. Войдя в систему с полученными учётными данными, я убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus (рис. [??]).



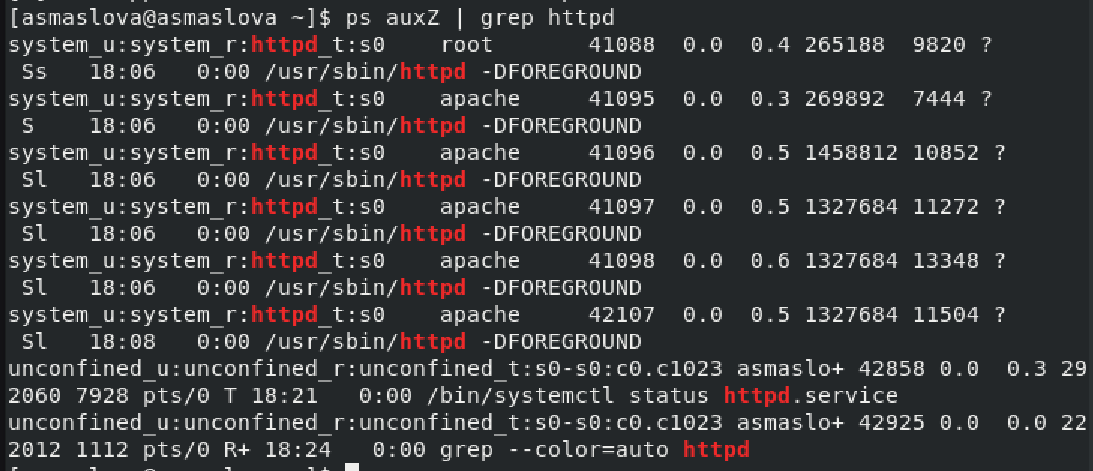
Выполнение команд getenforce и sestatus

1. С помощью браузера я обратилась к веб-серверу, запущенному на моем компьютере, и убедилась, что последний работает, с помощью команды service httpd status (рис. [??]).



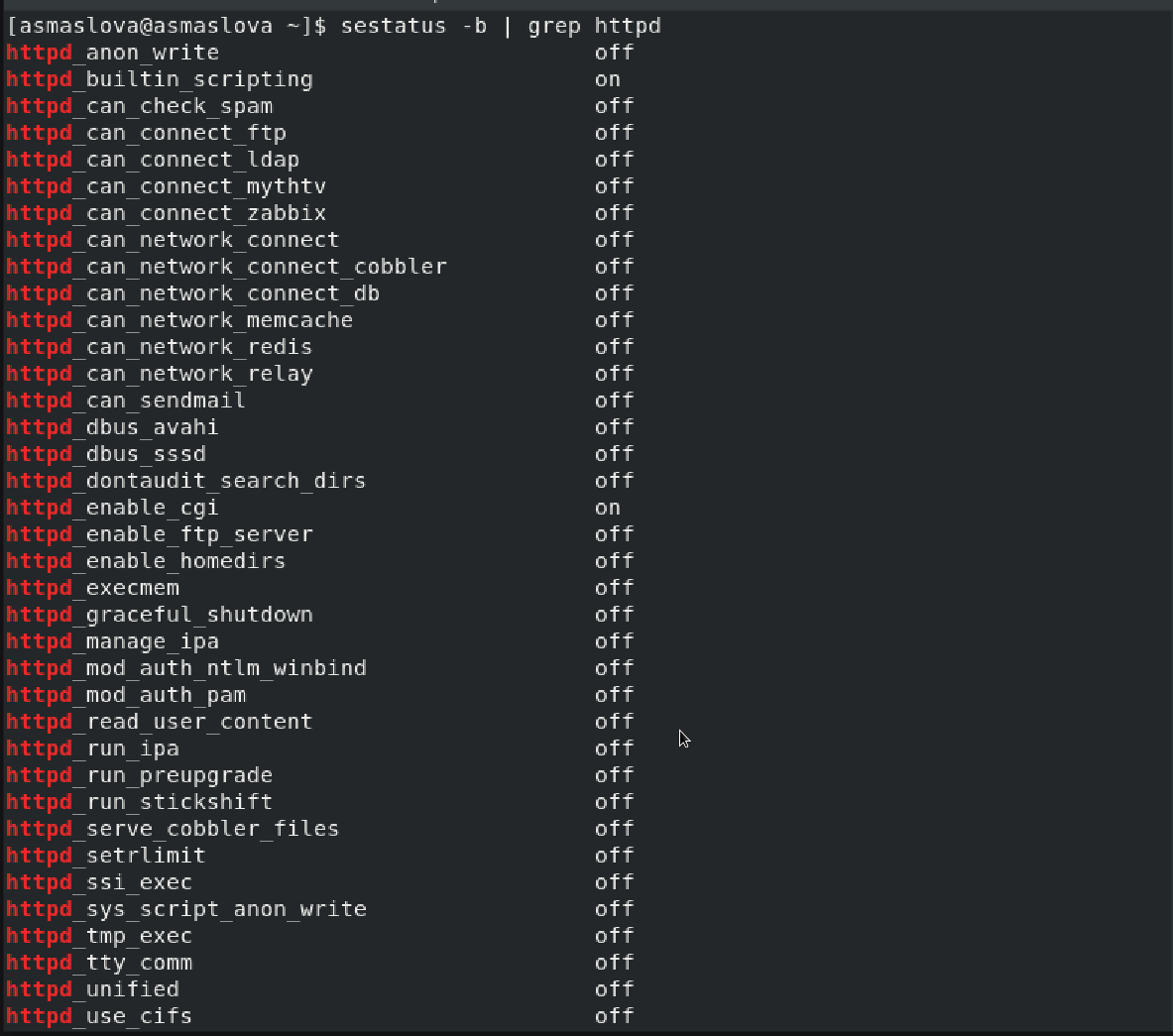
Выполнение команды service httpd status

1. В списке процессов я нашла веб-сервер Apache и определила его контекст безопасности. Для этого я использовала команду ps auxZ | grep httpd (рис. [??]).

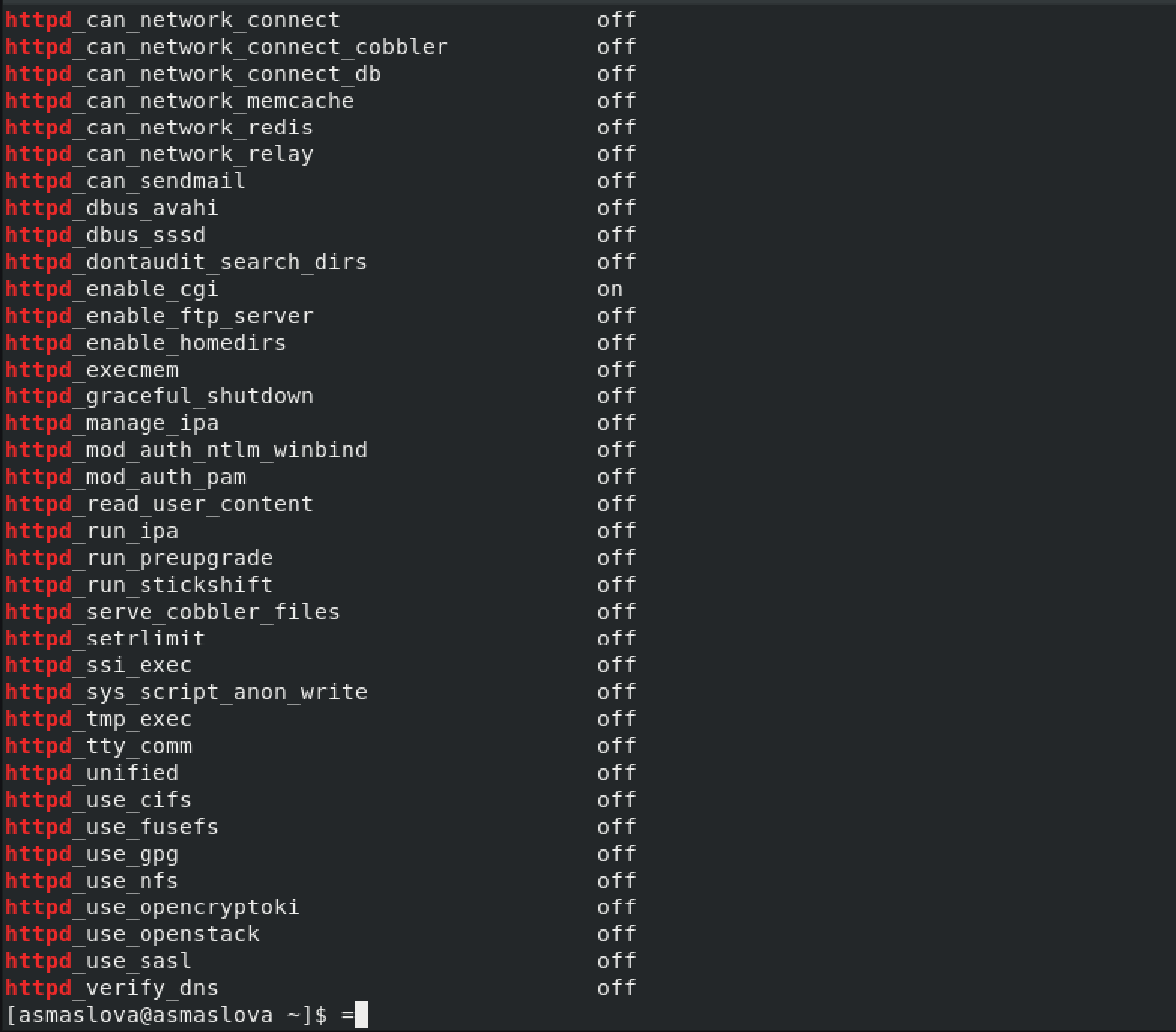


Выполнение команды ps auxZ | grep httpd

1. С помощью команды sestatus -bigrep httpd я посмотрела текущее состояние переключателей SELinux для Apache (рис. [??], [??]). Многие переключатели находятся в положении «off».

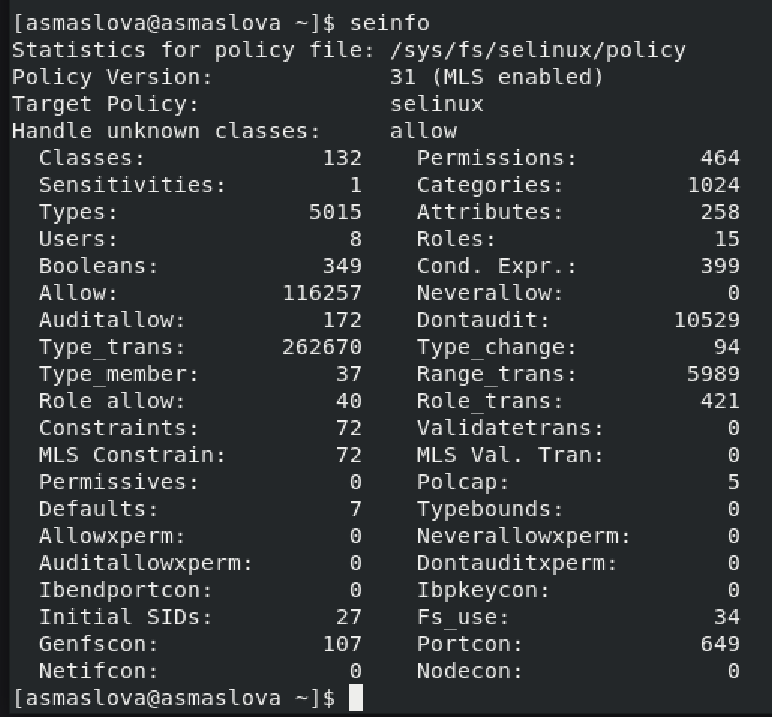


Выполнение команды sestatus -bigrep httpd



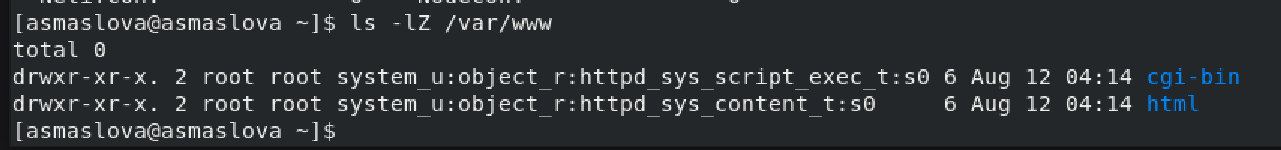
Выполнение команды sestatus -bigrep httpd

1. С помощью команды seinfo я посмотрела статистику по политике, а также определила множество пользователей, ролей, типов (рис. [??]).



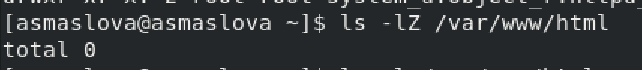
Выполнение команды seinfo

1. С помощью команды ls -lZ /var/www я посмотрела тип файлов и поддиректорий, находящихся в директории /var/www (рис. [??]).



Выполнение команды ls -lZ /var/www

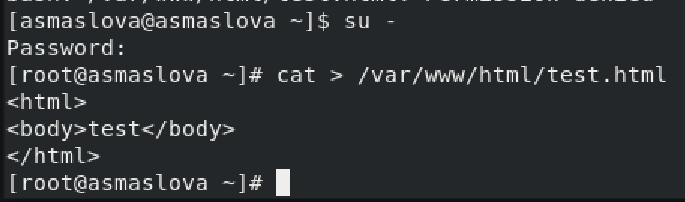
1. С помощью команды ls -lZ /var/www/html я посмотрела тип файлов, находящихся в директории /var/www/html (рис. [??]).



Выполнение команды ls -lZ /var/www/html

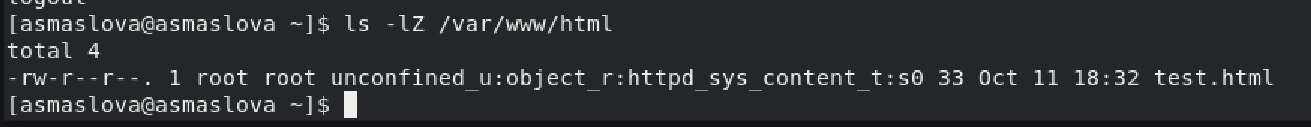
1. По выводу команды ls -lZ /var/www я определила круг пользователей, которым разрешено создание файлов в директории /var/www/html (рис. [??]).
2. От имени суперпользователя я создала html-файл /var/www/html/test.html следующего содержания (рис. [??]):

<html>  
<body>test</body>  
</html>



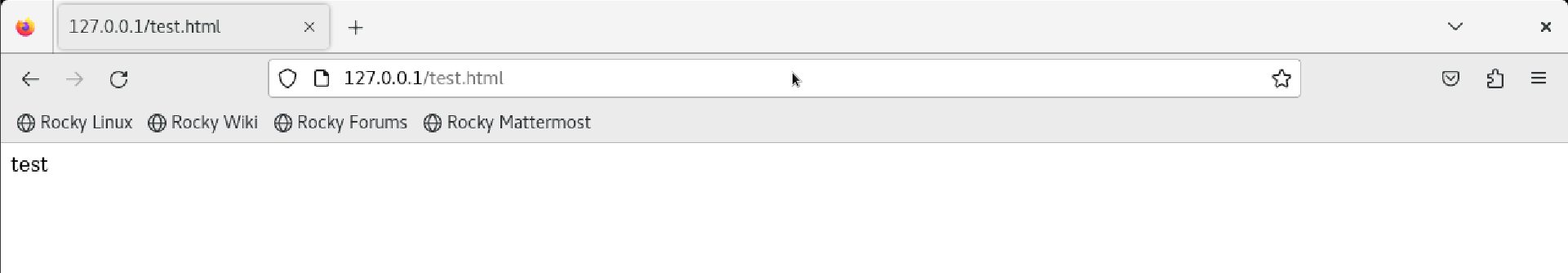
Создание html-файл /var/www/html/test.html

1. С помощью команды ls -lZ /var/www/html/test.html я проверила контекст созданного мною файла (рис. [??]).



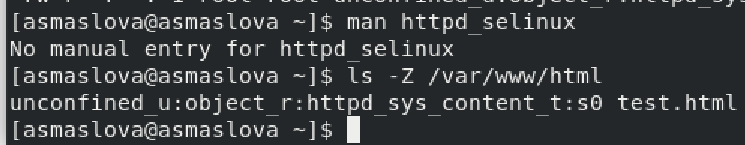
Проверка контекста созданного мною файла

1. Введя в браузере адрес http://127.0.0.1/test.html, я обратилась к файлу через веб-сервер. Он был успешно отображен (рис. [??]).



Обращение к файлу через веб-сервер

1. Я попыталась изучить справку man httpd\_selinux и выяснить, какие контексты файлов определены для httpd, но у меня отсутствует эта справка по неизвестным причинам, поэтомуя просто решила еще раз проверить контекст файла командой ls -Z /var/www/html/test.html (рис. [??]).

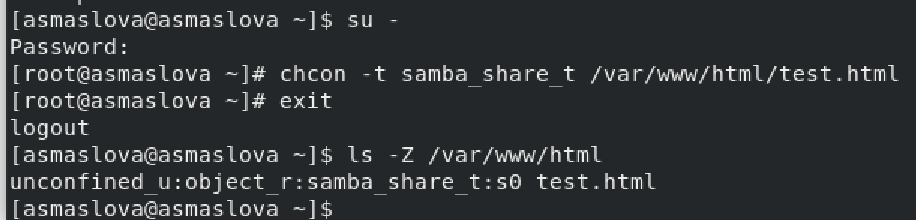


Проверка контекста файла test.html

1. После я изменила контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t с помощью команд:

chcon -t samba\_share\_t /var/www/html/test.html  
ls -Z /var/www/html/test.html

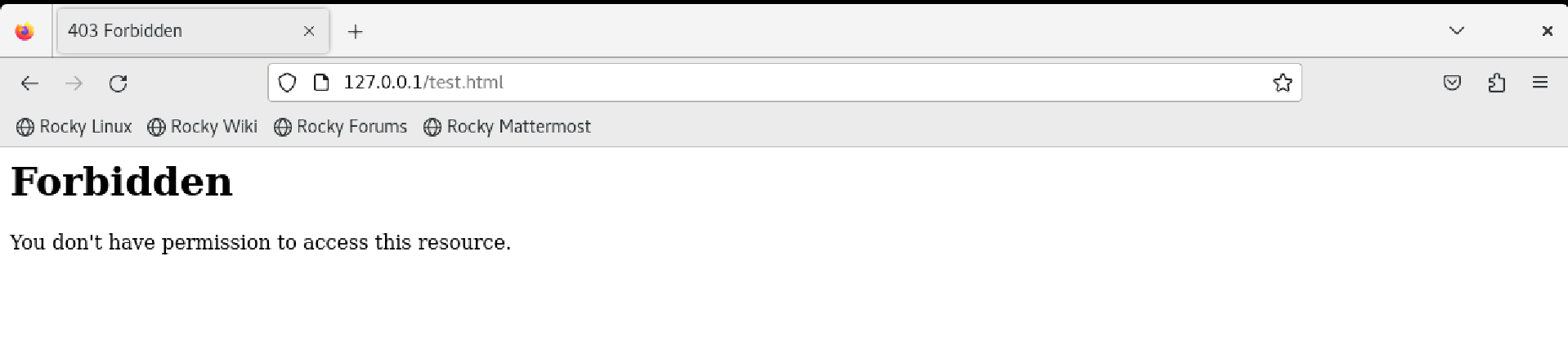
После этого я проверила, что контекст поменялся (рис. [??]).



Изменение контекста файла test.html

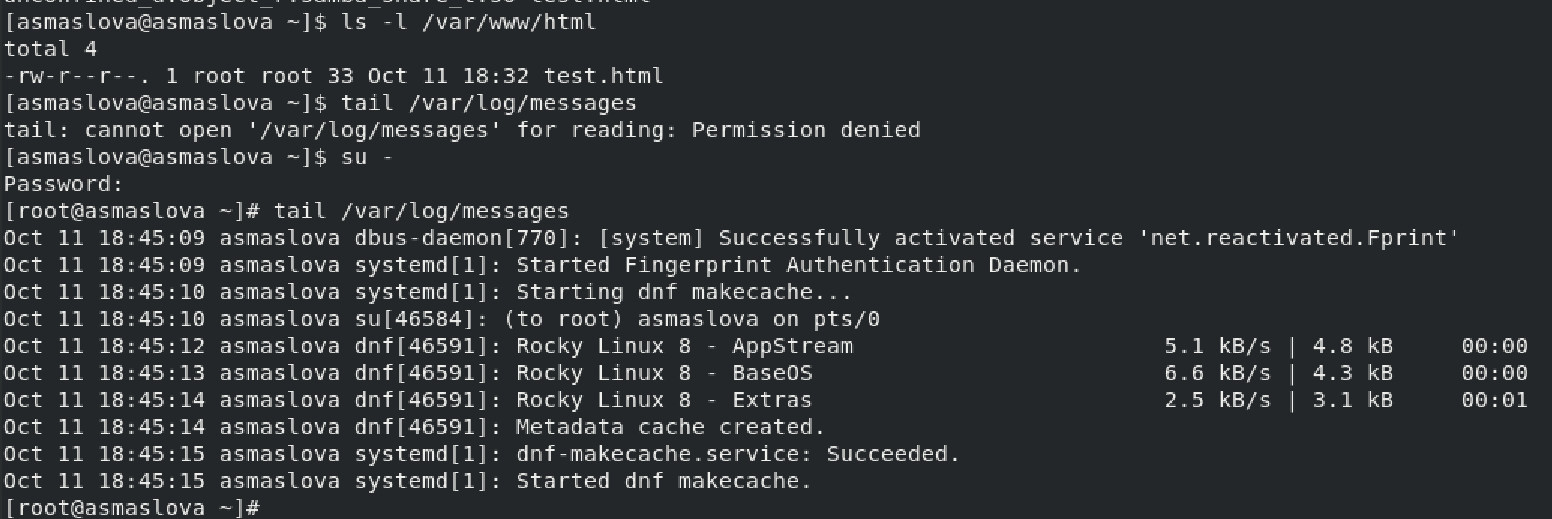
1. Введя в браузере адрес http://127.0.0.1/test.html, я ещё раз попробовала получить доступ к файлу через веб-сервер и получила сообщение об ошибке (рис. [??]):

Forbidden  
You don't have permission to access /test.html on this server.



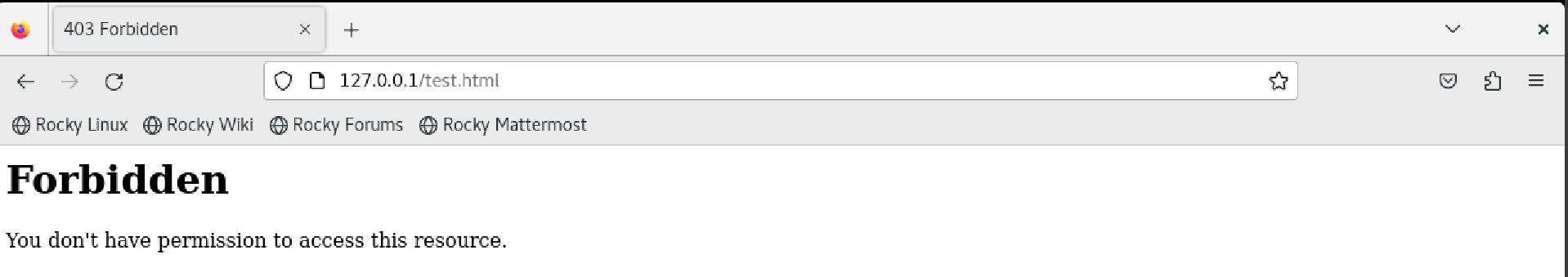
Доступ к файлу через веб-сервер

1. Я просмотрела системный лог-файл с помощью команды tail /var/log/messages, чтобы понять, почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю (рис. [??]).



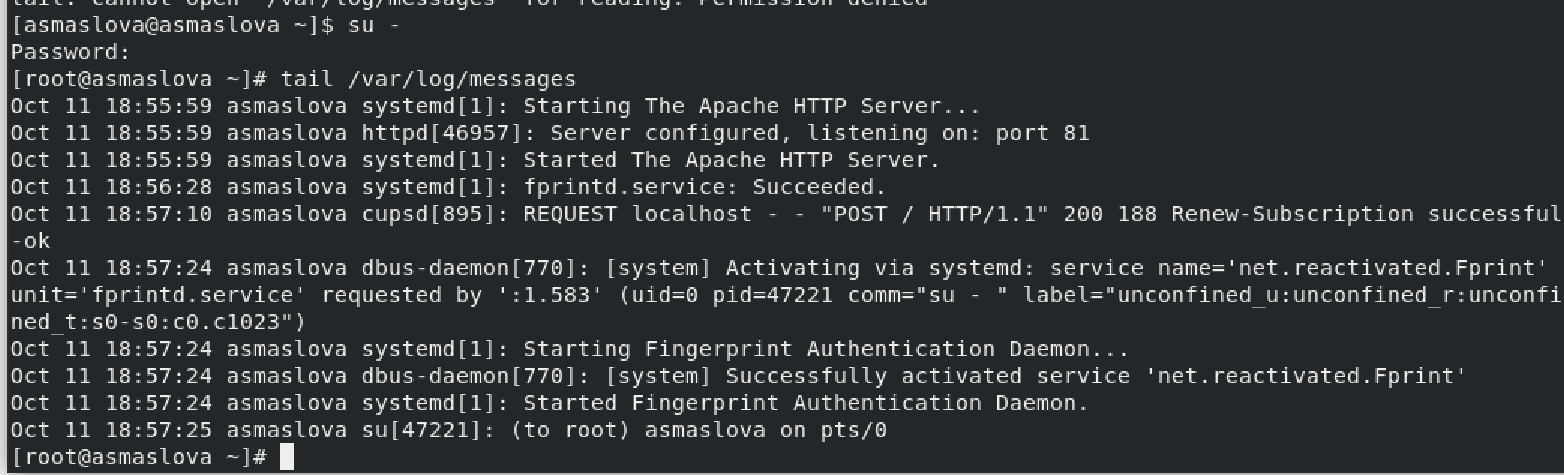
Просмотр системного лог-файла

1. Я попробовала запустить веб-сервер Apache на прослушивание ТСР-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf я нашла строчку Listen 80 и заменила её на Listen 81.
2. Я выполнила перезапуск веб-сервера Apache, но произошел сбой (рис. [??])

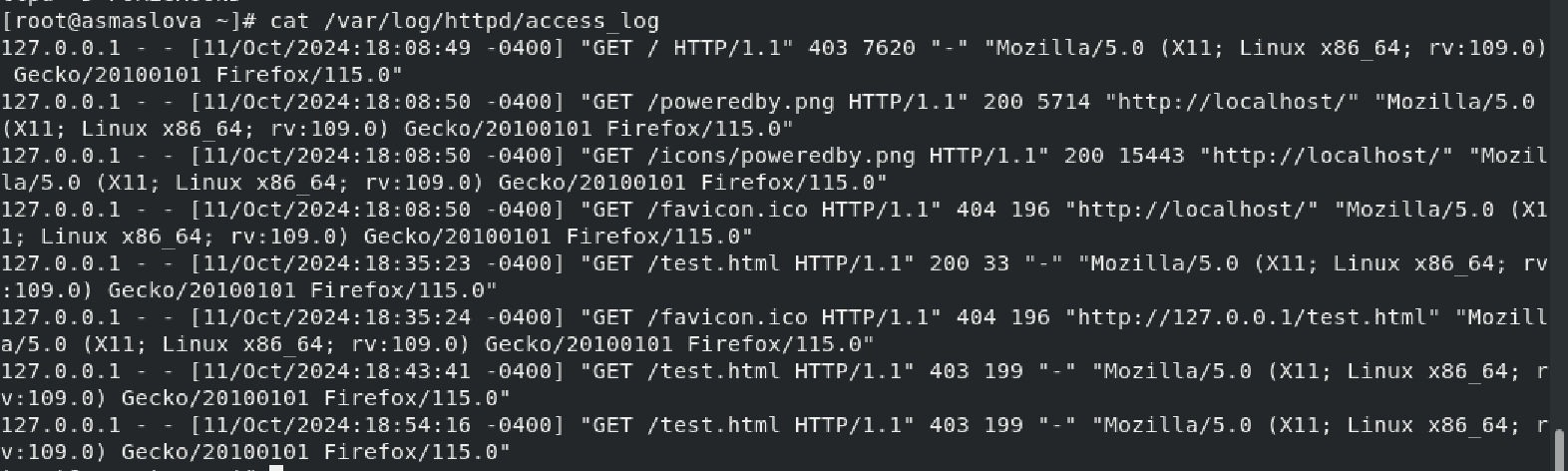


Перезапуск веб-сервера Apache

1. Я проанализировала лог-файлы командой tail -nl /var/log/messages, просмотрела файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log (рис. [??], [??]).

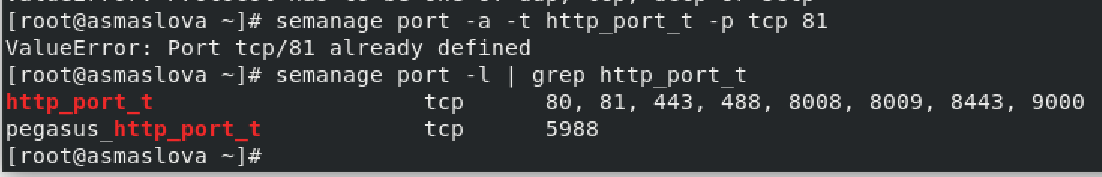


Выполнение команды tail -nl /var/log/messages



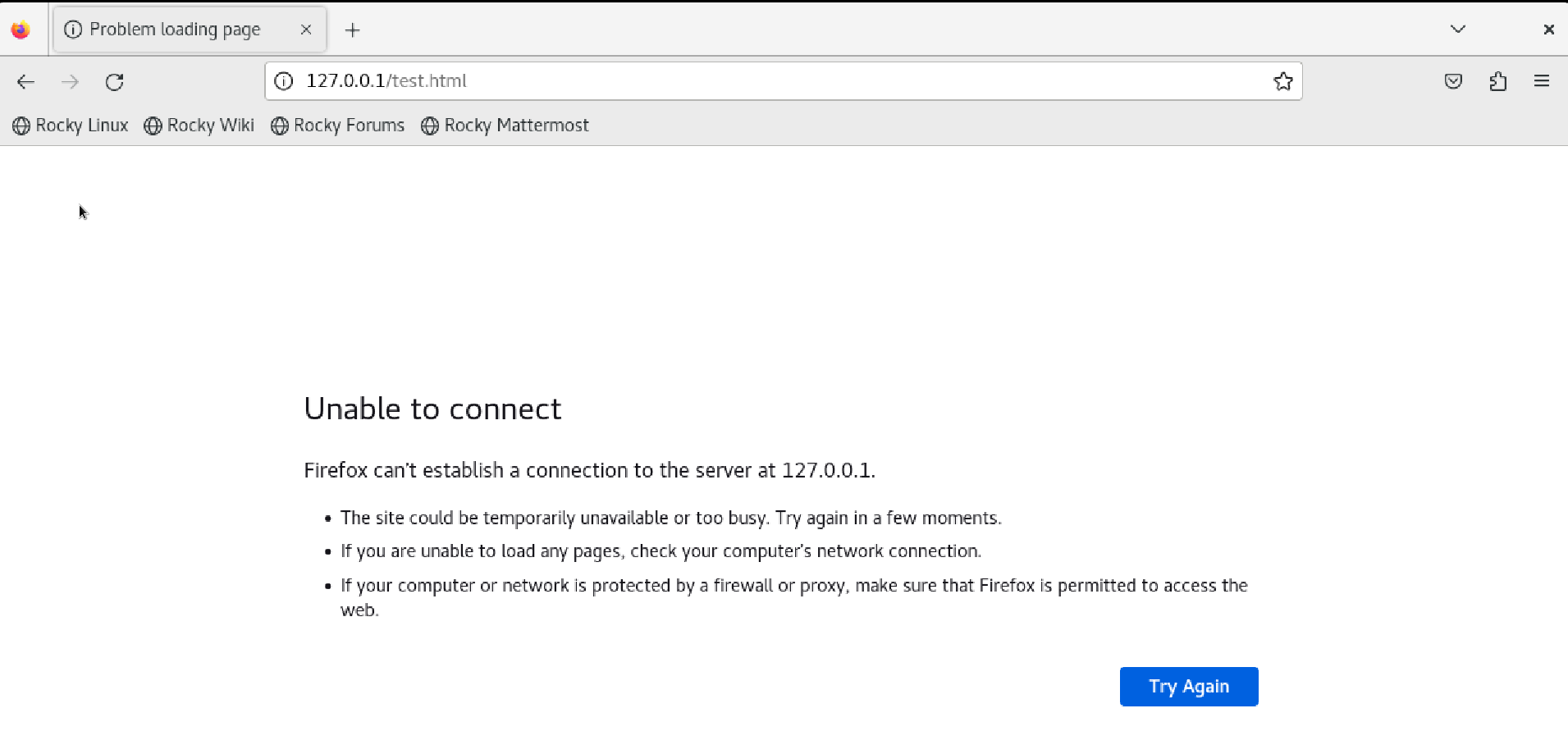
Просмотр файла /var/log/http/access\_log

1. Я выполнила команду semanage port -a -t http\_port\_t -р tcp 81, после чего проверила список портов командой semanage port -l | grep http\_port\_t (рис. [??]).



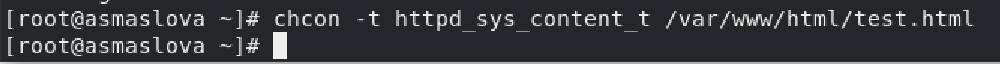
Выполнение команды semanage port -a -t http\_port\_t -р tcp 81 и проверка списка портов

1. Я попробовала запустить веб-сервер Apache ещё раз, но он как в прошлый раз не работал, так и сейчас не работает, просто теперь с другим системным сообщением (рис. [??]).

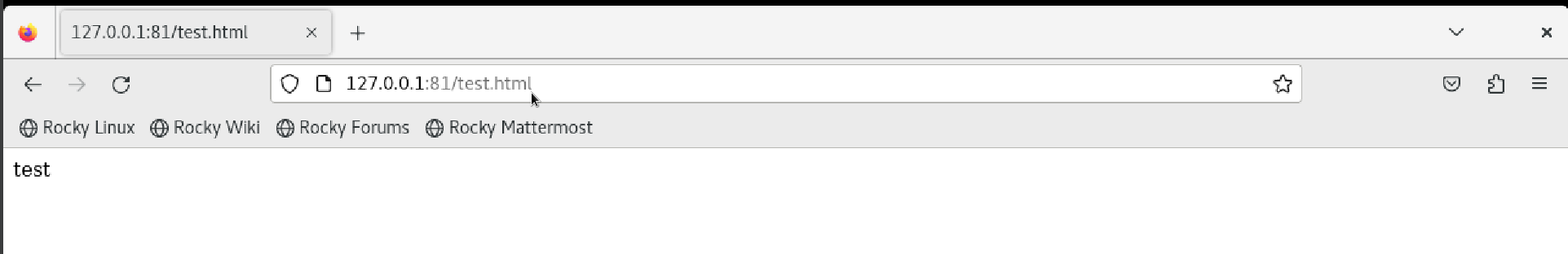


Запуск веб-сервера Apache

1. Я вернула контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/test.html командой chcon -t httpd\_sys\_content\_t /var/www/html/test.html (рис. [??]). После этого я попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html, и увидела содержимое файла — слово «test» (рис. [??]).

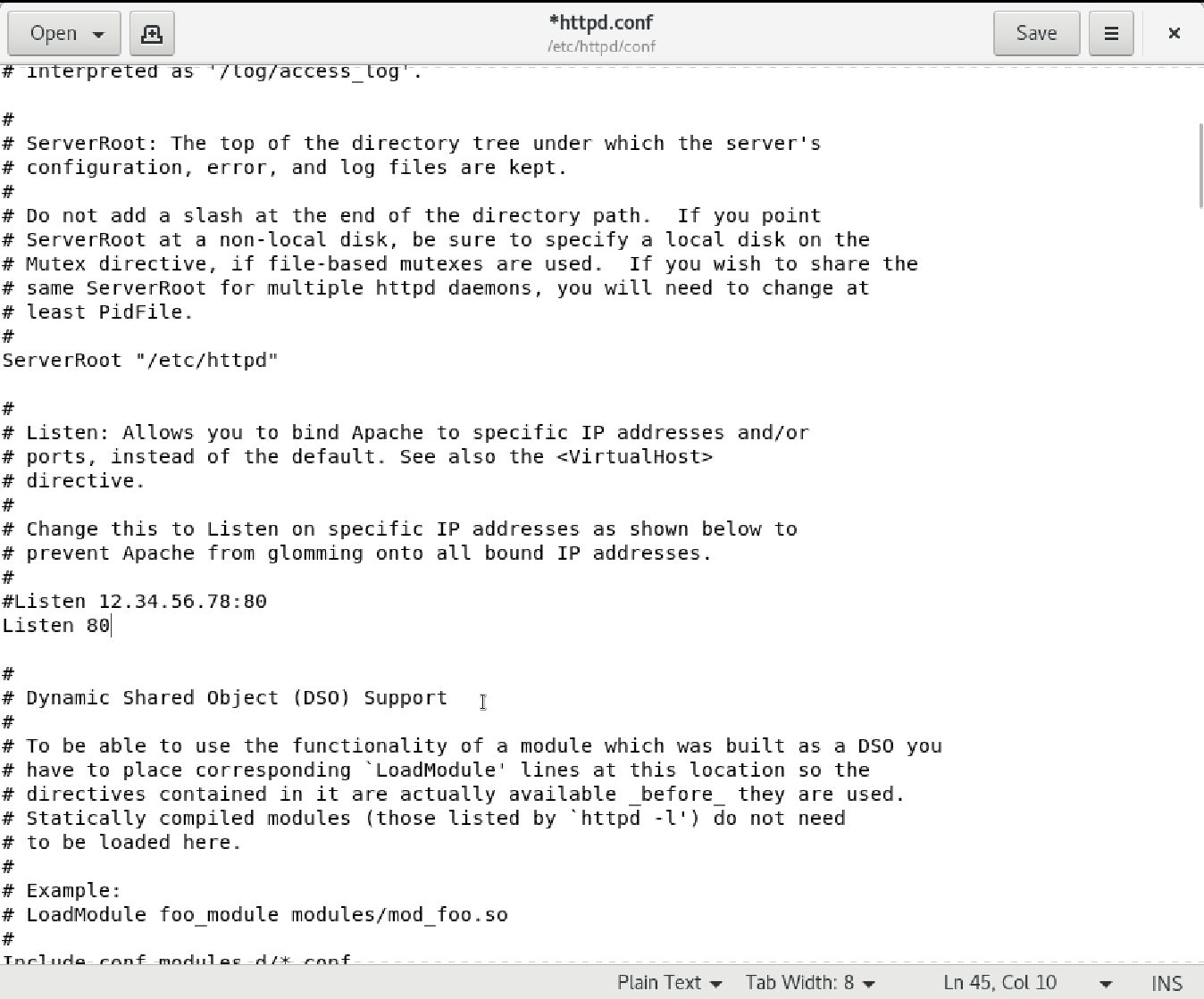


Возвращение контекста httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html



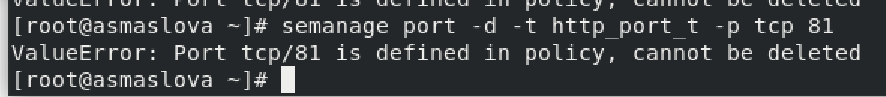
Получение доступа к файлу через веб-сервер

1. Я исправила обратно конфигурационный файл apache, вернув Listen 80 (рис. [??]).



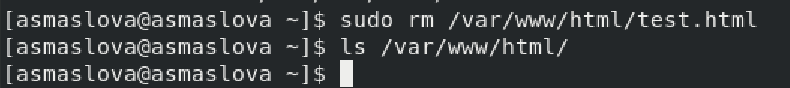
Исправление конфигурационного файла apache

1. Я удалила привязку http\_port\_t к 81 порту командой semanage port -d -t http\_port\_t -p tcp 81 (рис. [??]).



Удаление привязки http\_port\_t к 81 порту

1. В конце я удалила файл /var/www/html/test.html командой rm /var/www/html/test.html (рис. [??]).



Удаление файла /var/www/html/test.html

# 3 Вывод

В ходе лабораторной работы я развила навыки администрирования ОС Linux, получила первое практическое знакомство с технологией SELinux1 и проверила работу SELinx на практике совместно с веб-сервером Apache.

# Список литературы