

Лабораторная работа №6

Мандатное разграничение прав в Linux

Кекишева Анастасия Дмитриевна

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	8
5	Выводы	22
	Список литературы	23

Список иллюстраций

4.1	Задание параметра	8
4.2	Отключение пакетного фильтра и вход в систему	9
4.3	Проверка статуса веб-сервера	9
4.4	Список процессов	10
4.5	Состояния переключателей	11
4.6	Статистика - команда seinfo	12
4.7	Определение типов файлов	12
4.8	Файл test.html	13
4.9	Отображение содержимого файла в браузере	13
4.10	Команда man httpd_selinux - контексты для httpd	14
4.11	Команда chcon	15
4.12	Отказ в доступе - сообщение об ошибке от браузера	15
4.13	Просмотр системных лог-файлов	15
4.14	Изменение Listen 80 на Listen 81	16
4.15	Перезапуск Apache	17
4.16	Содержимое файла - /var/log/audit/audit.log	18
4.17	Список портов	18
4.18	перезапуск и изменение контекста	19
4.19	Просмотр содержимого файла через браузер	19
4.20	Исправление конфигурационный файл	20
4.21	Удаление привязки к порту 81 и удаление файла	21

Список таблиц

1 Цель работы

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

2 Задание

Описание задания и рекомендованная последовательность выполнения работы, описана [1]

3 Теоретическое введение

Apache - популярный бесплатный opensource веб-сервер. Он является частью стека LAMP (Linux, Apache, MySQL, PHP), который обеспечивает большую часть Интернета [2]. Логи Apache расположены тут: - /var/log/httpd/ - расположение файлов логов Apache - /var/log/httpd/access_log - показывает журнал систем, которые обращались к серверу - /var/log/httpd/error_log - показывает список любых ошибок, с которыми сталкивается Apache

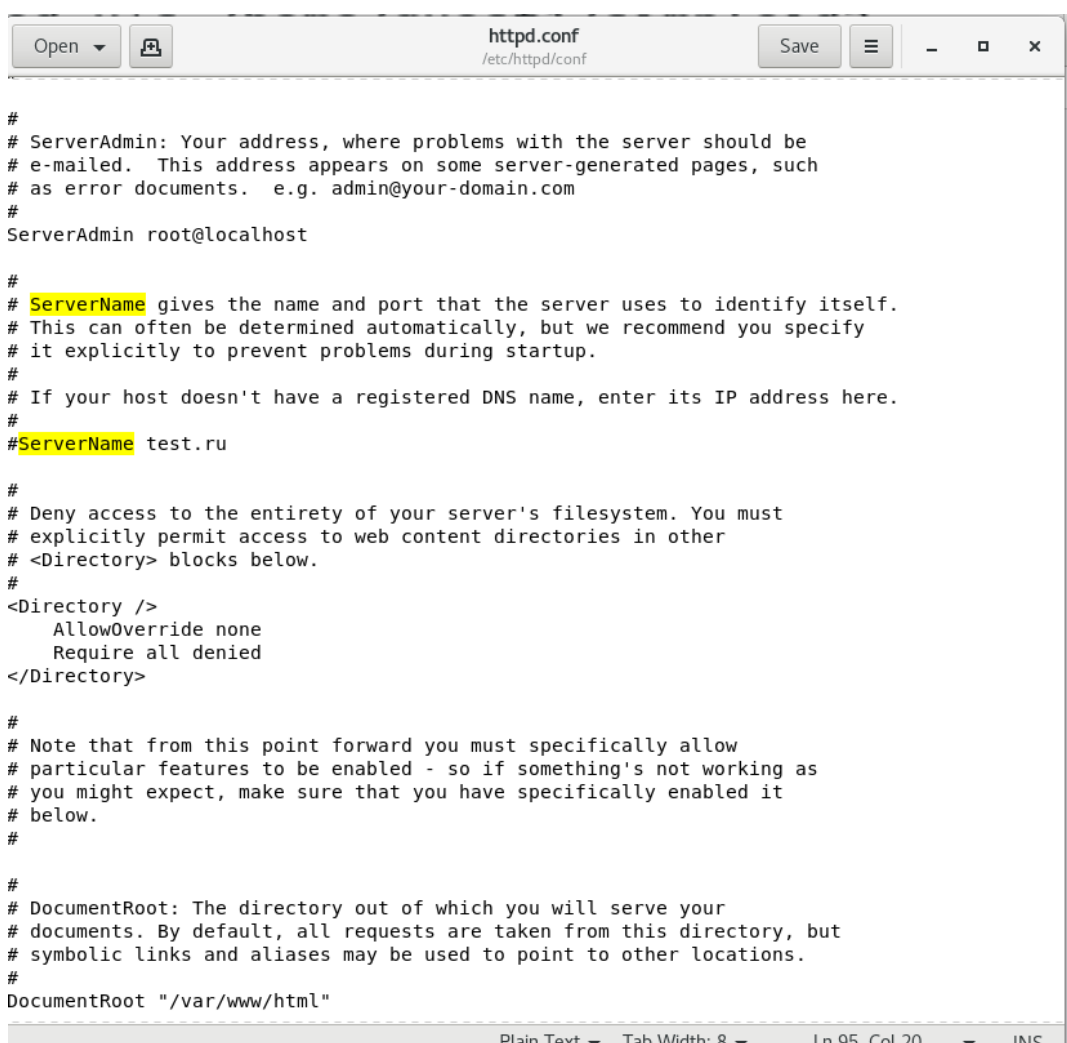
Контекст безопасности это набор всех атрибутов, связанных с объектами и па файлов, каталогов, процессов, TCP сокетов и т.п. Контекст безопасности состоит из сущности, роли и домена или типа. У процессов есть домен. Когда вы смотрите контекст безопасности процесса последнее поле – это домен, например *user_passwd_t*.

Команда `chcon` позволяет изменить контекст, но он не работает на файловой системе `/proc`, т.к. она не поддерживает изменение меток.

Контекст безопасности файла, например, может варьироваться в зависимости от домена, который создал файл. По умолчанию, новый файл или каталог наследует тип от родительского каталога, однако вы можете задать иную политику [bib3?].

4 Выполнение лабораторной работы

1. В конфигурационном файле /etc/httpd/httpd.conf необходимо задать параметр ServerName: ServerName test.ru (рис. 4.1).



```
#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed. This address appears on some server-generated pages, such
# as error documents. e.g. admin@your-domain.com
#
ServerAdmin root@localhost

#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
#ServerName test.ru

#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory />
    AllowOverride none
    Require all denied
</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/html"
```

Рис. 4.1: Задание параметра

2. Проследила, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключить фильтр можно командами `iptables -F` и `iptables -P INPUT ACCEPT` (рис. 4.2).

```
[root@adkekisheva conf]# iptables -F
[root@adkekisheva conf]# iptables -P INPUT ACCEPT
[root@adkekisheva conf]# getenforce
Enforcing
[root@adkekisheva conf]# sestatus
SELinux status:                enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:        /etc/selinux
Loaded policy name:              targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      31
```

Рис. 4.2: Отключение пакетного фильтра и вход в систему

3. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus` (рис. 4.2).
4. Обратилась командой `service httpd status` с помощью браузера к веб-серверу, запущенному на моём компьютере, и убедилась, что всё работает (рис. 4.3).

```
[root@adkekisheva conf]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Mon 2023-10-02 21:15:10 MSK; 6 days ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 28449 (httpd)
    Status: "Total requests: 3; Current requests/sec: 0; Current traffic:  0 B/sec"
    Tasks: 7
   CGroup: /system.slice/httpd.service
           └─28449 /usr/sbin/httpd -DFOREGROUND
             └─28454 /usr/sbin/httpd -DFOREGROUND
               └─28455 /usr/sbin/httpd -DFOREGROUND
                 └─28456 /usr/sbin/httpd -DFOREGROUND
                   └─28457 /usr/sbin/httpd -DFOREGROUND
                     └─28458 /usr/sbin/httpd -DFOREGROUND
                       └─28542 /usr/sbin/httpd -DFOREGROUND

Oct 02 21:15:10 adkekisheva.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 02 21:15:10 adkekisheva.localdomain httpd[28449]: AH00558: httpd: Could not reliably dete...ge
Oct 02 21:15:10 adkekisheva.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
```

Рис. 4.3: Проверка статуса веб-сервера

3. Командой `ps -auxZ | grep httpd` найдла веб-сервер Apache в списке процессов. Его контекст безопасности: `httpd_t` (рис. 4.4).

```
[root@adkekisheva ~]# ps -auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 15236 0.0 0.0 112812 980 pts/6 R+ 15:12 0:00 grep --color=auto httpd
system_u:system_r:httpd_t:s0 root 28449 0.0 0.0 230448 432 ? Ss Oct08 0:06 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 28454 0.0 0.0 232532 64 ? S Oct08 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 28455 0.0 0.0 232532 40 ? S Oct08 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 28456 0.0 0.0 232532 40 ? S Oct08 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 28457 0.0 0.0 232668 68 ? S Oct08 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 28458 0.0 0.0 232668 80 ? S Oct08 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 28542 0.0 0.0 232532 40 ? S Oct08 0:00 /usr/sbin/httpd -DFOREGROUND
```

Рис. 4.4: Список процессов

4. Посмотрела состояние переключателей SELinux для Apache с помощью `sestatus -b | grep httpd`. Многие из состояний находятся в положении «off» (рис. 4.5).

```
[root@adkekisheva ~]# sestatus -b |grep httpd
httpd_anon_write off
httpd_builtin_scripting on
httpd_can_check_spam off
httpd_can_connect_ftp off
httpd_can_connect_ldap off
httpd_can_connect_mythtv off
httpd_can_connect_zabbix off
httpd_can_network_connect off
httpd_can_network_connect_cobbler off
httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_relay off
httpd_can_sendmail off
httpd_dbus_avahi off
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_homedirs off
httpd_execmem off
httpd_graceful_shutdown on
httpd_manage_ipa off
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ipa off
httpd_run_preupgrade off
httpd_run_stickshift off
httpd_serve_cobbler_files off
httpd_setrlimit off
```

Рис. 4.5: Состояния переключателей

5. Посмотрела статистику по политике с помощью команды seinfo. Множество пользователей - 8, ролей - 14, типов- 4793 (рис. 4.6).

```
[root@adkekisheva ~]# seinfo

Statistics for policy file: /sys/fs/selinux/policy
Policy Version & Type: v.31 (binary, mls)

Classes:          130      Permissions:       272
Sensitivities:    1        Categories:       1024
Types:            4793     Attributes:        253
Users:            8        Roles:            14
Booleans:         316     Cond. Expr.:      362
Allow:            107834   Neverallow:        0
Auditallow:       158     Dontaudit:         10022
Type_trans:       18153   Type_change:       74
Type_member:      35      Role_allow:        37
Role_trans:       414     Range_trans:       5899
Constraints:      143     Validatetrans:     0
Initial SIDs:     27      Fs_use:            32
Genfscon:         103     Portcon:           614
Netifcon:         0       Nodecon:            0
Permissives:      0       Polcap:             5
```

Рис. 4.6: Статистика - команда seinfo

6. Определила типы файлов и поддиректорий, находящихся в директории /var/www, с помощью команды `ls -lZ /var/www` (рис. 4.7).

```
[root@adkekisheva ~]# ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[root@adkekisheva ~]# ls -lZ /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
```

Рис. 4.7: Определение типов файлов

7. Определите тип файлов, находящихся в директории /var/www/html: `ls -lZ /var/www/html` (рис. 4.7).
8. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html - можно владельцу файла.

9. Создайте от имени суперпользователя html-файл `/var/www/html/test.html` следующего содержания (рис. 4.8): >

test

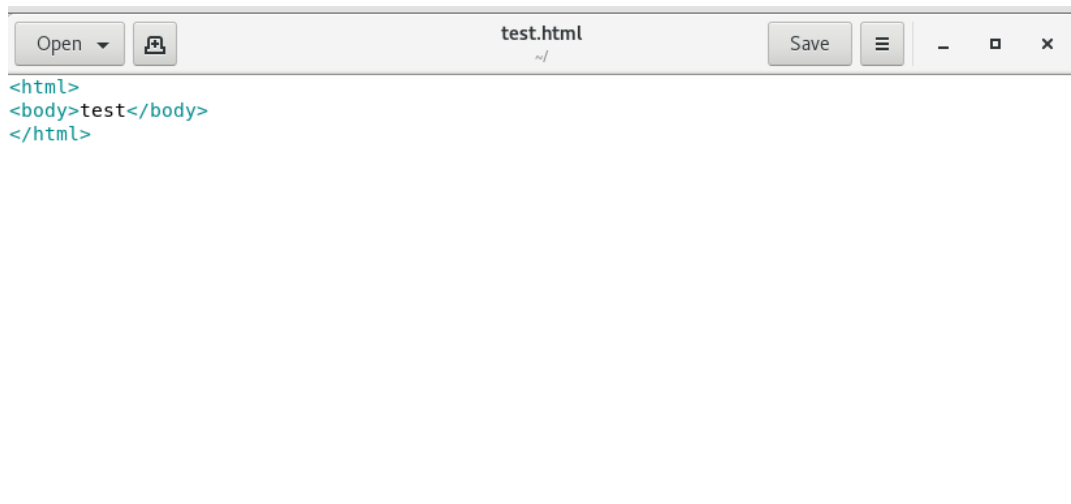


Рис. 4.8: Файл test.html

10. Проверила контекст созданного файла. Контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`: `httpd_sys_content_t` (рис. 4.7).
11. Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедилась, что файл был успешно отображён (рис. 4.9).

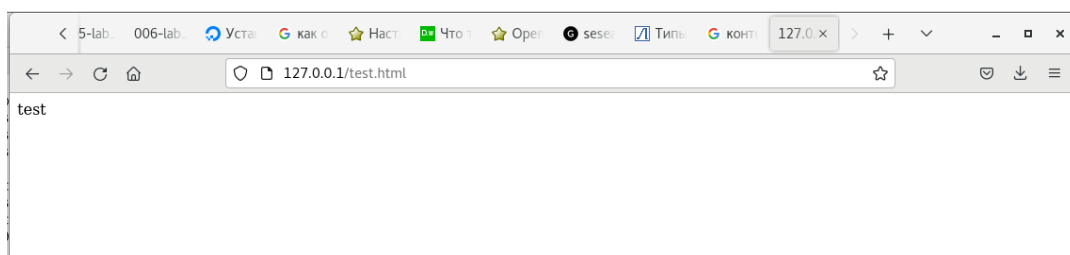
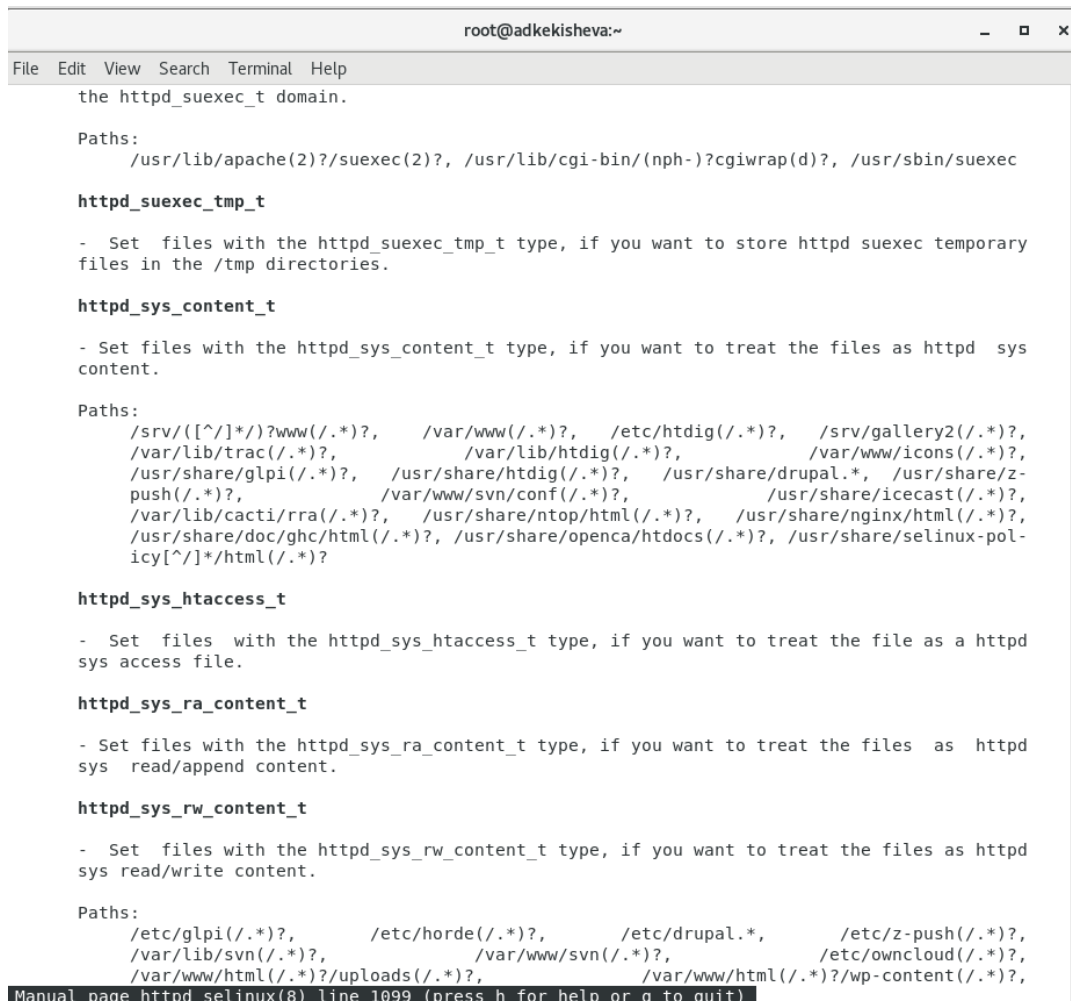


Рис. 4.9: Отображение содержимого файла в браузере

12. Изучила справку `man httpd_selinux` и выяснила, какие контексты файлов определены для `httpd` (рис. 4.10).



```
root@adkekisheva:~  
File Edit View Search Terminal Help  
the httpd_suexec_t domain.  
  
Paths:  
    /usr/lib/apache(2)?/suexec(2)?, /usr/lib/cgi-bin/(nph-)?cgiwrap(d)?, /usr/sbin/suexec  
  
httpd_suexec_tmp_t  
  
- Set files with the httpd_suexec_tmp_t type, if you want to store httpd suexec temporary  
  files in the /tmp directories.  
  
httpd_sys_content_t  
  
- Set files with the httpd_sys_content_t type, if you want to treat the files as httpd sys  
  content.  
  
Paths:  
    /srv/([^\s]*)?www(/.*)?, /var/www(/.*)?, /etc/htdig(/.*)?, /srv/gallery2(/.*)?,  
    /var/lib/trac(/.*)?, /var/lib/htdig(/.*)?, /var/www/icons(/.*)?,  
    /usr/share/glpi(/.*)?, /usr/share/htdig(/.*)?, /usr/share/drupal.*, /usr/share/z-  
    push(/.*)?, /var/www/svn/conf(/.*)?, /usr/share/icecast(/.*)?,  
    /var/lib/cacti/rra(/.*)?, /usr/share/ntop/html(/.*)?, /usr/share/nginx/html(/.*)?,  
    /usr/share/doc/ghc/html(/.*)?, /usr/share/opencard/htdocs(/.*)?, /usr/share/selinux-pol-  
    icy[^\s]*/html(/.*)?  
  
httpd_sys_htaccess_t  
  
- Set files with the httpd_sys_htaccess_t type, if you want to treat the file as a httpd  
  sys access file.  
  
httpd_sys_ra_content_t  
  
- Set files with the httpd_sys_ra_content_t type, if you want to treat the files as httpd  
  sys read/append content.  
  
httpd_sys_rw_content_t  
  
- Set files with the httpd_sys_rw_content_t type, if you want to treat the files as httpd  
  sys read/write content.  
  
Paths:  
    /etc/glpi(/.*)?, /etc/horde(/.*)?, /etc/drupal.*, /etc/z-push(/.*)?,  
    /var/lib/svn(/.*)?, /var/www/svn(/.*)?, /etc/owncloud(/.*)?,  
    /var/www/html(/.*)?/uploads(/.*)?, /var/www/html(/.*)?/wp-content(/.*)?,  
Manual page httpd_selinux(8) line 1099 (press h for help or q to quit)
```

Рис. 4.10: Команда `man httpd_selinux` - контексты для `httpd`

13. Изменила 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` и проверила командой: `ls -Z /var/www/html/test.html` (рис. 4.11).

```
[root@adkekisheva ~]# chcon -t samba_share_t /var/www/html/test.html
[root@adkekisheva ~]# s -Z /var/www/html/test.html
bash: s: command not found...
[root@adkekisheva ~]# ls -Z /var/www/html/test.html
-rw-r--r-- . root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Рис. 4.11: Команда chcon

14. 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. При изменении контекста http считает файл чужим. (рис. 4.12).

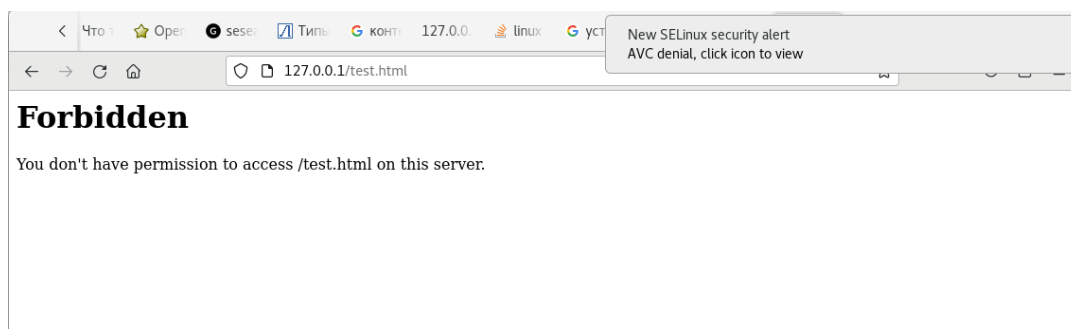


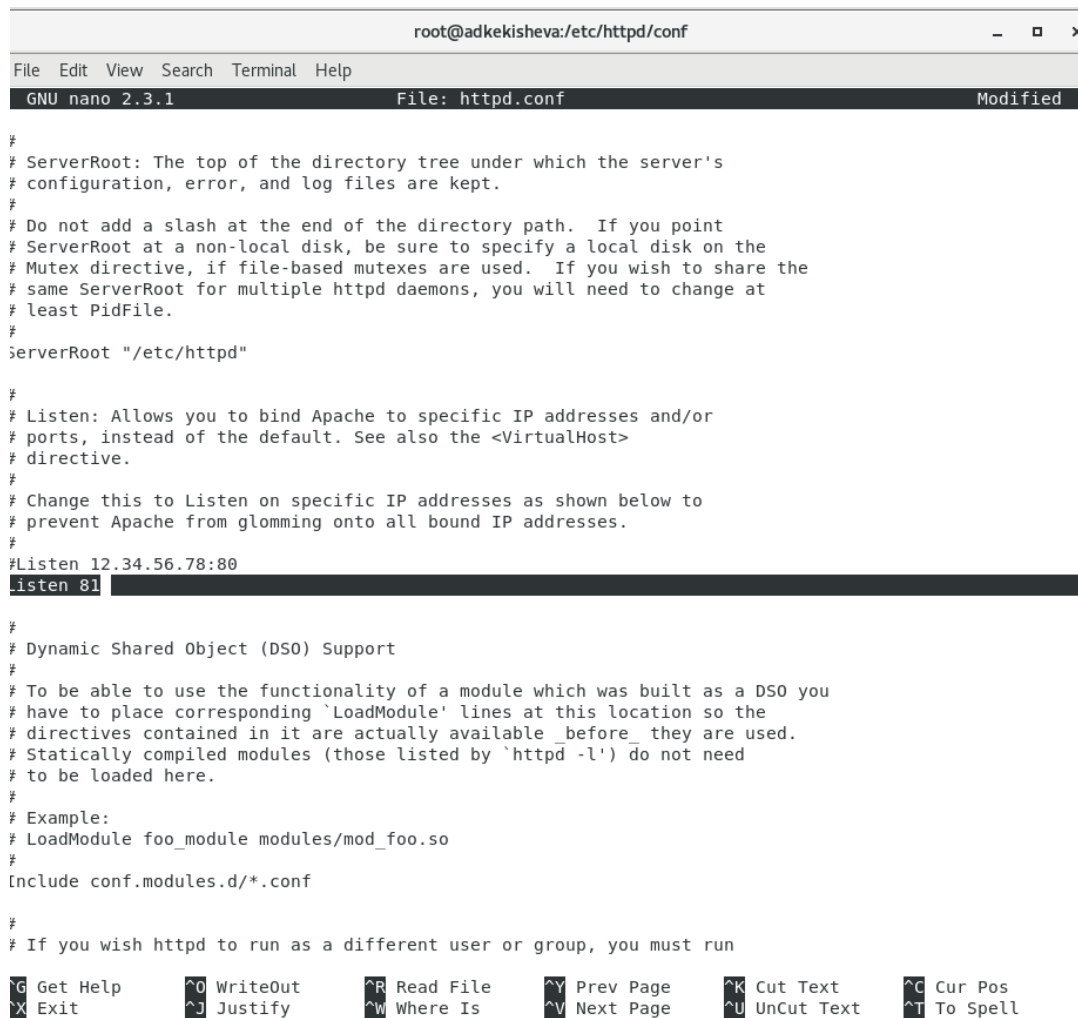
Рис. 4.12: Отказ в доступе - сообщение об ошибке от браузера

15. Просмотрела системный лог-файл: `tail /var/log/messages` и увидела ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log` (рис. 4.13).

```
[root@adkekisheva conf]# tail /var/log/messages
Oct 10 10:11:10 adkekisheva systemd: Starting Fingerprint Authentication Daemon...
Oct 10 10:11:10 adkekisheva dbus[718]: [system] Successfully activated service 'net.reactivated.Fp
print'
Oct 10 10:11:10 adkekisheva systemd: Started Fingerprint Authentication Daemon.
Oct 10 10:11:14 adkekisheva NetworkManager[886]: <info> [1696921874.4907] agent-manager: req[0x55
ef01b3f4280, :1.61/org.gnome.Shell.NetworkAgent/1000]: agent registered
Oct 10 10:11:14 adkekisheva dbus[718]: [system] Activating via systemd: service name='org.freedesk
top.hostname1' unit='dbus-org.freedesktop.hostname1.service'
Oct 10 10:11:14 adkekisheva systemd: Starting Hostname Service...
Oct 10 10:11:14 adkekisheva dbus[718]: [system] Successfully activated service 'org.freedesktop.ho
stname1'
Oct 10 10:11:14 adkekisheva systemd: Started Hostname Service.
Oct 10 10:14:02 adkekisheva journal: Failed to open file "/home/adkekisheva/.cache/thumbnails/norm
al/24b9406ce5a0e0d87929bb8b9b055e17.png": No such file or directory
Oct 10 10:14:40 adkekisheva org.gnome.Shell.desktop: Window manager warning: Buggy client sent a _
NET_ACTIVE_WINDOW message with a timestamp of 0 for 0x44000f8 (httpd.conf)
```

Рис. 4.13: Просмотр системных лог-файлов

16. Попробуйте запустить веб-сервер Apache на прослушивание TCP-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. 4.14).



```
root@adkekisheva:/etc/httpd/conf
File Edit View Search Terminal Help
GNU nano 2.3.1 File: httpd.conf Modified

#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used. If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"

#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
listen 81

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
Include conf.modules.d/*.conf

#
# If you wish httpd to run as a different user or group, you must run
```

Рис. 4.14: Изменение Listen 80 на Listen 81

17. Выполните перезапуск веб-сервера Apache (рис. 4.15).


```

[root@adkekisheva conf]# service httpd stop
Redirecting to /bin/systemctl stop httpd.service
[root@adkekisheva conf]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@adkekisheva conf]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-10-10 10:24:11 MSK; 1s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 29886 (httpd)
    Status: "Processing requests..."
     Tasks: 6
    CGroup: /system.slice/httpd.service
            └─29886 /usr/sbin/httpd -DFOREGROUND
              └─29890 /usr/sbin/httpd -DFOREGROUND
                └─29891 /usr/sbin/httpd -DFOREGROUND
                  └─29892 /usr/sbin/httpd -DFOREGROUND
                    └─29893 /usr/sbin/httpd -DFOREGROUND
                      └─29894 /usr/sbin/httpd -DFOREGROUND

Oct 10 10:24:11 adkekisheva.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 10 10:24:11 adkekisheva.localdomain httpd[29886]: AH00558: httpd: Could not reliably dete...ge
Oct 10 10:24:11 adkekisheva.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@adkekisheva conf]# █

```

Рис. 4.15: Перезапуск Apache

18. Просмотрела лог-файлы: `tail -nl /var/log/messages` и файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log`, в последнем появились записи (рис. 4.16).

```
root@adkekisheva:~  
File Edit View Search Terminal Help  
ocaluser acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'  
type=CRED_ACQ msg=audit(1695723601.768:6041): pid=3736 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'  
type=LOGIN msg=audit(1695723601.768:6042): pid=3736 uid=0 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 old-auid=4294967295 auid=0 tty=(none) old-ses=4294967295 ses=614 res=1  
type=USER_START msg=audit(1695723601.860:6043): pid=3736 uid=0 auid=0 ses=614 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_open grantors=pam_loginuid,pam_keyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'  
type=CRED_REFR msg=audit(1695723601.861:6044): pid=3736 uid=0 auid=0 ses=614 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'  
type=CRED_DISP msg=audit(1695723601.934:6045): pid=3736 uid=0 auid=0 ses=614 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'  
type=USER_END msg=audit(1695723601.941:6046): pid=3736 uid=0 auid=0 ses=614 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_close grantors=pam_loginuid,pam_keyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'  
type=SERVICE_START msg=audit(1695723949.076:6047): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dnf-makecache comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'  
type=SERVICE_STOP msg=audit(1695723949.076:6048): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dnf-makecache comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'  
type=USER_ACCT msg=audit(1695726602.022:6049): pid=3863 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_access,pam_unix,pam_localuser acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'  
type=CRED_ACQ msg=audit(1695726602.022:6050): pid=3863 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'  
type=LOGIN msg=audit(1695726602.025:6051): pid=3863 uid=0 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 old-auid=4294967295 auid=0 tty=(none) old-ses=4294967295 ses=615 res=1  
type=USER_START msg=audit(1695726602.134:6052): pid=3863 uid=0 auid=0 ses=615 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_open grantors=pam_loginuid,pam_keyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'  
type=CRED_REFR msg=audit(1695726602.136:6053): pid=3863 uid=0 auid=0 ses=615 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'  
type=CRED_DISP msg=audit(1695726602.210:6054): pid=3863 uid=0 auid=0 ses=615 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'  
type=USER_END msg=audit(1695726602.214:6055): pid=3863 uid=0 auid=0 ses=615 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_close grantors=pam_loginuid,pam_keyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
```

Рис. 4.16: Содержимое файла - /var/log/audit/audit.log

19. Выполнила команду *semanage port -a -t http_port_t -p tcp 81* После проверила список портов командой *semanage port -l | grep http_port_t* Убедилась, что порт 81 появился в списке (рис. 4.17).

```
[root@adkekisheva ~]# semanage port -a -t http_port_t -p tcp 81  
usage: semanage [-h]  
  
                {import,export,login,user,port,ibpkey,ibendport,interface,module,node,fcontext,boolean,permissive,  
,dontaudit}  
  
                ...  
semanage: error: unrecognized arguments: -p 81  
[root@adkekisheva ~]# semanage port -l | grep http_port_t  
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000  
pegasus http_port_t      tcp      5988  
[root@adkekisheva ~]#
```

Рис. 4.17: Список портов

20. Перезапустила веб-сервер Apache ещё раз. Он сейчас запустился, так

как мы добавили порт. Вернула контекст `*httpd_sys_content_t*` к файлу `/var/www/html/test.html: chcon -t httpd_sys_content_t /var/www/html/test.html` (рис. ??).

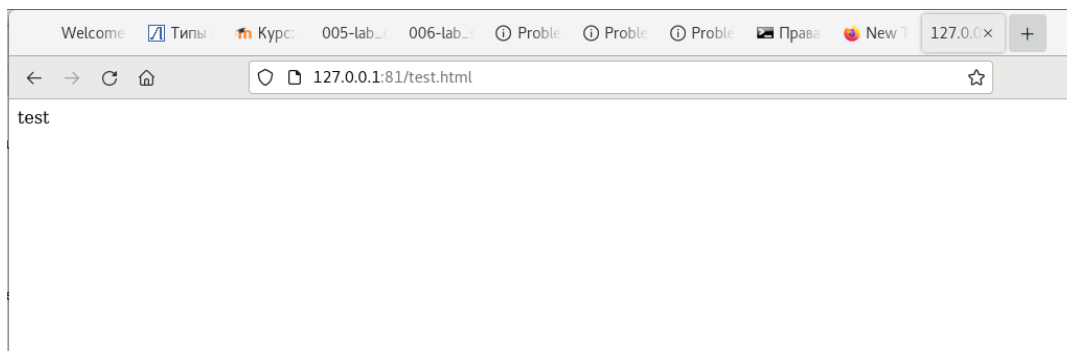


Рис. 4.18: перезапуск и изменение контекста

21. После этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Увидела содержимое — слово «test» (рис. 4.19).

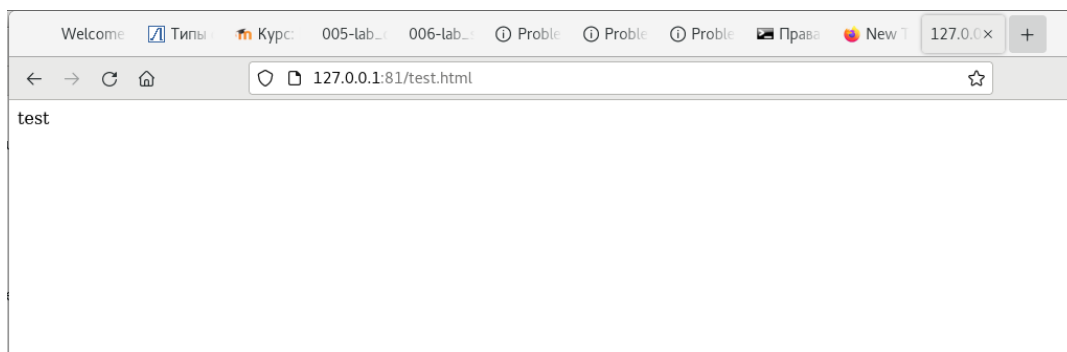
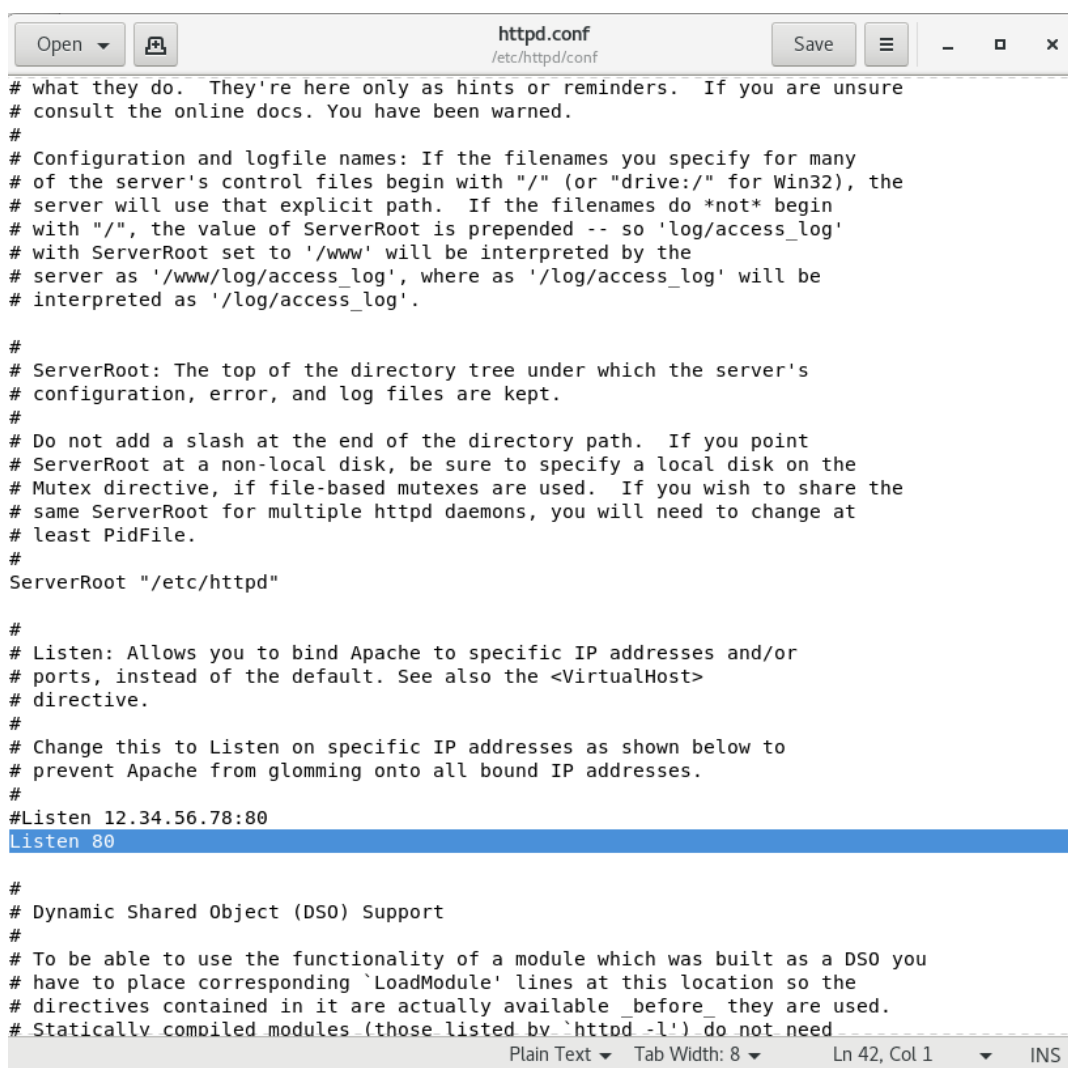


Рис. 4.19: Просмотр содержимого файла через браузер

22. Исправила обратно конфигурационный файл `apache`, вернув `Listen 80` (рис. 4.20).



```
# what they do. They're here only as hints or reminders. If you are unsure
# consult the online docs. You have been warned.
#
# Configuration and logfile names: If the filenames you specify for many
# of the server's control files begin with "/" (or "drive:/" for Win32), the
# server will use that explicit path. If the filenames do *not* begin
# with "/", the value of ServerRoot is prepended -- so 'log/access_log'
# with ServerRoot set to '/www' will be interpreted by the
# server as '/www/log/access_log', where as '/log/access_log' will be
# interpreted as '/log/access_log'.

#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used. If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"

#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
```

Рис. 4.20: Исправление конфигурационный файл

23. Удалила привязку *http_port_t* к 81 порту: *semanage port -d -t http_port_t -p tcp 81* - это оказалось запрещено (рис. 4.21).
24. Удалите файл */var/www/html/test.html*: *rm /var/www/html/test.html* (рис. 4.21).

```
[root@adkekisheva conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@adkekisheva conf]# cd
[root@adkekisheva ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@adkekisheva ~]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@adkekisheva ~]# cd /var/www/html
[root@adkekisheva html]# ls
```

Рис. 4.21: Удаление привязки к порту 81 и удаление файла

5 Выводы

1. Развила навыки администрирования ОС Linux.
2. Получила первое практическое знакомство с технологией SELinux1.
3. Проверила работу SELinx на практике совместно с веб-сервером Apache.

Список литературы

1. Лабораторная работа No 6. Мандатное разграничение прав в Linux [Электронный ресурс]. URL: https://esystem.rudn.ru/pluginfile.php/2090419/mod_resource/content/2/006-lab_selinux.pdf.
2. Введение в SELinux (security acl selinux limit linux kernel) [Электронный ресурс]. URL: https://www.opennet.ru/base/sec/intro_selinux.txt.html.