

Лабораторная работа №6

Лабораторная работа №6

Цель работы

Задание

Теоретическое введение

Оборудование

Выполнение лабораторной работы

Выводы

Список литературы

Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux¹.

Проверить работу SELinux 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:
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`
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 `/proc` 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.
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 `log`-файл:
`tail /var/log/messages`
Если в системе окажутся запущенными процессы `setroubleshoold` 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 TCP-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 -p 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_content_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 `Listen 80`.
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. Удалите файл `/var/www/html/test.html`:
`rm /var/www/html/test.html`

Теоретическое введение

В операционной системе Linux есть много отличных функций безопасности, но она из самых важных - это система прав доступа к файлам. Linux, как последователь идеологии ядра Linux в отличие от Windows, изначально проектировался как многопользовательская система, поэтому права доступа к файлам в linux продуманы очень хорошо. И это очень важно, потому что локальный доступ к файлам для всех программ и всех пользователей позволил бы вирусам без проблем уничтожить систему [1].

SELinux (SELinux) — это система принудительного контроля доступа, реализованная на уровне ядра. Впервые эта система появилась в четвертой версии CentOS, а в 5 и 6 версии реализация была существенно дополнена и улучшена. Эти улучшения позволили SELinux стать универсальной системой, способной эффективно решать массу актуальных задач. Стоит помнить, что классическая система прав Unix применяется первой, и управление перейдет к SELinux только в том случае, если эта первичная проверка будет успешно пройдена. [2].

По сути, в традиционной модели избирательного управления доступом (DAC), хорошо реализованы только два уровня доступа — пользователь и суперпользователь. Нет простого метода, который позволил бы устанавливать для каждого пользователя необходимый минимум привилегий.

Конечно, есть множество методов обхода этих проблем в рамках классической модели безопасности, но ни один из них не является универсальным.

SELinux имеет три основных режим работы, при этом по умолчанию установлен режим Enforcing. Это довольно жесткий режим, и в случае необходимости он может быть изменен на более удобный для конечного пользователя. [3]

Enforcing: Режим по-умолчанию. При выборе этого режима все действия, которые каким-то образом нарушают текущую политику безопасности, будут блокироваться, а попытка нарушения будет зафиксирована в журнале. [3]

Permissive: В случае использования этого режима, информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы. [3]

Disabled: Полное отключение системы принудительного контроля доступа. [3].

Оборудование

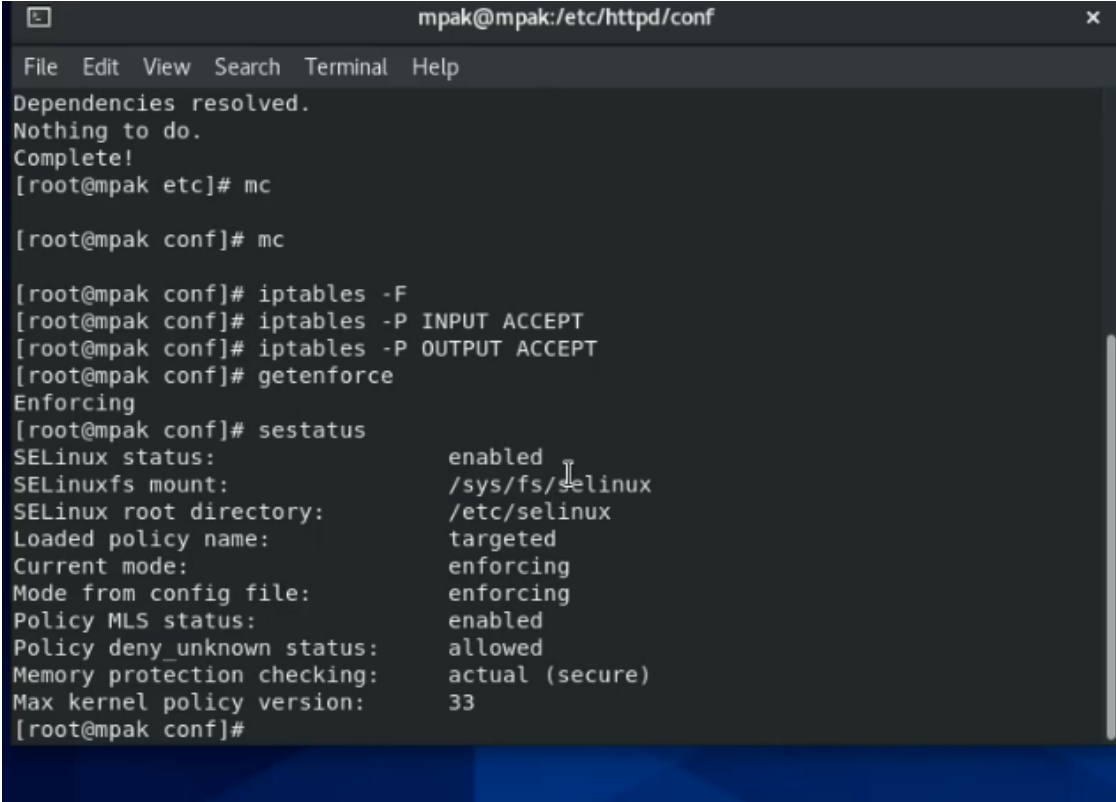
Лабораторная работа выполнялась дома со следующими характеристиками техники:

- Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz 2.81GHz
- ОС Майкрософт Windows 10
- VirtualBox верс. 6.1.26

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. -@fig:001)



```
mpak@mpak:/etc/httpd/conf
File Edit View Search Terminal Help
Dependencies resolved.
Nothing to do.
Complete!
[root@mpak etc]# mc

[root@mpak conf]# mc

[root@mpak conf]# iptables -F
[root@mpak conf]# iptables -P INPUT ACCEPT
[root@mpak conf]# iptables -P OUTPUT ACCEPT
[root@mpak conf]# getenforce
Enforcing
[root@mpak 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
Memory protection checking:    actual (secure)
Max kernel policy version:     33
[root@mpak conf]#
```

2. С помощью команды `service httpd status` видим, что наш сервер работает.

(рис. -@fig:002)

```
mpak@mpak:/etc/httpd/conf
File Edit View Search Terminal Help
Policy deny_unknown status: allowed
Memory protection checking: actual (secure)
Max kernel policy version: 33
[root@mpak 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; enabled; vendor prese
   Active: active (running) since Fri 2021-11-26 22:26:48 MSK; 4h 3min ago
     Docs: man:httpd.service(8)
   Main PID: 41688 (httpd)
    Status: "Running, listening on: port 80"
     Tasks: 213 (limit: 5838)
    Memory: 10.2M
    CGroup: /system.slice/httpd.service
            └─41688 /usr/sbin/httpd -DFOREGROUND
              └─41703 /usr/sbin/httpd -DFOREGROUND
                └─41704 /usr/sbin/httpd -DFOREGROUND
                  └─41705 /usr/sbin/httpd -DFOREGROUND
                    └─41706 /usr/sbin/httpd -DFOREGROUND

Nov 26 22:26:47 mpak.localdomain systemd[1]: Starting The Apache HTTP Server...
Nov 26 22:26:48 mpak.localdomain systemd[1]: Started The Apache HTTP Server.
Nov 26 22:26:48 mpak.localdomain httpd[41688]: Server configured, listening on:
lines 1-18/18 (END)
```

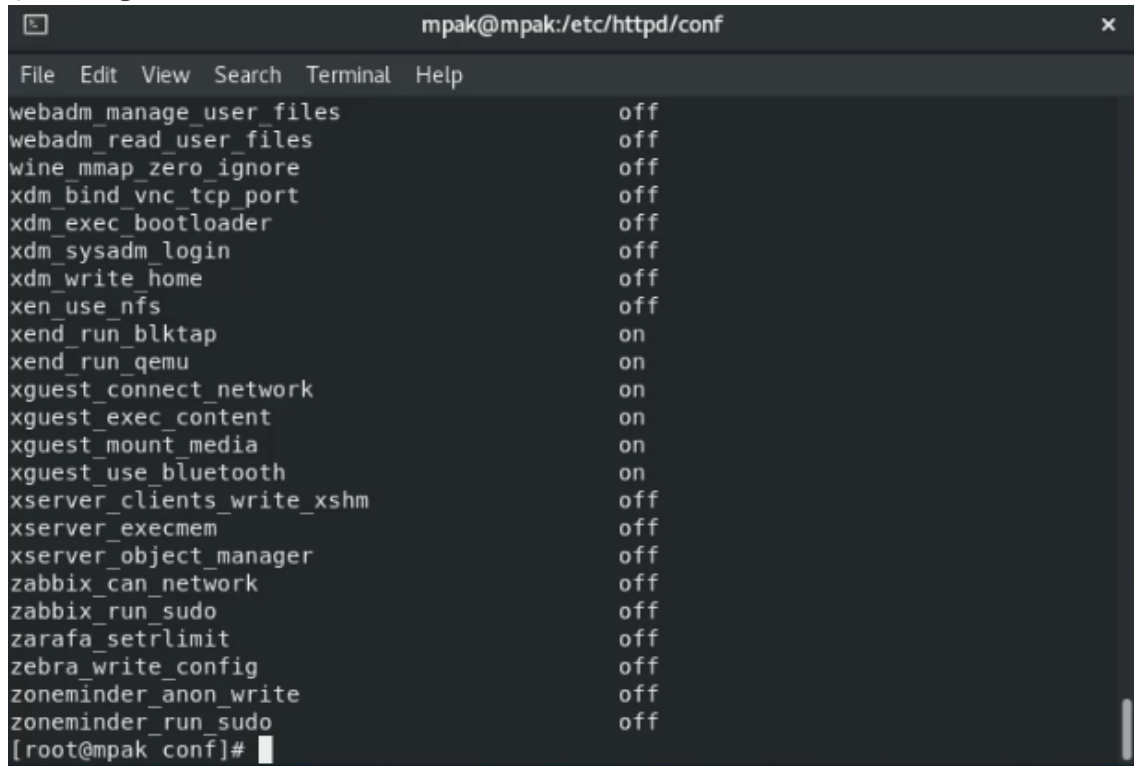
3. Нашла веб-сервер Apache в списке процессов, его контекст безопасности - httpd_t (рис. -@fig:003)

```
mpak@mpak:/etc/httpd/conf
File Edit View Search Terminal Help
└─41706 /usr/sbin/httpd -DFOREGROUND

Nov 26 22:26:47 mpak.localdomain systemd[1]: Starting The Apache HTTP Server...
Nov 26 22:26:48 mpak.localdomain systemd[1]: Started The Apache HTTP Server.
Nov 26 22:26:48 mpak.localdomain httpd[41688]: Server configured, listening on:
[root@mpak conf]# ps -Z
LABEL                                PID TTY          TIME CMD
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 45895 pts/0 00:00:00 su
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 45911 pts/0 00:00:00 bash
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 49426 pts/0 00:00:00 ps
[root@mpak conf]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0        root      41688  0.0  0.2 282900 2764 ?
Ss  Nov26   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0        apache    41703  0.0  0.1 296780 1388 ?
S   Nov26   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0        apache    41704  0.0  0.2 1485696 2016 ?
Sl  Nov26   0:03 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0        apache    41705  0.0  0.2 1354568 2080 ?
Sl  Nov26   0:02 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0        apache    41706  0.0  0.2 1354568 2052 ?
Sl  Nov26   0:02 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root      49457  0.0  0.1 12136
1044 pts/0 R+  02:31   0:00 grep --color=auto httpd
[root@mpak conf]#
```

4. Посмотрела текущее состояние переключателей SELinux для Apache. Большинство из них находятся в положении «off».

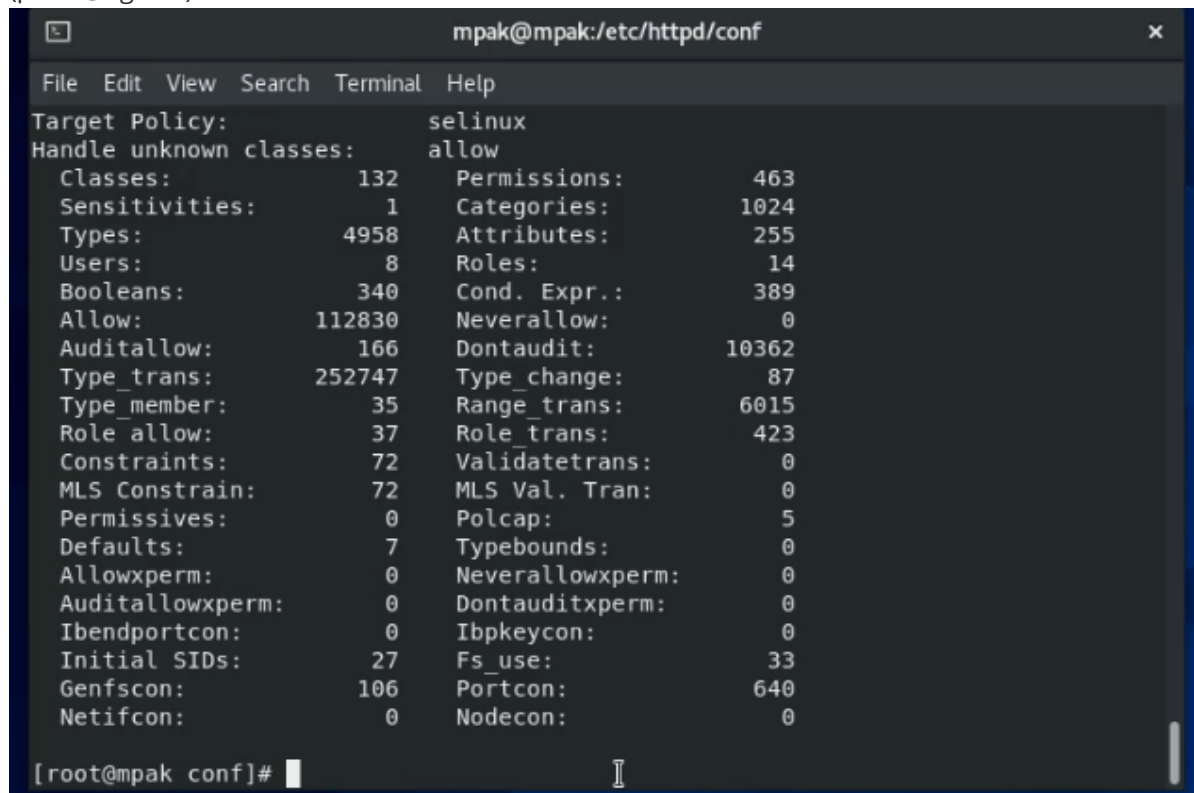
(рис. -@fig:004)



```
mpak@mpak:/etc/httpd/conf
File Edit View Search Terminal Help
webadm_manage_user_files      off
webadm_read_user_files       off
wine_mmap_zero_ignore        off
xdm_bind_vnc_tcp_port         off
xdm_exec_bootloader           off
xdm_sysadm_login              off
xdm_write_home                off
xen_use_nfs                   off
xend_run_blktp               on
xend_run_qemu                 on
xguest_connect_network        on
xguest_exec_content           on
xguest_mount_media            on
xguest_use_bluetooth          on
xserver_clients_write_xshm    off
xserver_execmem               off
xserver_object_manager        off
zabbix_can_network            off
zabbix_run_sudo               off
zaraafa_setrlimit             off
zebra_write_config            off
zoneminder_anon_write         off
zoneminder_run_sudo           off
[root@mpak conf]#
```

5.Посмотрела статистику по политике с помощью команды seinfo. Определите множество пользователей - 8, ролей - 37, типов - 4958.

(рис. -@fig:005)



```
mpak@mpak:/etc/httpd/conf
File Edit View Search Terminal Help
Target Policy:                selinux
Handle unknown classes:       allow
Classes:                      132
Sensitivities:                 1
Types:                        4958
Users:                         8
Booleans:                     340
Allow:                        112830
Auditallow:                   166
Type_trans:                   252747
Type_member:                   35
Role allow:                   37
Constraints:                   72
MLS Constrain:                72
Permissives:                  0
Defaults:                     7
Allowxperm:                   0
Auditallowxperm:              0
Ibendportcon:                 0
Initial SIDs:                 27
Genfscon:                    106
Netifcon:                     0
Permissions:                   463
Categories:                   1024
Attributes:                   255
Roles:                        14
Cond. Expr.:                  389
Neverallow:                   0
Dontaudit:                   10362
Type_change:                   87
Range_trans:                  6015
Role_trans:                   423
Validatetrans:                0
MLS Val. Tran:                0
Polcap:                       5
Typebounds:                   0
Neverallowxperm:              0
Dontauditxperm:              0
Ibpkeycon:                    0
Fs_use:                       33
Portcon:                      640
Nodecon:                      0
[root@mpak conf]#
```

6-8. Определила тип файлов и поддиректорий, находящихся в директории /var/www. Там находятся директории html и cgi-bin, где будут храниться файлы соответствующей категории. В директории html пока нет файлов, так как я не создавала пока странички сайтов сервера.

(рис. -@fig:006)


```
[root@mpak conf]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Nov 12 07
:58 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Nov 12 07
:58 html
[root@mpak conf]# ls -lZ /var/www/html
total 0
[root@mpak conf]#
```

Как видно по информации директории html, создание файлов разрешено там только пользователю рут.

9. Создала от имени суперпользователя html-файл test.html.

(рис. -@fig:007)

```
[root@mpak conf]# cd /var/www/html
bash: cd: /var/www/html: No such file or directory
[root@mpak conf]# cd /var/www/html
[root@mpak html]# vi test.html
[root@mpak html]# cat test.html
<html>
<body>tets</body>
</html>

[root@mpak html]#
```

10. Проверила контекст только что созданного файла test.html.

Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.

(рис. -@fig:008)

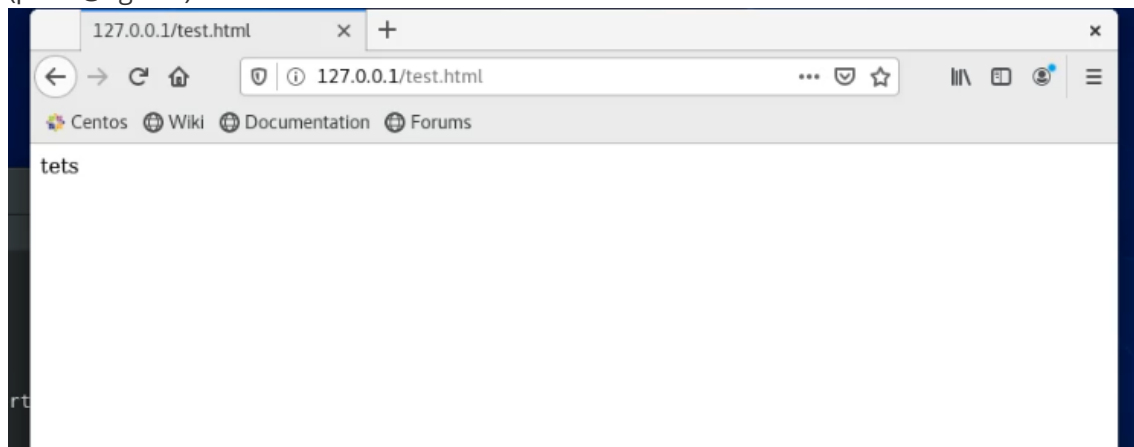
```
[root@mpak html]# ls -lZ
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 Nov 27 0
3:14 test.html
[root@mpak html]#
```

По умолчанию вновь созданным файлам в директории /var/www/html присваивается контекст httpd_sys_content_t. Этот контекст дает права процессам Апаче обрабатывать файлы.

11. Обратилась к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>.

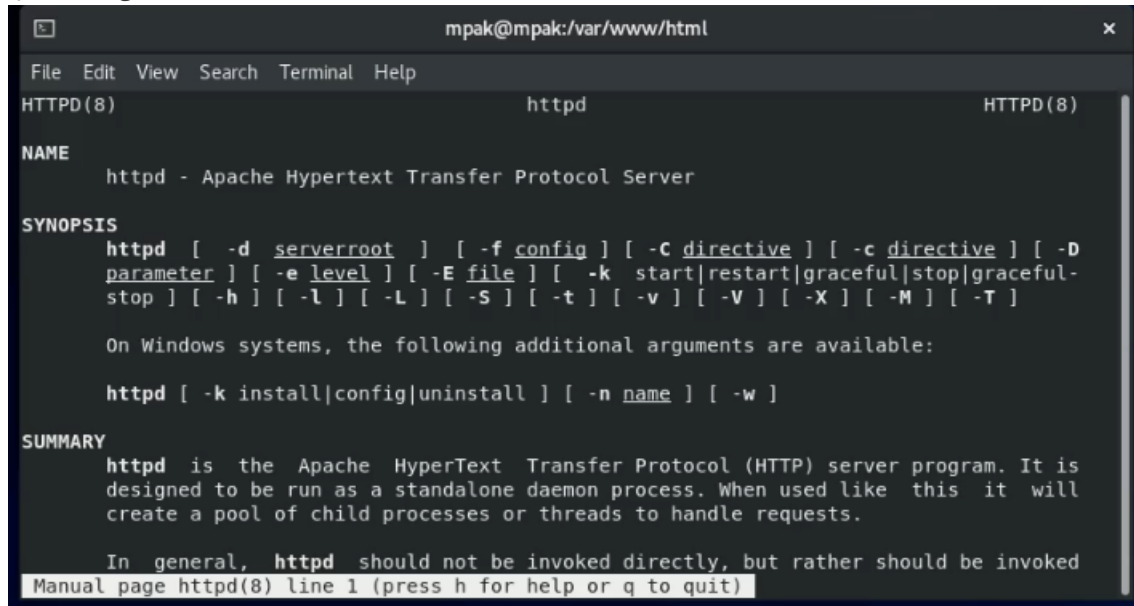
Убедилась, что файл был успешно отображён.

(рис. -@fig:009)



12. Изучите справку man httpd_selinux и выясните, какие контексты файлов определены для httpd. Сопоставьте их с типом файла test.html.

(рис. -@fig:010)



```
mpak@mpak:/var/www/html
File Edit View Search Terminal Help
HTTPD(8) httpd HTTPD(8)
NAME
    httpd - Apache Hypertext Transfer Protocol Server
SYNOPSIS
    httpd [ -d serverroot ] [ -f config ] [ -C directive ] [ -c directive ] [ -D
    parameter ] [ -e level ] [ -E file ] [ -k start|restart|graceful|stop|graceful-
    stop ] [ -h ] [ -l ] [ -L ] [ -S ] [ -t ] [ -v ] [ -V ] [ -X ] [ -M ] [ -T ]

    On Windows systems, the following additional arguments are available:

    httpd [ -k install|config|uninstall ] [ -n name ] [ -w ]

SUMMARY
    httpd is the Apache HyperText Transfer Protocol (HTTP) server program. It is
    designed to be run as a standalone daemon process. When used like this it will
    create a pool of child processes or threads to handle requests.

    In general, httpd should not be invoked directly, but rather should be invoked
    Manual page httpd(8) line 1 (press h for help or q to quit)
```

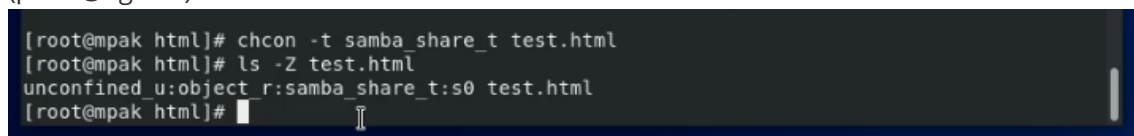
Контекст имеет схему: Тип, роль, домен

Тип `unconfined_u` - создал пользователь, свободный от типа (типично для пользователей CentOS)

Роль - `object_r` используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах.

Домен - `httpd_sys_content_t` позволяет процессу `httpd` получить доступ к файлу

13. Изменила контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`:
(рис. -@fig:011)

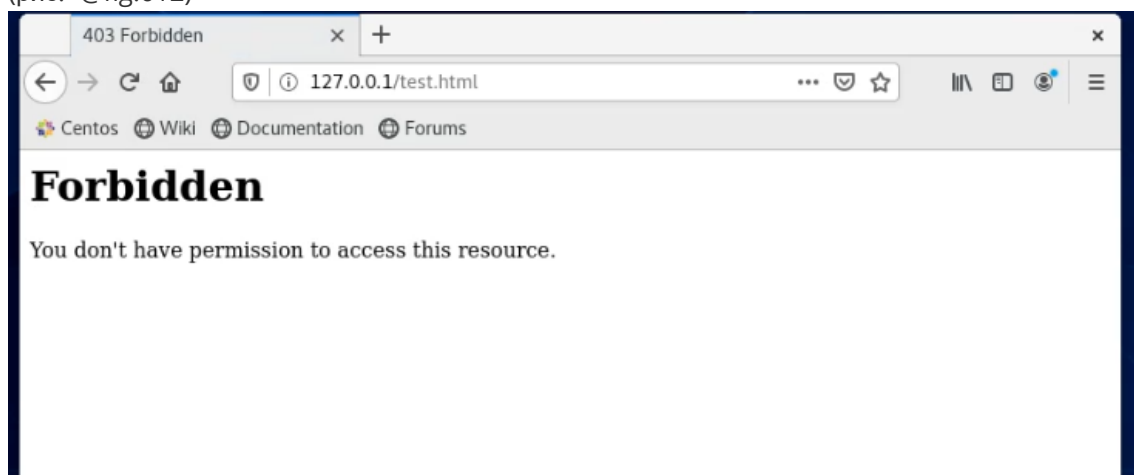


```
[root@mpak html]# chcon -t samba_share_t test.html
[root@mpak html]# ls -Z test.html
unconfined_u:object_r:samba_share_t:s0 test.html
[root@mpak html]#
```

Контекст действительно поменялся.

14. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. И получила сообщение об ошибке.

(рис. -@fig:012)



15. Файл не был отображён, потому что то процесс апаче, который должен был отобразить страничку `html`, не смог получить доступ к файлу из-за измененного контекста. Это специальное свойство контекста, которое защищает систему от взлома злоумышленниками.

Просмотрела log-файлы веб-сервера Apache.

/var/log/messages

(рис. -@fig:013)

```
[root@mpak html]# tail /var/log/messages
Nov 27 03:58:20 mpak dbus-daemon[853]: [system] Activating service name='org.fedoraproject.
SetroubleshootPrivileged' requested by ':1.447' (uid=979 pid=3752 comm="/usr/libexec/platfo
rm-python -Es /usr/sbin/setroub" label="system_u:system_r:setroubleshootd_t:s0-s0:c0.c1023"
) (using servicehelper)
Nov 27 03:58:20 mpak dbus-daemon[3773]: [system] Failed to reset fd limit before activating
service: org.freedesktop.DBus.Error.AccessDenied: Failed to restore old fd limit: Operatio
n not permitted
Nov 27 03:58:25 mpak dbus-daemon[853]: [system] Successfully activated service 'org.fedorap
roject.SetroubleshootPrivileged'
Nov 27 03:58:29 mpak setroubleshoot[3752]: SELinux is preventing /usr/sbin/httpd from getat
tr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -
l 3f74440d-2e95-4f7a-b5a9-1df1573472dd
Nov 27 03:58:30 mpak setroubleshoot[3752]: SELinux is preventing /usr/sbin/httpd from getat
tr access on the file /var/www/html/test.html.#012#012**** Plugin restorecon (92.2 confid
ence) suggests *****#012#012If you want to fix the label. #012/var/www
/html/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon
. The access attempt may have been stopped due to insufficient permissions to access a pare
nt directory in which case try to change the following command accordingly.#012Do#012# /sbi
n/restorecon -v /var/www/html/test.html#012#012**** Plugin public content (7.83 confidenc
e) suggests *****#012#012If you want to treat test.html as public content#
012Then you need to change the label on test.html to public_content_t or public_content_rw_
t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# resto
recon -v '/var/www/html/test.html'#012#012**** Plugin catchall (1.41 confidence) suggests
*****#012#012If you believe that httpd should be allowed getattr ac
cess on the test.html file by default.#012Then you should report this as a bug.#012You can
generate a local policy module to allow this access.#012Do#012allow this access for now by
```

/var/log/audit/audit.log.

(рис. -@fig:014)

```
3 debounce: scheduled expiry is in the past (-503ms), your system is too slow
Nov 27 03:58:35 mpak org.gnome.Shell.desktop[2135]: libinput error: client bug: timer event
3 debounce short: scheduled expiry is in the past (-516ms), your system is too slow
[root@mpak html]# tail /var/log/audit/audit.log
type=SERVICE_START msg=audit(1637973506.273:199): pid=1 uid=0 auid=4294967295 ses=429496729
5 subj=system_u:system_r:init_t:s0 msg='unit=systemd-tmpfiles-clean comm="systemd" exe="/us
r/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' AUID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1637973506.274:200): pid=1 uid=0 auid=4294967295 ses=4294967295
subj=system_u:system_r:init_t:s0 msg='unit=systemd-tmpfiles-clean comm="systemd" exe="/usr
/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' AUID="root" AUID="unset"
type=AVC msg=audit(1637974684.878:201): avc: denied { getattr } for pid=1312 comm="httpd
" path="/var/www/html/test.html" dev="dm-0" ino=2720956 scontext=system_u:system_r:httpd_t:
s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file permissive=0
type=SYSCALL msg=audit(1637974684.878:201): arch=c000003e syscall=4 success=no exit=-13 a0=
7f2b04002e70 a1=7f2b12ffc890 a2=7f2b12ffc890 a3=7f2b12ffd4f0 items=0 ppid=1211 pid=1312 aui
d=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses
=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)
ARCH=x86_64 SYSCALL=stat AUID="unset" UID="apache" GID="apache" EUID="apache" SUID="apache"
FSUID="apache" EGID="apache" SGID="apache" FSGID="apache"
type=PROCTITLE msg=audit(1637974684.878:201): proctitle=2F7573722F7362696E2F6874747064002D4
4464F524547524F554E44
type=AVC msg=audit(1637974684.878:202): avc: denied { getattr } for pid=1312 comm="httpd
" path="/var/www/html/test.html" dev="dm-0" ino=2720956 scontext=system_u:system_r:httpd_t:
```

В обоих файлах можно найти записи процессы setroubleshootd и audtd, где можно увидеть ошибки, аналогичные указанным выше.

16-17. Попробовала запустить веб-сервер Apache на прослушивание TCP-порта 81 . Для этого в файле /etc/httpd/httpd.conf заменила строчку на Listen 81.

(рис. -@fig:015)

```
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 81

#
# Dynamic Shared Object (DSO) Support
```

Выполнила перезапуск веб-сервера Apache. Должен был произойти сбой, но он не произошел, так как у меня порт 81 был уже записан в системе как используемый.

(рис. -@fig:016)

```
[root@mpak conf]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@mpak 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; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2021-11-27 04:09:44 MSK; 7s ago
     Docs: man:httpd.service(8)
  Main PID: 4043 (httpd)
    Status: "Started, listening on: port 81"
     Tasks: 213 (limit: 5838)
    Memory: 20.6M
    CGroup: /system.slice/httpd.service
            └─4043 /usr/sbin/httpd -DFOREGROUND
              └─4047 /usr/sbin/httpd -DFOREGROUND
                └─4048 /usr/sbin/httpd -DFOREGROUND
                  └─4049 /usr/sbin/httpd -DFOREGROUND
                    └─4050 /usr/sbin/httpd -DFOREGROUND

Nov 27 04:09:44 mpak.localdomain systemd[1]: Starting The Apache HTTP Server...
Nov 27 04:09:44 mpak.localdomain systemd[1]: Started The Apache HTTP Server.
Nov 27 04:09:44 mpak.localdomain httpd[4043]: Server configured, listening on: port 81
[root@mpak conf]#
```

18. Проанализировала лог-файлы:

tail -nl /var/log/messages

(рис. -@fig:017)

```
[root@mpak conf]# cat /var/log/http/error_log
cat: /var/log/http/error_log: No such file or directory
[root@mpak conf]# cat /var/log/http/error_log
```

/var/log/http/error_log

(рис. -@fig:018)

```
[Sat Nov 27 03:58:04.907517 2021] [core:error] [pid 1312:tid 139822979077888] (13)Permission denied
: [client 127.0.0.1:50474] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Sat Nov 27 04:09:41.698713 2021] [mpm_event:notice] [pid 1211:tid 139823716702528] AH00492: caught SIGWINCH, shutting down gracefully
[Sat Nov 27 04:09:44.761949 2021] [core:notice] [pid 4043:tid 140097269520704] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Nov 27 04:09:44.806320 2021] [suexec:notice] [pid 4043:tid 140097269520704] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Nov 27 04:09:44.826382 2021] [lua_method_heartbeat:notice] [pid 4043:tid 140097269520704] AH02282: No slotmem from mod_heartbeat
[Sat Nov 27 04:09:44.826917 2021] [http2:warn] [pid 4043:tid 140097269520704] AH02951: mod_ssl does not seem to be enabled
[Sat Nov 27 04:09:44.828838 2021] [mpm_event:notice] [pid 4043:tid 140097269520704] AH00489: Apache/2.4.37 (centos) configured -- resuming normal operations
[Sat Nov 27 04:09:44.828861 2021] [core:notice] [pid 4043:tid 140097269520704] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[root@mpak conf]#
```

/var/log/http/access_log

(рис. -@fig:019)

```
[Sat Nov 27 04:09:44.826917 2021] [http2:warn] [pid 4043:tid 140097269520704] AH02951: mod_ssl does not seem to be enabled
[Sat Nov 27 04:09:44.828838 2021] [mpm_event:notice] [pid 4043:tid 140097269520704] AH00489: Apache/2.4.37 (centos) configured -- resuming normal operations
[Sat Nov 27 04:09:44.828861 2021] [core:notice] [pid 4043:tid 140097269520704] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[root@mpak conf]# cat /var/log/httpd/access_log
127.0.0.1 - - [27/Nov/2021:03:36:38 +0300] "\x16\x03\x01\x02" 400 226 "-" "-"
127.0.0.1 - - [27/Nov/2021:03:37:08 +0300] "GET /test.html HTTP/1.1" 200 34 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [27/Nov/2021:03:37:09 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [27/Nov/2021:03:41:36 +0300] "GET /test.html HTTP/1.1" 200 34 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [27/Nov/2021:03:41:36 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [27/Nov/2021:03:58:04 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
[root@mpak conf]#
```

/var/log/audit/audit.log

(рис. -@fig:020)


```

FSUID="apache"
type=PROCTITLE msg=audit(1637974684.878:202): proctitle=2F7573722F7362696E2F6874747064002D44464F52
4547524F554E44
type=SERVICE_START msg=audit(1637974919.431:203): 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' UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1637974919.431:204): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=s
ystem_u:system_r:init_t:s0 msg='unit=dnf-makecache comm="systemd" exe="/usr/lib/systemd/systemd" h
ostname=? addr=? terminal=? res=success' UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1637975384.014:205): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=s
ystem_u:system_r:init_t:s0 msg='unit=httpd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=
? addr=? terminal=? res=success' UID="root" AUID="unset"
type=SERVICE_START msg=audit(1637975384.833:206): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=
system_u:system_r:init_t:s0 msg='unit=httpd comm="systemd" exe="/usr/lib/systemd/systemd" hostname
=? addr=? terminal=? res=success' UID="root" AUID="unset"
[root@mpak conf]# tail /var/log/audit/audit.log

```

Так как у меня все же запустился сервер, то я просто назову, где бы появились сообщения об ошибках. Ошибки будут в : /var/log/httpd/error_log, /var/log/audit/audit.log и /var/log/messages

19. Добавила 81 порт командой.

(рис. -@fig:021)

```

[root@mpak conf]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@mpak conf]# 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@mpak conf]#

```

Убедилась, что порт 81 появился в списке.

20. Попробовала запустить веб-сервер Apache ещё раз. Он запустился сейчас, так как мы добавили порт к используемым в сервисе Apache.

(рис. -@fig:022)

```

File Edit View Search Terminal Help
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2021-11-27 04:23:53 MSK; 8s ago
     Docs: man:httpd.service(8)
  Main PID: 4521 (httpd)
    Status: "Started, listening on: port 81"
   Tasks: 213 (limit: 5838)
  Memory: 28.3M
   CGroup: /system.slice/httpd.service
           └─4521 /usr/sbin/httpd -DFOREGROUND
             4526 /usr/sbin/httpd -DFOREGROUND
             4527 /usr/sbin/httpd -DFOREGROUND
             4528 /usr/sbin/httpd -DFOREGROUND
             4529 /usr/sbin/httpd -DFOREGROUND

Nov 27 04:23:52 mpak.localdomain systemd[1]: Starting The Apache HTTP Server...
Nov 27 04:23:53 mpak.localdomain systemd[1]: Started The Apache HTTP Server.
Nov 27 04:23:53 mpak.localdomain httpd[4521]: Server configured, listening on: port 81
[root@mpak conf]# chcon -t httpd_sys_content_t /var/www/html/test.html

```

21. Вернула контекст httpd_sys_content_t

(рис. -@fig:023)

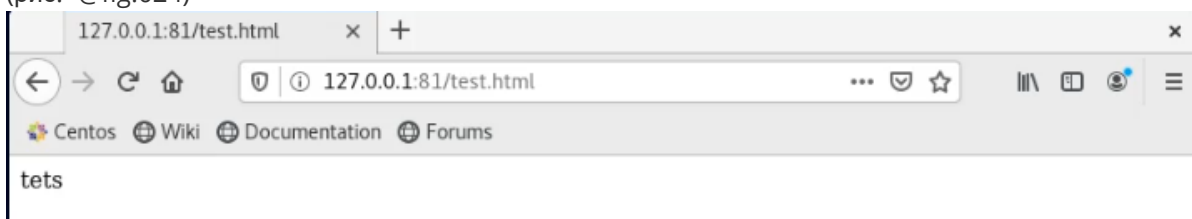
```

[root@mpak conf]# chcon -t httpd_sys_content_t /var/www/html/test.html
chcon: failed to change context of '/var/www/html/test.html' to 'unconfined_u:object_r:httpd_sys_c
ontent_t:s0': Invalid argument
[root@mpak conf]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@mpak conf]#

```

Теперь веб-сервер открывается, введя в браузере адрес <http://127.0.0.1:81/test.html>.

(рис. -@fig:024)



22-24. Исправила обратно конфигурационный файл apache, вернув Listen 80.

Удалила привязку http_port_t к 81 порту

Удалите файл /var/www/html/test.html

(рис. -@fig:025)

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

Не забыла выйти из режима суперпользователя.

Выводы

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

Список литературы

- 1.SELinux – описание и особенности работы с системой. Часть 1 // Habr URL: <https://habr.com/ru/company/kingsservers/blog/209644/> (дата обращения: 26.11.2021).
- 2.Контексты SELinux // fedora URL: https://docs.fedoraproject.org/ru-RU/Fedora/13/html/Security-Enhanced_Linux/chap-Security-Enhanced_Linux-SELinux_Contexts.html (дата обращения: 25.11.2021).
- 3.Безопасная эксплуатация Apache, часть 1: базовые понятия // rus-linux URL: <http://rus-linux.net/MyLDP/server/securing-apache-part-1.html> (дата обращения: 26.11.2021).