Лабораторная работа №6

Мандатное разграничение прав в Linux

Кекишева Анастасия Дмитриевна

Содержание

# 1 Цель работы

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

# 2 Задание

Описание задания и рекомендованная последовательность выполнения работы, описана [1]

# 3 Теоретическое введение

Apache - популярный бесплатный opensource веб-сервер. Он является частью стека LAMP (Linux, Apache, MySQL, PHP), который обеспечивает большую часть Интернета [2]. Логи Apache расположены тут: - /var/log/httpd/ - расположение файлов логов Apache - /var/log/httpd/access\_log - показывает журнал систем, которые обращались к серверу - /var/log/httpd/error\_log - показывает список любых ошибок, с которыми сталкивается Apache

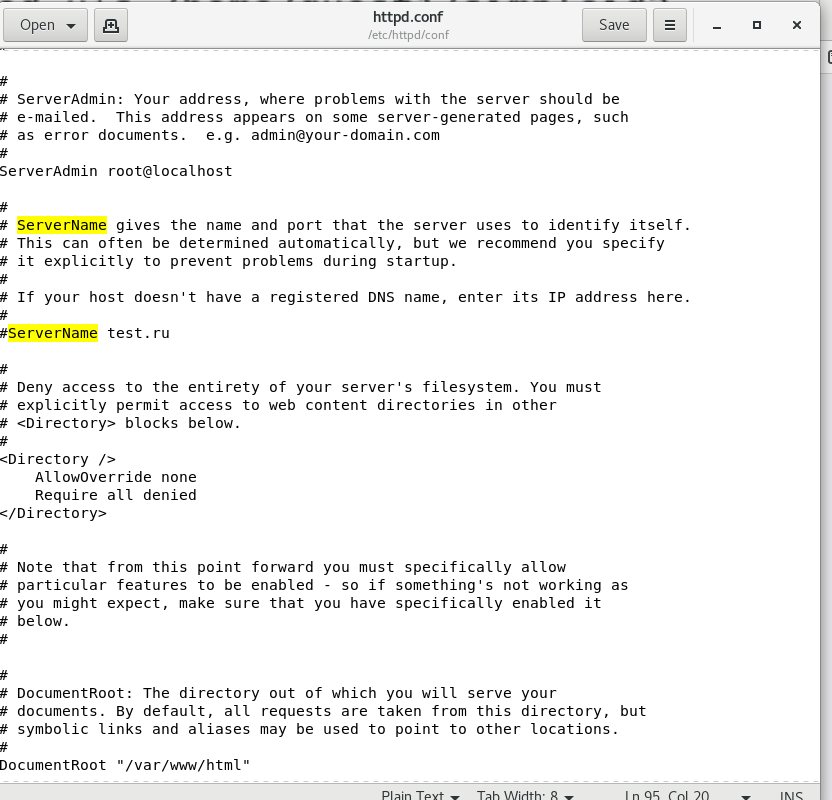
Контекст безопасности это набор всех атрибутов, связанных с объектами ипа файлов, каталогов, процессов, TCP сокетов и т.п. Контекст безопасности состоит из сущности, роли и домена или типа. У процессов есть домен. Когда вы смотрите контекст безопасности процесса последнее поле – это домен, например *user\_passwd\_t*.

Команда chcon позволяет изменить контекст, но он не работает на файловой системе /proc, т.к. она не поддерживает изменение меток.

Контекст безопасности файла, например, может варьироваться в зависимости от домена, который создал файл. По умолчанию, новый файл или каталог наследует тип от родительского каталога, однако вы можете задать иную политику [**bib3?**].

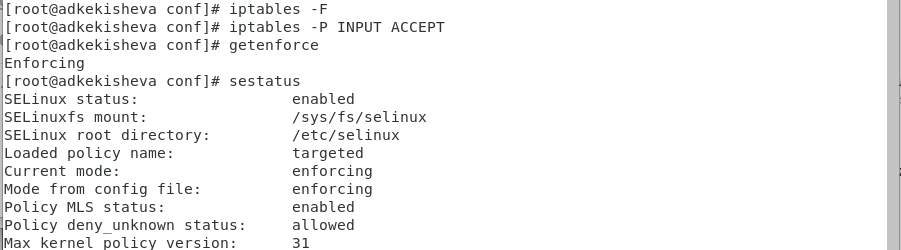
# 4 Выполнение лабораторной работы

1. В конфигурационном файле /etc/httpd/httpd.conf необходимо задала параметр ServerName: ServerName test.ru (рис. ??).



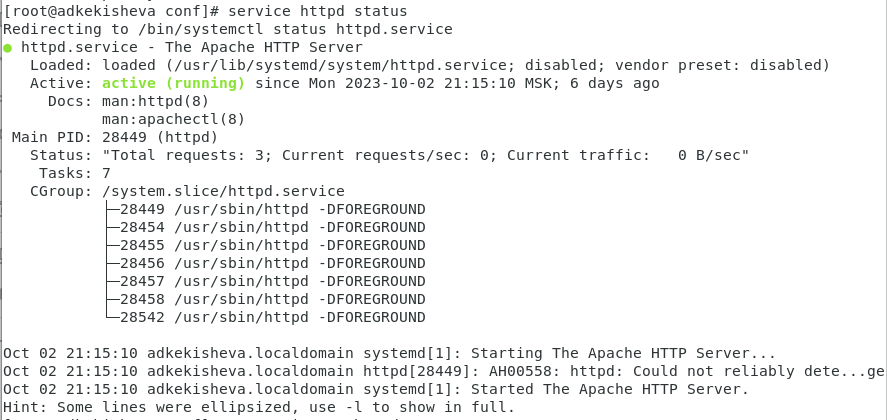
Задание параметра

1. Проследила, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключить фильтр можно командами iptables -F и iptables -P INPUT ACCEPT (рис. ??).



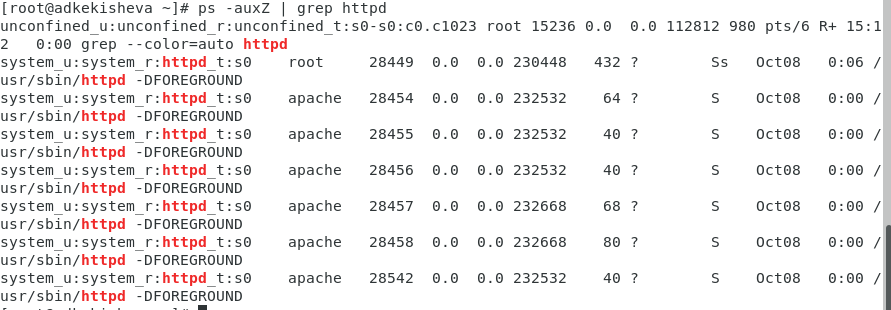
Отключение пакетного фильтра и вход в систему

1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus (рис. ??).
2. Обратилась командой service httpd status с помощью браузера к веб-серверу, запущенному на моём компьютере, и убедилась, что всё работает (рис. ??).



Проверка статуса веб-сервера

1. Командой ps -auxZ | grep httpd найшла веб-сервер Apache в списке процессов. Его контекст безопасности: httpd\_t (рис. ??).



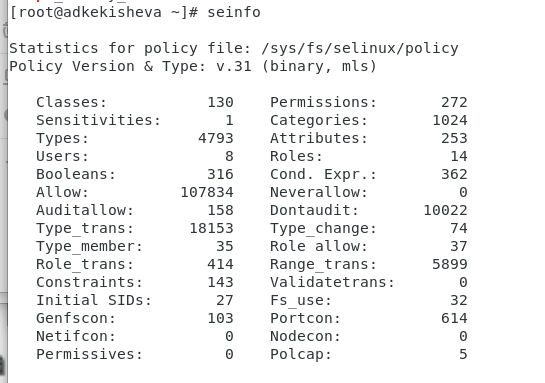
Список процессов

1. Посмотрела состояние переключателей SELinux для Apache с помощью sestatus -b | grep httpd. Многие из состояний находятся в положении «off» (рис. ??).



Состояния переключателей

1. Посмотрела статистику по политике с помощью команды seinfo. Множество пользователей - 8, ролей - 14, типов- 4793 (рис. ??).



Статистика - команда seinfo

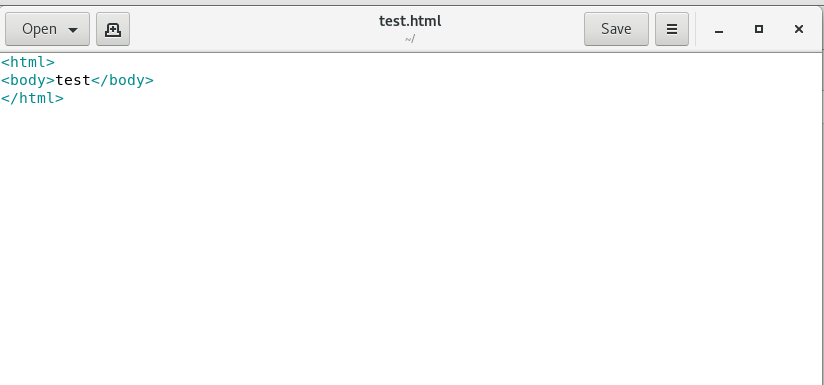
1. Определила типы файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www (рис. ??).



Определение типов файлов

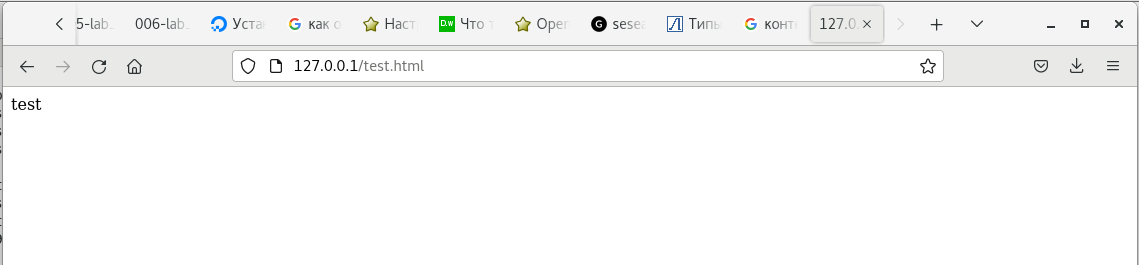
1. Определите тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html (рис. ??).
2. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html - можно владельцу файла.
3. Создайте от имени суперпользователя html-файл /var/www/html/test.html следующего содержания (рис. ??): >

* test



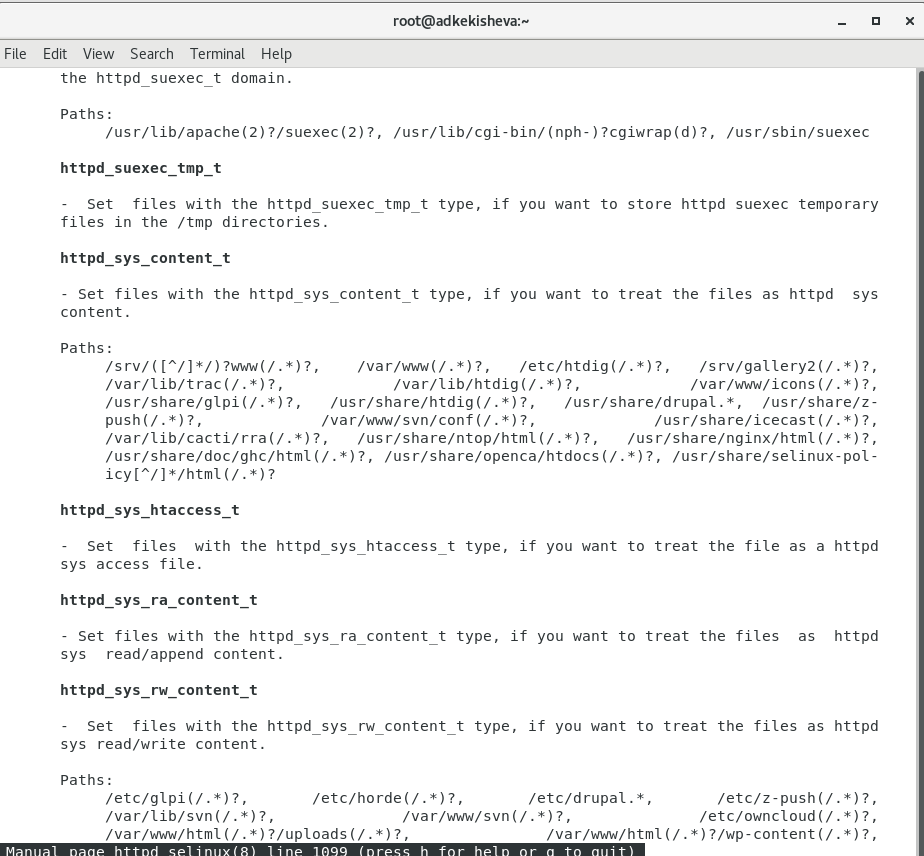
Файл test.html

1. Проверила контекст созданного файла. Контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html: httpd\_sys\_content\_t (рис. ??).
2. Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедилась, что файл был успешно отображён (рис. ??).



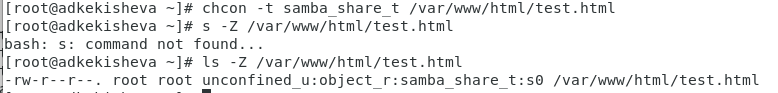
Отображение содержимого файла в браузере

1. Изучила справку man httpd\_selinux и выяснила, какие контексты файлов определены для httpd (рис. ??).



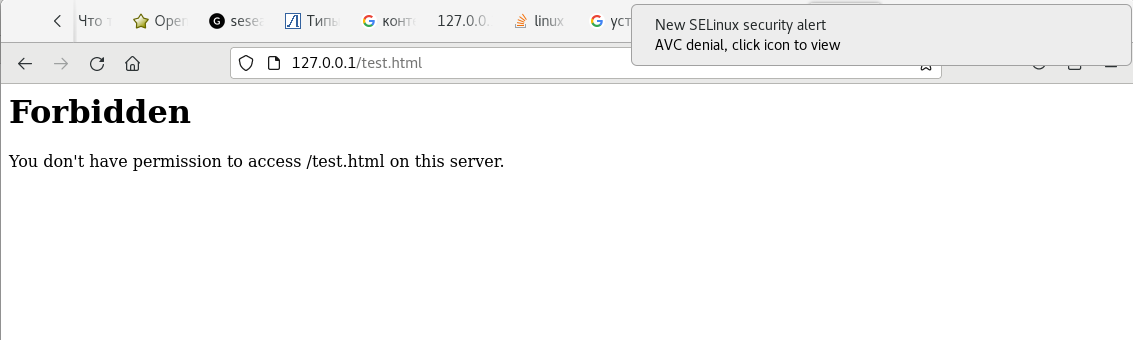
Команда man httpd\_selinux - контексты для httpd

1. Изменила контекст файла /var/www/html/test.html с *httpd\_sys\_content\_t* на любой другой, к которому процесс httpd не должен иметь доступа, например, на *samba\_share\_t*: chcon -t samba\_share\_t /var/www/html/test.html и проверила командой: ls -Z /var/www/html/test.html (рис. ??).



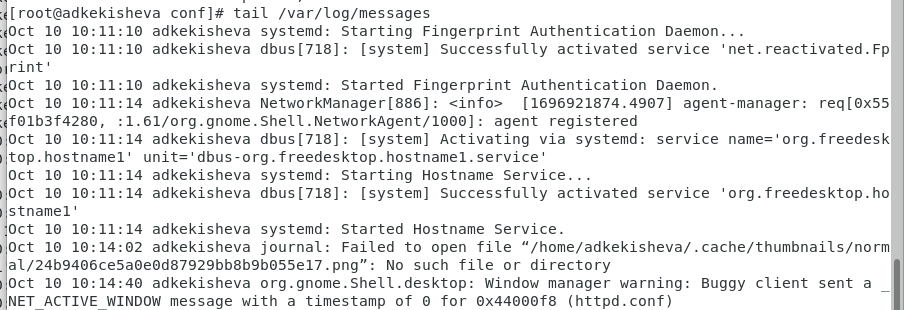
Команда chcon

1. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Получила сообщение об ошибке. При изменении контекста http считает файл чужим. (рис. ??).



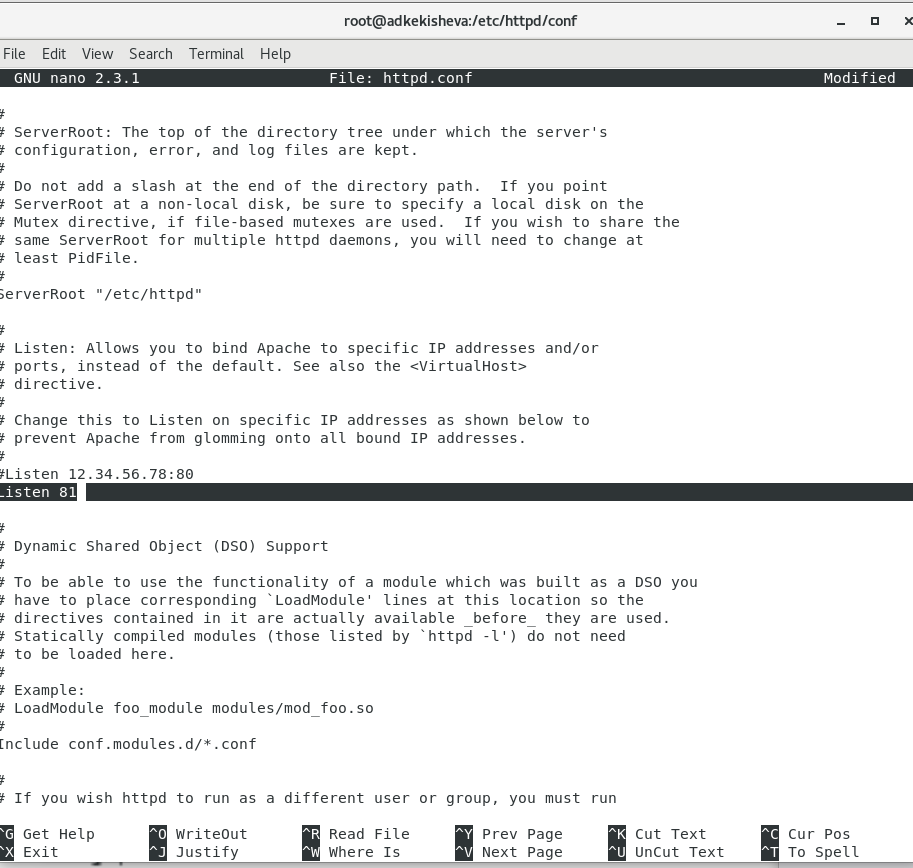
Отказ в доступе - соообщение об ошибке от браузера

1. Просмотрела системный лог-файл: tail /var/log/messages и увидела ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log (рис. ??).



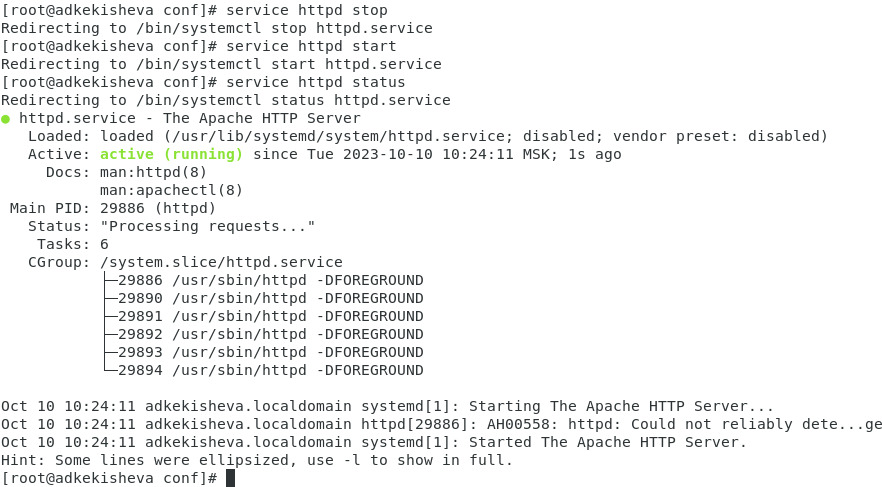
Просмотр системых лог-фвйлов

1. Попробуйте 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 нашла строчку Listen 80 и заменила её на Listen 81 (рис. ??).



Изменение Listen 80 на Listen 81

1. Выполните перезапуск веб-сервера Apache (рис. ??).



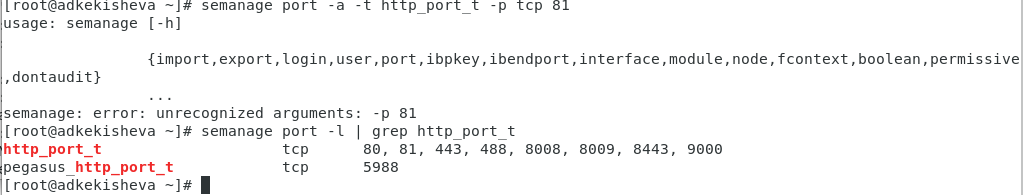
Перезапуск Apache

1. Проcмотрела лог-файлы: tail -nl /var/log/messages и файлы */var/log/http/error\_log*, */var/log/http/access\_log* и */var/log/audit/audit.log*, в последнием появились записи (рис. ??).



Содержимое файла - /var/log/audit/audit.log

1. Выполнила команду *semanage port -a -t http\_port\_t -р tcp 81* После проверила список портов командой semanage port -l | grep http\_port\_t Убедилась, что порт 81 появился в списке (рис. ??).



Список портов

1. Перезапустила веб-сервер Apache ещё раз. Он сейчас запустился, так как мы добавили порт. Вернула контекст \*httpd\_sys\_cоntent\_\_t\* к файлу /var/www/html/test.html: *chcon -t httpd\_sys\_content\_t /var/www/html/test.html* (рис. ??).



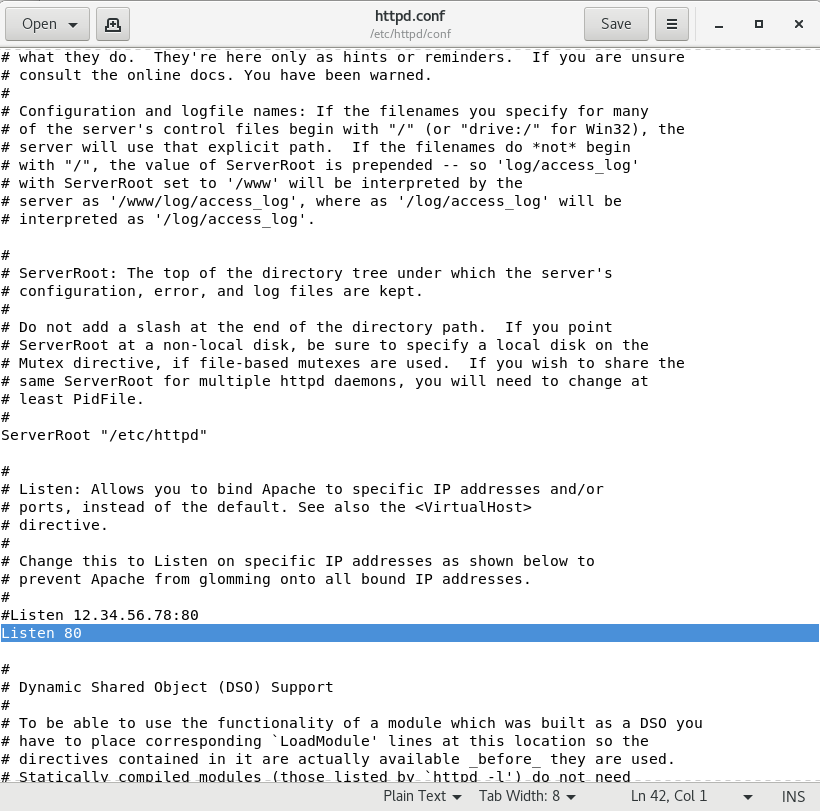
перезапуск и изменение контекста

1. После этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Увидела содержимое — слово «test» (рис. ??).



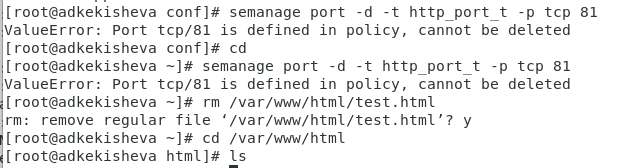
Просмотр содеримого файла через браузер

1. Исправила обратно конфигурационный файл apache, вернув Listen 80 (рис. ??).



Исправление конфигурационный файл

1. Удалила привязку *http\_port\_t* к 81 порту: *semanage port -d -t http\_port\_t -p tcp 81* - это оказалось запрещено (рис. ??).
2. Удалите файл /var/www/html/test.html: rm /var/www/html/test.html (рис. ??).



Удаление привязки к порту 81 и удаление файла

# 5 Выводы

1. Развила навыки администрирования ОС Linux.
2. Получила первое практическое знакомство с технологией SELinux1.
3. Проверила работу SELinx на практике совместно с веб-сервером Apache.

# Список литературы

1. Лабораторная работа No 6. Мандатное разграничение прав в Linux [Электронный ресурс]. URL: <https://esystem.rudn.ru/pluginfile.php/2090419/mod_resource/content/2/006-lab_selinux.pdf>.

2. Введение в SELinux (security acl selinux limit linux kernel) [Электронный ресурс]. URL: <https://www.opennet.ru/base/sec/intro_selinux.txt.html>.