Информационная безопасность

Л.6. Мандатное разграничение прав в Linux

Ширяев Кирилл Владимирович

2022

Содержание

[Цель работы 1](#_Toc96438811)

[Порядок выполнения работы 2](#_Toc96438815)

[Режим SELinux 2](#_Toc96438816)

[Рабочий веб-сервер 2](#_Toc96438817)

[Веб-сервер Apache 3](#_Toc96438818)

[Переключатели SELinux для Apache 4](#_Toc96438819)

[Команда seinfo 5](#_Toc96438820)

[Тип файлов и поддиректорий www 6](#_Toc96438821)

[Тип файлов и поддиректорий html 7](#_Toc96438822)

[Cоздание файлов в директории html 8](#_Toc96438823)

[Создание test.html 9](#_Toc96438824)

[Проверка контекста 9](#_Toc96438825)

[Файл из браузера и справка 10](#_Toc96438826)

[Изменение контекста 10](#_Toc96438827)

[Доступ к файлу 11](#_Toc96438828)

[Вывод 12](#_Toc96438835)

# Цель работы

Развить навыки администрирования ОС Linux.

Получить первое практическое знакомство с технологией SELinux.

Проверить работу SELinx на практике совместно с веб-сервером Apache.

# Порядок выполнения работы

## Режим SELinux

Вошли в систему со своими учётными данными и убедитесь (рис. 3), что SELinux работает в режиме *enforcing* политики *targeted* с помощью команд:

* getenforce
* sestatus

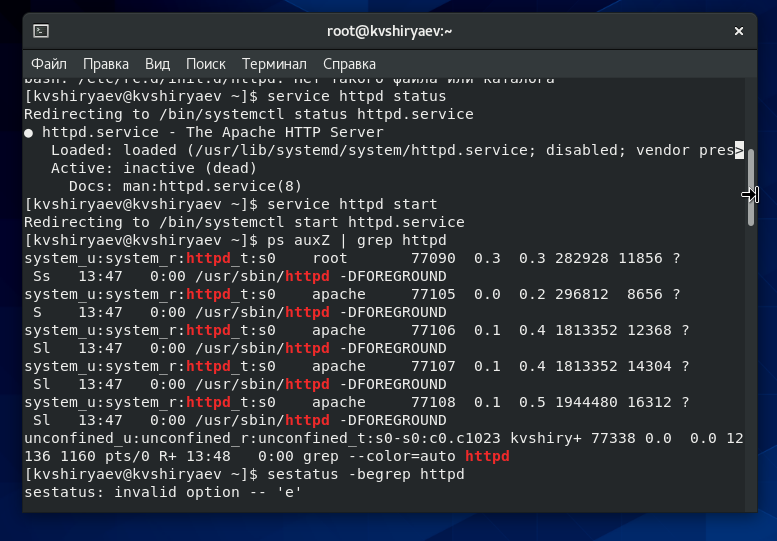


Figure 3: Режим SELinux

## Рабочий веб-сервер

Обратились через терминал к веб-серверу (рис. 4), запущенному на компьютере, и убедились, что последний работает:

* service httpd status
* /etc/rc.d/init.d/httpd status

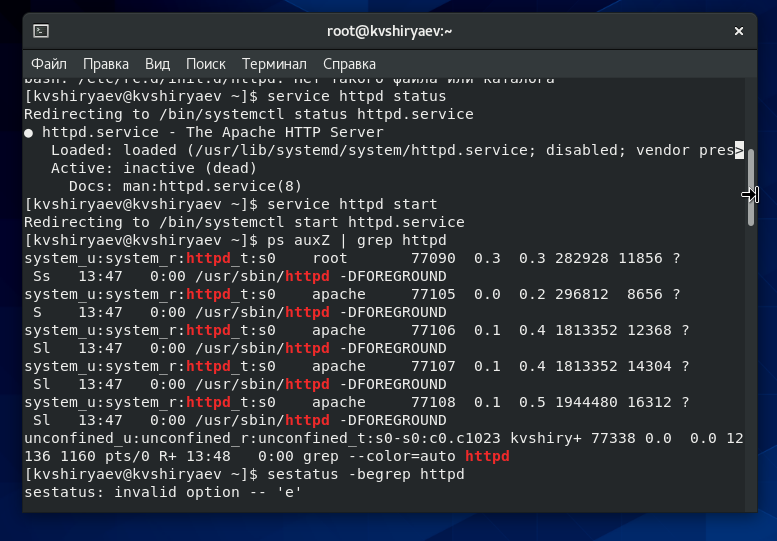


Figure 4: Рабочий веб-сервер

## Веб-сервер Apache

Нашли веб-сервер Apache (рис. 5) в списке процессов, определили его контекст безопасности:

* ps auxZ | grep httpd

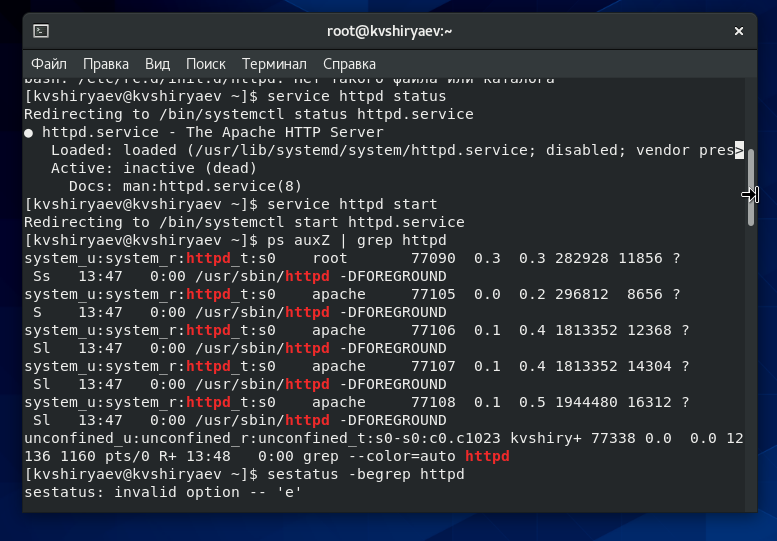


Figure 5: Веб-сервер Apache

## Переключатели SELinux для Apache

Посмотрели текущее состояние переключателей SELinux для Apache с помощью команды:

* sestatus -bigrep httpd

Обратили внимание (рис. 6), что многие из них находятся в положении *«off»*:

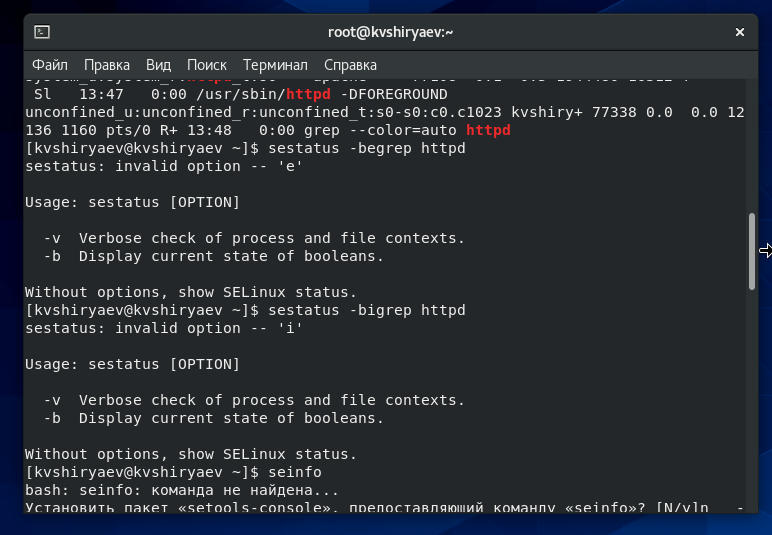


Figure 6: Переключатели SELinux для Apache

## Команда seinfo

Посмотрели статистику по политике с помощью команды seinfo (рис. 7), также определили множество пользователей, ролей, типов:

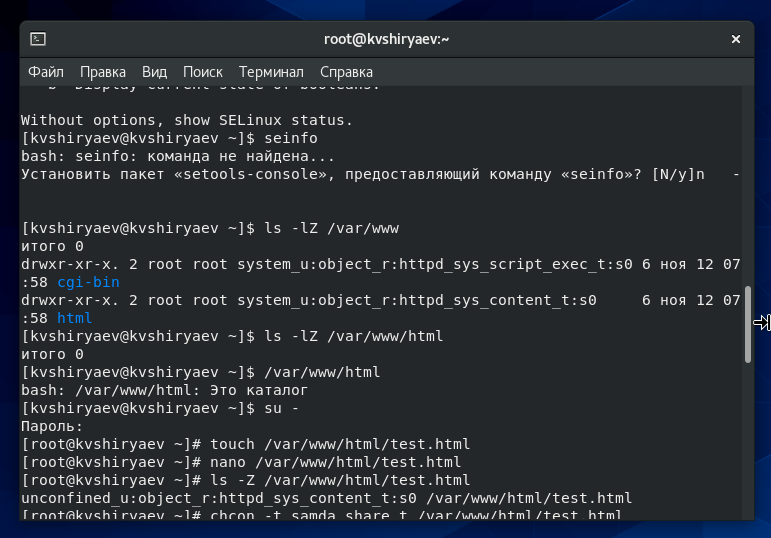


Figure 7: Команда seinfo

## Тип файлов и поддиректорий www

Определили тип файлов и поддиректорий (рис. 8), находящихся в директории */var/www*, с помощью команды:

* ls -lZ /var/www

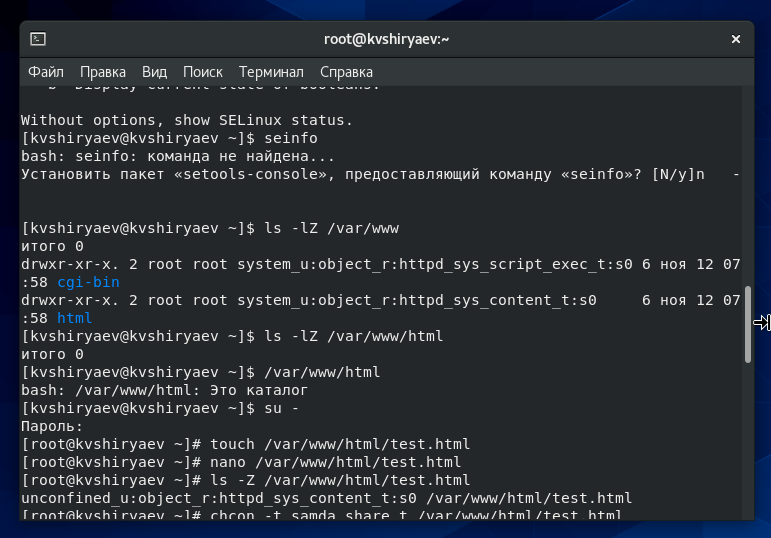


Figure 8: Тип файлов и поддиректорий www

## Тип файлов и поддиректорий html

Определили тип файлов (рис. 9), находящихся в директории */var/www/html* с помощью команды:

* ls -lZ /var/www/html

Убедились, что файлы отсутствуют.

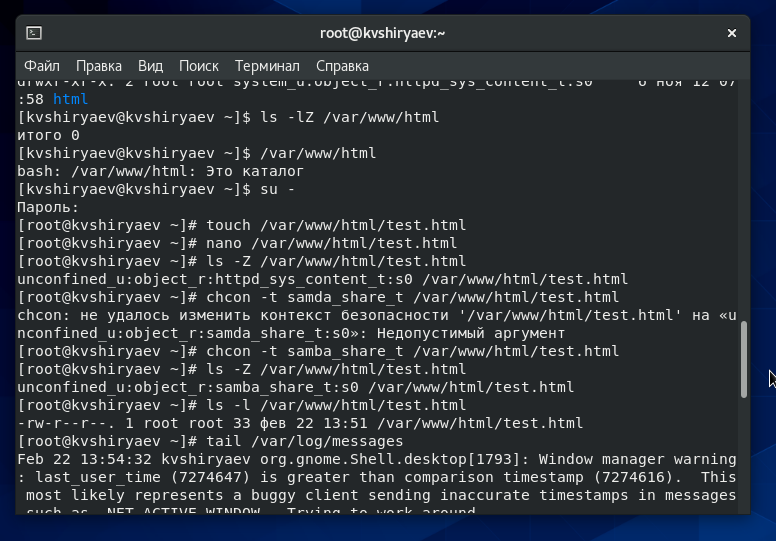


Figure 9: Тип файлов и поддиректорий www

## Cоздание файлов в директории html

Определили круг пользователей (рис. 10), которым разрешено создание файлов в директории */var/www/html* - пользователи с root правами:

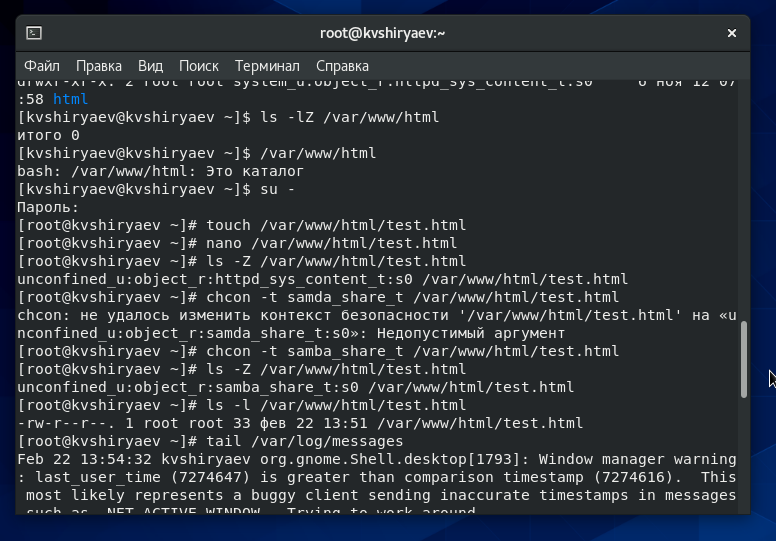


Figure 10: Тип файлов и поддиректорий www

## Создание test.html

Создали от имени суперпользователя html-файл */var/www/html/test.html* (рис. 11) следующего содержания:

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

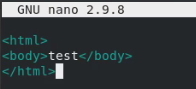


Figure 11: Создание test.html

## Проверка контекста

Проверили контекст созданного файла и контекст, присваиваемый по умолчанию (рис. 12) вновь созданным файлам в директории */var/www/html*:

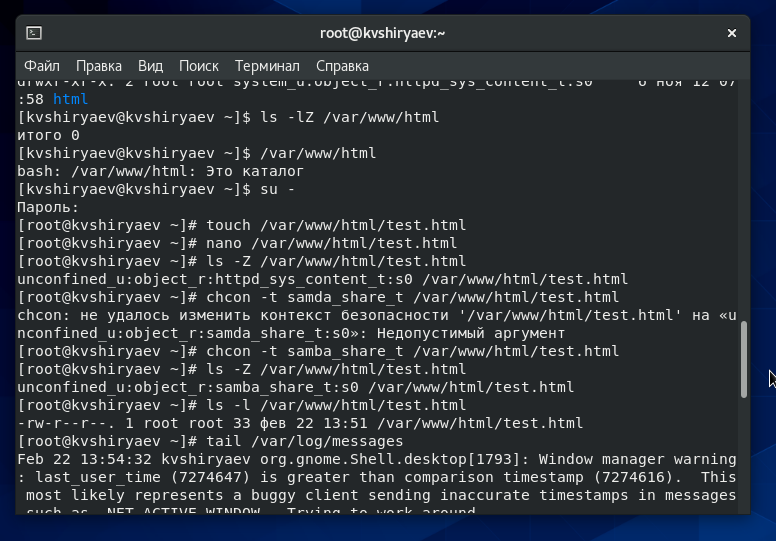


Figure 12: Проверка контекста

## Файл из браузера и справка

Обратитились к файлу через веб-сервер, введя в браузере адрес *http://127.0.0.1/test.html*.

Убедились, что файл был успешно отображён.

Изучили справку *man httpd\_selinux* и выяснили, какие контексты файлов определены для httpd.

## Изменение контекста

Изменили контекст файла */var/www/html/test.html* (рис. 13) с *httpd\_sys\_content\_t* на *samba\_share\_t*, к которому процесс httpd не должен иметь доступа, и проверили, что он поменялся:

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

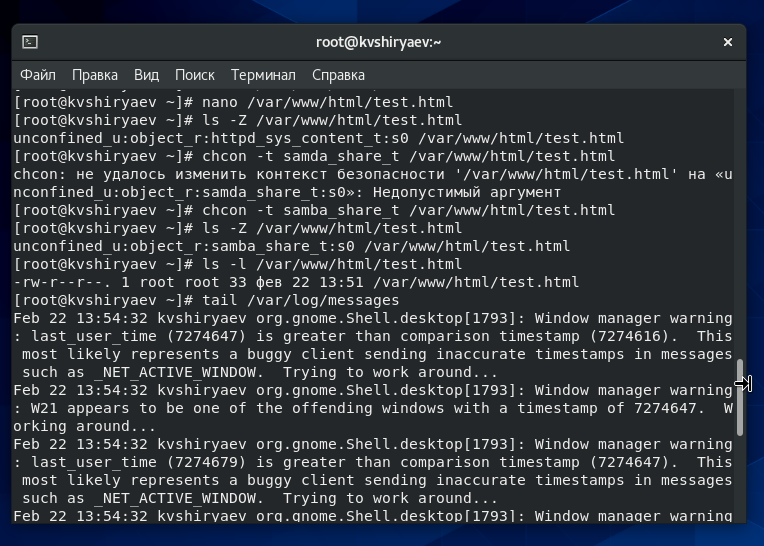


Figure 13: Изменение контекста

## Доступ к файлу

Попробовали получить доступ к файлу через веб-сервер, введя в браузере адрес *http://127.0.0.1/test.html*, и получили сообщение об ошибке.

Хоть права доступа и позволяют читать этот файл любому пользователю (рис. 14), однако из-за контекста файл нет был отображён.

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

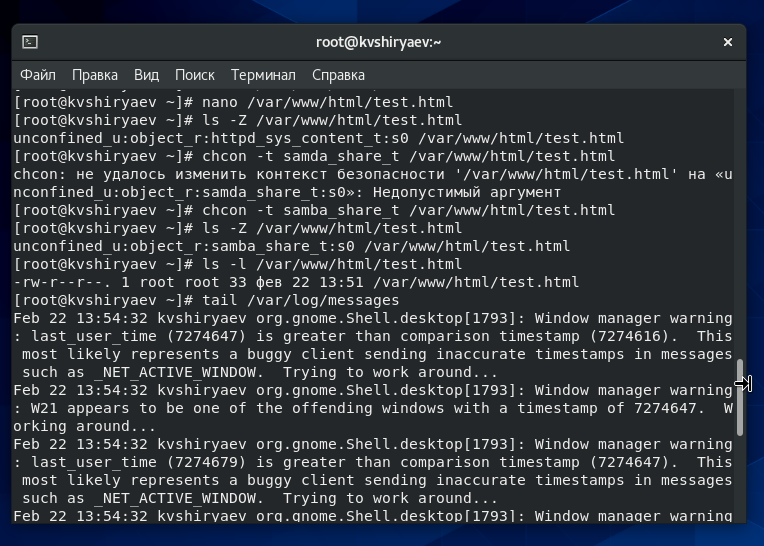


Figure 14: Доступ к файлу

# Вывод

Развили навыки администрирования ОС Linux.

Получили первое практическое знакомство с технологией SELinux.

Проверили работу SELinx на практике совместно с веб-сервером Apache.