

---

## Front matter

title: "Отчёт по лабораторной работе 6" sub-title: "Мандатное разграничение прав в Linux" author: "Дунашсимуенту Висенте Феликс"

## Generic options

lang: ru-RU toc-title: "Содержание"

## Bibliography

bibliography: bib/cite.bib csl: pandoc/csl/gost-r-7-0-5-2008-numeric.csl

## Pdf output format

toc: true # Table of contents toc-depth: 2 lof: true # List of figures lot: true # List of tables fontsize: 12pt  
linestretch: 1.5 papersize: a4 documentclass: scrreprt

## l18n polyglossia

polyglossia-lang: name: russian options:

```
- babelshorthands=true
```

polyglossia-otherlangs: name: english

## l18n babel

babel-lang: russian babel-otherlangs: english

## Fonts

mainfont: PT Serif romanfont: PT Serif sansfont: PT Sans monofont: PT Mono mainfontoptions: Ligatures=TeX  
romanfontoptions: Ligatures=TeX sansfontoptions: Ligatures=TeX,Scale=MatchLowercase monofontoptions:  
Scale=MatchLowercase,Scale=0.9

## Biblatex

biblatex: true biblio-style: "gost-numeric" biblatexoptions:

- parenttracker=true
- backend=biber
- hyperref=auto
- language=auto
- autolang=other\*
- citestyle=gost-numeric

## Pandoc-crossref LaTeX customization

figureTitle: "Рис." tableTitle: "Таблица" listingTitle: "Листинг" lofTitle: "Список иллюстраций" lotTitle: "Список таблиц" lolTitle: "Листинги"

## Misc options

indent: true header-includes:

- `\usepackage{indentfirst}`
- `\usepackage{float} # keep figures where there are in the text`
- `\floatplacement{figure}{H} # keep figures where there are in the text`

---

### 6.1. Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux<sup>1</sup>. Проверить работу SELinx на практике совместно с веб-сервером Apache.

### 6.2. Порядок выполнения работы

1. Вошел в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.
2. Обратил 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`.

```
bash: getenforce: command not found...
^[[A[vfdunashsimentu@vfdunashsimentu ~]$ getenforce
Enforcing
[vfdunashsimentu@vfdunashsimentu ~]$ 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
```

```
[vfdunashsimentu@vfdunashsimentu ~]$ 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 pr
   Active: active (running) since Sat 2023-10-14 16:31:41 MSK; 33s ago
     Docs: man:httpd.service(8)
  Main PID: 4600 (httpd)
    Status: "Running, listening on: port 80"
    Tasks: 213 (limit: 24644)
   Memory: 49.9M
    CGroup: /system.slice/httpd.service
            └─4600 /usr/sbin/httpd -DFOREGROUND
              └─4616 /usr/sbin/httpd -DFOREGROUND
                └─4617 /usr/sbin/httpd -DFOREGROUND
                  └─4619 /usr/sbin/httpd -DFOREGROUND
                    └─4620 /usr/sbin/httpd -DFOREGROUND
lines 1-14/14 (END)
```

3. Нашёл веб-сервер Apache в списке процессов, определил его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду `ps auxZ | grep httpd` или `ps -eZ | grep httpd`.
4. Посмотрел текущее состояние переключателей SELinux для Apache с помощью команды `sestatus - bigrep httpd` Обратите внимание, что многие из них находятся в положении «off»

```

4620 /usr/sbin/httpd -DFOREGROUND
[vfdunashsimentu@vfdunashsimentu ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 4600 1.2 0.2 265104 11752 ?
Ss 16:31 0:01 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 4616 0.0 0.2 269808 8668 ?
S 16:31 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 4617 2.0 0.4 2507248 18520 ?
Sl 16:31 0:01 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 4619 2.5 0.5 2769460 22596 ?
Sl 16:31 0:02 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 4620 1.7 0.4 2572784 18520 ?
Sl 16:31 0:01 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 vfdunas+ 4911 0.0 0.0 2
21940 1180 pts/0 S+ 16:33 0:00 grep --color=auto httpd
[vfdunashsimentu@vfdunashsimentu ~]$ sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

-v Verbose check of process and file contexts.
-b Display current state of booleans.

```

Without options, show SELinux status.

```

Without options, show SELinux status.
[vfdunashsimentu@vfdunashsimentu ~]$ 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_redis 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 off
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
httpd_ssi_exec off
httpd_sys_script_anon_write off
httpd_tmp_exec off
httpd_tty_comm off
httpd_unified off

```

- 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`

```
[vfdunashsimentu@vfdunashsimentu ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          31 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:          132      Permissions:        464
Sensitivities:    1        Categories:         1024
Types:            5012     Attributes:         258
Users:            8        Roles:              15
Booleans:         347     Cond. Expr.:       397
Allow:            115669   Neverallow:         0
Auditallow:       170     Dontaudit:          10514
Type_trans:       259809  Type_change:        94
Type_member:       37     Range_trans:        5989
Role_allow:       39     Role_trans:         421
Constraints:      72     Validatetrans:      0
MLS Constrain:    72     MLS Val. Tran:      0
Permissives:      0      Polcap:             5
Defaults:         7      Typebounds:         0
Allowxperm:       0      Neverallowxperm:    0
Auditallowxperm:  0      Dontauditxperm:     0
Ibendportcon:     0      Ibpkeycon:          0
Initial SIDs:     27     Fs_use:             34
Genfscon:         107    Portcon:            649
Netifcon:         0      Nodecon:            0

[vfdunashsimentu@vfdunashsimentu ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Aug 17
17:09 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 Aug 17
17:09 html
[vfdunashsimentu@vfdunashsimentu ~]$ ls -lZ /var/www/html
total 0

[root@vfdunashsimentu vfdunashsimentu]# touch /var/www/html/test.html
[root@vfdunashsimentu vfdunashsimentu]# vi /var/www/html/test.html
```

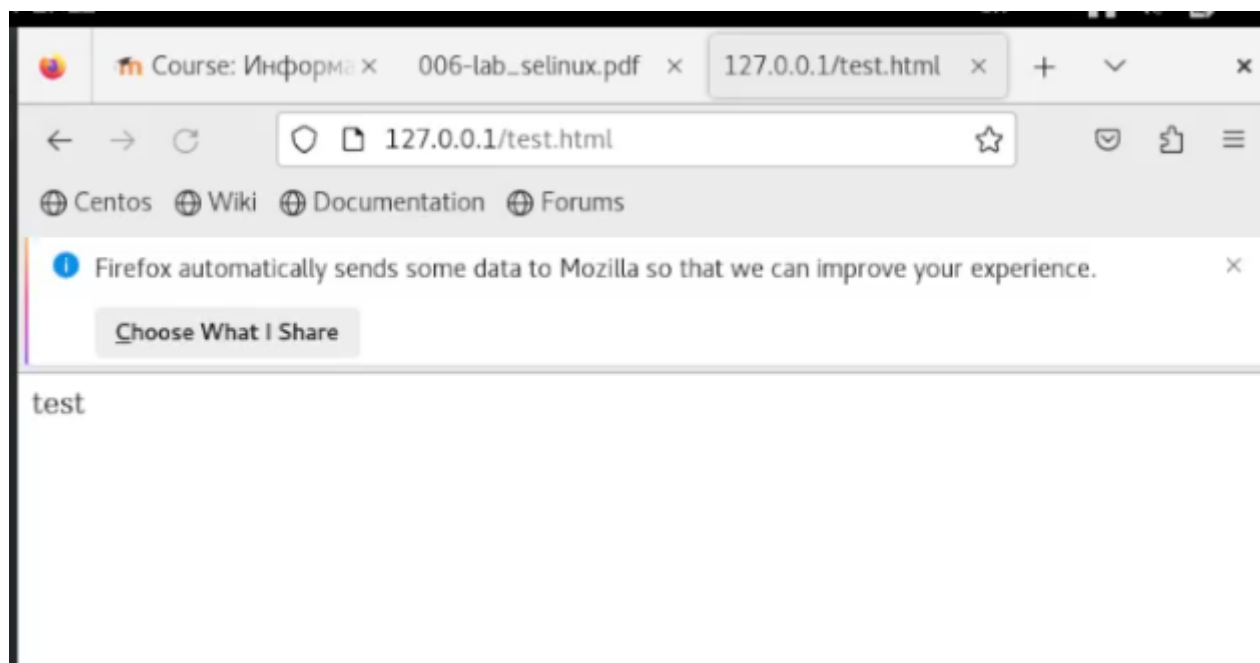
8. Создал от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания:

```
vfdunashsimentu@vfdunashsimentu:/home/vfdunashsimentu
File Edit View Search Terminal Help
<html>
<body>test</body>
</html>
~
~
```

9. Проверил контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.

```
[root@vfdunashsimentu vfdunashsimentu]# touch /var/www/html/test.html
[root@vfdunashsimentu vfdunashsimentu]# vi /var/www/html/test.html
[root@vfdunashsimentu vfdunashsimentu]# ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct 14
17:07 test.html
```

10. Обратил к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедил, что файл был успешно отображён.



12. Изучил справку `man httpd_selinux` и выяснил, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверил контекст файла можно командой `ls -Z. ls -Z /var/www/html/test.html` Рассмотрел 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`

```
[root@vfdunashsimentu vfdunashsimentu]# man httpd_selinux
No manual entry for httpd_selinux
[root@vfdunashsimentu vfdunashsimentu]# ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct 14
17:07 test.html
[root@vfdunashsimentu vfdunashsimentu]# chcon -t samba share_t /var/www/html/t
est.html
chcon: cannot access 'share_t': No such file or directory
chcon: failed to change context of '/var/www/html/test.html' to 'unconfined_u:
object_r:samba:s0': Invalid argument
[root@vfdunashsimentu vfdunashsimentu]# chcon -t samba_share_t /var/www/html/t
est.html
[root@vfdunashsimentu vfdunashsimentu]# ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 33 Oct 14 17:07
test.html
[root@vfdunashsimentu vfdunashsimentu]#
```

14.

Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Я получил сообщение об ошибке: `Forbidden You don't have permission to access /test.html on this server.`

16. Попробуем 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`.



```

mc [root@vfdunashsimentu]:/etc/httpd/conf
File Edit View Search Terminal Help
httpd.conf [~ ~ ~] 9 L: [ 7+38 45/357] *(1919/11899b) 0010 0x00[*][X]
# for a discussion of each configuration directive.
#
# See the httpd.conf(5) man page for more information on this configuration,
# and httpd.service(8) on using and configuring the httpd service.
#
# Do NOT simply read the instructions in here without understanding
# 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 81
#
# Dynamic Shared Object (DSO) Support

```

17. 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.

```

[root@vfdunashsimentu vfdunashsimentu]# semanage port -l | grep http_port_t
http_port_t          tcp      80, 81, 443, 488, 8008, 8009, 8443, 90
00
pegasus_http_port_t  tcp      5988

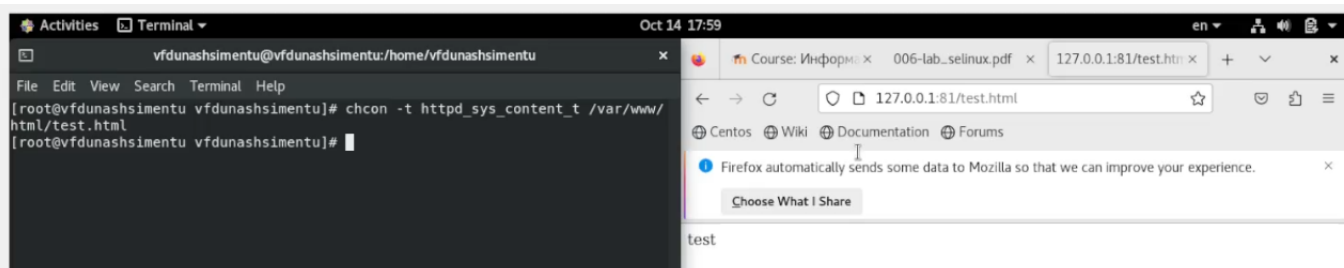
```

18.

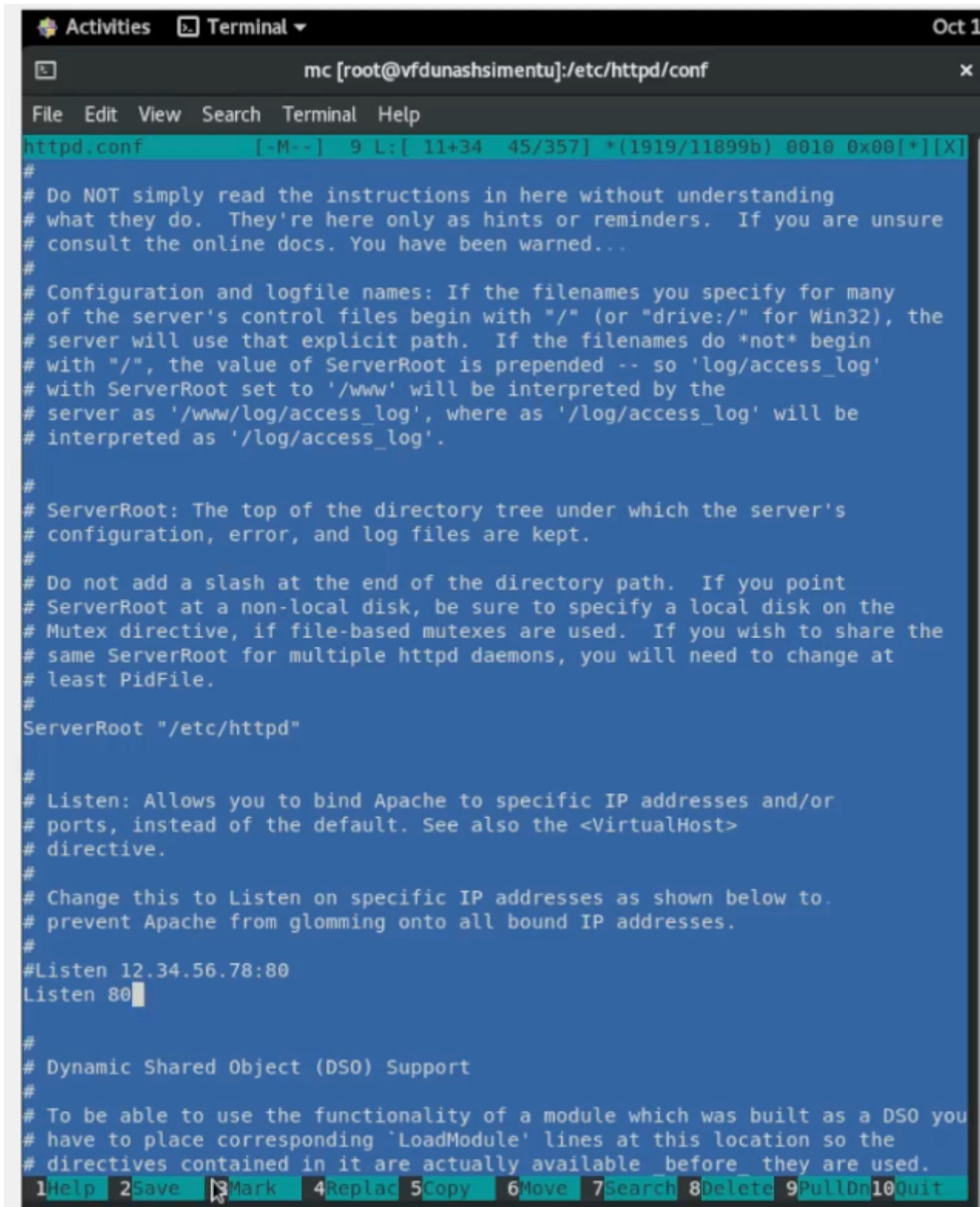
Вернул контекст `httpd_sys_content_t` к файлу `/var/www/html/ test.html`: `chcon -t httpd_sys_content_t /var/www/html/test.html` После этого попробуйте получить доступ к файлу через веб-сервер, введя в



браузере адрес `http://127.0.0.1:81/test.html`.



19. Исправил обратно конфигурационный файл apache, вернув Listen 80.



20. Удалите привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81 и проверьте, что порт 81 удалён.
21. Удалите файл /var/www/html/test.html: rm /var/www/html/test.html

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

## Выводы

SELinux предоставляет надежную и гибкую платформу для обеспечения соблюдения политик безопасности контроля доступа.