# Лабораторная работа №6

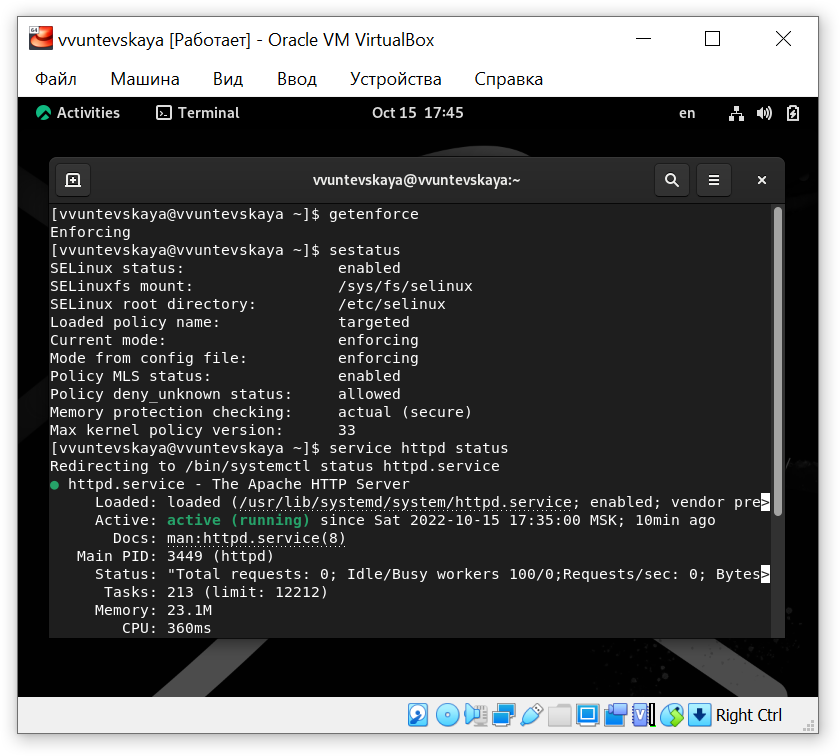
Унтевская Валерия НПИбд-02-19

# Цель работы

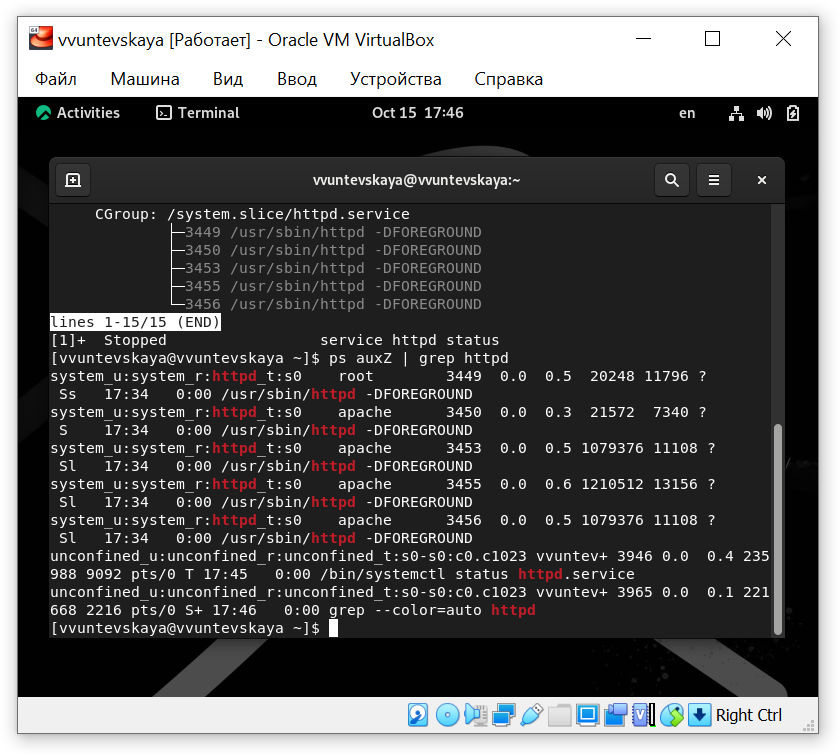
Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinx на практике совместно с веб-сервером Apache.

# Выполнение лабораторной работы

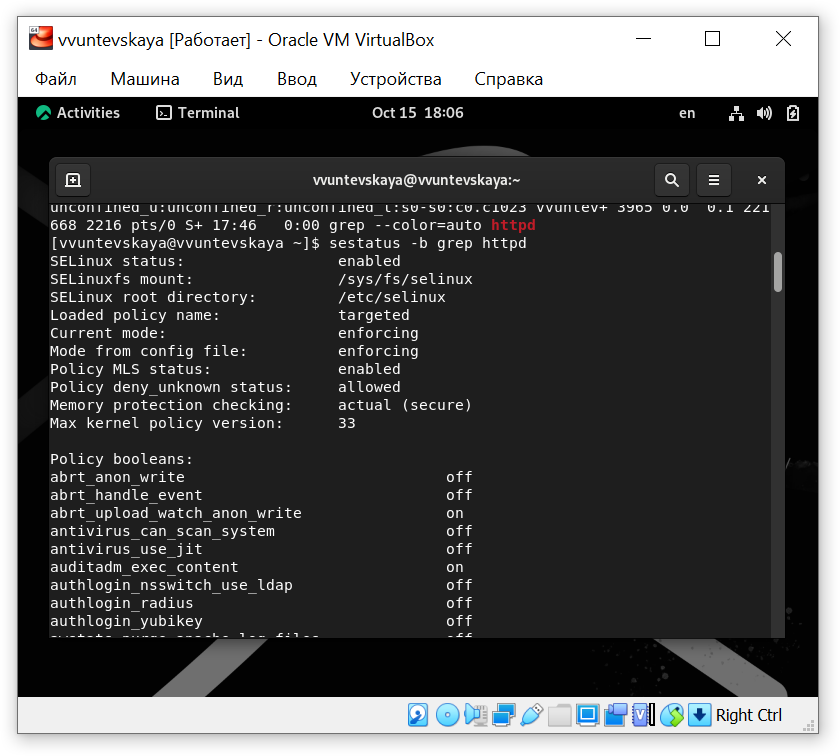
1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted. Обратилась с помощью браузера к веб-серверу, запущенному на компьютере, и убедилась, что последний работает (рис. 1).



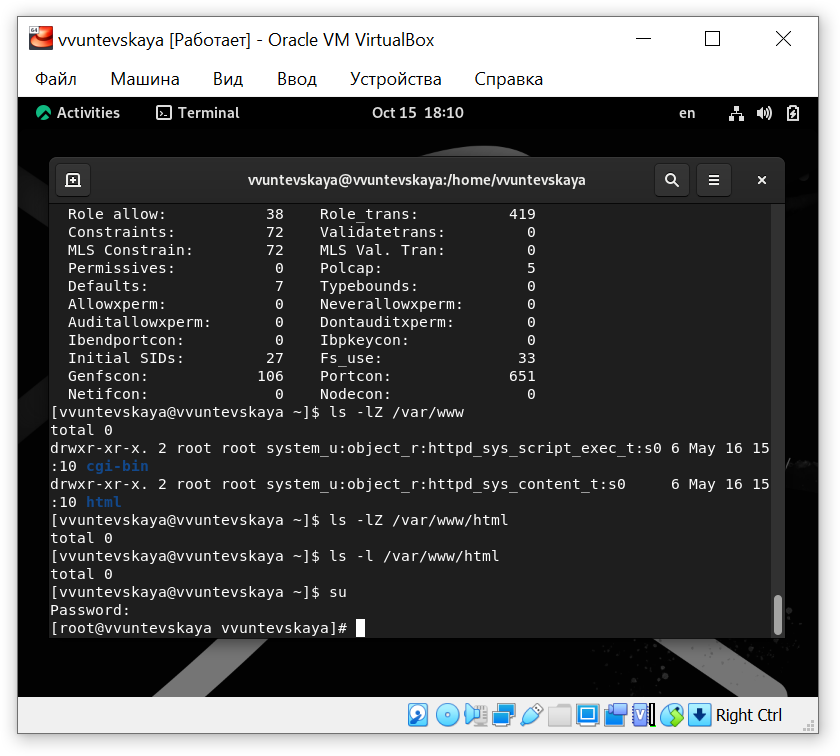
1. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности (рис. 2).



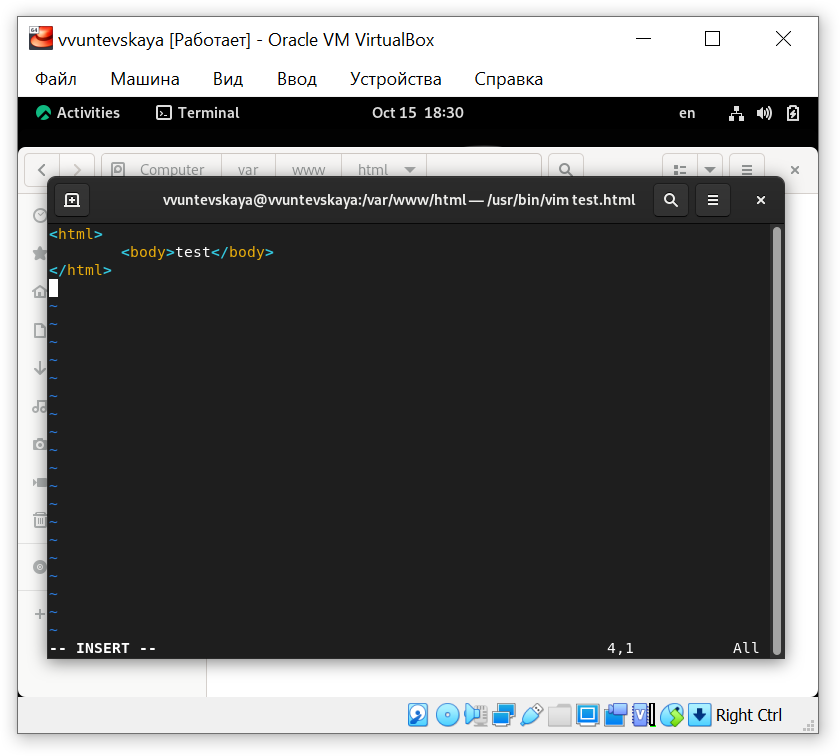
1. Посмотрела текущее состояние переключателей SELinux для Apache (рис. 3).



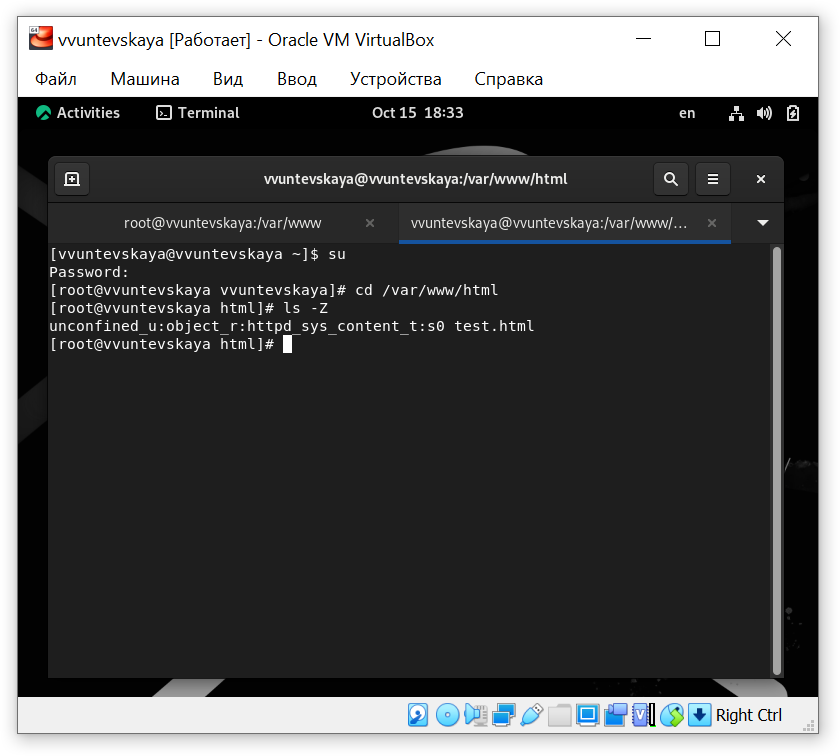
1. Посмотрела статистику по политике с помощью команды seinfo, также определила множество пользователей, ролей, типов.
2. Определила тип файлов и поддиректорий, находящихся в директории /var/www. Определила тип файлов, находящихся в директории /var/www/html. Определила круг пользователей, которым разрешено создание файлов в директории (рис. 4).

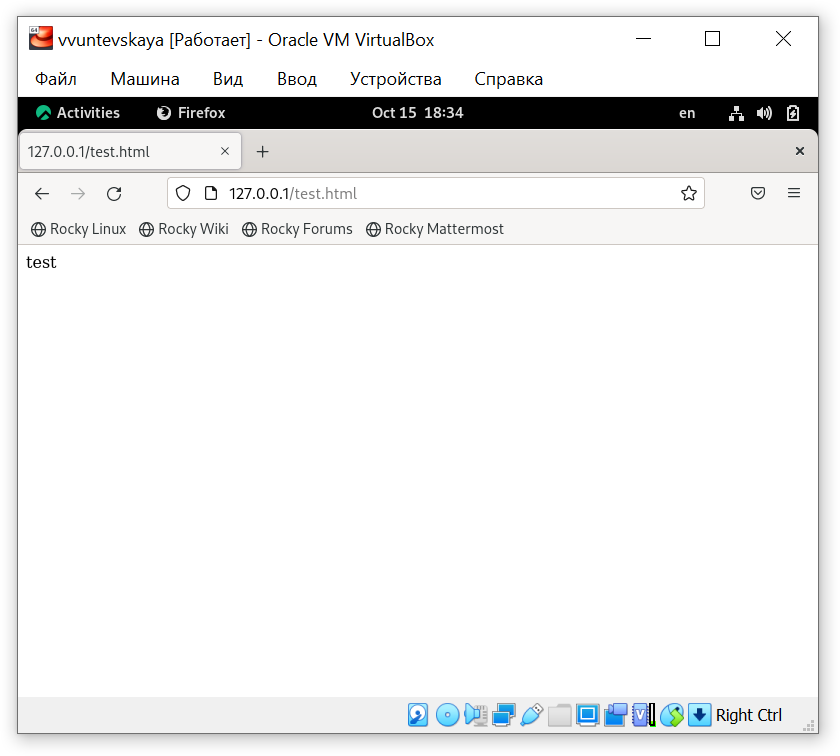
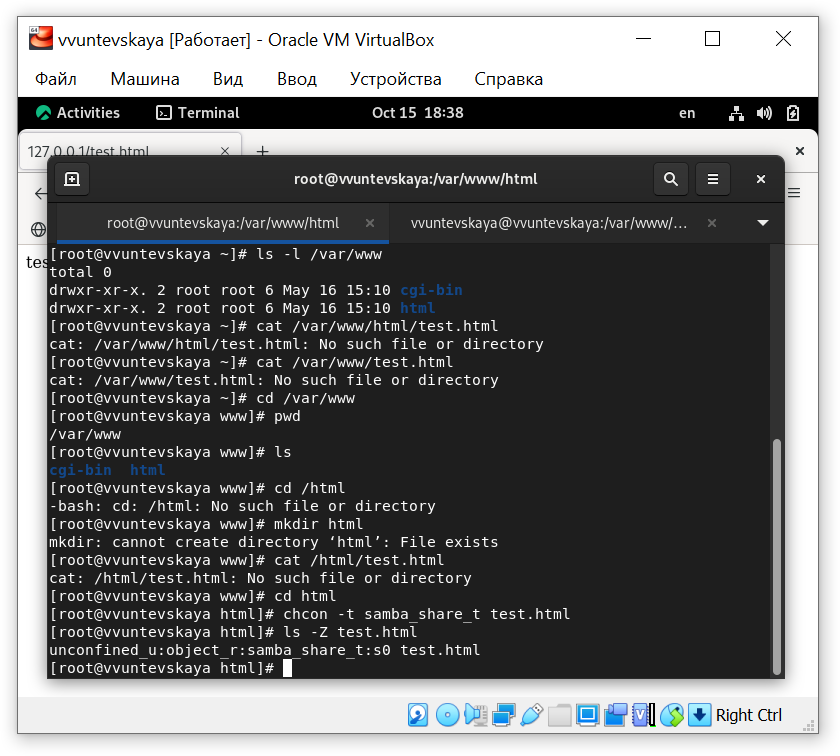
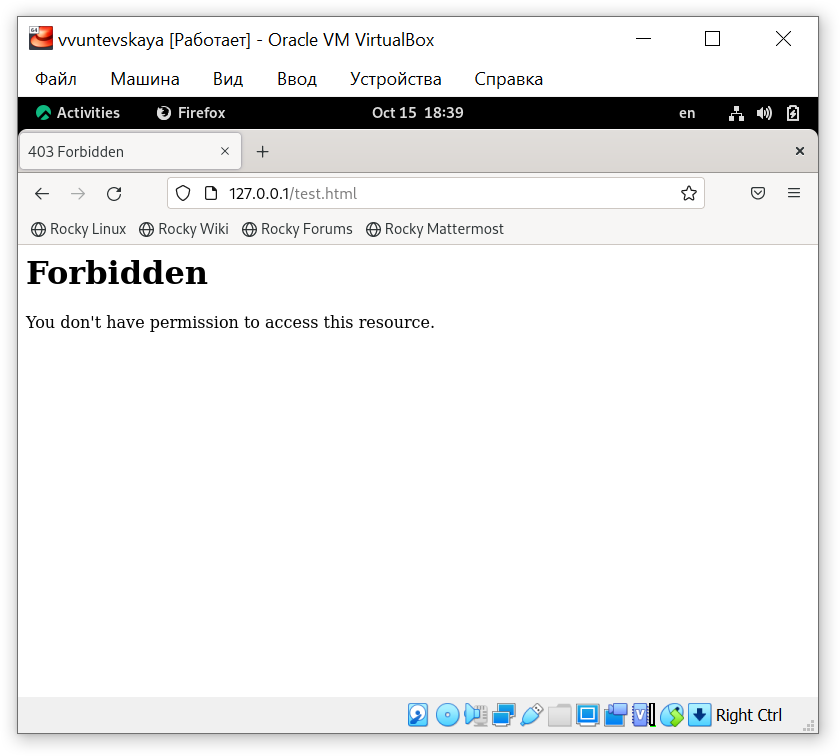
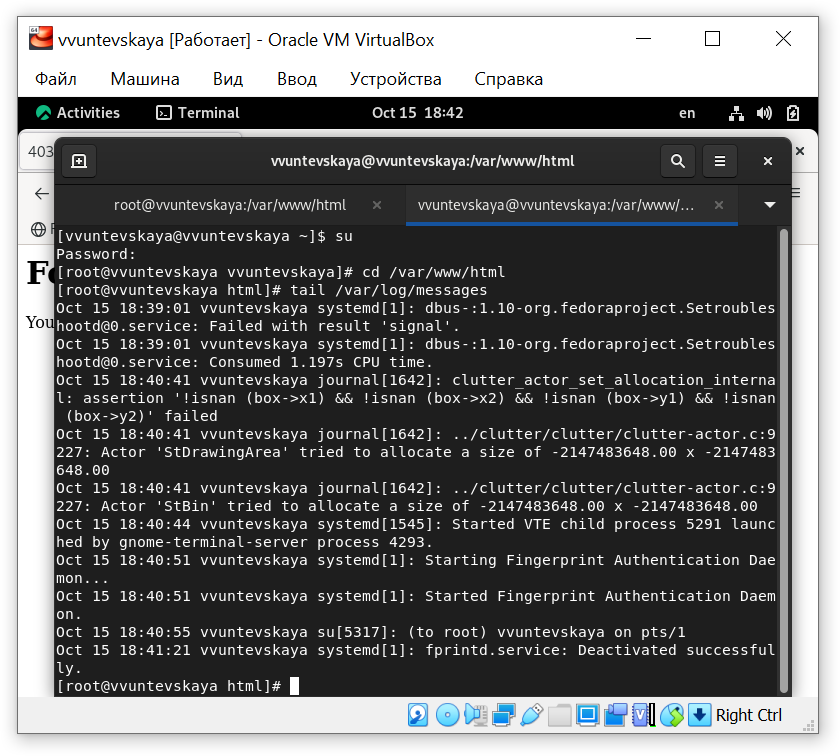
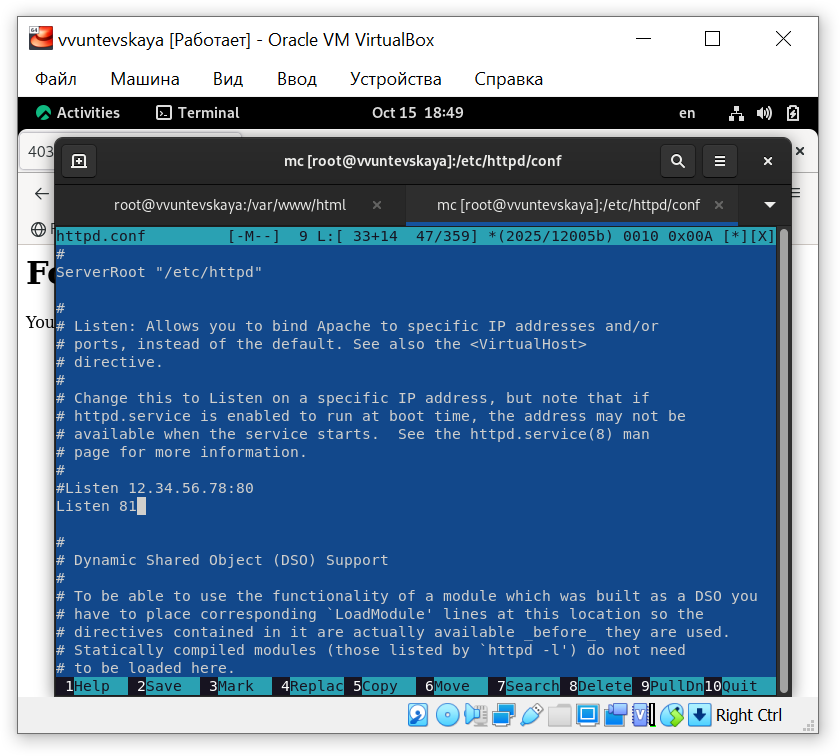
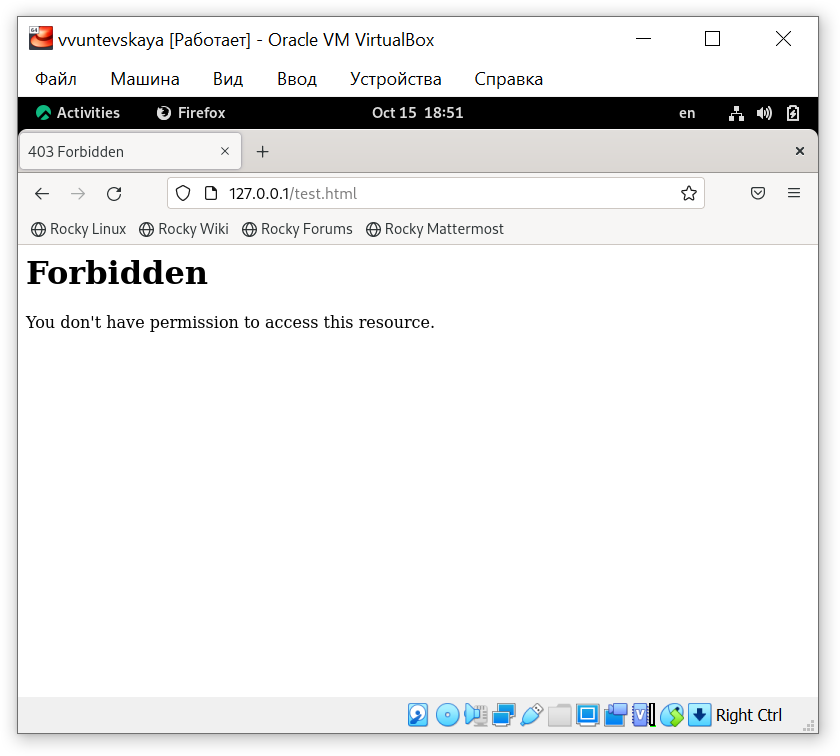
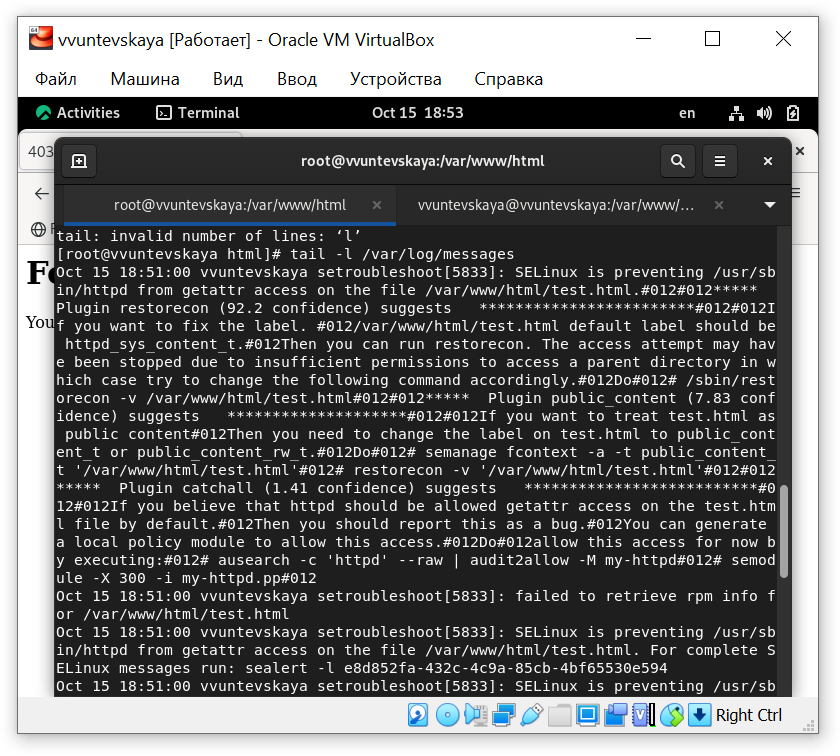
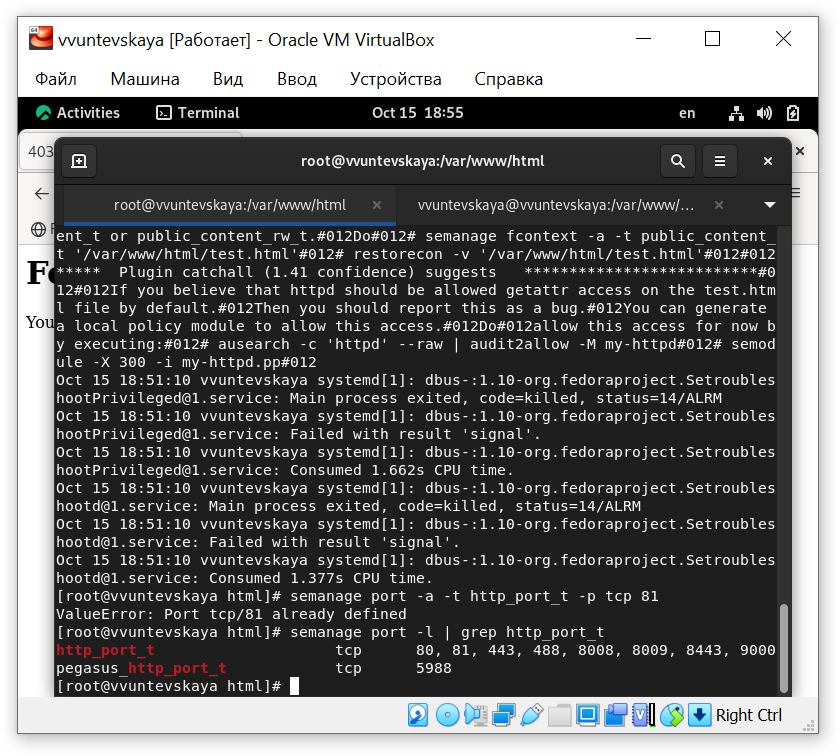
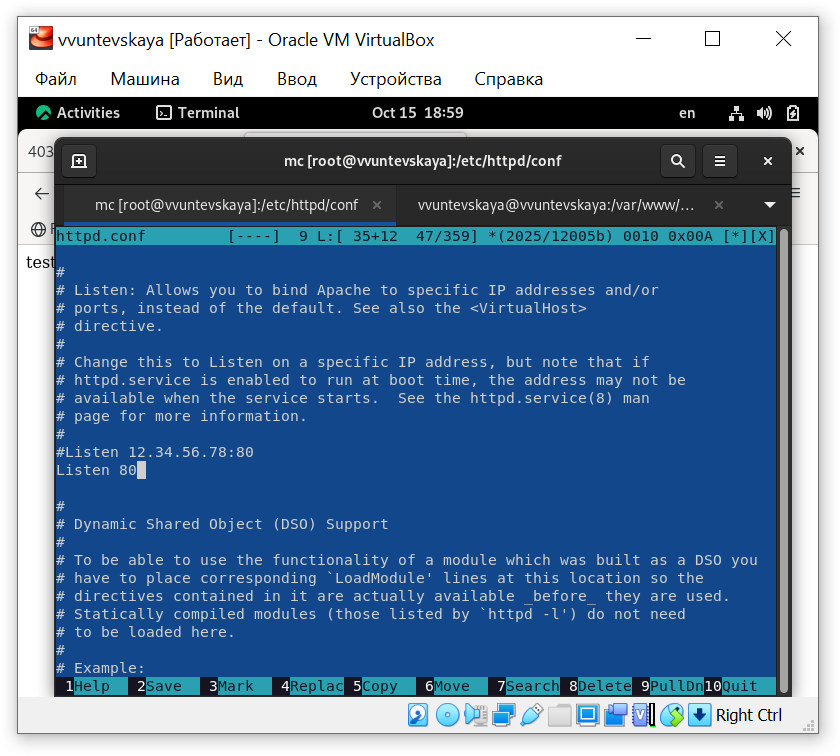
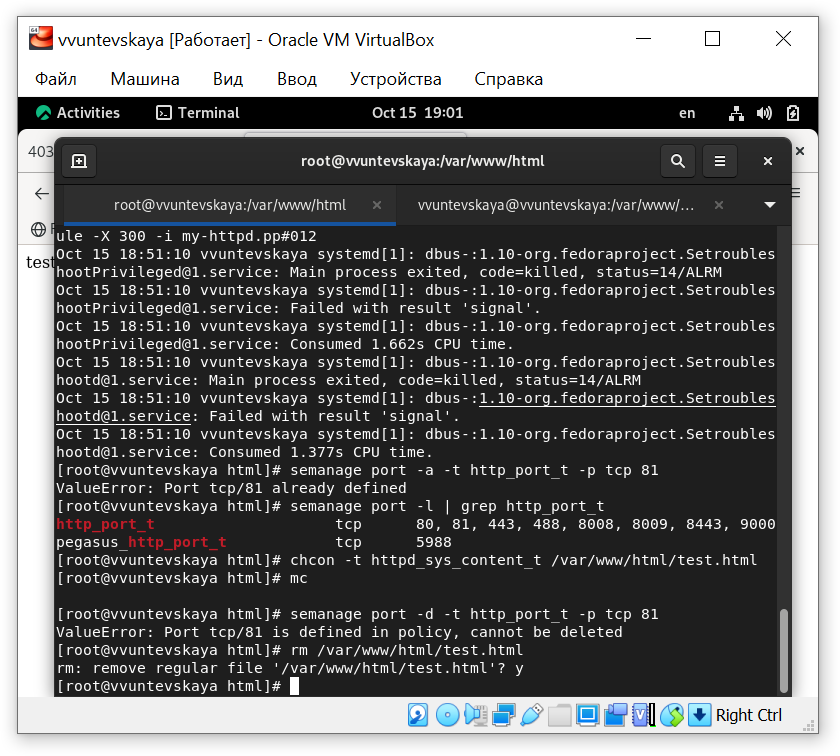


1. Создала от имени суперпользователя html-файл (рис. 5).



1. Проверила контекст созданного файла. Контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html: httpd\_sys\_content (рис. 6).



1. Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедилась, что файл успешно отображён (рис. 7). 
2. Изменила контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t. После этого проверила, что контекст поменялся (рис. 8). 
3. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html (рис. 9). 
4. Проанализировала ситуацию. Почему файл не был отображён,если права доступа позволяют читать этот файл любому пользователю? Просмотрела log-файлы веб-сервера Apache. Также просмотрите системный лог-файл. 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 (рис. 10). 
5. Попробовала запустить веб-сервер Apache на прослушивание ТСР-порта 81. Для этого в файле /etc/httpd/httpd.conf нашёл строчку Listen 80 и заменил её на Listen 81 (рис. 11). 
6. Выполнила перезапуск веб-сервера Apache. (рис. 12). 
7. Проанализировала лог-файлы. Просмотрела файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log (рис. 13). 
8. Выполнила команду semanage port -a -t http\_port\_t -р tcp 81. После этого проверила список портов. Убедилась, что порт 81 появился в списке (рис. 14). 
9. Вернула контекст httpd\_sys\_cоntent\_\_t к файлу/var/www/html/test.html (рис. 15). 
10. Исправила обратно конфигурационный файл apache, вернув Listen80.
11. Удалила привязку http\_port\_t к 81 порту. Удалила файл /var/www/html/test.html (рис. 16). 

# Выводы

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