Информационная безопасность. Лабораторная работа #6.

Мандатное разграничение прав в Linux

Хохлачева Яна

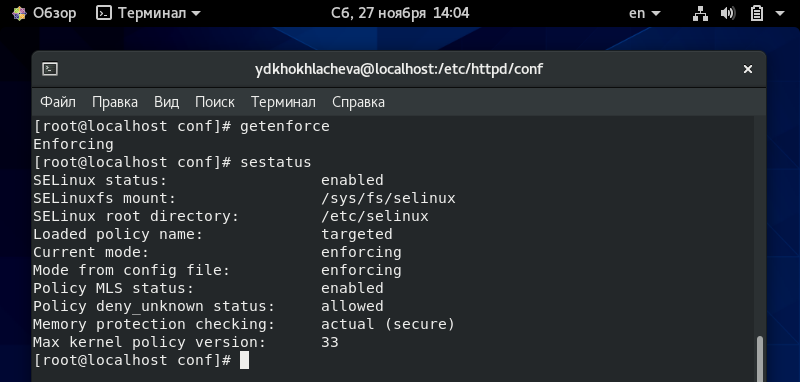
Содержание

## Цель работы

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

# Создание программы

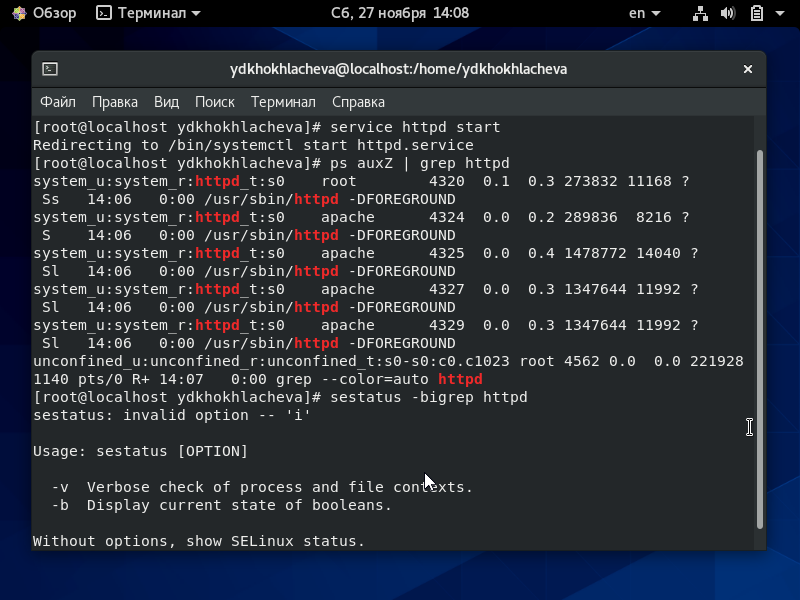
1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд **getenforce** и **sestatus**.



Проверка SELinux

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

Если не работает, запустите его так же, но с параметром **start**.

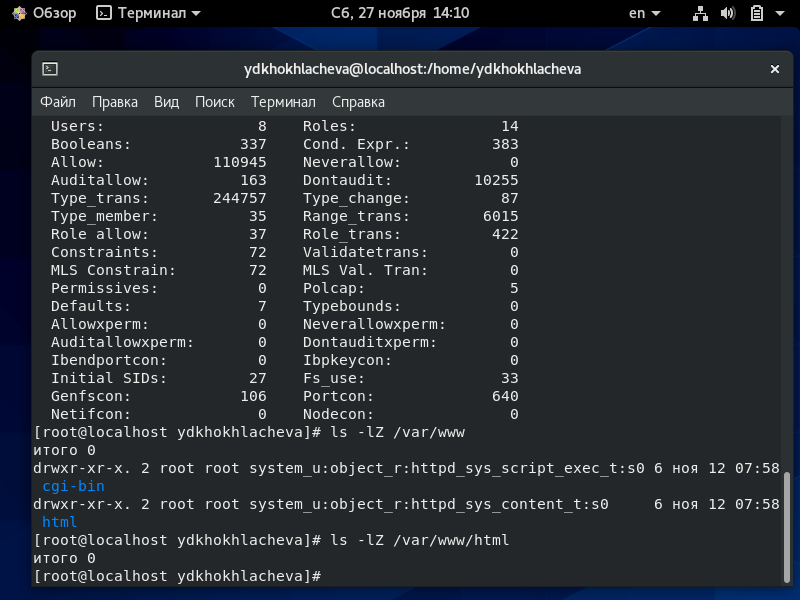


Запуск Apache

1. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду **ps auxZ | grep httpd**
2. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды **sestatus -bigrep httpd**

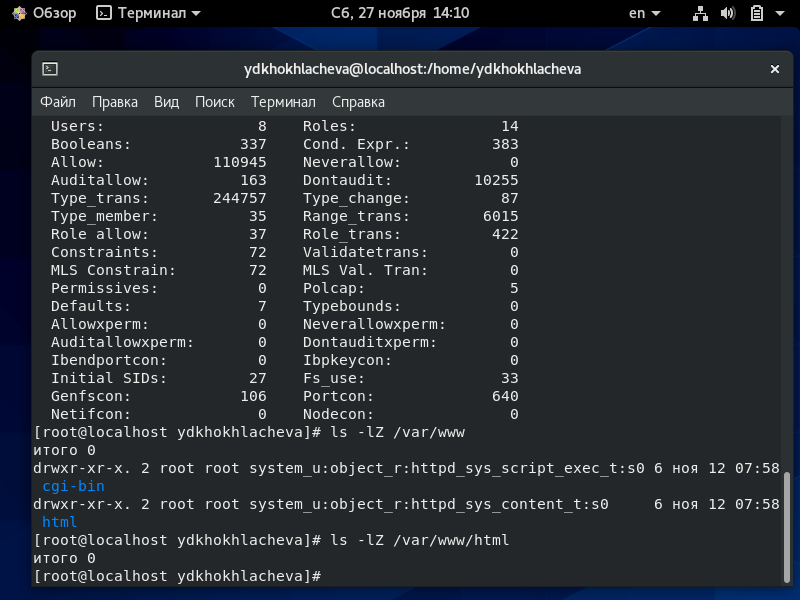
Обратите внимание, что многие из них находятся в положении «off».

1. Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов.



Статистика по политикеSELinux

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

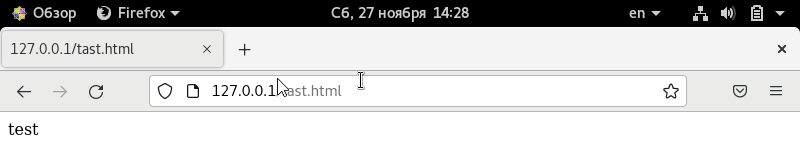


Файлы в директории html

1. Определите круг пользователей, которым разрешено создание файлов в директории **/var/www/html**.
2. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл **/var/www/html/test.html** следующего содержания:

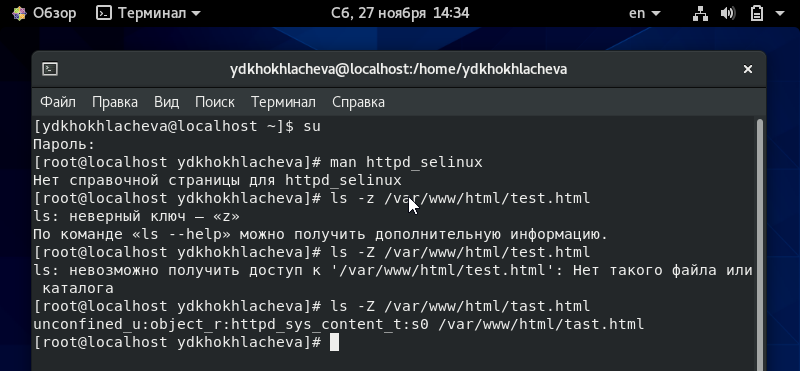
<html>  
<body>test</body>  
</html>

1. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории **/var/www/html**.
2. Обратитесь к файлу через веб-сервер, введя в браузере адрес \*\* http://127.0.0.1/test.html\*\*. Убедитесь, что файл был успешно отображён.



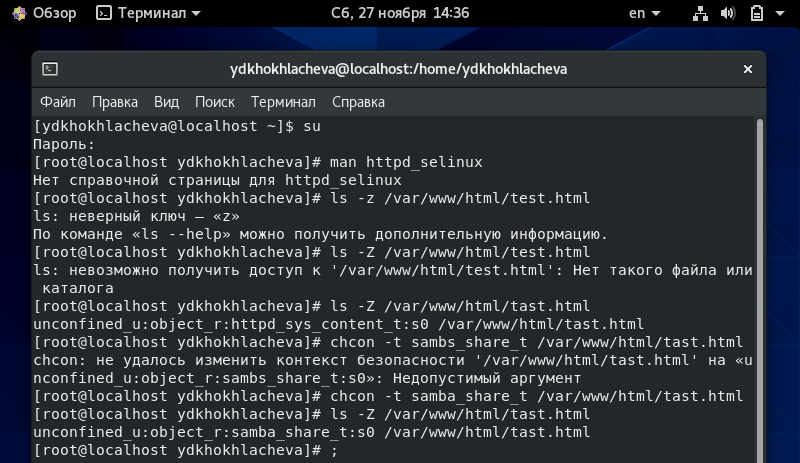
127.0.0.1/test.html

1. Изучите справку **man httpd\_selinux** и выясните, какие контексты файлов определены для **httpd**. Сопоставьте их с типом файла **test.html**. Проверить контекст файла можно командой \*\* ls -Z /var/www/html/test.html **Рассмотрим полученный контекст детально. Обратите внимание, что так как по умолчанию пользователи CentOS являются свободными от типа (unconfined в переводе с англ. означает свободный), созданному нами файлу** test.html\*\* был сопоставлен SELinux, пользователь **unconfined\_u**. Это первая часть контекста. Далее политика ролевого разделения доступа RBAC используется процессами, но не файлами, поэтому роли не имеют никакого значения для файлов. Роль **object\_r** используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. (В директории **/ргос** файлы, относящиеся к процессам, могут иметь роль **system\_r**. Если активна политика MLS, то могут использоваться и другие роли, например, **secadm\_r**. Данный случай мы рассматривать не будем, как и предназначение **:s0**). Тип **httpd\_sys\_content\_t** позволяет процессу **httpd** получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.



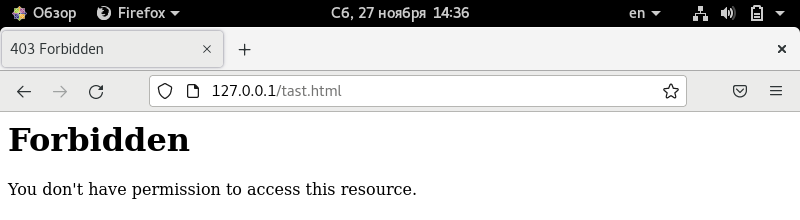
Контекст

1. Измените 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**



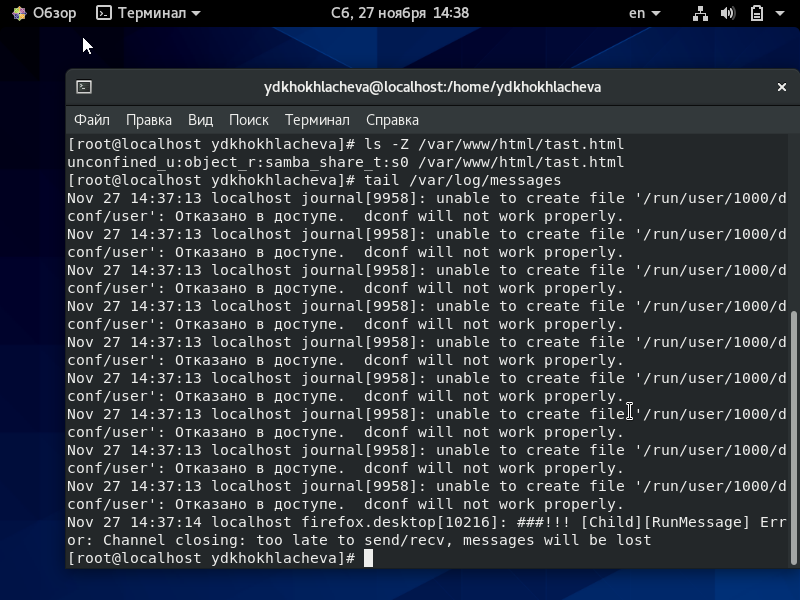
Изменение контекста файла

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.**



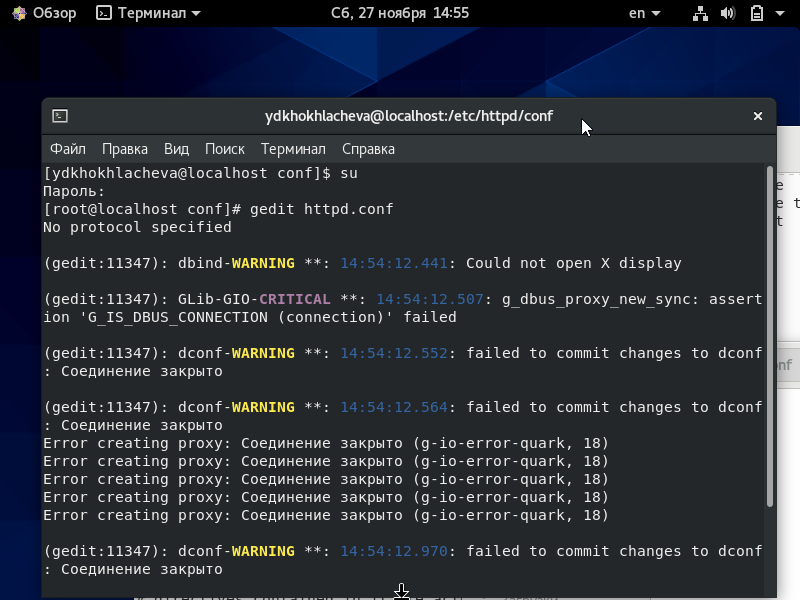
Потерянный доступ

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.



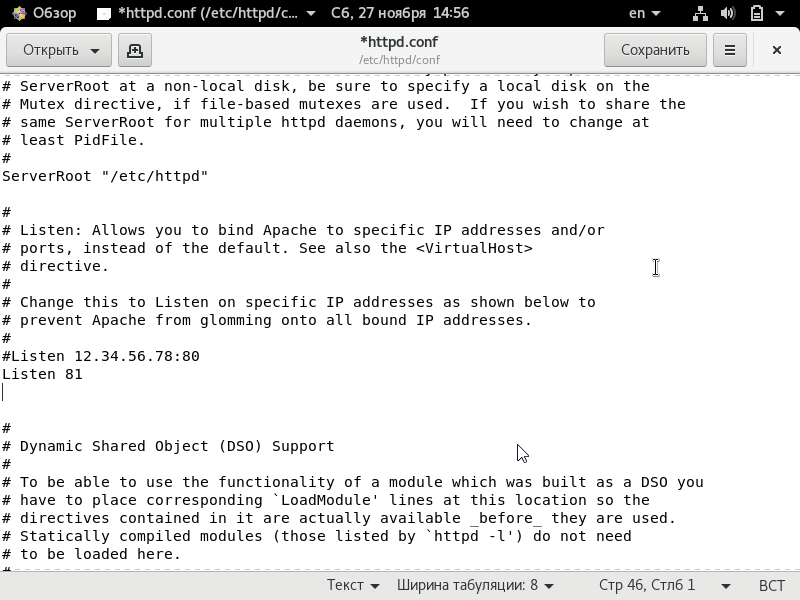
Права пользователей

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** найдите строчку **Listen 80** и замените её на **Listen 81**.



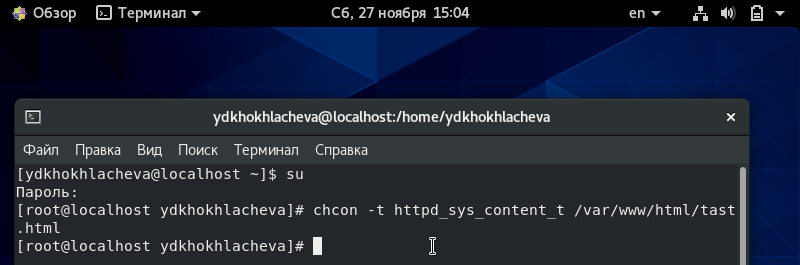
Изменение прослушивания порта

1. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему?
2. Проанализируйте лог-файлы: **tail -nl /var/log/messages** Просмотрите файлы **/var/log/http/error\_log**, **/var/log/http/access\_log** и **/var/log/audit/audit.log** и выясните, в каких файлах появились записи.
3. Выполните команду **semanage port -a -t http\_port\_t -р tcp 81** После этого проверьте список портов командой **semanage port -l | grep http\_port\_t** Убедитесь, что порт 81 появился в списке.



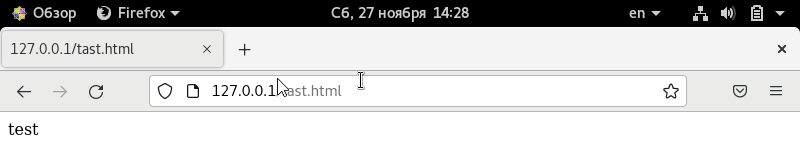
Изменение списка портов

1. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог?
2. Верните контекст \*\*httpd\_sys\_cоntent\_\_t\*\* к файлу **/var/www/html/ test.html**: **chcon -t httpd\_sys\_content\_t /var/www/html/test.html**



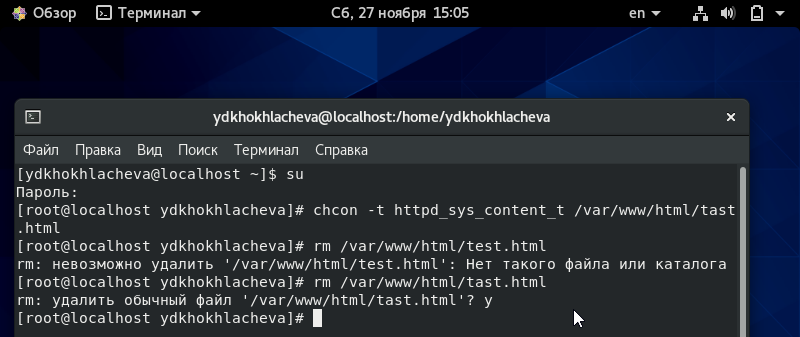
Возвращение контекста

После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес **http://127.0.0.1:81/test.html**. Вы должны увидеть содержимое файла — слово «test».



Повторное обращение к test.html

1. Исправьте обратно конфигурационный файл apache, вернув **Listen 80**.
2. Удалите привязку **http\_port\_t к 81** порту: **semanage port -d -t http\_port\_t -p tcp 81** и проверьте, что порт 81 удалён.
3. Удалите файл **/var/www/html/test.html**: **rm /var/www/html/test.html**



Удаление файла 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.