Лабораторная работа №6

Титаренко Анастасия Дмитриевна

Содержание

[Цель работы 1](#_Toc116652242)

[Выполнение лабораторной работы 1](#_Toc116652243)

[Вывод 10](#_Toc116652244)

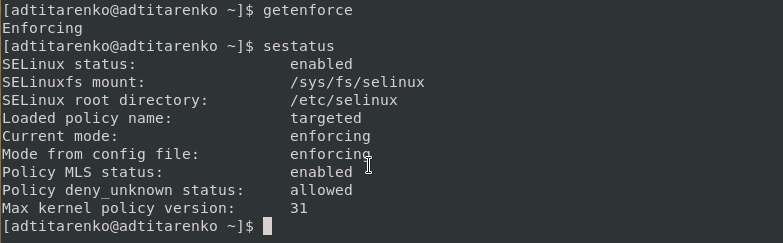
[Список литературы 10](#_Toc116652245)

# Цель работы

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

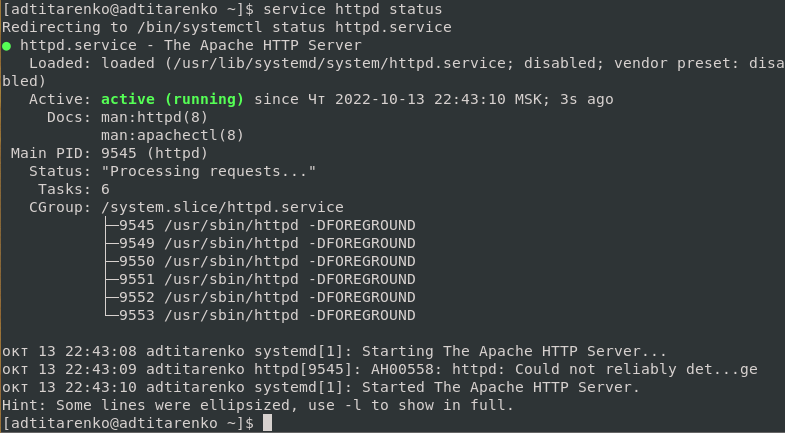
# Выполнение лабораторной работы

1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus.



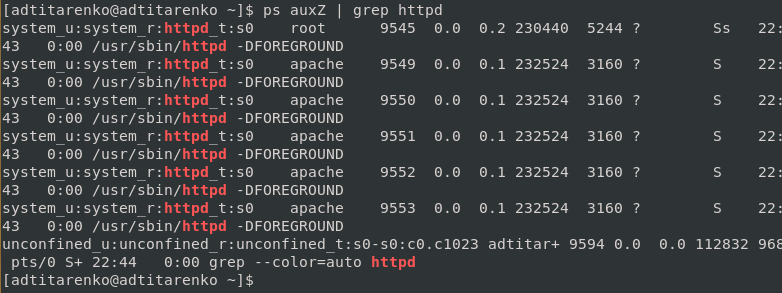
Проверка, что SELinux работает в режиме enforcing политики targeted

1. Обратилась с помощью браузера к веб-серверу, запущенному на компьютере, и убедилась, что последний работает: service httpd status или /etc/rc.d/init.d/httpd status



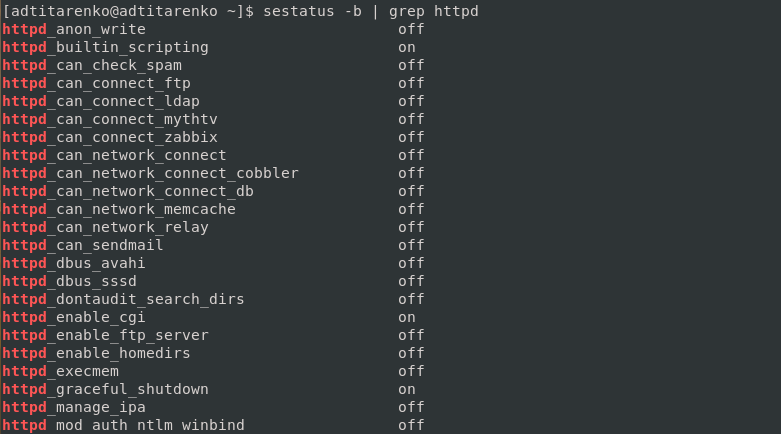
Проверка, что веб-сервис запущен

1. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности. Используя команду: ps auxZ | grep httpd



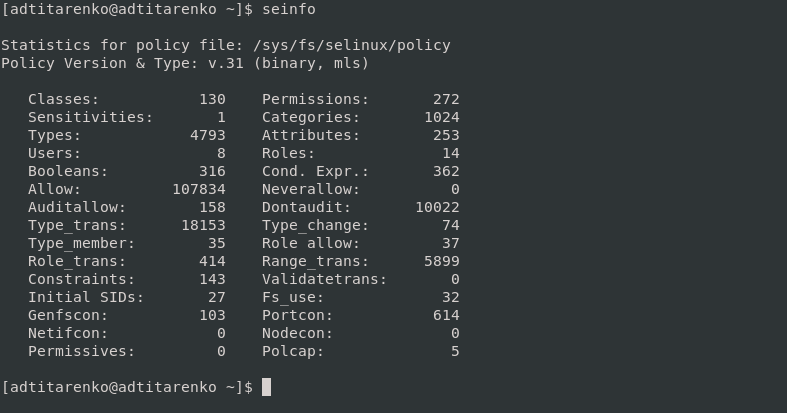
Нахождение веб-сервер Apache в списке процессов

1. Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды: sestatus -bigrep httpd. Обратила внимание, что многие из них находятся в положении «off»



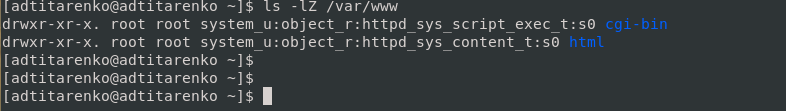
Текущее состояние переключателей SELinux для Apache

1. Посмотрела статистику по политике с помощью команды seinfo, также определила множество пользователей, ролей, типов.



Статистика по политике с помощью команды seinfo

1. Определила тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды: ls -lZ /var/www



Типы файлов и поддиректорий, находящихся в директории /var/www

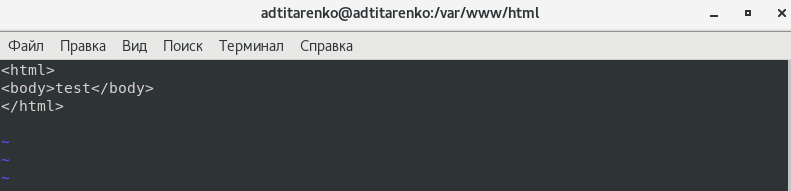
1. Определила тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html



Типы файлов, находящихся в директории /var/www/html

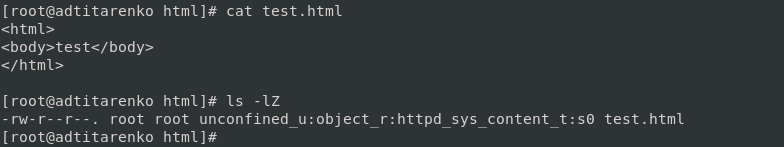
1. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html.
2. Создала от имени суперпользователя html-файл /var/www/html/test.html следующего содержания:

* test



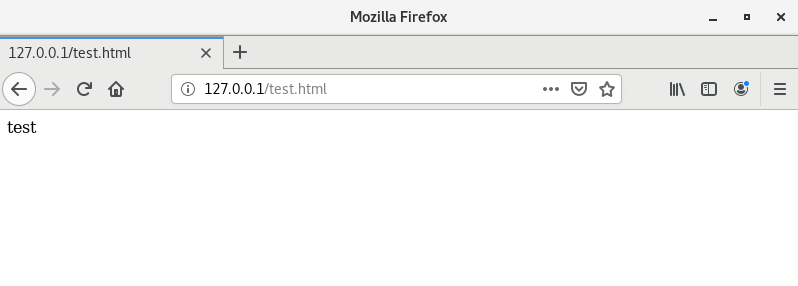
Создание html-файла test.html

1. Проверила контекст созданного файла.



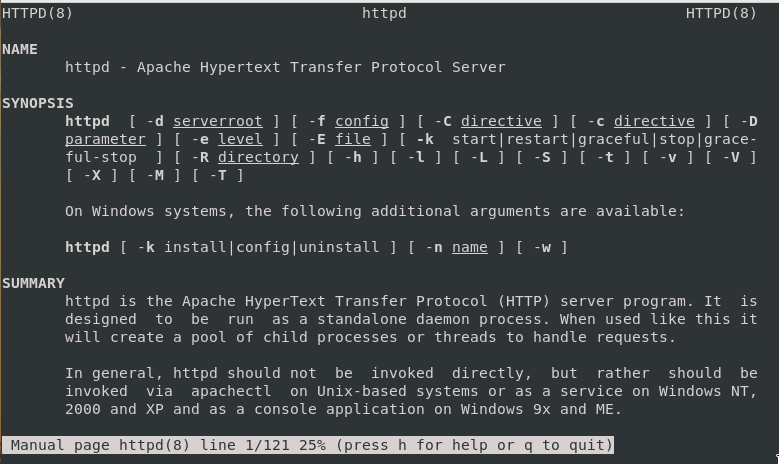
Контекст созданного файла

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



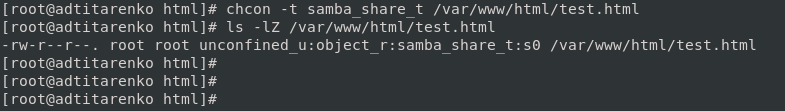
Обращение к файлу через веб-сервер

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



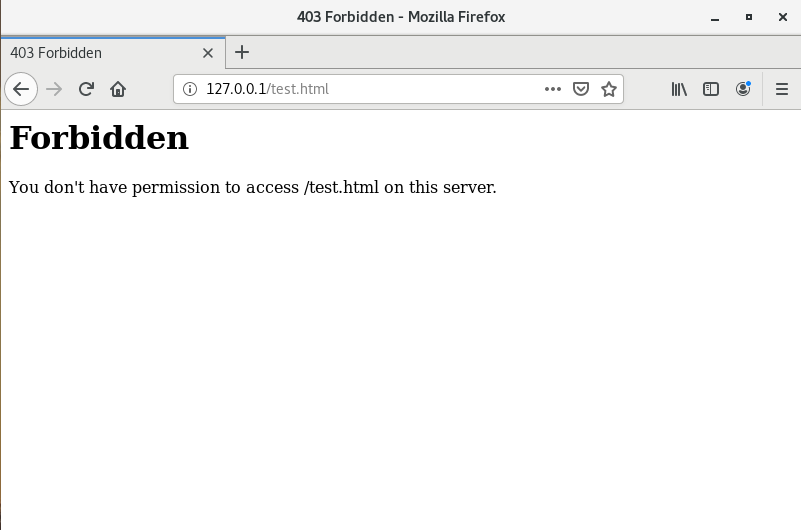
Справка man httpd

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 ls -Z /var/www/html/test.html После этого проверила, что контекст поменялся.



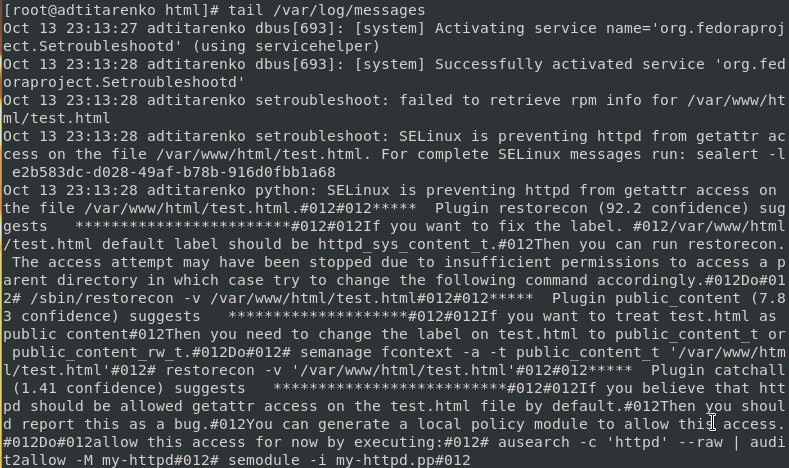
Изменение контекста файла /var/www/html/test.html

1. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Вы должны получить сообщение об ошибке: Forbidden. You don’t have permission to access /test.html on this server.



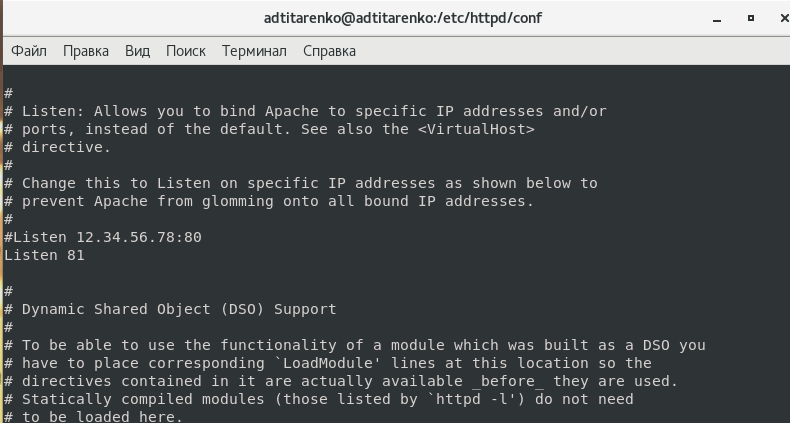
Доступ к файлу через веб-сервер

1. Проанализируйте 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: tail /var/log/messages Если в системе окажутся запущенными процессы setroubleshootd и audtd, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log. Проверьте это утверждение самостоятельно.



log-файлы веб-сервера Apache

1. 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 нашла строчку Listen 80 и заменила её на Listen 81.



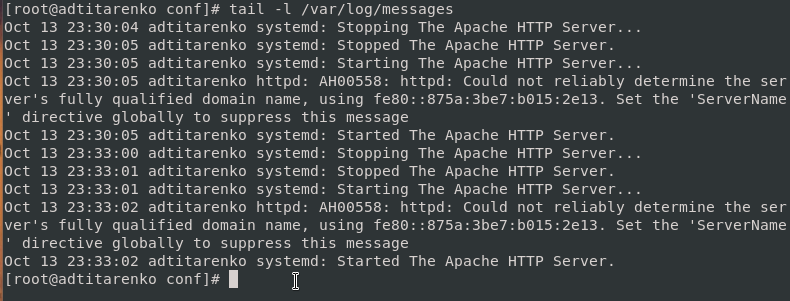
Запуск веб-сервер Apache на прослушивание ТСР-порта 81

1. Выполнила перезапуск веб-сервера Apache. Произошёл сбой.

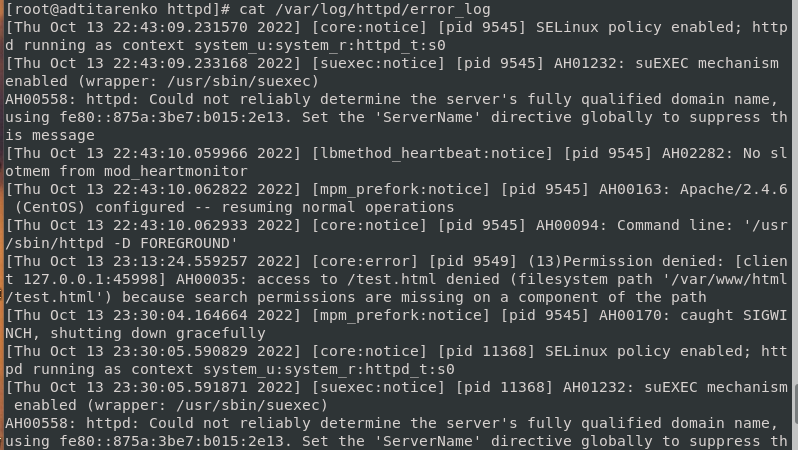


Перезапуск веб-сервера Apache

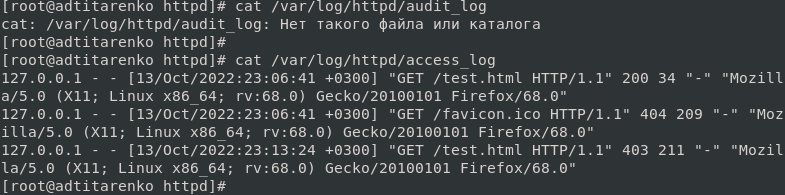
1. Проанализировала лог-файлы: tail -nl /var/log/messages. Просмотрела файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log и выяснила, в каких файлах появились записи.



Лог-файлы: tail -nl /var/log/messages

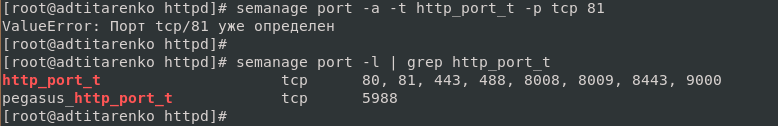


Файл /var/log/http/error\_log



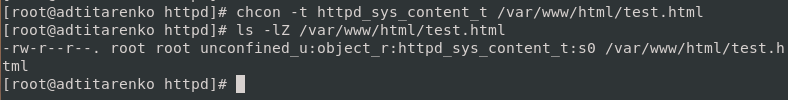
Файлы /var/log/http/access\_log и /var/log/audit/audit.log

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

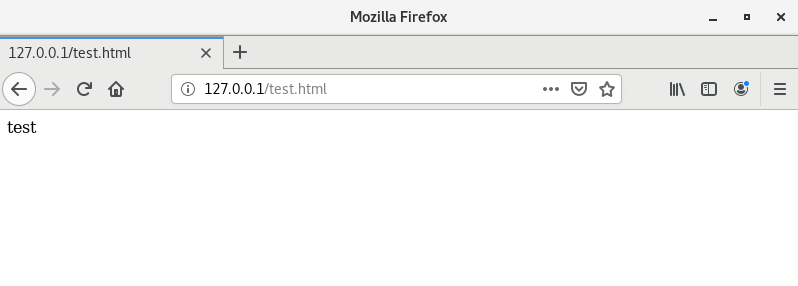


Список портов

1. Попробовала запустить веб-сервер Apache ещё раз.
2. Вернула контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/test.html: chcon -t httpd\_sys\_content\_t /var/www/html/test.html. После этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html.

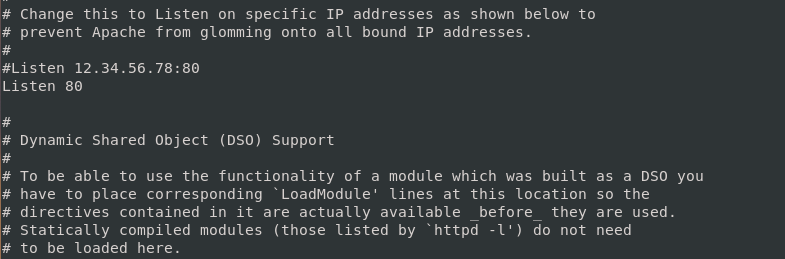


Возвращение контекста httpd\_sys\_cоntent\_\_t к файлу /var/www/html/test.html



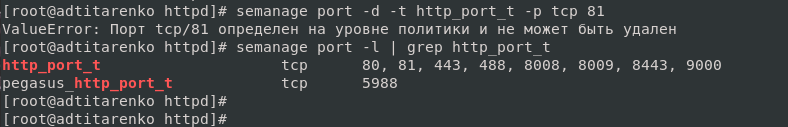
Доступ к файлу через веб-сервер

1. Исправила обратно конфигурационный файл apache, вернув Listen 80.



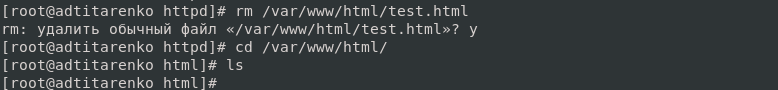
Исправление конфигурационного файла apache (Listen 80)

1. Удалила привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81. Проверила, что порт 81 удалён.



Удаление привязки http\_port\_t к 81 порту

1. Удалила файл /var/www/html/test.html: rm /var/www/html/test.html



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

# Вывод

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

# Список литературы

1. [Лабораторная работа № 6. Мандатное разграничение прав в Linux](https://esystem.rudn.ru/pluginfile.php/1652027/mod_resource/content/2/006-lab_selinux.pdf)