

Отчет по лабораторной работе №6

Мандатное разграничение прав в Linux

Гурбангельдиев Мухаммет НФИ-03-18

Содержание

1	Цель работы	3
2	Последовательность выполнения работы	4
3	Выводы	16

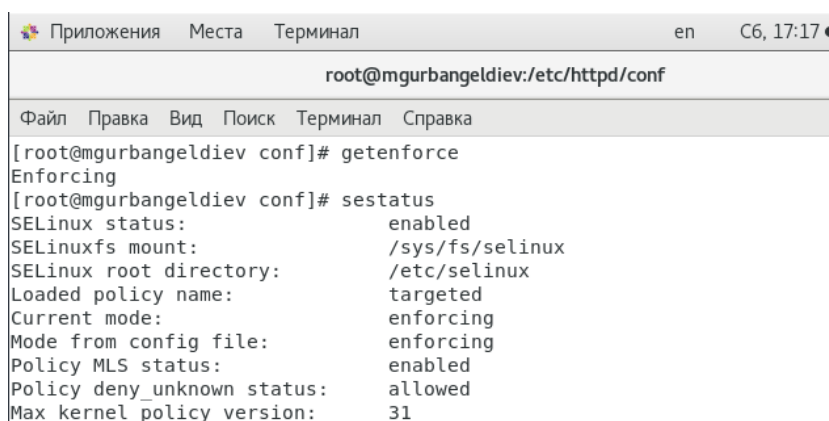
1 Цель работы

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

Проверить работу SELinux на практике совместно с веб-сервером Apache.

2 Последовательность выполнения работы

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus` (рис. 2.1)



The screenshot shows a terminal window with a title bar containing icons for applications, locations, and a terminal, along with the text 'Приложения Места Терминал', 'en', and 'C6, 17:17'. The terminal prompt is 'root@mgurbangeldiev:/etc/httpd/conf'. The user has entered the command 'getenforce', which returns 'Enforcing'. Then, the user enters 'sestatus', which returns the following output:

```
[root@mgurbangeldiev conf]# getenforce
Enforcing
[root@mgurbangeldiev 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
```

Figure 2.1: SELinux

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`. (рис. 2.2)

```
[root@mgurbangeldiev mgurbangeldiev]# 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 Co 2021-11-27 16:50:37 MSK; 32min ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 3042 (httpd)
    Status: "Total requests: 0; Current requests/sec: 0; Current traffic:  0 B/sec"
     Tasks: 6
    CGroup: /system.slice/httpd.service
            └─3042 /usr/sbin/httpd -DFOREGROUND
              └─3047 /usr/sbin/httpd -DFOREGROUND
                └─3048 /usr/sbin/httpd -DFOREGROUND
                  └─3049 /usr/sbin/httpd -DFOREGROUND
                    └─3050 /usr/sbin/httpd -DFOREGROUND
                      └─3051 /usr/sbin/httpd -DFOREGROUND

ноя 27 16:50:37 mgurbangeldiev.localdomain systemd[1]: Starting The Apache HTTP Server...
ноя 27 16:50:37 mgurbangeldiev.localdomain httpd[3042]: AH00558: httpd: Could not reliably determin...ge
ноя 27 16:50:37 mgurbangeldiev.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@mgurbangeldiev mgurbangeldiev]#
```

Figure 2.2: Apache HTTP Server

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` (рис. 2.3)

```
[root@mgurbangeldiev mgurbangeldiev]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      3042  0.0  0.5 230440  5204 ?        Ss   16:50   0:00 /usr/sbin/
httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache   3047  0.0  0.3 232524  3152 ?        S    16:50   0:00 /usr/sbin/
httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache   3048  0.0  0.3 232524  3152 ?        S    16:50   0:00 /usr/sbin/
httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache   3049  0.0  0.3 232524  3152 ?        S    16:50   0:00 /usr/sbin/
httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache   3050  0.0  0.3 232524  3152 ?        S    16:50   0:00 /usr/sbin/
httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache   3051  0.0  0.3 232524  3152 ?        S    16:50   0:00 /usr/sbin/
httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 3882  0.0  0.0 112836  972 pts/0  S+   17:23   0:00 g
rep --color=auto httpd
[root@mgurbangeldiev mgurbangeldiev]#
```

Figure 2.3: Apache в списке процессов

4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды

`sestatus -b | grep httpd`

Обратите внимание, что многие из них находятся в положении «off». (рис. 2.4)

mgurbangeldiev@mgurbangeldiev:/home/mgurbangeldiev	
Файл	Правка Вид Поиск Терминал Справка
virt_sandbox_use_audit	on
virt_sandbox_use_fusefs	off
virt_sandbox_use_mknod	off
virt_sandbox_use_netlink	off
virt_sandbox_use_sys_admin	off
virt_transition_userdomain	off
virt_use_comm	off
virt_use_execmem	off
virt_use_fusefs	off
virt_use_glusterd	off
virt_use_nfs	off
virt_use_rawip	off
virt_use_samba	off
virt_use_sanlock	off
virt_use_usb	on
virt_use_xserver	off
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
zarafa_setrlimit	off
zebra_write_config	off
zoneminder_anon_write	off
zoneminder_run_sudo	off

Figure 2.4: Текущее состояние переключателей SELinux для Apache

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов. (рис. 2.5)

```
[root@mgurbangeldiev mgurbangeldiev]# 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
```

Figure 2.5: Статистику по политике

Множество типов: 4793. Множество пользователей: 8. Множество ролей: 14.

6. Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды (рис. 2.6)

`ls -lZ /var/www`

```
[root@mgurbangeldiev mgurbangeldiev]# 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@mgurbangeldiev mgurbangeldiev]#
```

Figure 2.6: Определение типов файлов и поддиректорий

7. Определите тип файлов, находящихся в директории /var/www/html:

`ls -lZ /var/www/html` (рис. 2.7)

8. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html.

```
[root@mgurbangeldiev html]# ls -lZ /var/www/html
[root@mgurbangeldiev html]#
```

Figure 2.7: Определение типов файлов и поддиректорий

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: (рис. 2.8)

test

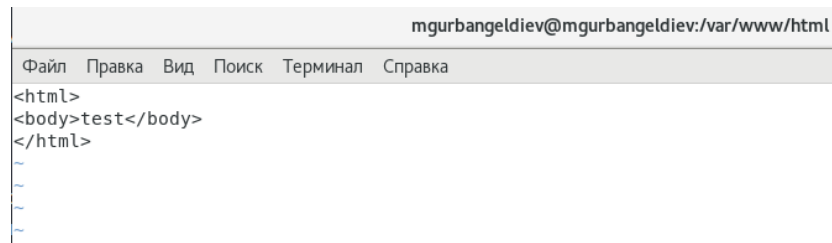


Figure 2.8: Файл test.html

10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории

/var/www/html (рис. 2.9)

```
[root@mgurbangeldiev html]# ls -lZ /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@mgurbangeldiev html]#
```

Figure 2.9: Контекст файла

11. Обратитесь к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Убедитесь, что файл был успешно отображён. (рис. 2.10)

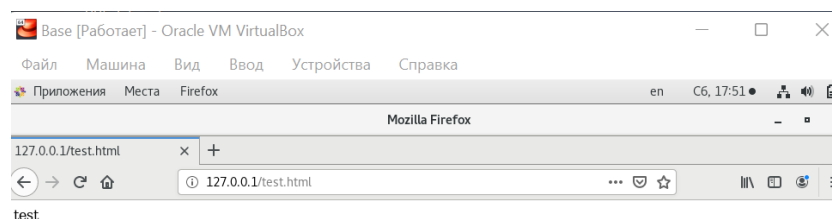


Figure 2.10: Обращение к файлу через браузер

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 `/ргос` файлы, относящиеся к процессам, могут иметь роль `system_r`. Если активна политика MLS, то могут использоваться и другие роли, например, `secadm_r`. Данный случай мы рассматривать не будем, как и предназначение `:s0`).

Тип `httpd_sys_content_t` позволяет процессу `httpd` получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.

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`: (рис. 2.11)

```
chcon -t samba_share_t /var/www/html/test.html
```

```
ls -Z /var/www/html/test.html
```

После этого проверьте, что контекст поменялся

```
[root@mgurbangeldiev html]# chcon -t samba_share_t /var/www/html/test.html
[root@mgurbangeldiev html]# 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
[root@mgurbangeldiev html]# █
```

Figure 2.11: Изменение контекста файла

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: (рис. 2.12)

Forbidden

You don't have permission to access /test.html on this server.



Figure 2.12: Обращение к файлу через браузер

15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? (рис. 2.13) (рис. 2.14)

```
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 `auditd`, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. Проверьте это утверждение самостоятельно.

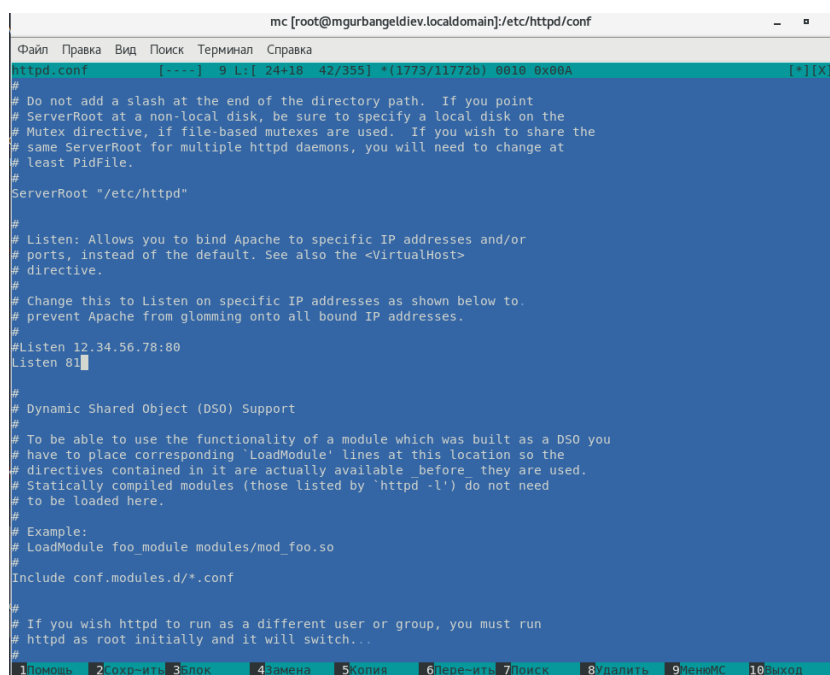
```
[root@mgurbangeldiev html]# chcon -t samba_share_t /var/www/html/test.html
[root@mgurbangeldiev html]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@mgurbangeldiev html]#
```

Figure 2.13: Права доступа

```
mgurbangeldiev@mgurbangeldiev:/var/www/html
Файл Правка Вид Поиск Терминал Справка
[root@mgurbangeldiev html]# tail /var/log/messages
Nov 27 17:59:19 mgurbangeldiev setroubleshoot: SELinux is preventing httpd from getattr access on the file
/var/www/html/test.html. For complete SELinux messages run: sealert -l e08b0f50-a6e6-4061-b835-7dffe2379b6e
Nov 27 17:59:19 mgurbangeldiev python: SELinux is preventing httpd from getattr access on the file /var/www
/html/test.html.#012#012***** Plugin restorecon (92.2 confidence) suggests *****#012#
012If you want to fix the label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#0
12Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to
access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/r
estorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggests *****
*****#012#012If you want to treat test.html as public_content#012Then you need to change the labe
l on test.html to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_conten
t_t /var/www/html/test.html#012# restorecon -v '/var/www/html/test.html'#012#012***** Plugin catchall (1
.41 confidence) suggests *****#012#012If you believe that httpd should be allowed ge
tattr access 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 executing:#012# ausearch
-c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -i my-httpd.pp#012
Nov 27 17:59:31 mgurbangeldiev dbus[746]: [system] Activating service name='org.fedoraproject.Setroubleshoo
td' (using servicehelper)
Nov 27 17:59:32 mgurbangeldiev dbus[746]: [system] Successfully activated service 'org.fedoraproject.Setrou
bleshootd'
Nov 27 17:59:33 mgurbangeldiev setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Nov 27 17:59:33 mgurbangeldiev setroubleshoot: SELinux is preventing httpd from getattr access on the file
/var/www/html/test.html. For complete SELinux messages run: sealert -l e08b0f50-a6e6-4061-b835-7dffe2379b6e
Nov 27 17:59:33 mgurbangeldiev python: SELinux is preventing httpd from getattr access on the file /var/www
/html/test.html.#012#012***** Plugin restorecon (92.2 confidence) suggests *****#012#
012If you want to fix the label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#0
12Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to
access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/r
estorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggests *****
*****#012#012If you want to treat test.html as public_content#012Then you need to change the labe
l on test.html to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_conten
t_t /var/www/html/test.html#012# restorecon -v '/var/www/html/test.html'#012#012***** Plugin catchall (1
.41 confidence) suggests *****#012#012If you believe that httpd should be allowed ge
tattr access 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 executing:#012# ausearch
-c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -i my-httpd.pp#012
Nov 27 18:00:01 mgurbangeldiev systemd: Created slice User Slice of root.
Nov 27 18:00:01 mgurbangeldiev systemd: Started Session 10 of user root.
Nov 27 18:00:02 mgurbangeldiev systemd: Removed slice User Slice of root.
[root@mgurbangeldiev html]#
```

Figure 2.14: log-файлы веб-сервера Apache

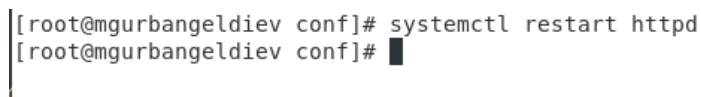
16. Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81. (рис. 2.15)



```
mc [root@mgurbangeldiev.localdomain]:/etc/httpd/conf
Файл Правка Вид Поиск Терминал Справка
httpd.conf [----] 9 L: [ 24+18 42/355] *(1773/11772b) 0010 0x00A [*][X]
#
# 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
# httpd as root initially and it will switch...
#
1Помощь 2Сохранить 3Замок 4Замена 5Копия 6Перезагрузить 7Поиск 8Удалить 9Меню 10Выход
```

Figure 2.15: TCP-порт 81

17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему? (рис. 2.16)

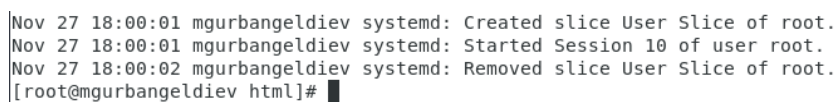


```
[root@mgurbangeldiev conf]# systemctl restart httpd
[root@mgurbangeldiev conf]#
```

Figure 2.16: Перезапуск веб-сервера Apache

Никакого сбоя не произошло.

18. Проанализируйте лог-файлы: (рис. 2.17)



```
Nov 27 18:00:01 mgurbangeldiev systemd: Created slice User Slice of root.
Nov 27 18:00:01 mgurbangeldiev systemd: Started Session 10 of user root.
Nov 27 18:00:02 mgurbangeldiev systemd: Removed slice User Slice of root.
[root@mgurbangeldiev html]#
```

Figure 2.17: log-файлы веб-сервера Apache

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. (рис. 2.18)

```
[root@mgurbangeldiev conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@mgurbangeldiev 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@mgurbangeldiev conf]# █
```

Figure 2.18: Проверка порта

20. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог? (рис. 2.19)

```
[root@mgurbangeldiev conf]# systemctl restart httpd
[root@mgurbangeldiev conf]# █
```

Figure 2.19: Презапущек веб-сервера Apache

21. Верните контекст `httpd_sys_content_t` к файлу `/var/www/html/ test.html`: (рис. 2.20)

```
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». (рис. 2.21)

```
mgurbangeldiev@mgurbangeldiev:/etc/httpd/conf
Файл Правка Вид Поиск Терминал Справка
[root@mgurbangeldiev conf]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@mgurbangeldiev conf]# mc
```

Figure 2.20: Изменение контекста

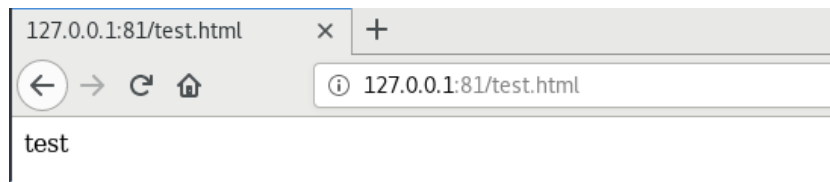


Figure 2.21: Обращение к файлу через браузер

22. Исправьте обратно конфигурационный файл apache, вернув Listen 80. (рис. 2.22)

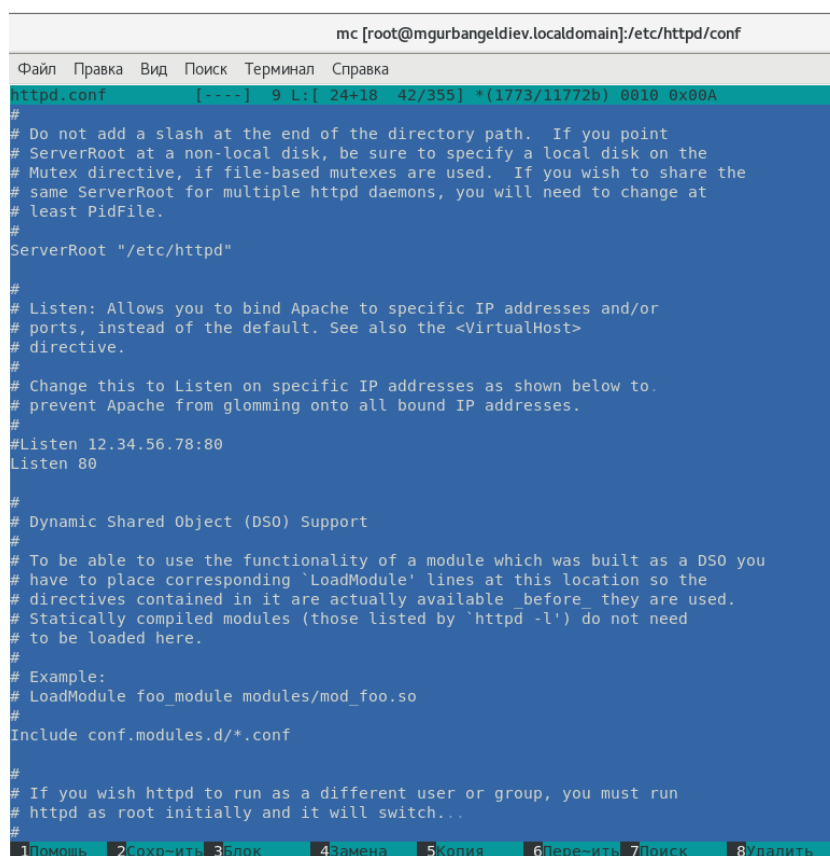


Figure 2.22: TCP-порт 80

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. (рис. 2.23) (рис. 2.24)

```
[root@mgurbangeldiev conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@mgurbangeldiev 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@mgurbangeldiev conf]#
```

Figure 2.23: Удаление TCP-порта 81

```
[root@mgurbangeldiev conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@mgurbangeldiev 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@mgurbangeldiev conf]#
```

Figure 2.24: Удаление TCP-порта 81

24. Удалите файл /var/www/html/test.html:

`rm /var/www/html/test.html` (рис. 2.25)

```
[root@mgurbangeldiev conf]# 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@mgurbangeldiev conf]# ls -lZ /var/www/html/
[root@mgurbangeldiev conf]#
```

Figure 2.25: Удаление файла

3 Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux.

Проверил работу SELinux на практике совместно с веб-сервером Apache.