Отчет по лаборатной работе №6

по предмету Информационная безопасность

Алхимова Дарья Сергеевна

Содержание

[Цель работы 1](#__RefHeading___Toc2810_1588871184)

[Задание 1](#__RefHeading___Toc2812_1588871184)

[Теоретическое введение 3](#__RefHeading___Toc2814_1588871184)

[Выполнение лабораторной работы 3](#__RefHeading___Toc2816_1588871184)

[Выводы 14](#__RefHeading___Toc2818_1588871184)

[Список литературы 15](#__RefHeading___Toc2820_1588871184)

# Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache.

# Задание

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus.
2. 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.
3. 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 или ps -eZ | grep httpd.
4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды sestatus -bigrep httpd. Обратите внимание, что многие из них находятся в положении «off».
5. Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов.
6. Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www.
7. Определите тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html.
8. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html.
9. 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>
10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.
11. Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён.
12. 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 (ls -Z /var/www/html/test.html)
13. 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. После этого проверьте, что контекст поменялся.
14. 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.
15. 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.
16. 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.
17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему?
18. 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.
19. 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.
20. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог?
21. Верните 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 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».
22. Исправьте обратно конфигурационный файл apache, вернув Listen80.
23. Удалите привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81 и проверьте, что порт 81 удалён.
24. Удалитефайл/var/www/html/test.html: rm /var/www/html/test.html

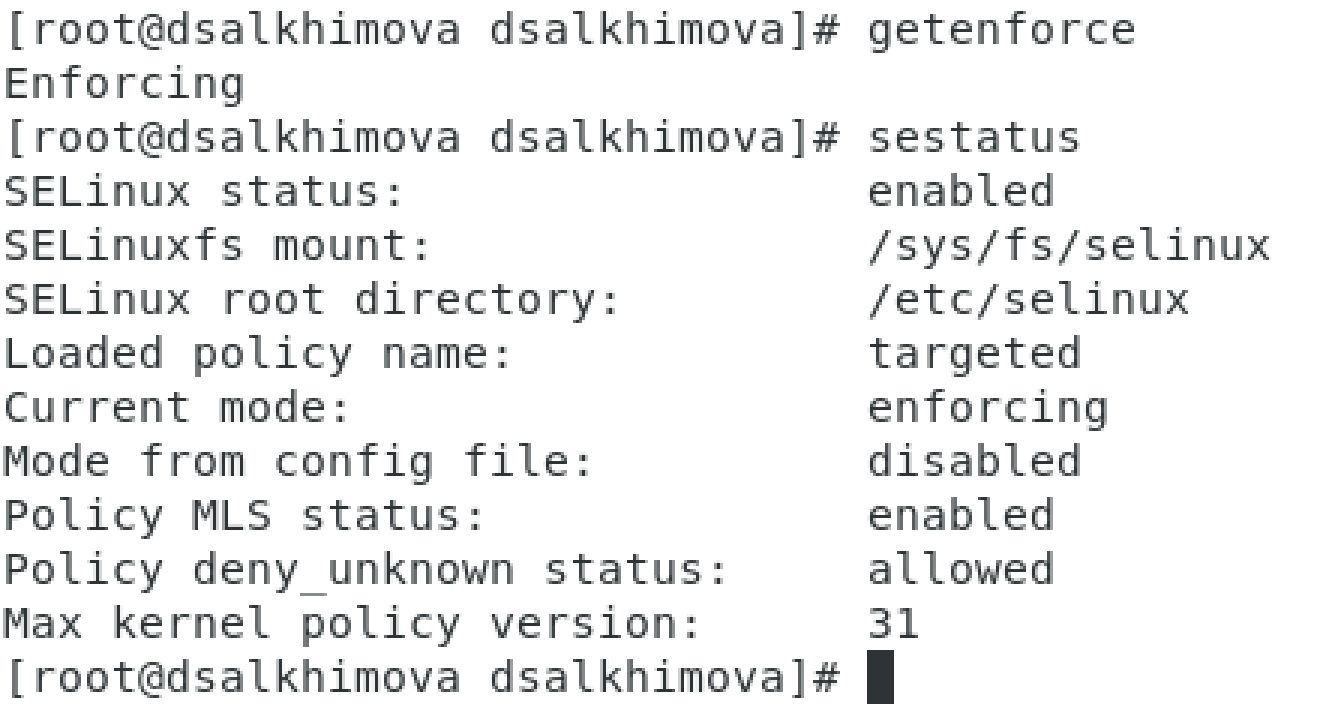
# Теоретическое введение

Так как по умолчанию пользователи CentOS являются свободными от типа (unconfined в переводе с англ. означает свободный), созданным фвйлам по умолчанию сопоставляется SELinux, пользователь unconfined\_u. Это первая часть контекста.

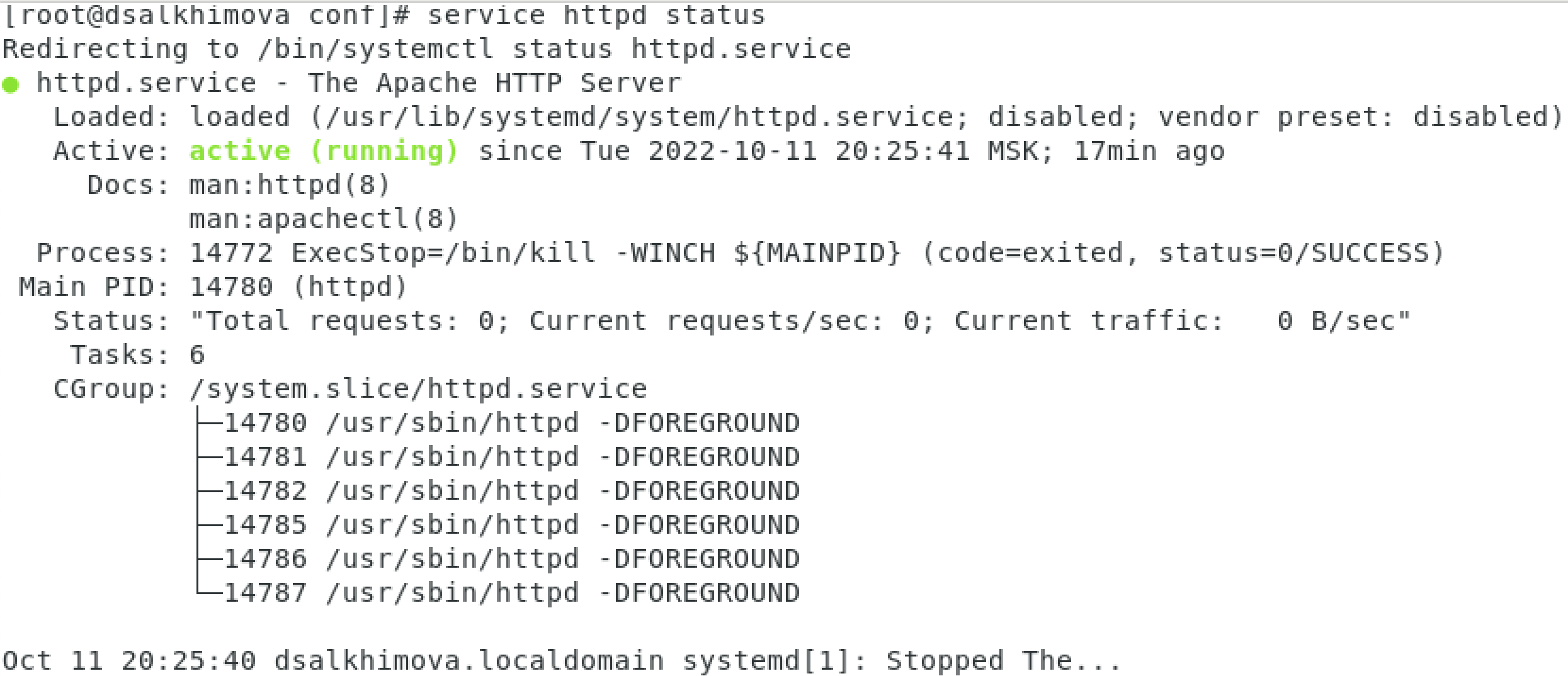
Далее политика ролевого разделения доступа RBAC используется процессами, но не файлами, поэтому роли не имеют никакого значения для файлов. Роль object\_r используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. (В директории /ргос файлы, относящиеся к процессам, могут иметь роль system\_r. Если активна политика MLS, то могут использоваться и другие роли, например, secadm\_r. Тип httpd\_sys\_content\_t позволяет процессу httpd получить доступ к файлу. Благодаря наличию последнего типа можно получить доступ к файлу при обращении к нему через браузер.

# Выполнение лабораторной работы

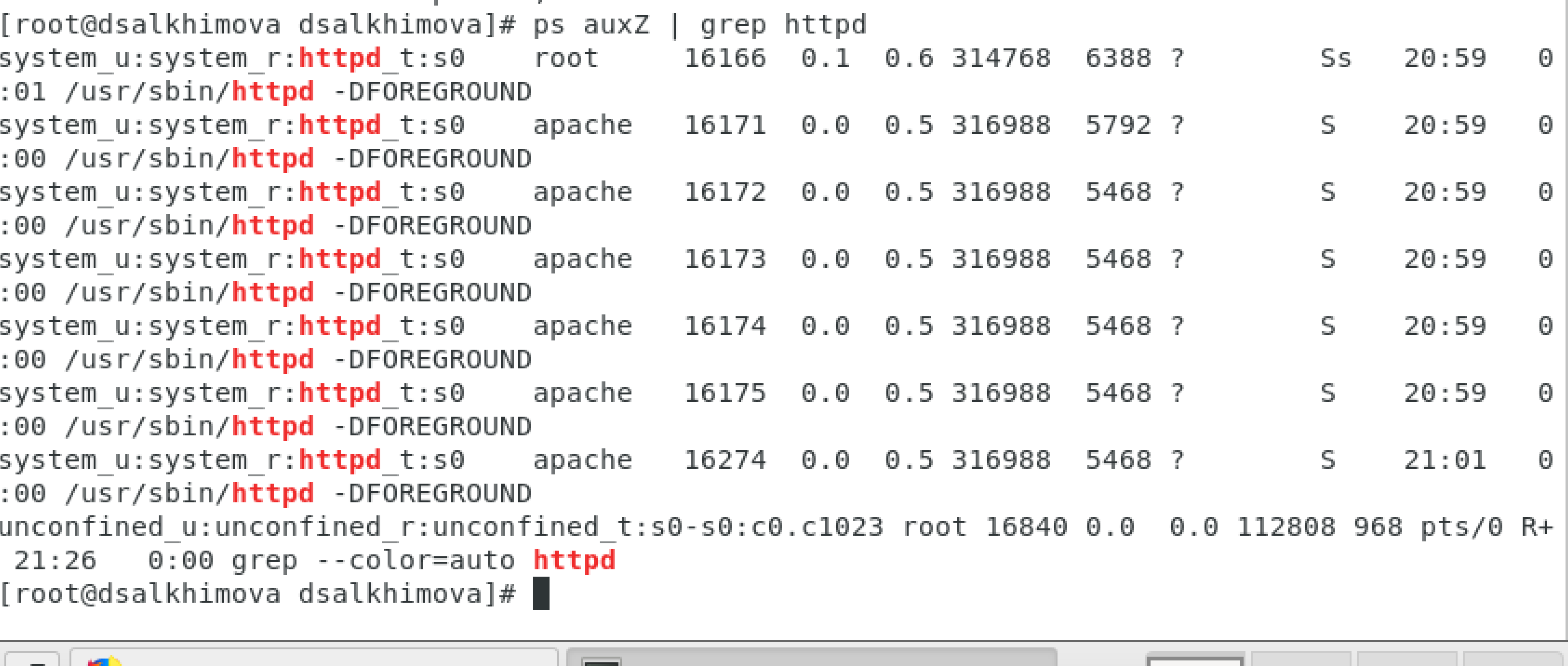
1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus ([рис. 1](images6/1.png)).

* 
* Проверка работы SELinux

1. Обратилась с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедилась, что последний работает: service httpd status или /etc/rc.d/init.d/httpd status ([рис. 2](images6/2.png)).

* 
* Проверка работы веб-сервера

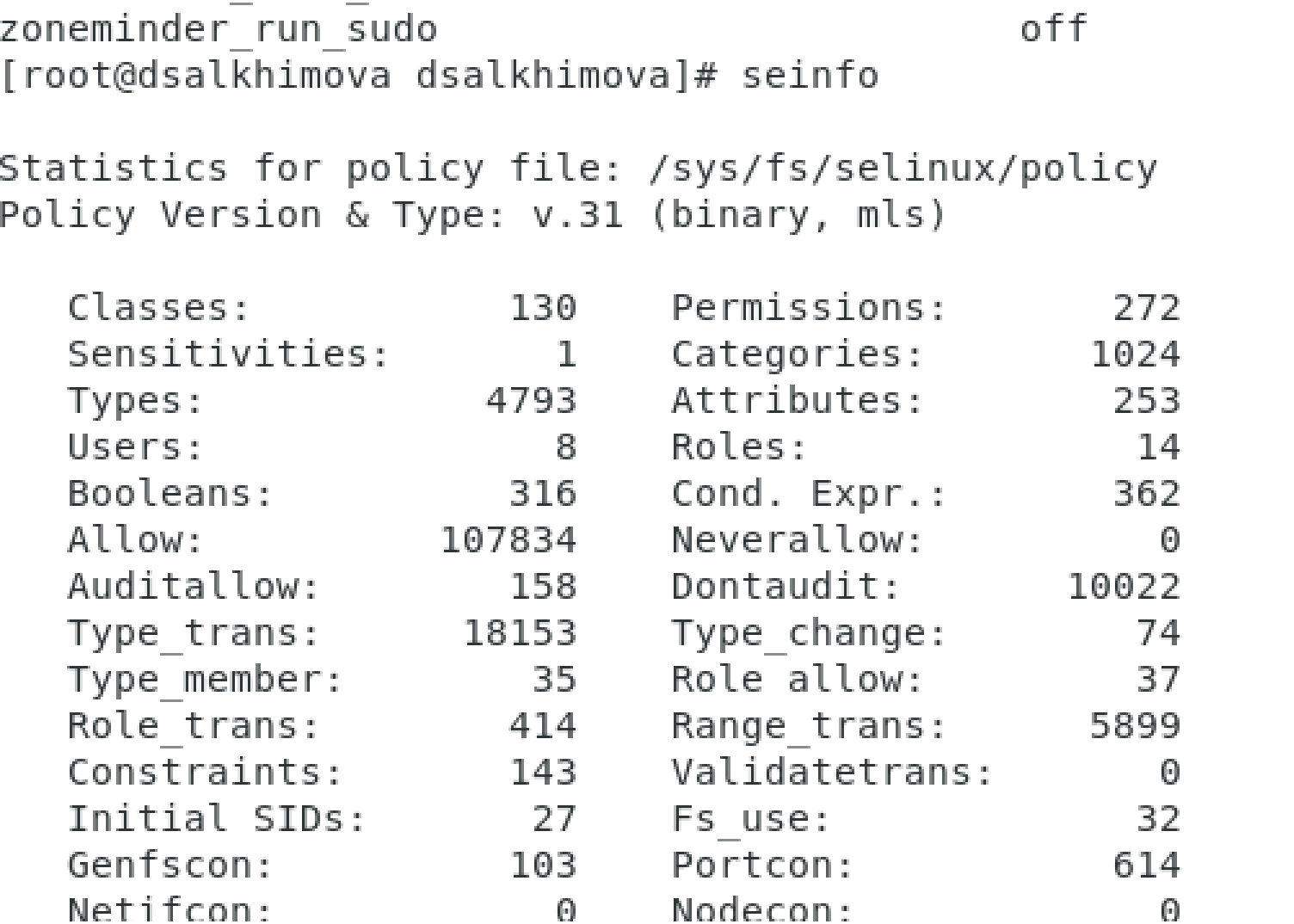
1. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности (unconfined\_t). Использовала команду ps auxZ | grep httpd ([рис. 3](images6/3.png)).

* 
* Контекст Apache

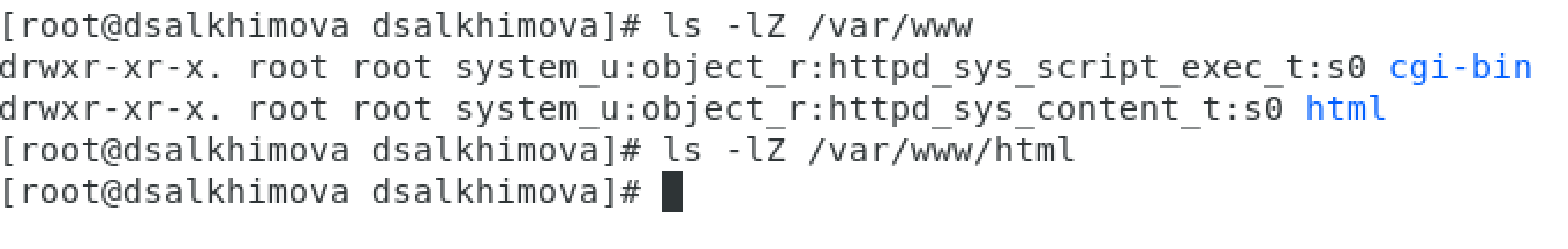
1. Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды sestatus -bigrep httpd ([рис. 4](images6/4.png)).

* 
* Состояние переключателей SELinux для Apache

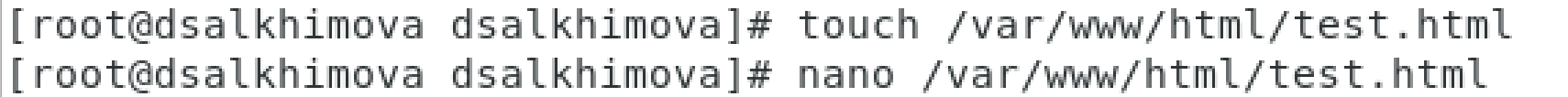
1. Посмотрела статистику по политике с помощью команды seinfo, также определила множество пользователей, ролей, типов ([рис. 5](images6/5.png)).

* 
* Статистика по политике

1. Определила тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www ([рис. 6](images6/6.png)).
2. Определила тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html ([рис. 6](images6/6.png)) - нет файлов и поддиректорий в данной директории.
3. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html ([рис. 6](images6/6.png)) - только владельцу.

* 
* Типы файлов, поддиректорий и права для /www и /html

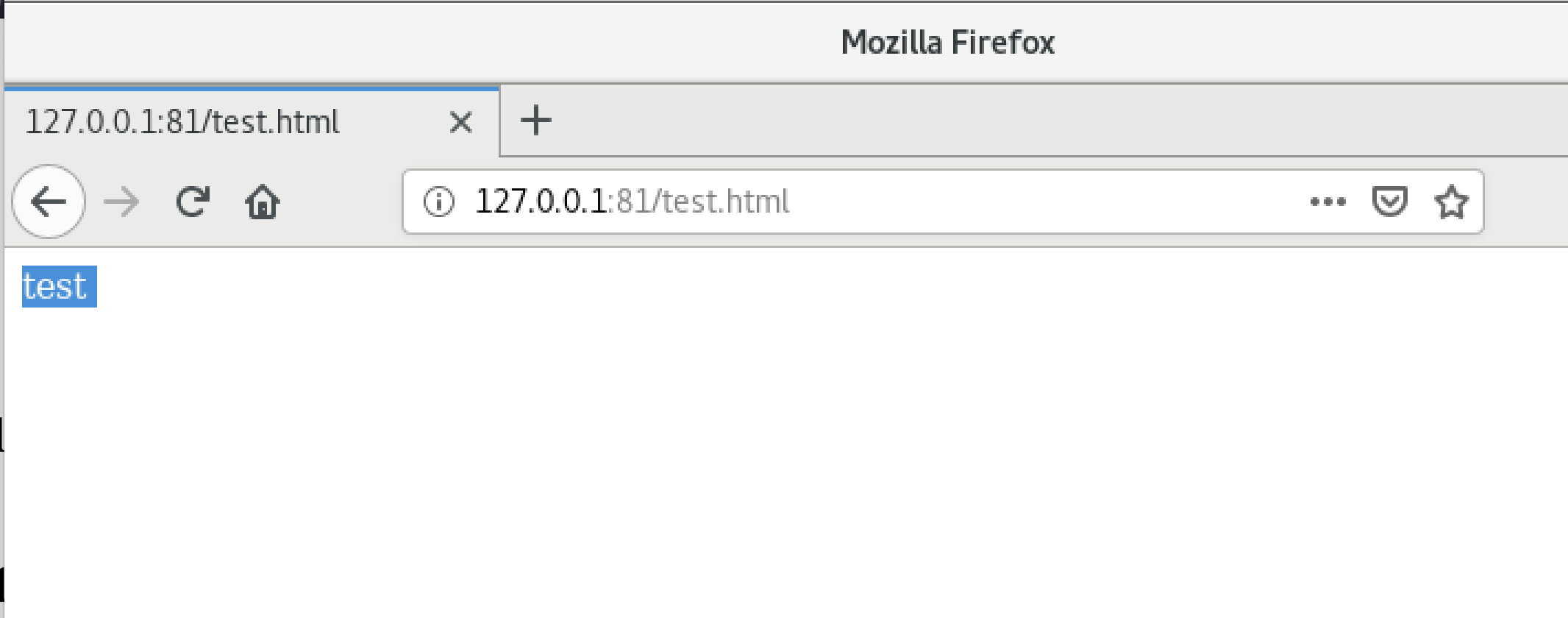
1. Создала от имени суперпользователя html-файл /var/www/html/test.html следующего содержания:  
   <html>  
   <body>test</body>  
   </html> ([рис. 7](images6/7.png))

* 
* Создание файла test.html

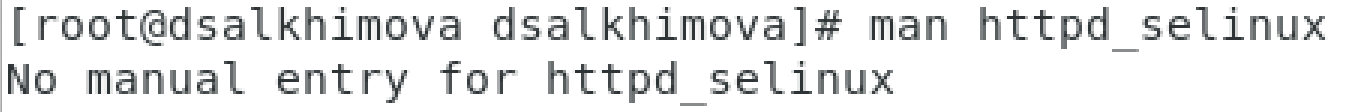
1. Проверила контекст созданного файла командой ls -Z /var/www/html/test.html. Контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html - httpd\_sys\_content\_t ([рис. 8](images6/8.png)).

* 
* Контекст файла test.html

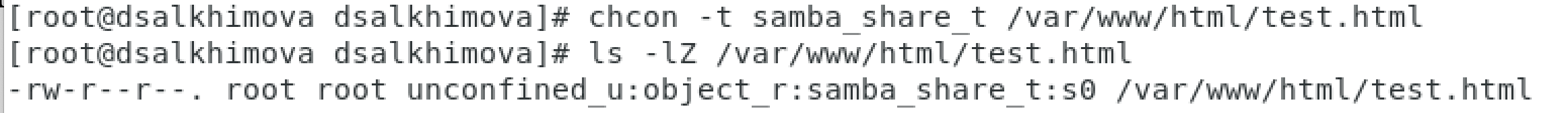
1. Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедилась, что файл был успешно отображён ([рис. 9](images6/9.png)).

* 
* Открытие test.html через браузер

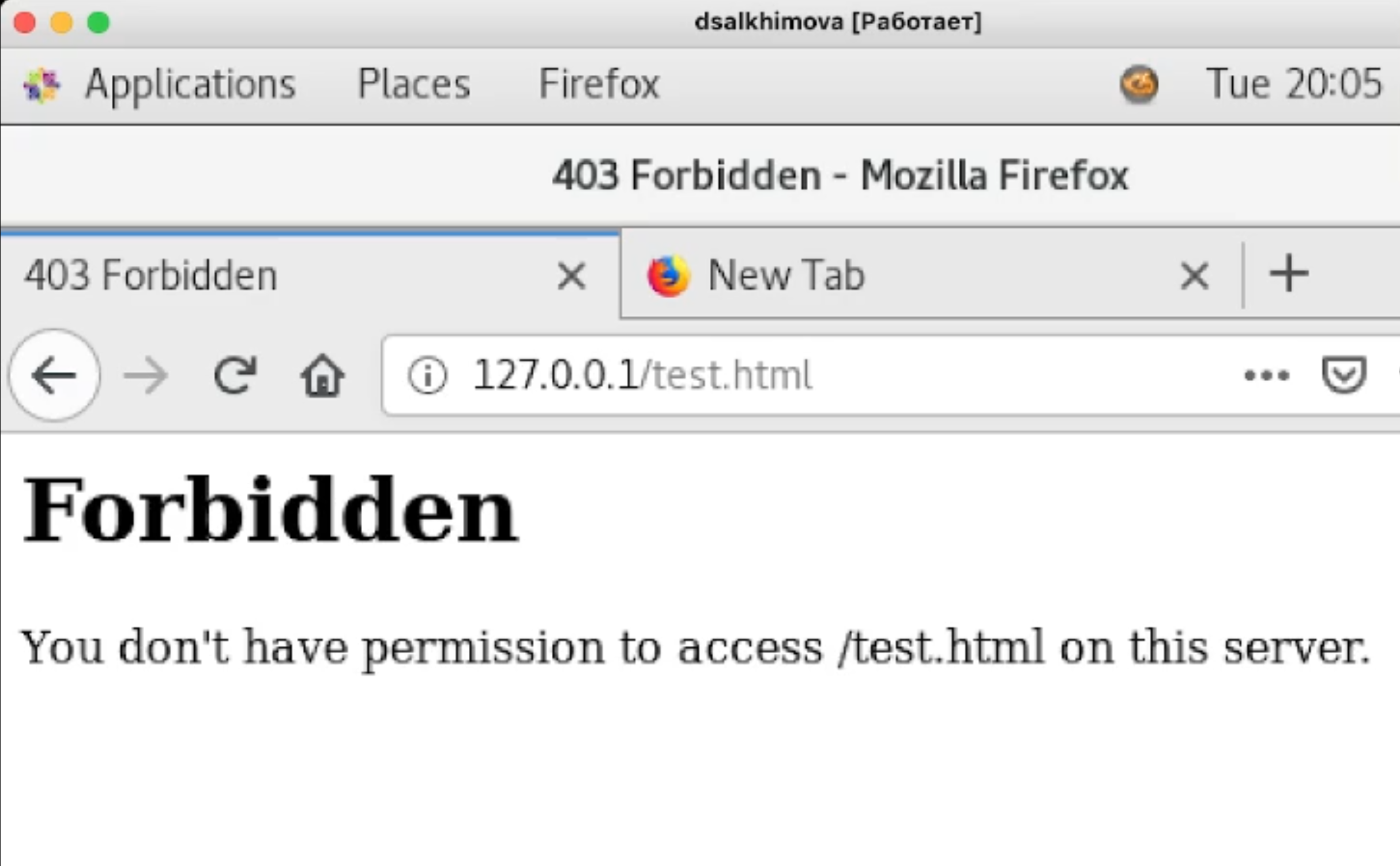
1. Справку по команде man httpd\_selinux не удалось получить, поэтому я изучила, какие контексты файлов определены для httpd с помощью интернета ([рис. 10](images6/10.png)).

* 
* Вызов справки httpd

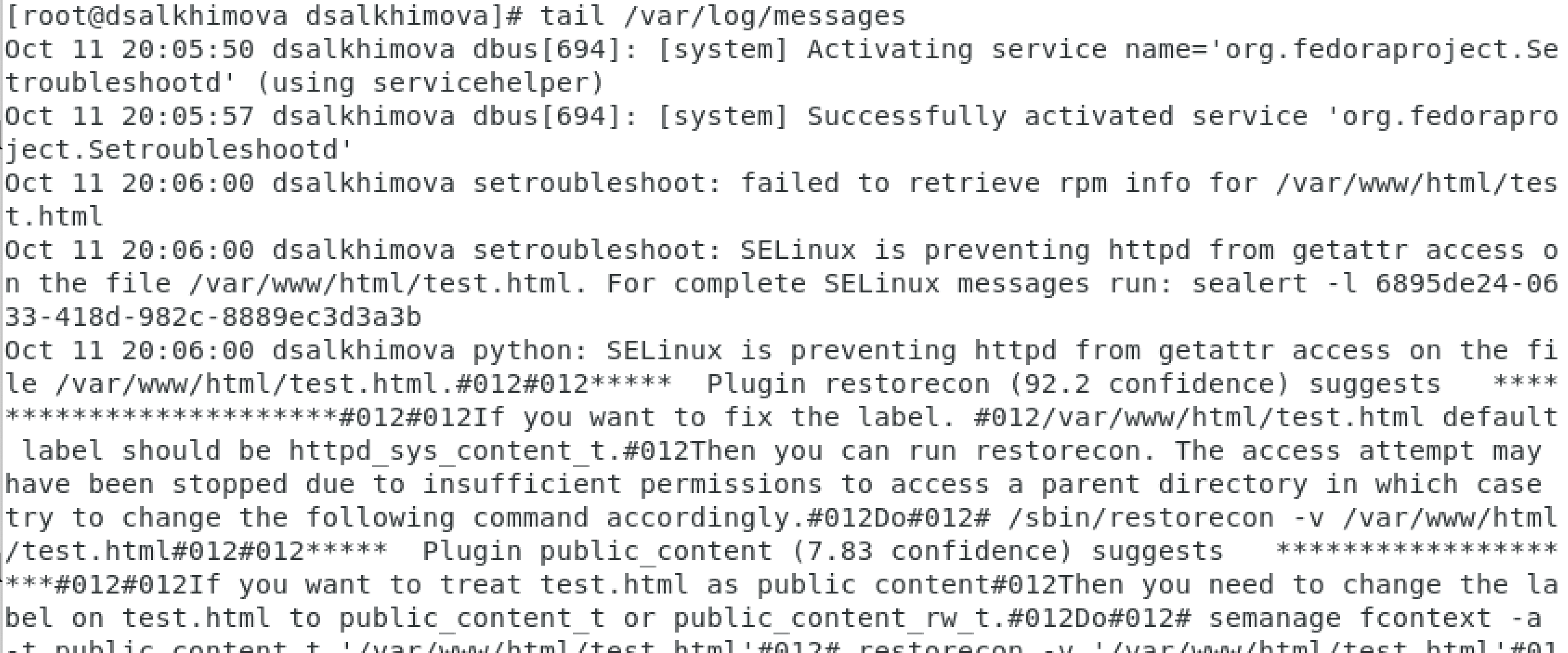
1. Изменила контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t:  
   chcon -t samba\_share\_t /var/www/html/test.html  
   ls -Z /var/www/html/test.html. После этого проверила, что контекст поменялся ([рис. 11](images6/11.png)).

* 
* Смена контекста файла test.html

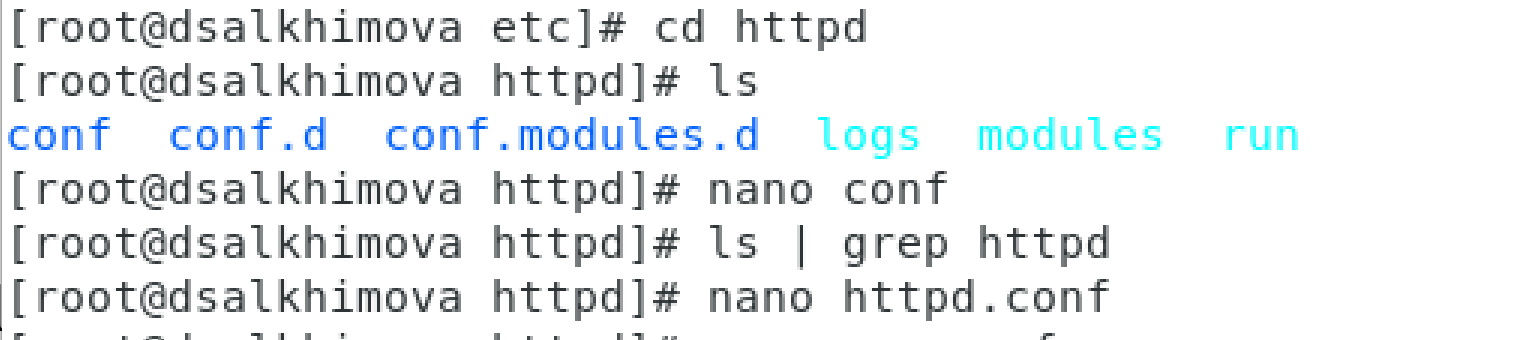
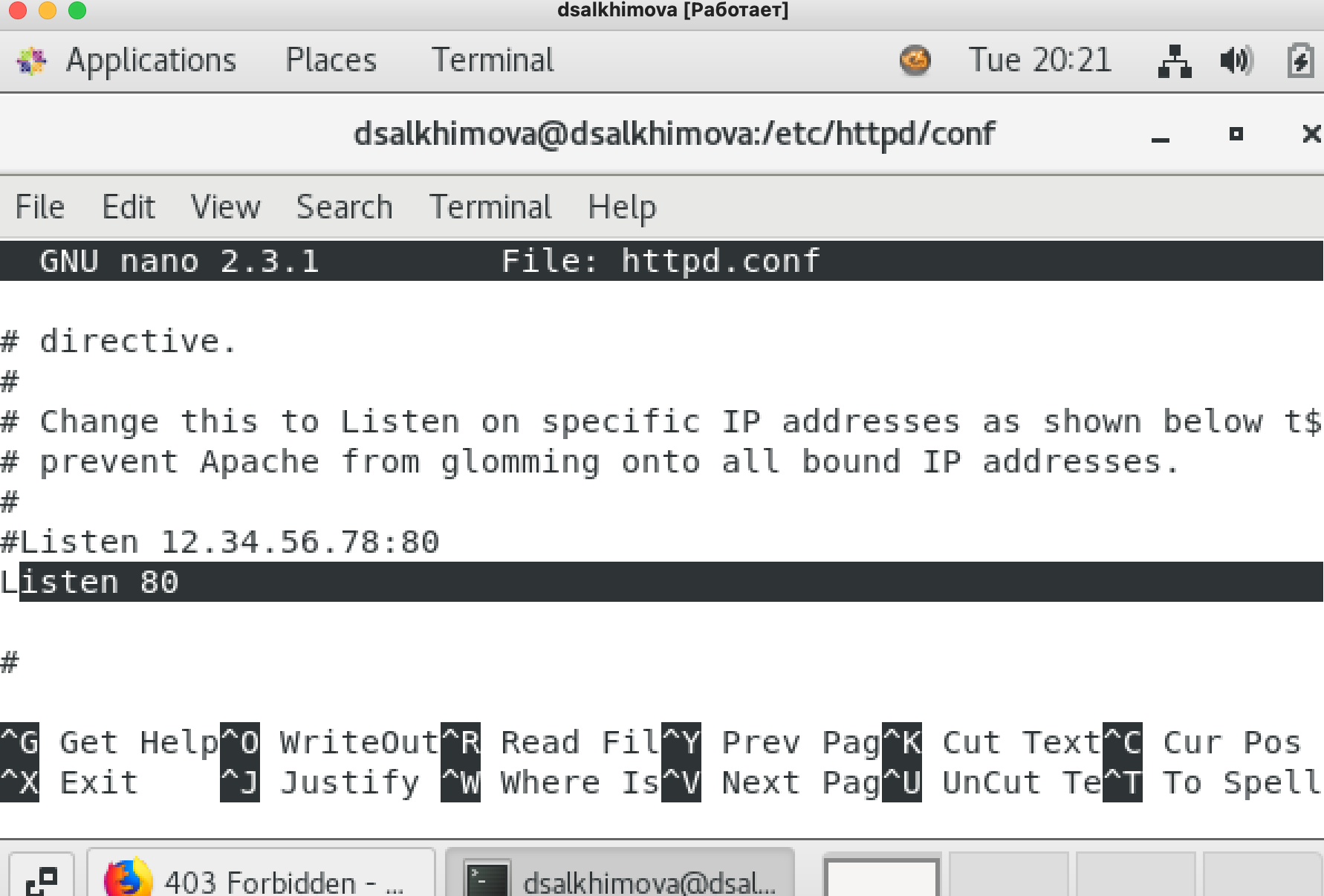
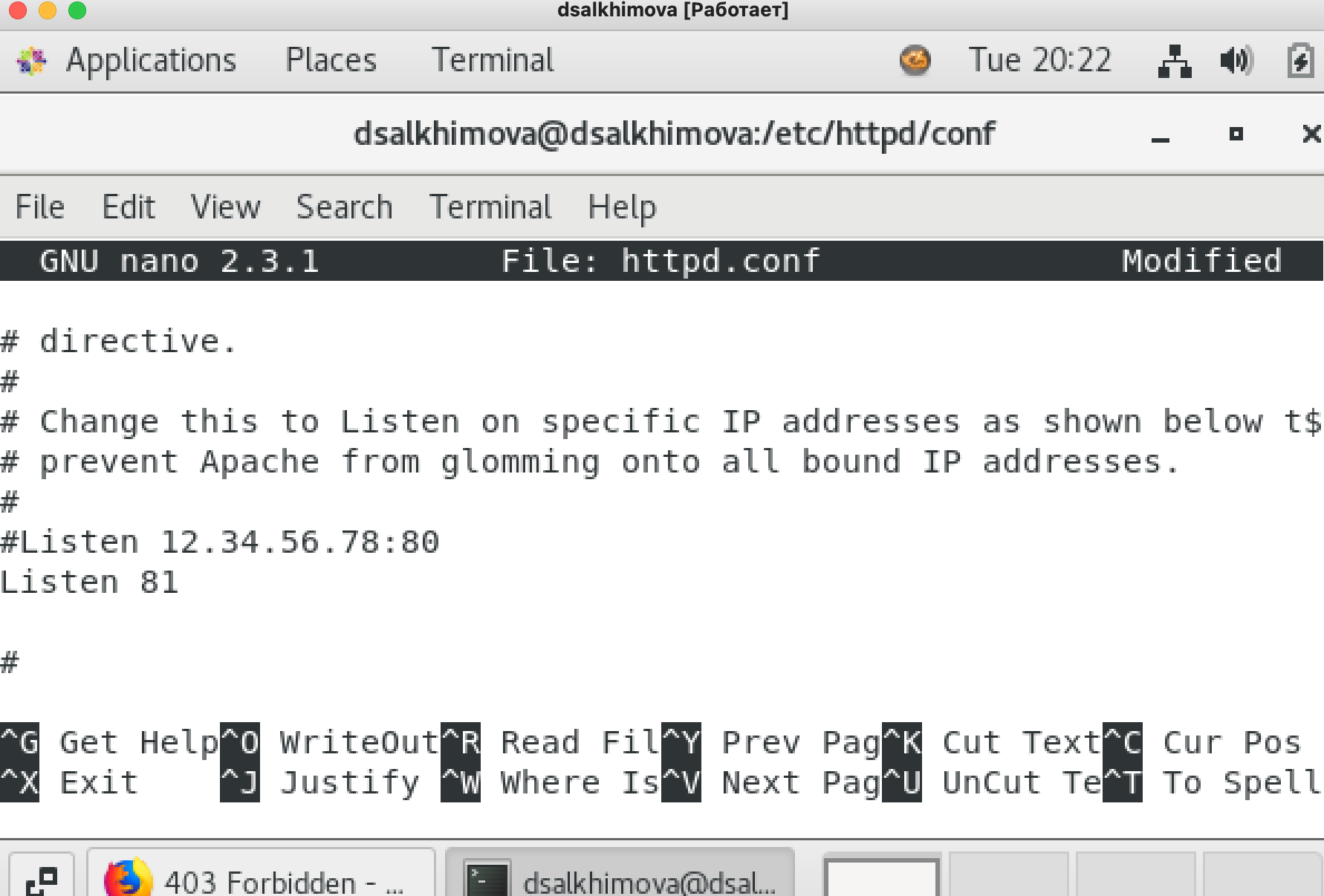
1. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Получила сообщение об ошибке ([рис. 12](images6/12.png)).

* 
* Повторное открытие test.html через браузер

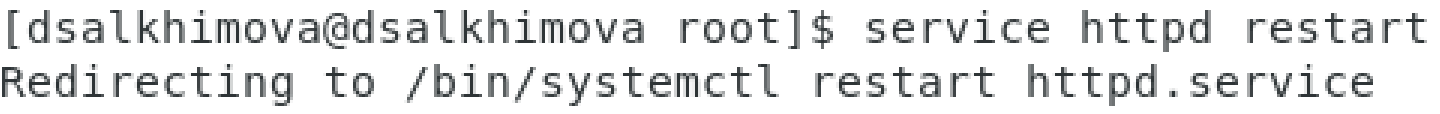
1. Файл не был отображён, т.к. политика ролевого разделения доступа RBAC используется процессами, но не файлами, поэтому роли не имеют никакого значения для файлов. Тип httpd\_sys\_content\_t позволял процессу httpd получить доступ к файлу, а тип samba\_share\_t - нет. Просмотрела системный лог-файл: tail /var/log/messages ([рис. 13](images6/13.png)).

* 
* Просмотр системного лога
* В системе были запущенными процессы setroubleshootd и audtd. Посмотрела ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log.

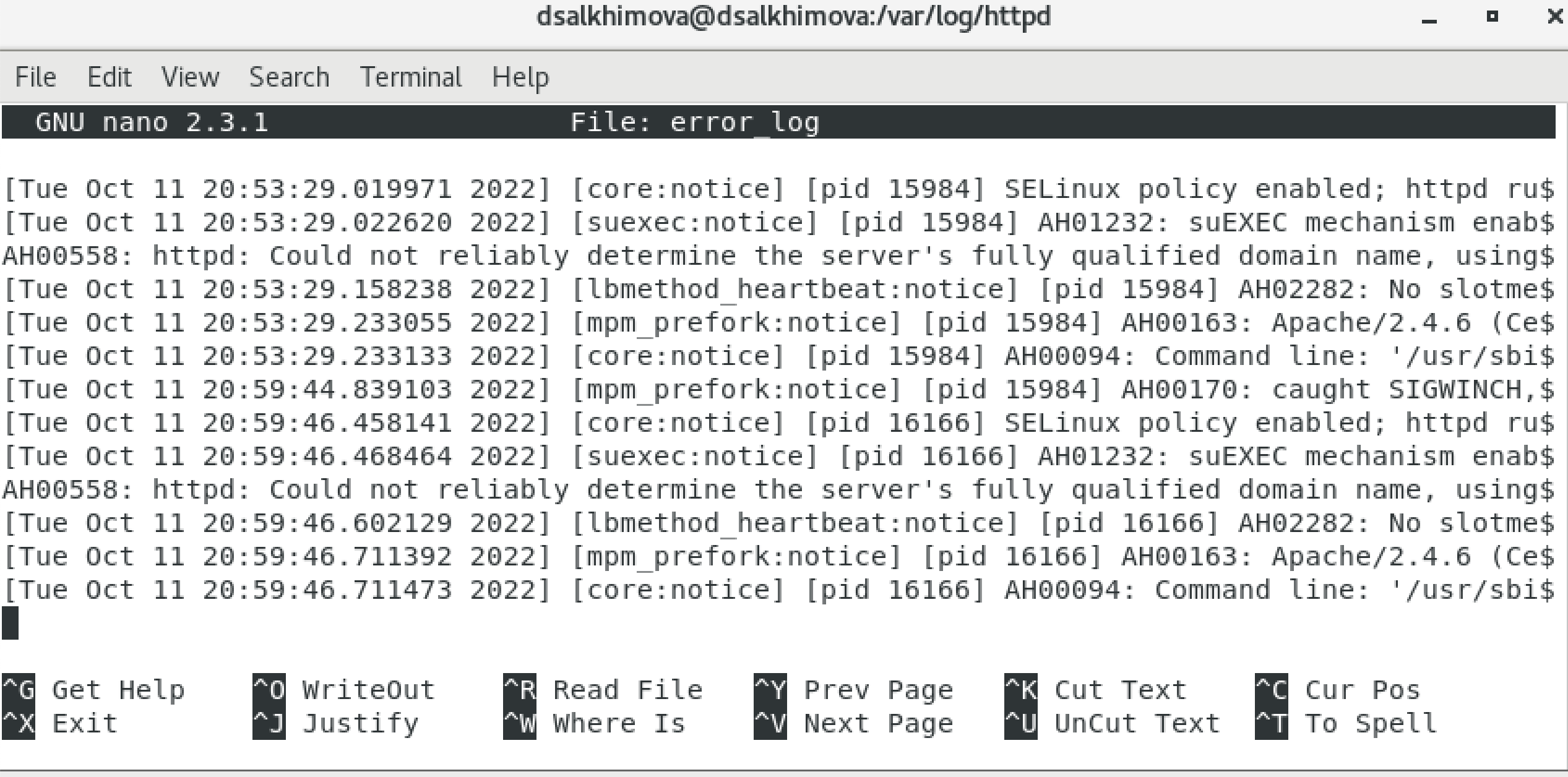
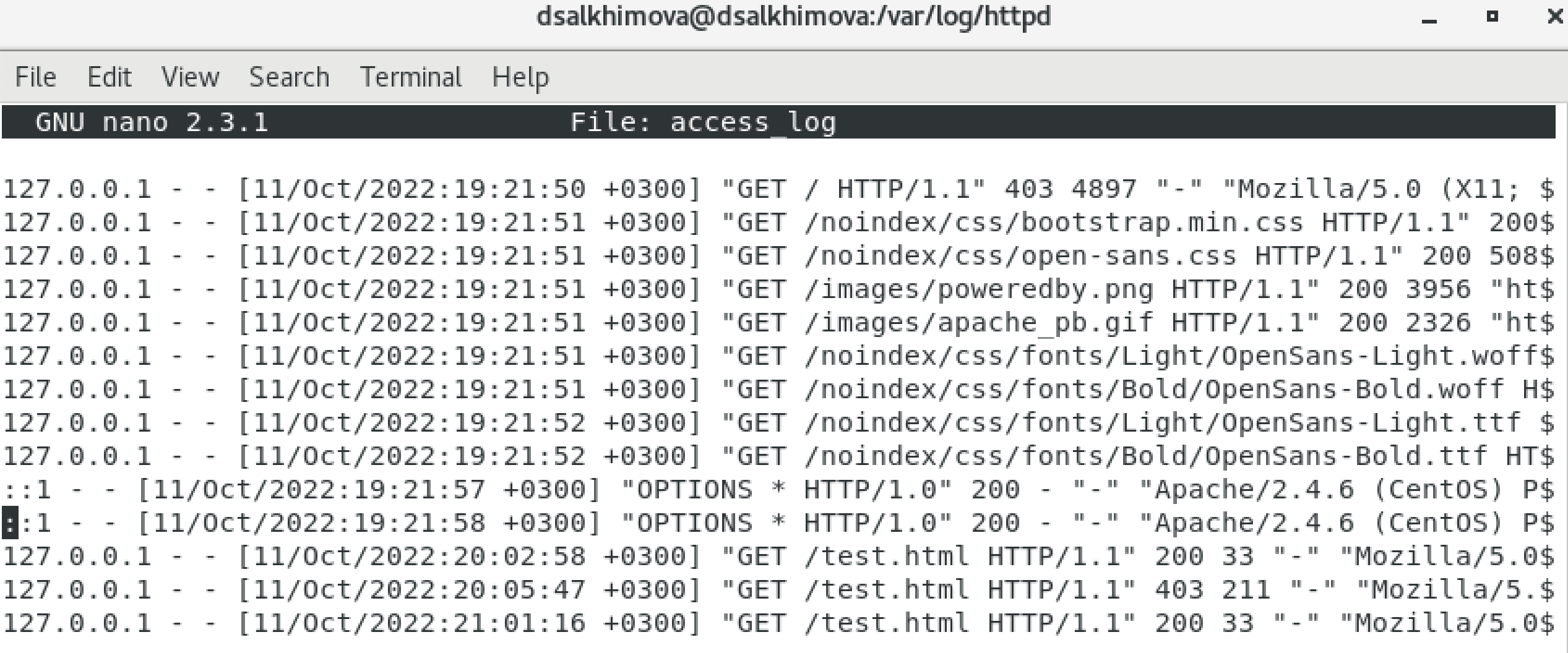
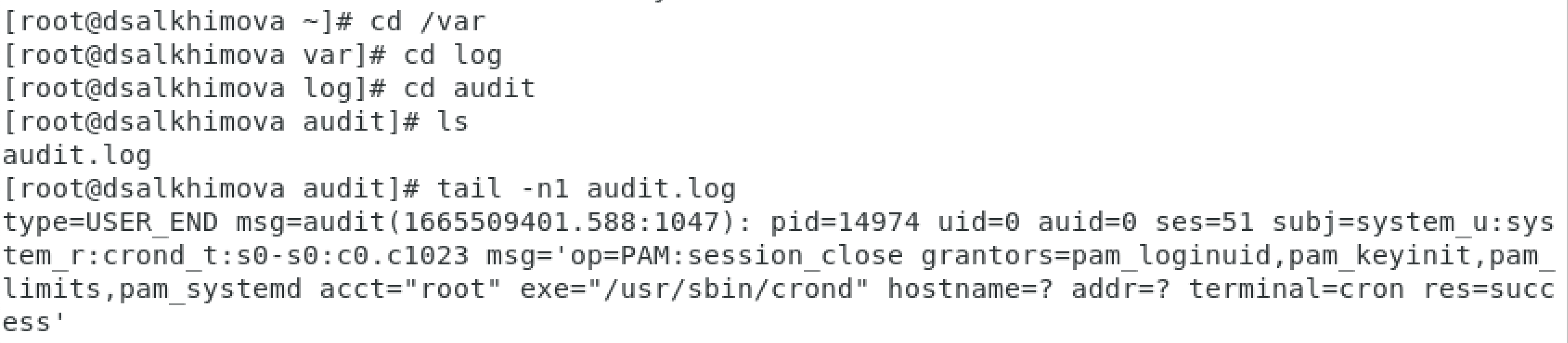
1. Попробовала запустить веб-сервер Apache на прослушивание ТСР-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf нашла строчку Listen 80 и заменила её на Listen 81 ([рис. 14](images6/14.png), [рис. 15](images6/15.png), [рис. 16](images6/16.png)).

* 
* Открытие httpd.conf
* 
* httpd.conf до исправления
* 
* httpd.conf после исправления

1. Выполнила перезапуск веб-сервера Apache ([рис. 17](images6/17.png)).

* 
* Перезапуск Apache

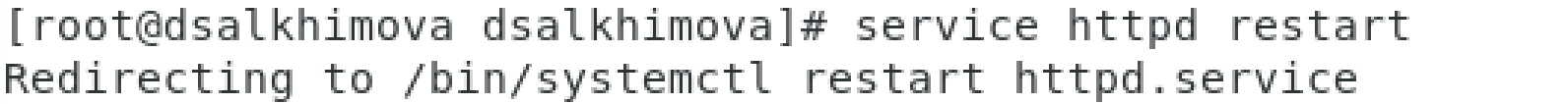
1. Проанализировала лог-файлы: tail -nl /var/log/messages ([рис. 18](images6/18.png)).

* 
* Просмотр логов
* Просмотрела файлы /var/log/http/error\_log ([рис. 20](images6/20.png)), /var/log/http/access\_log ([рис. 19](images6/19.png)) и /var/log/audit/audit.log. Записи появились в error\_log и access\_log ([рис. 21](images6/21.png)).
* 
* Просмотр access\_log
* 
* Просмотр error\_log
* 
* Просмотр audit.log

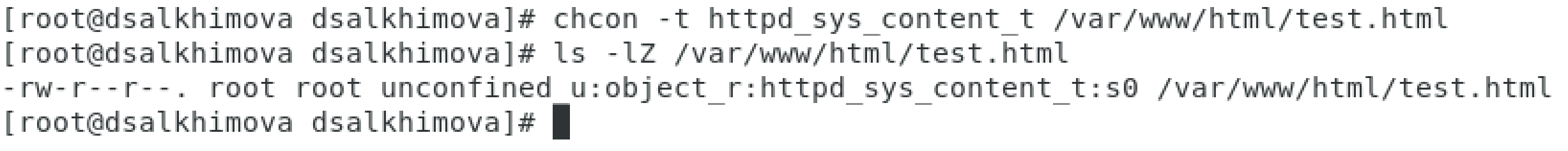
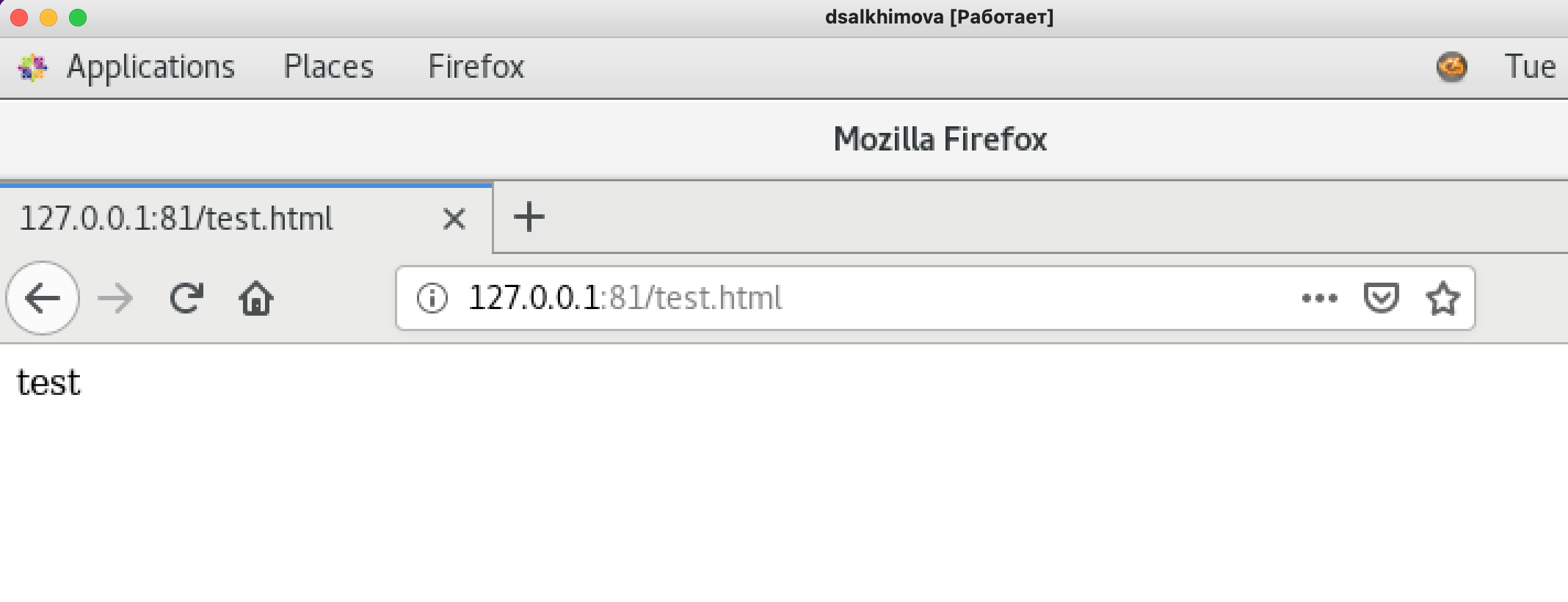
1. Выполнила команду semanage port -a -t http\_port\_t -р tcp 81 и проверила список портов командой semanage port -l | grep http\_port\_t ([рис. 22](images6/22.png)). Порт 81 присутствует в списке.

* 
* Добавление и просмотр наличия 81 порта

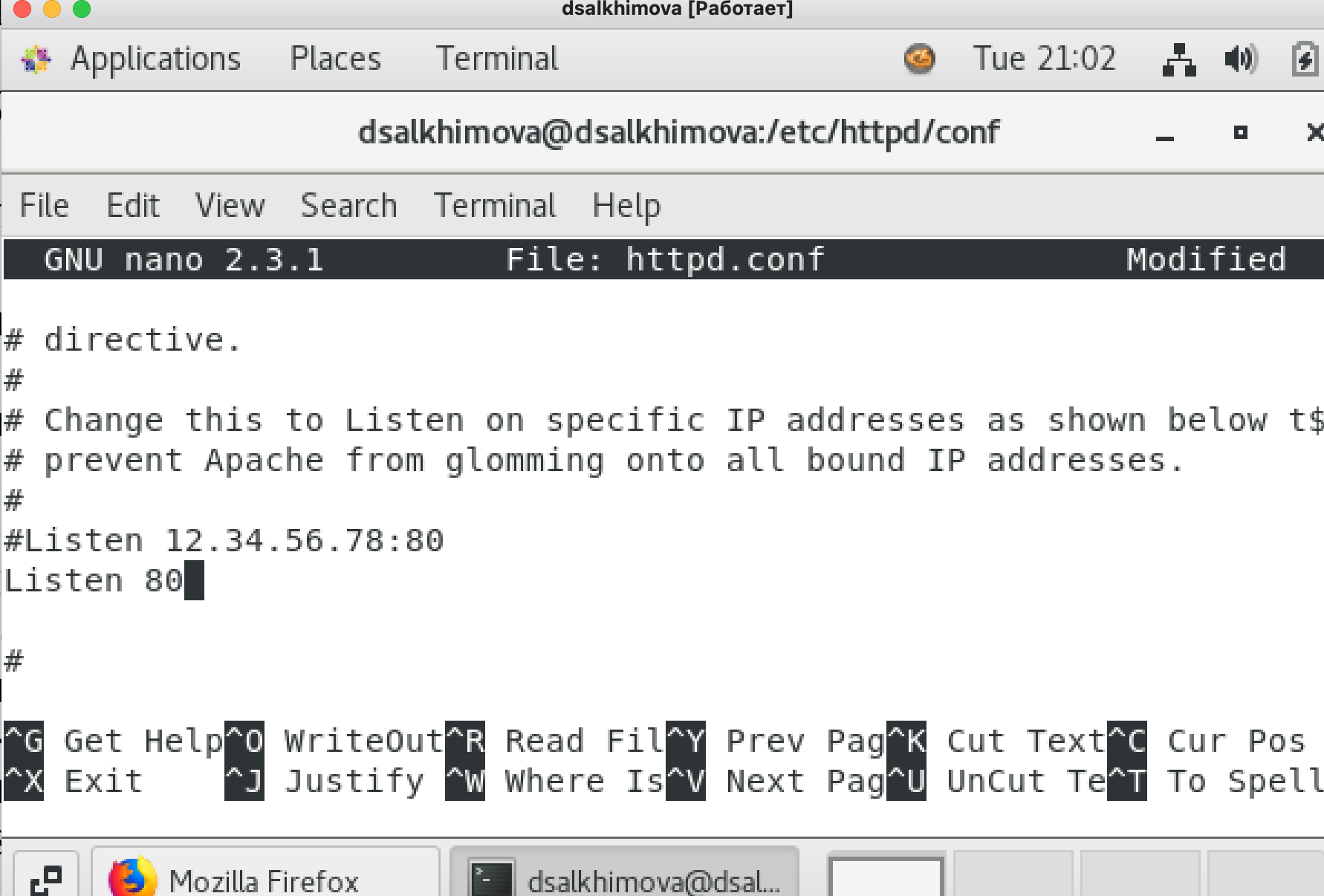
1. Попробовала запустить веб-сервер Apache ещё раз ([рис. 23](images6/23.png)). Запуск прошел успешно.

* 
* Запуск Apache

1. Вернула контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/test.html: chcon -t httpd\_sys\_content\_t /var/www/html/test.html ([рис. 24](images6/24.png)).

* 
* Возвращение контекста файлу test.html
* После этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Открылось содержимое файла — слово «test» ([рис. 25](images6/25.png)).
* 
* Открытие файла test.html через браузер

1. Исправила обратно конфигурационный файл apache, вернув Listen80 ([рис. 26](images6/26.png)).

* 
* Возвращение настроек на 80 порт httpd.conf

1. Пропробовала удалить привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81 - операция запрещена ([рис. 27](images6/27.png)). Порт 81 остался в списке.

* 
* Попытка удаления 81 порта

1. Удалила файл /var/www/html/test.html: rm /var/www/html/test.html ([рис. 28](images6/28.png)).

* 
* Удаление файла test.html

# Выводы

В процессе выполнения данной лабораторной работы я приобрела навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux и проверила работу SELinx на практике совместно с веб-сервером Apache.

# Список литературы

1. Описание лабораторной работы 6 - URL: <https://esystem.rudn.ru/pluginfile.php/1652173/mod_resource/content/2/006-lab_selinux.pdf>
2. Активация Apache - URL: <https://stackoverflow.com/questions/51108495/fresh-install-httpd-service-unit-not-found>