Лабораторная работа №6.

Мандатное разграничение прав в Linux

Стариков Данила Андреевич

Содержание

# 1 Цель работы

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

# 2 Выполнение лабораторной работы

1. Вошли в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus (Рис. 1).

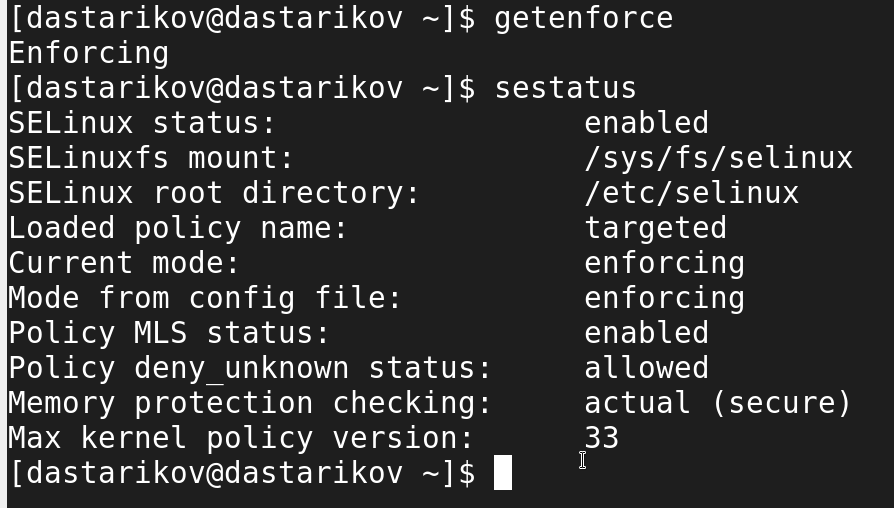


Рис. 1: Проверка режима работы SELinux.

1. Обратились с помощью браузера к веб-серверу, запущенному на компьютере, и убедились, что последний работает (Рис. 2):

service httpd status

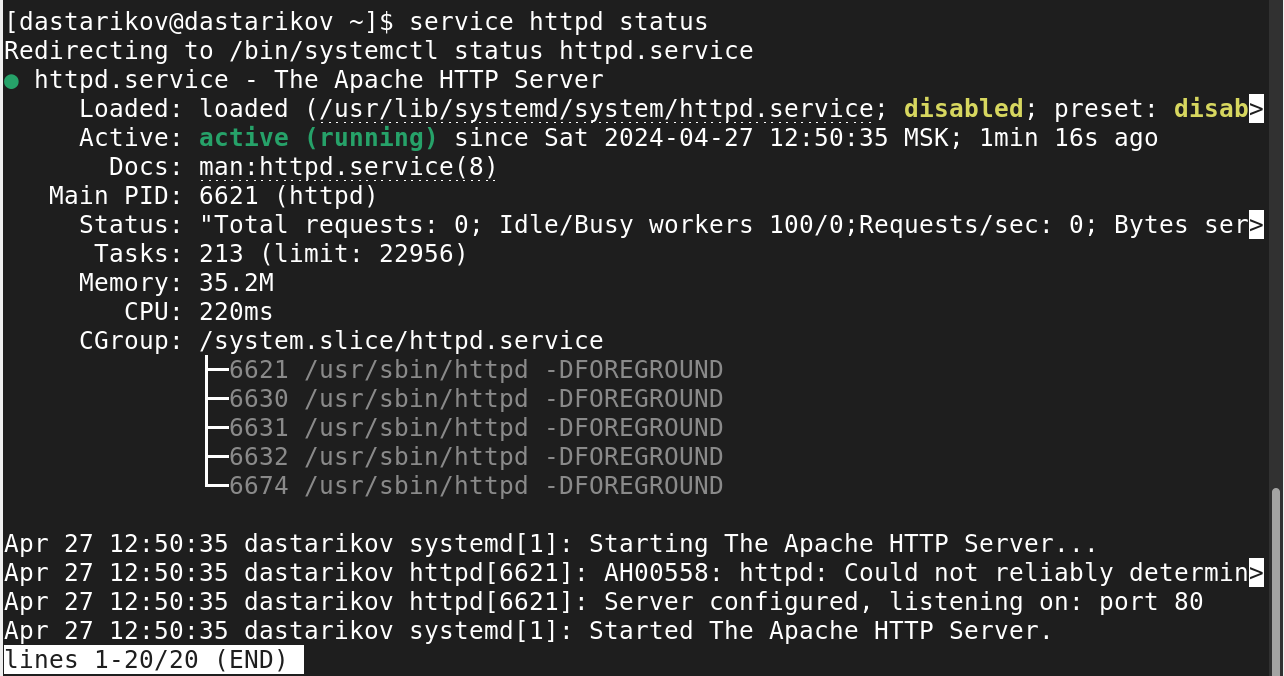


Рис. 2: Проверка режима работы httpd.

1. Нашли веб-сервер Apache в списке процессов, определили его контекст безопасности (Рис. 3)

ps auxZ | grep httpd

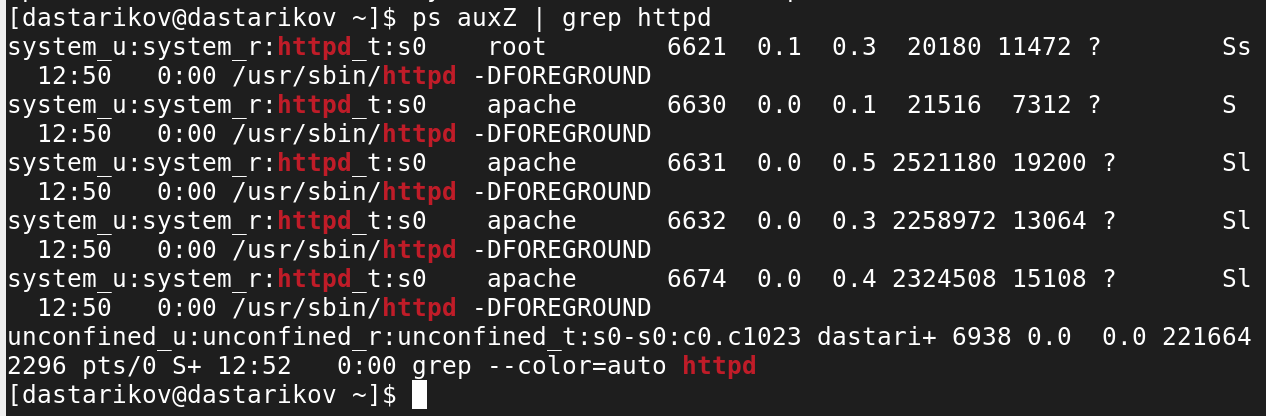


Рис. 3: Список всех связанных с httpd процессов.

1. Посмотрели текущее состояние переключателей SELinux для Apache с помощью команды (Рис. 4)

sestatus -b httpd

Обратили внимание, что многие из них находятся в положении «off».

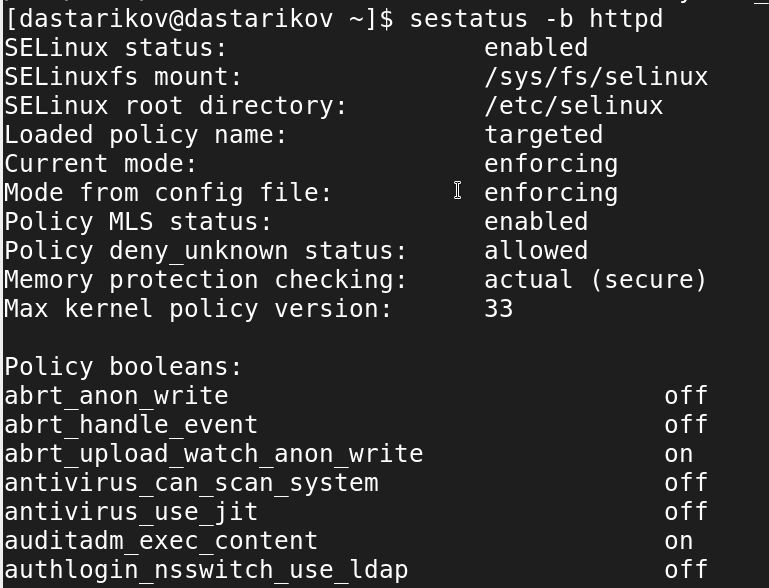


Рис. 4: Фрагмент справки текущих состояний httpd.

1. Посмотрели статистику по политике с помощью команды seinfo, также определили множество пользователей, ролей, типов (Рис. 5). Пользователей – 8, ролей – 15, типов – 5135.

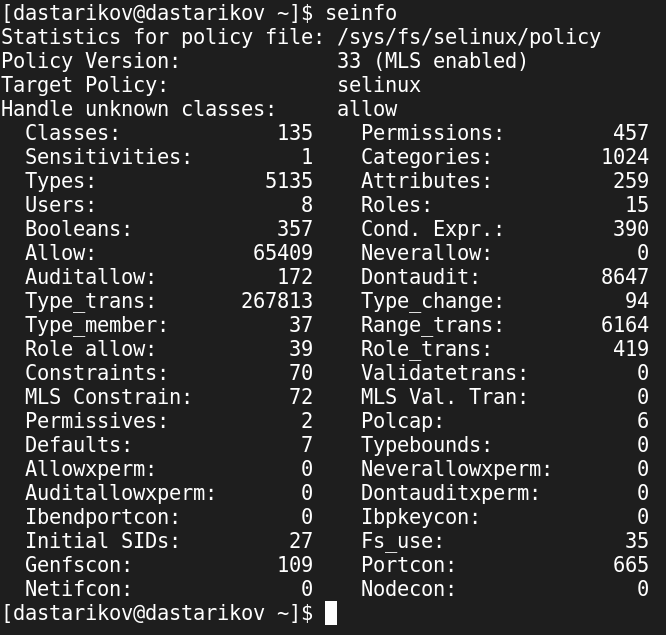


Рис. 5: Статистика по политике httpd.

1. Определили тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды (Рис. 6)

ls -lZ /var/www

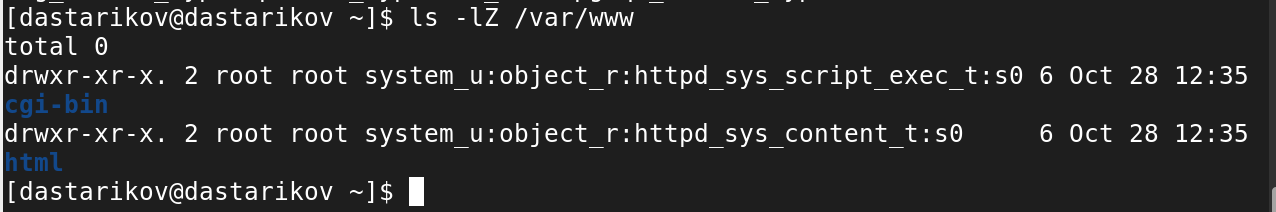


Рис. 6: Информация о содержимом каталога /var/www .

1. Определили тип файлов, находящихся в директории /var/www/html (Рис. 7):

ls -lZ /var/www/html

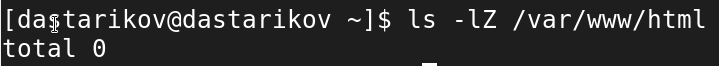


Рис. 7: Информация о содержимом каталога /var/www/html .

1. Определили круг пользователей, которым разрешено создание файлов в директории /var/www/html. Только пользователи root имеют право создавать файлы в директории /var/www/html.
2. Создали от имени суперпользователя html-файл /var/www/html/test.html следующего содержания (Рис. 8):

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

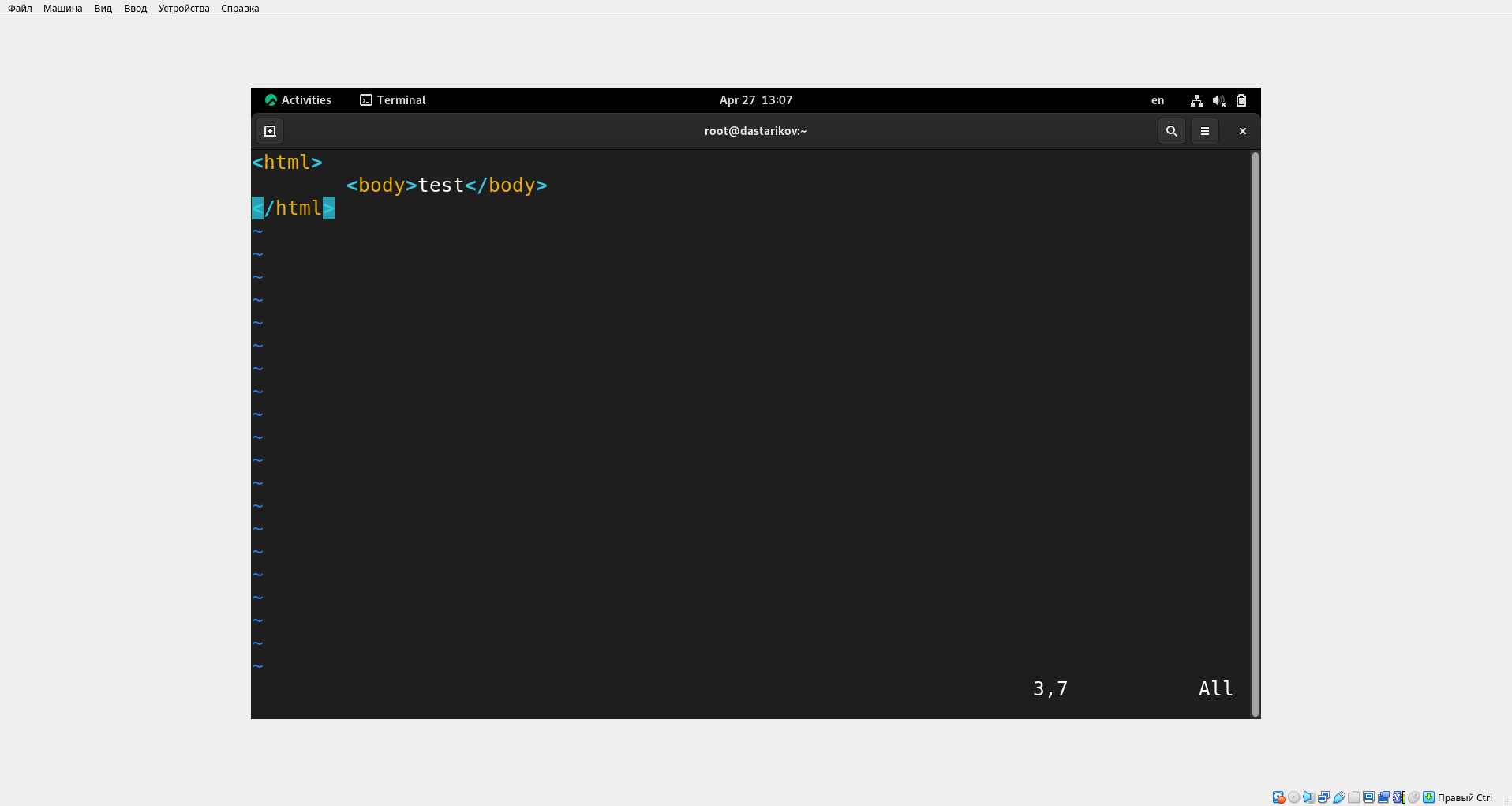


Рис. 8: Создание файла test.html.

1. Проверили контекст созданного вами файла. По умолчанию файлам присваивается контекст unconfined\_u:object\_u:httpd\_sys\_content\_t:s0 (Рис. 9).

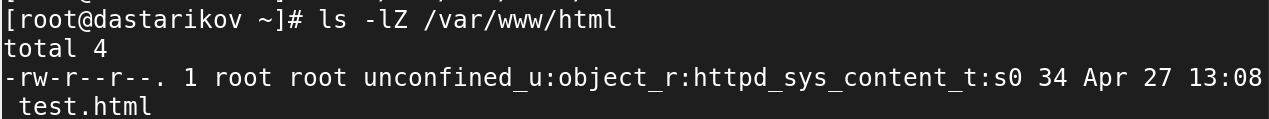


Рис. 9: Проверка контекста test.html.

1. Обратились к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедились, что файл был успешно отображён.

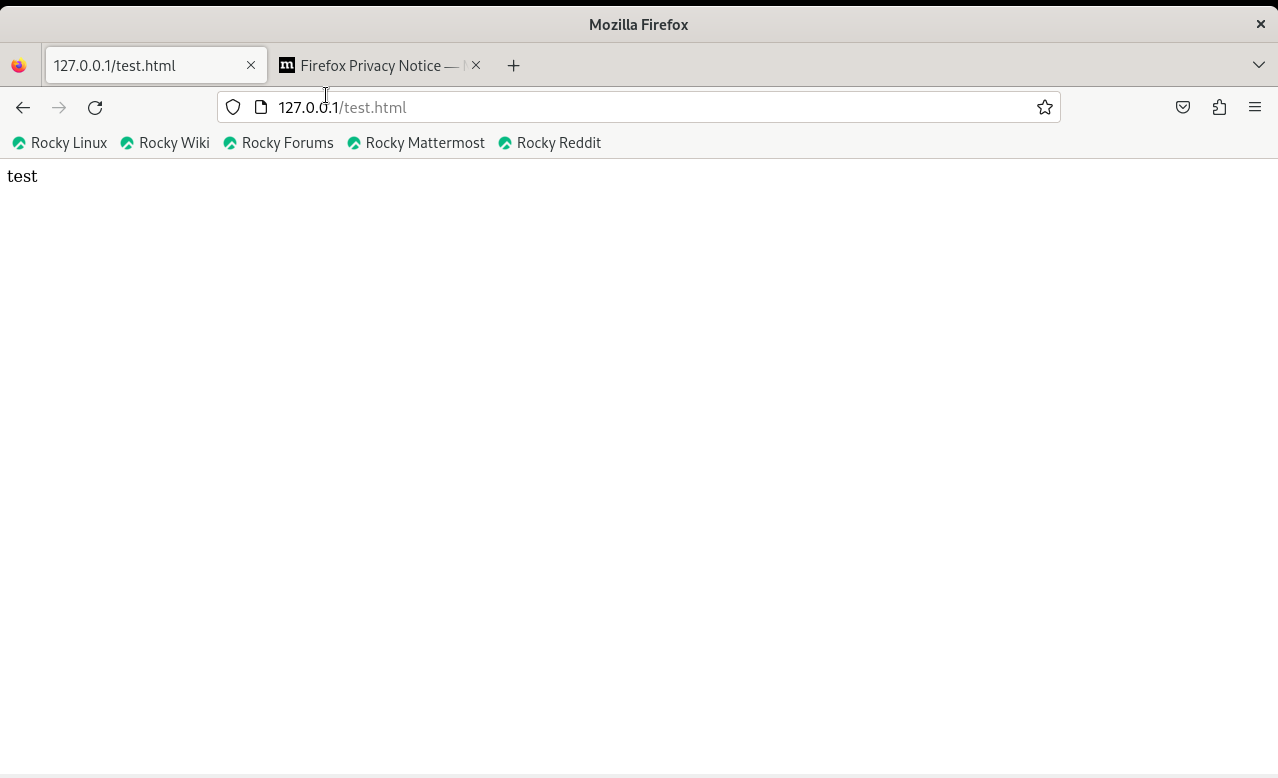


Рис. 10: Открытие файла через веб-браузер.

1. Изучили справку man httpd\_selinux и выяснили, какие контексты файлов определены для httpd. Сопоставили их с типом файла test.html (Рис. 9).

ls -Z /var/www/html/test.html

1. Изменили контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t(Рис. 11):

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

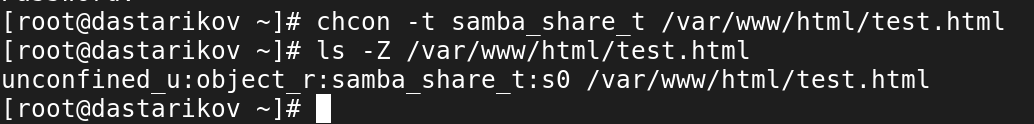


Рис. 11: Изменение контекста файла test.html.

1. Попробовали ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Получили сообщение об ошибке (Рис. 12):

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

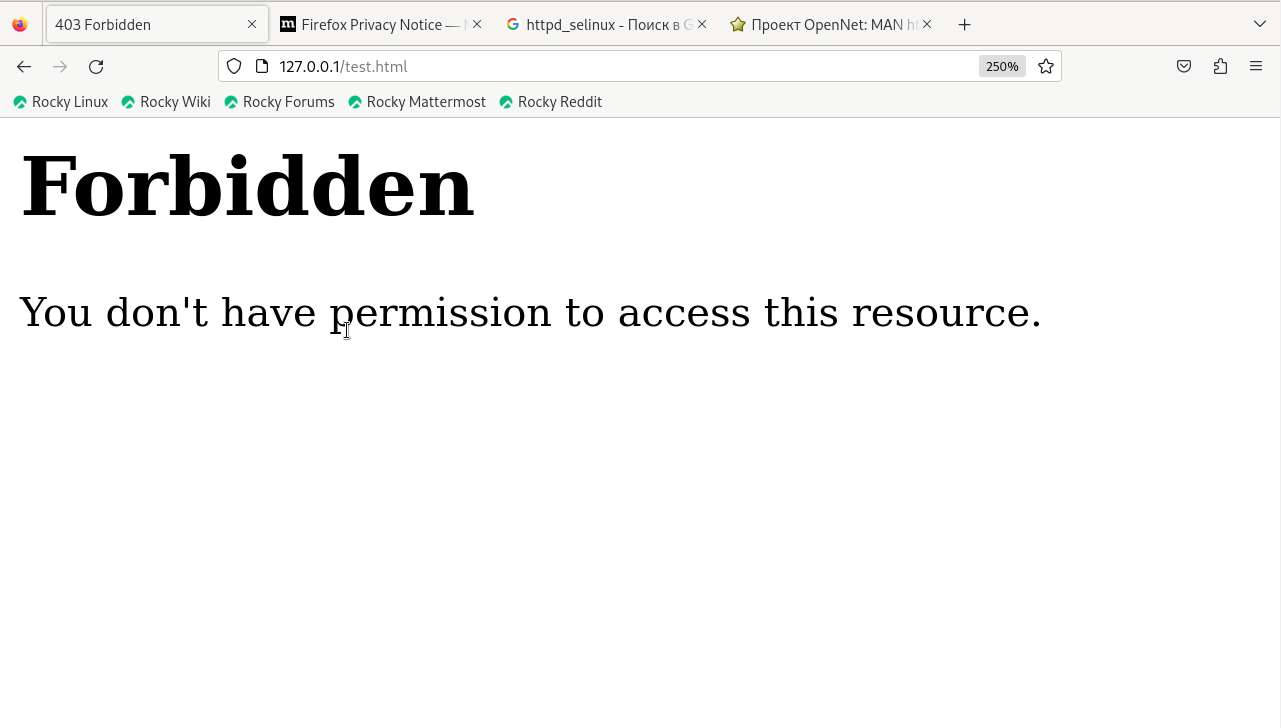


Рис. 12: Попытка открытия файла через веб-браузер.

1. Проанализировали ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю?

ls -l /var/www/html/test.html

Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл Рис. 13):

tail /var/log/messages

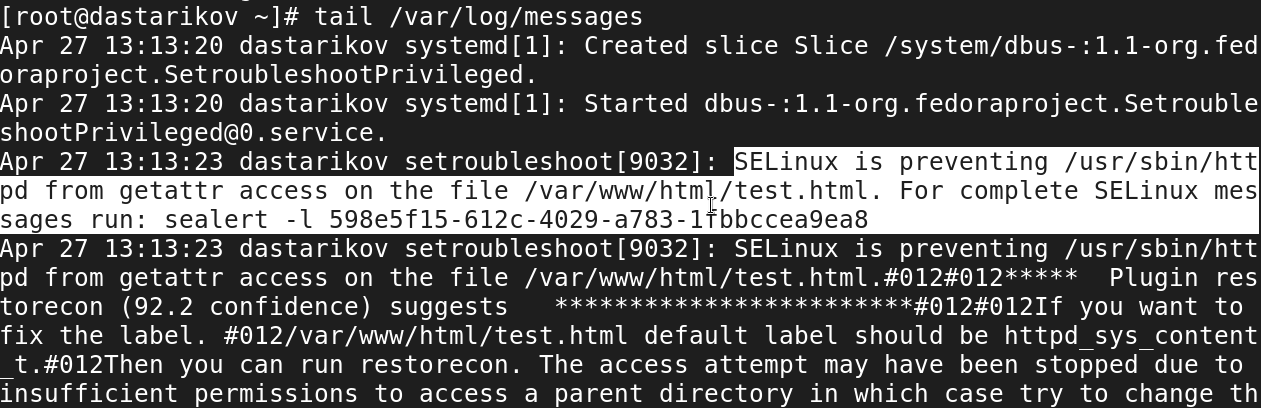


Рис. 13: Просмотр логов веб-сервера.

SELinux отказывает в доступе к файлу, так как нет соответствующего контекста безопасности.

1. Попробовали запустить веб-сервер Apache на прослушивание ТСР-порта 81. Для этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81.
2. Выполнили перезапуск веб-сервера Apache. Произошёл сбой (Рис. 14).

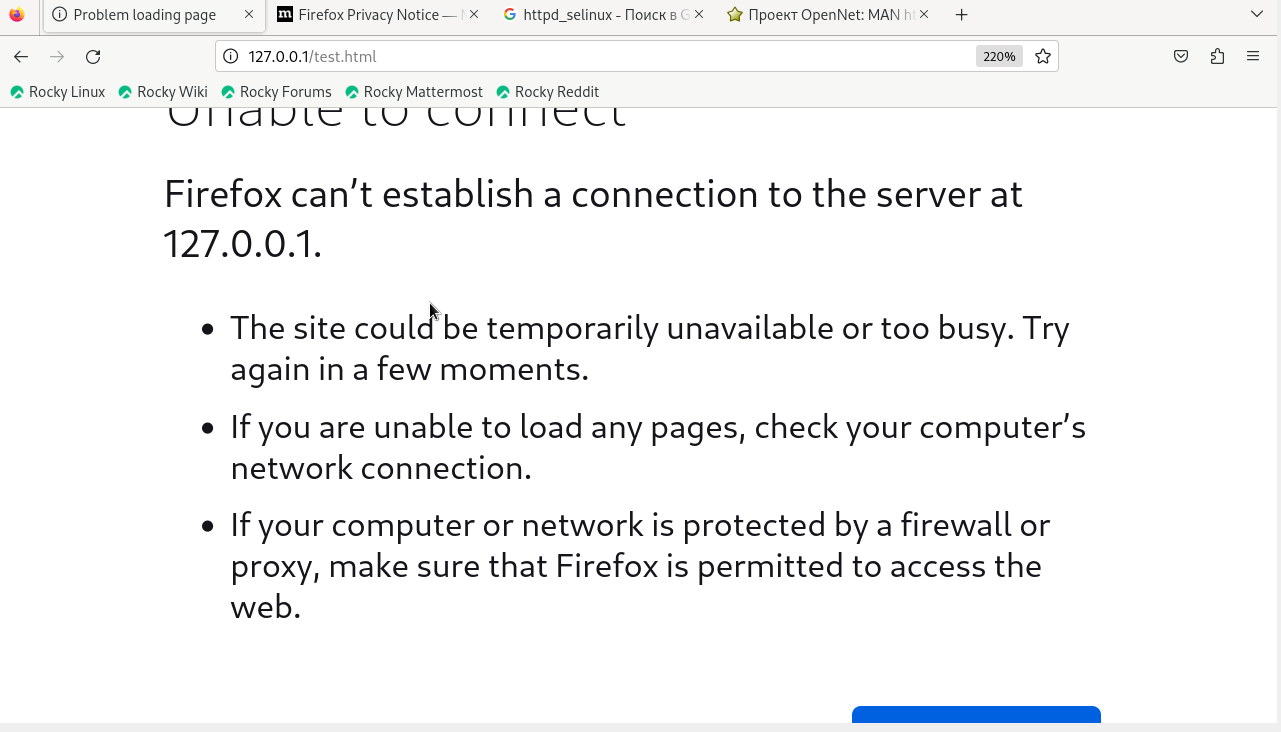


Рис. 14: Ошибка при попытке открытия файла через веб-браузер.

1. Проанализировали лог-файлы (Рис. 15 - 17):

tail -nl /var/log/messages

Просмотрели файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log и выяснили, в каких файлах появились записи.

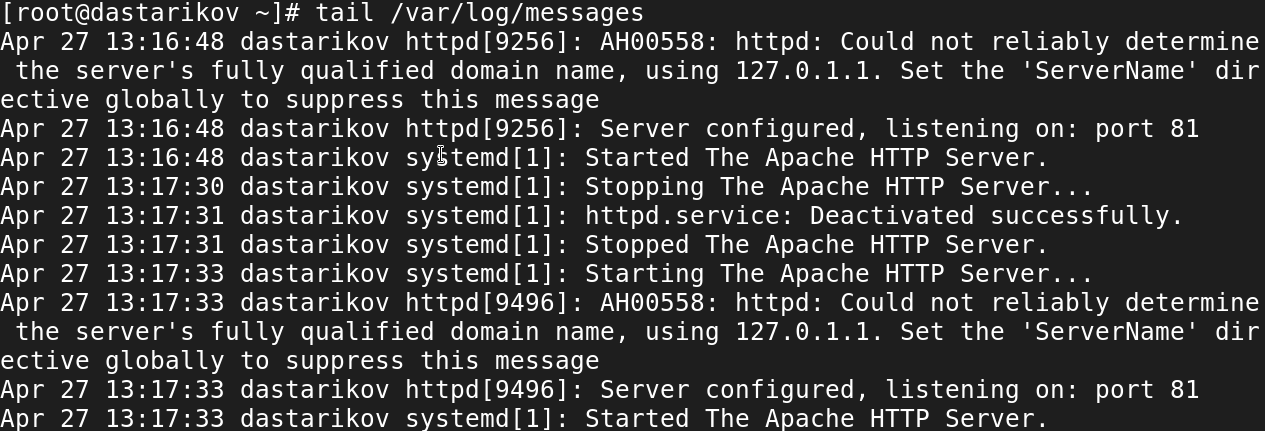


Рис. 15: Просмотр /var/log/messages.

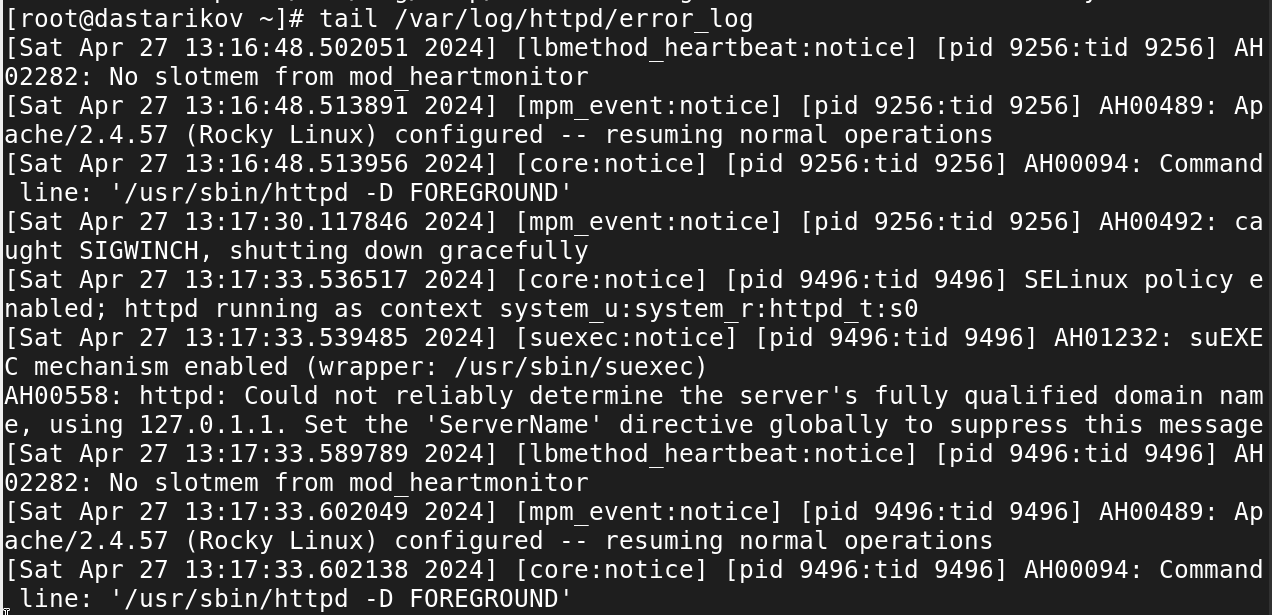


Рис. 16: Просмотр /var/log/httpd/error\_log.

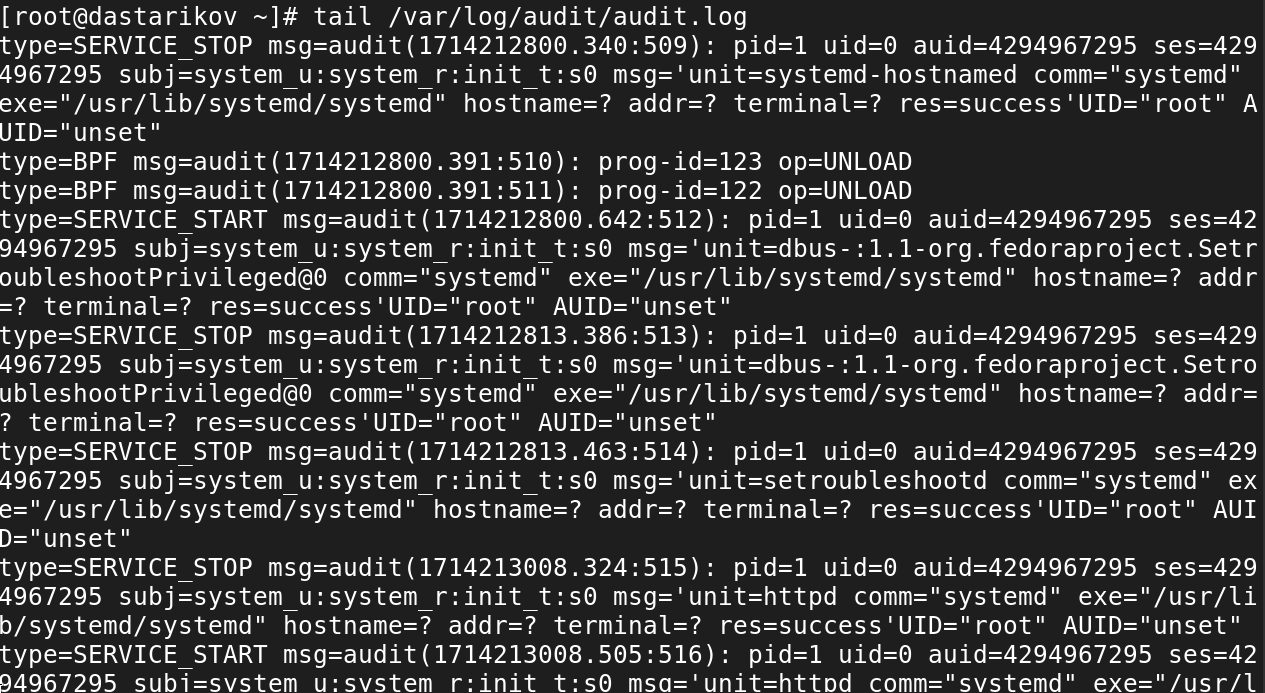


Рис. 17: Просмотр /var/log/audit/audit.log.

1. Выполнили команду (Рис. 18)

semanage port -a -t http\_port\_t -р tcp 81

После этого проверили список портов командой

semanage port -l | grep http\_port\_t

Убедились, что порт 81 появился в списке.

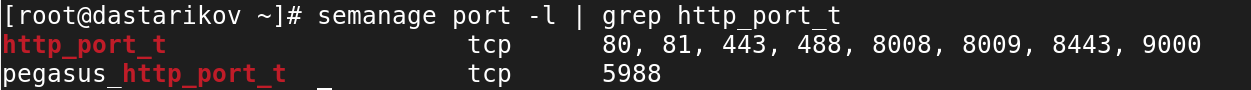


Рис. 18: Настройка прослушивания порта 81.

1. Вернули контекст httpd\_sys\_cоntent\_t к файлу /var/www/html/test.html (Рис. 19):

chcon -t httpd\_sys\_content\_t /var/www/html/test.html

Возвращение нужного контекста файлу test.html.

Рис. 19: Возвращение нужного контекста файлу test.html.

После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Вы должны увидеть содержимое файла — слово «test» (Рис. 20).

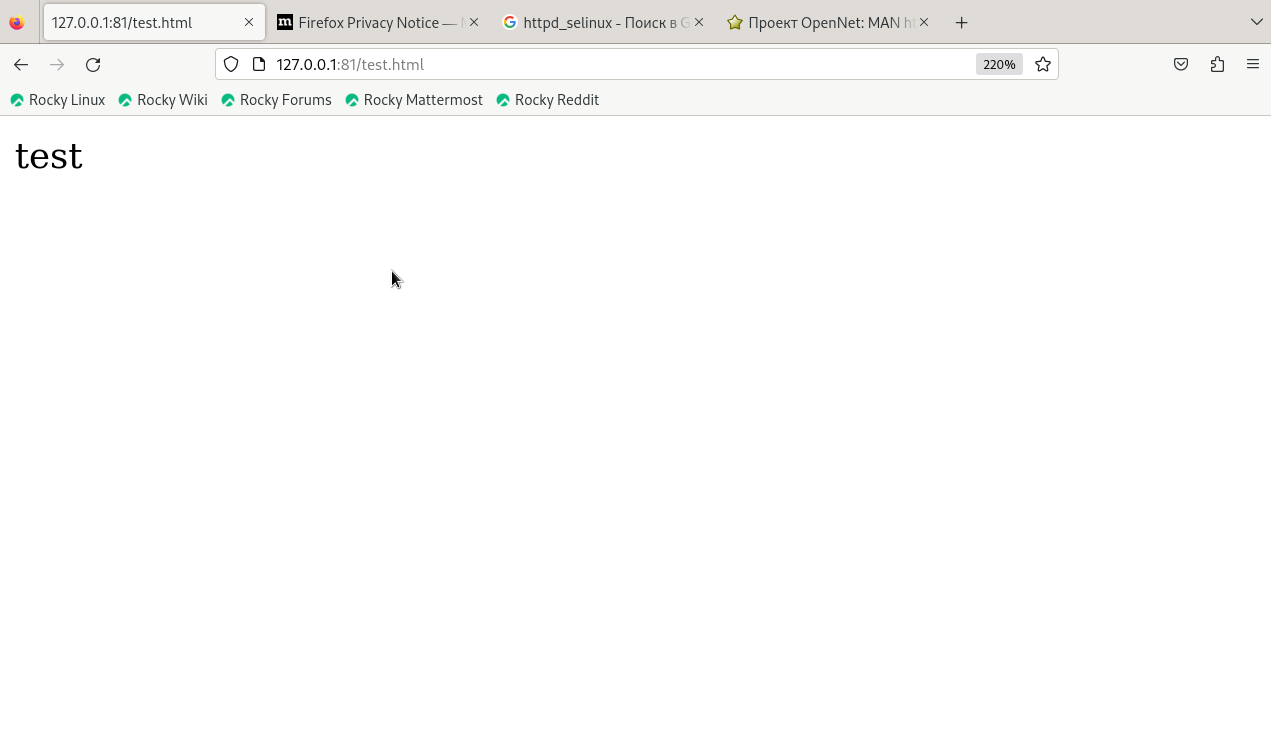


Рис. 20: Открытие файла через веб-браузер на порте 81.

1. Исправили обратно конфигурационный файл apache, вернув Listen 80.
2. Удалили файл /var/www/html/test.html:

rm /var/www/html/test.html

Более подробно о SELinux можно прочитать в книге [1].

# 3 Выводы

В рамках лабораторной работы развили навыки администрирования ОС Linux, получили первое практическое знакомство с технологией SELinux и проверили работу SELinux на практике совместно с веб-сервером Apache.

# Список литературы

1. Vermeulen S. SELinux System Administration. Second Edition. Packt Publishing, 2016. 300 с.