Лабораторная работа №6

Мандатное разграничение прав в Linux

Монастырская Кристина Владимировна

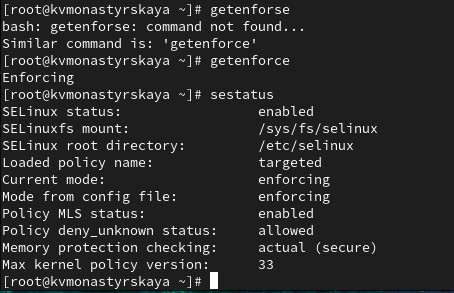
Содержание

# Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinux на практике совместно с веб-сервером Apache. [[1]](#список-литературы)

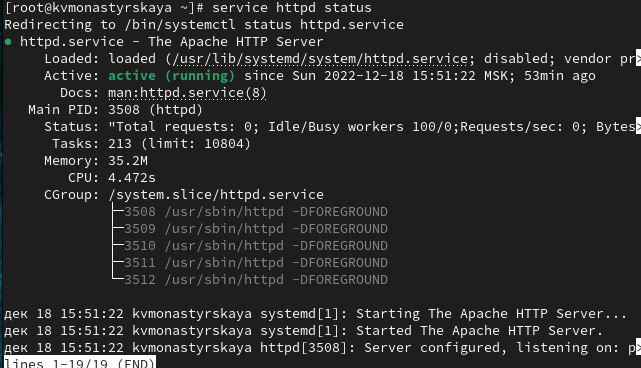
# Выполнение лабораторной работы

1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus. ([рис. 1](../images/1.jpg))



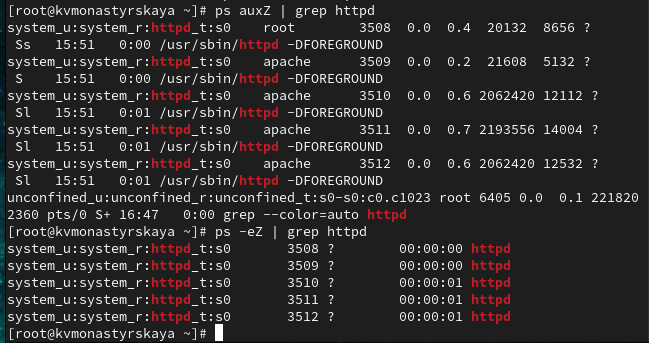
Режим SELinux

1. Запустила веб-сервер. Обратилась с помощью браузера к веб-серверу, запущенному на компьютере, и убедилась, что последний работает: service httpd status. ([рис. 2](../images/2.jpg)).



Проверка работы веб-сервера

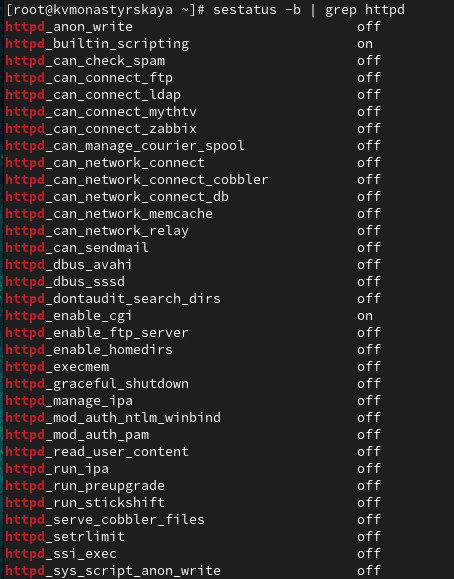
1. Нашла веб-сервер Apache в списке процессов. ([рис. 3](../images/3.jpg)).



Список процессов

Контекст безопасности: system\_u:system\_r:httpd\_t:s0

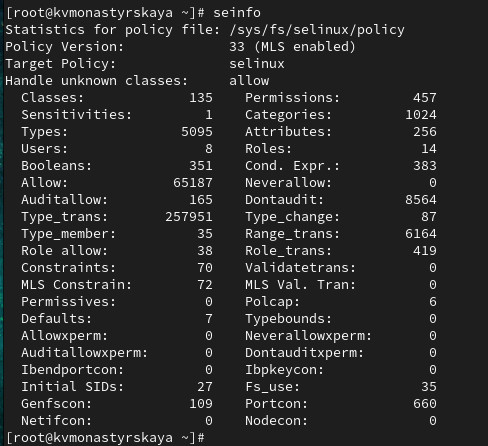
1. Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды sestatus -b | grep httpd. ([рис. 4](../images/4.jpg)).



Состояние переключателей SELinux

Многие из них находятся в положении «off»

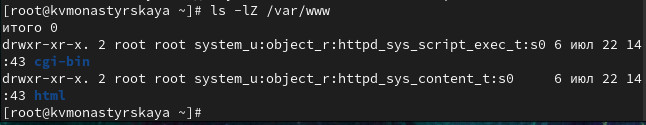
1. Посмотрела статистику по политике с помощью команды seinfo. ([рис. 5](../images/5.jpg)).



Статистика SELinux

Множество пользователей - 8  
Ролей - 14 Типов - 5002

1. Определила тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www ([рис. 6](../images/6.jpg)).



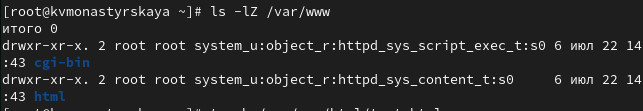
Тип поддиректорий в директории /var/www

1. Определила тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html ([рис. 7](../images/7.jpg)).

Директория /var/www/html

Директория /var/www/html

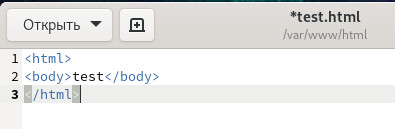
1. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html. ([рис. 8](../images/8.jpg)).



Право на создание файлов

Создавать файлы в директории может только её владелец.

1. Создала от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания: ([рис. 9](../images/9.jpg)).



HTML-файл /var/www/html/test.html

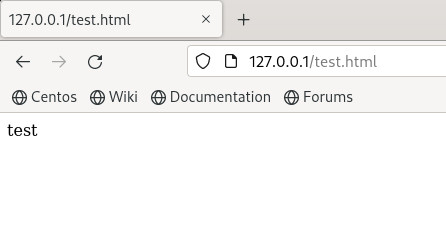
1. Проверила контекст созданного файла. ([рис. 10](../images/10.jpg)).

Контекст файла

Контекст файла

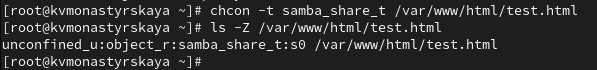
Контекст безопасности (по умолчания для новых файлов в директории): nconfined\_u:object\_r:httpd\_sys\_content\_t:s0

1. Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. ([рис. 11](../images/11.jpg)).



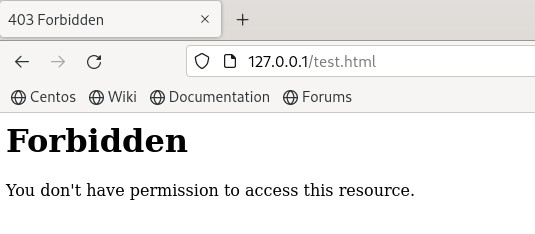
Отображение файла test.html

1. Изучила справку man httpd\_selinux ([рис. 12](../../image/12.png)).
2. Изменила контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на тот, к которому процесс httpd не имеет доступ (samba\_share\_t) ([рис. 13](../images/13.jpg)).



Изменение контекста файла

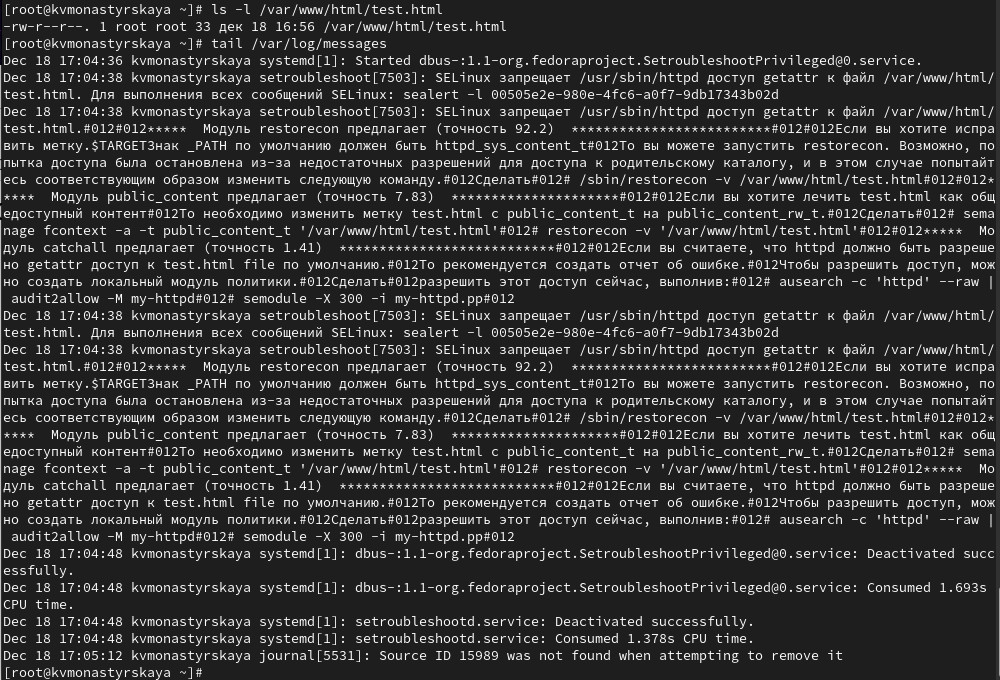
1. Попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. ([рис. 14](../images/14.jpg)).



Доступ через веб-сервер

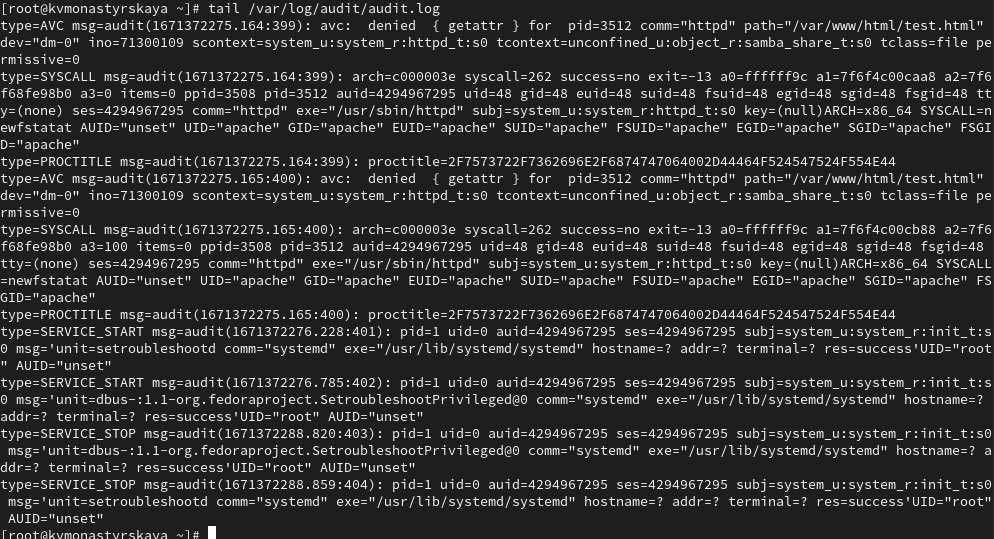
Файл не отображен, так как к заданному типу контекста httpd не имеет доступа.

1. Просмотрела log-файлы веб-сервера Apache. ([рис. 15](../images/15.jpg))



log-файл

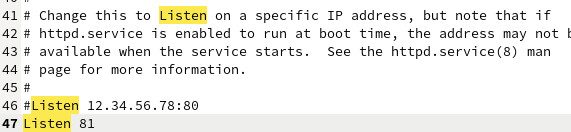
Посмотрела системный лог-файл ([рис. 16](../images/15_1.jpg)).



Системный log-файл

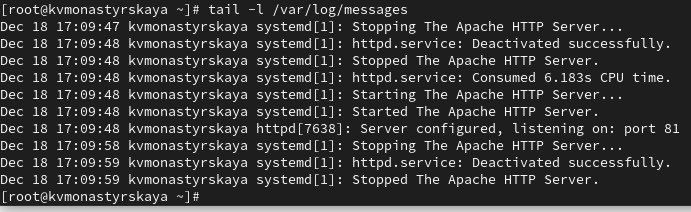
Можем видеть как отображаются ошибки.

1. Попробовала запустить веб-сервер Apache на прослушивание ТСР-порта 81 ([рис. 17](../images/16.jpg)).

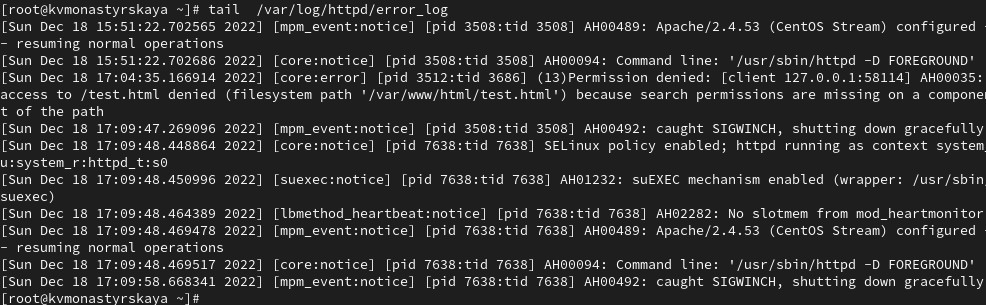


Включение прослушивания 81 порта

1. Выполнила перезапуск веб-сервера Apache и посмотрела лог-файлы ([рис. 17](../images/17.jpg)-[рис. 20](../images/18_3.jpg)).



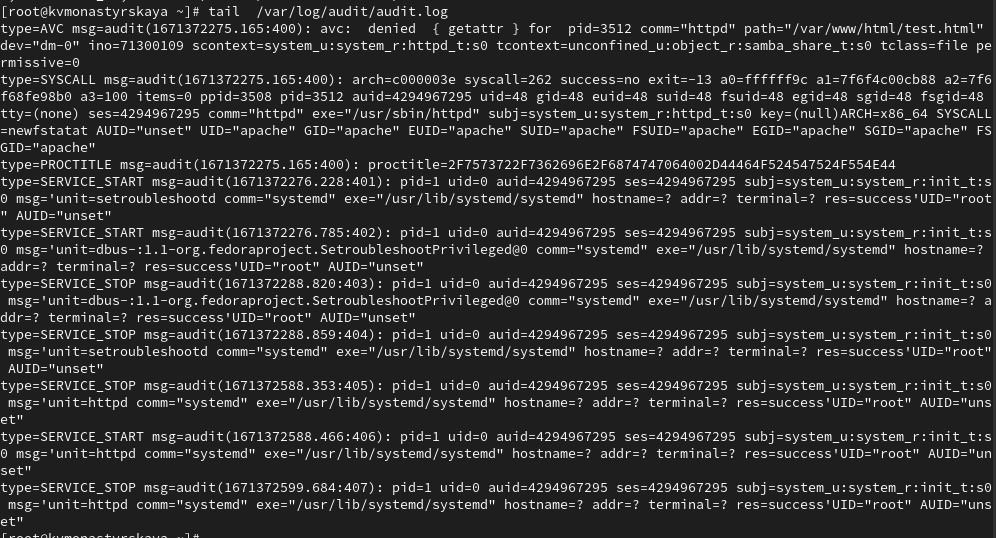
Лог-файл /var/log/messages



Лог-файл /var/log/http/error\_log

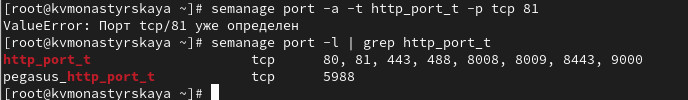


Лог-файл /var/log/http/access\_log

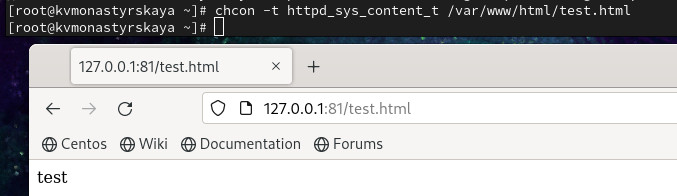


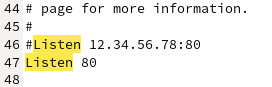
Лог-файл /var/log/audit/audit.log

1. Добавила порт 81 в список портов. ([рис. 21](../images/19.jpg)).



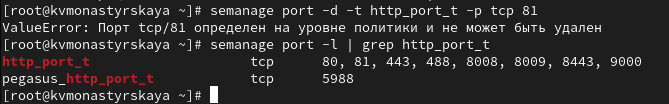
Список портов

1. Вернула контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html:. Попробовала получить доступ к файлу через веб-сервер по 81 порту ([рис. 24](../images/21.jpg)) 
2. Исправила обратно конфигурационный файл apache ([рис. 26](../images/22.jpg)).



Конфигурационный файл Apache

1. Попробовала удалить привязку http\_port\_t к 81 порту ([рис. 27](../images/23.jpg)).



Удаление порта из списка

1. Удалила файл /var/www/html/test.html ([рис. 28](../images/24.jpg)).

Удаление файла

Удаление файла

# Выводы

Получили практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache.

# Список литературы

1. [Основы безопасности информационных систем : Учеб. пособие для студентов вузов, обучающихся по специальностям “Компьютер. безопасность” и “Комплекс. обеспечение информ. безопасности автоматизир. систем” / Д.А. Зегжда, А.М. Ивашко. - М. : Горячая линия - Телеком, 2000. - 449, [2] с. : ил., табл.; 21 см.; ISBN 5-93517-018-3](https://search.rsl.ru/ru/record/01000682756).