

# Мандатное разграничение прав в Linux.

---

Гебриал Ибрам<sup>1</sup>

2021 Moscow, Russia

<sup>1</sup>RUDN University, Moscow, Russian Federation

## Цель работы

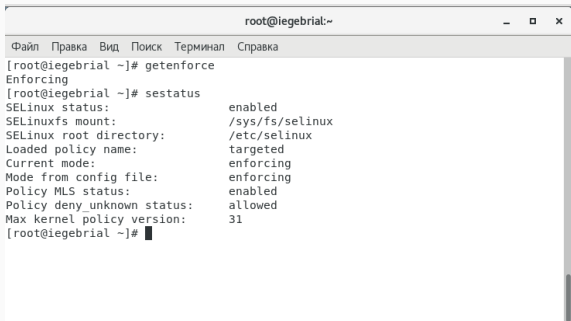
---

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

## Результаты

---

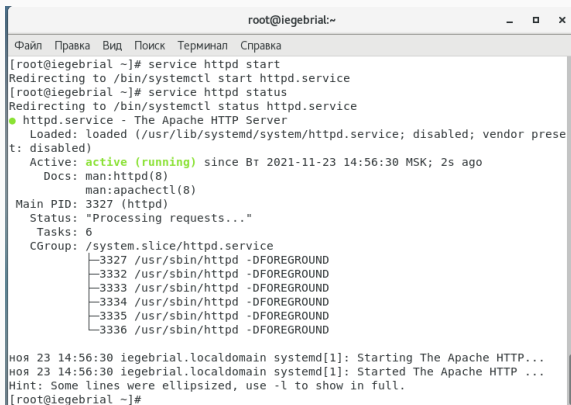
1. Вошёл в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`. (рис. 1)

A screenshot of a terminal window titled 'root@iegebrial:~'. The window has a menu bar with 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal shows the following commands and output:

```
[root@iegebrial ~]# getenforce
Enforcing
[root@iegebrial ~]# 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
[root@iegebrial ~]#
```

Figure 1: Проверка статуса

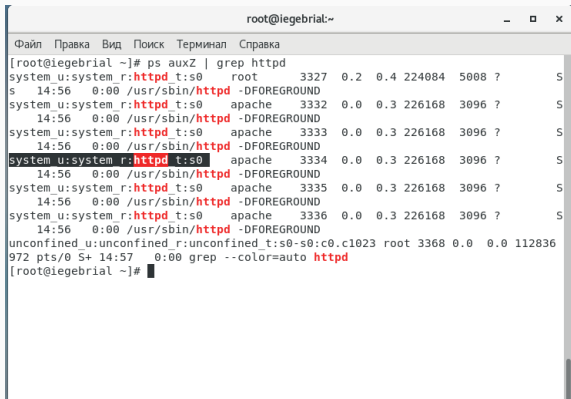
Проверял статус httpd. (рис. 2)



```
root@iegebr1al:~  
Файл Правка Вид Поиск Терминал Справка  
[root@iegebr1al ~]# service httpd start  
Redirecting to /bin/systemctl start httpd.service  
[root@iegebr1al ~]# 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 prese  
t: disabled)  
   Active: active (running) since Вт 2021-11-23 14:56:30 MSK; 2s ago  
     Docs: man:httpd(8)  
           man:apachectl(8)  
 Main PID: 3327 (httpd)  
   Status: "Processing requests..."  
    Tasks: 6  
   CGroup: /system.slice/httpd.service  
           └─3327 /usr/sbin/httpd -DFOREGROUND  
             └─3332 /usr/sbin/httpd -DFOREGROUND  
               └─3333 /usr/sbin/httpd -DFOREGROUND  
                 └─3334 /usr/sbin/httpd -DFOREGROUND  
                   └─3335 /usr/sbin/httpd -DFOREGROUND  
                     └─3336 /usr/sbin/httpd -DFOREGROUND  
  
ноя 23 14:56:30 iegebr1al.localdomain systemd[1]: Starting The Apache HTTP...  
ноя 23 14:56:30 iegebr1al.localdomain systemd[1]: Started The Apache HTTP ...  
Hint: Some lines were ellipsized, use -l to show in full.  
[root@iegebr1al ~]#
```

Figure 2: Запуск и проверка httpd

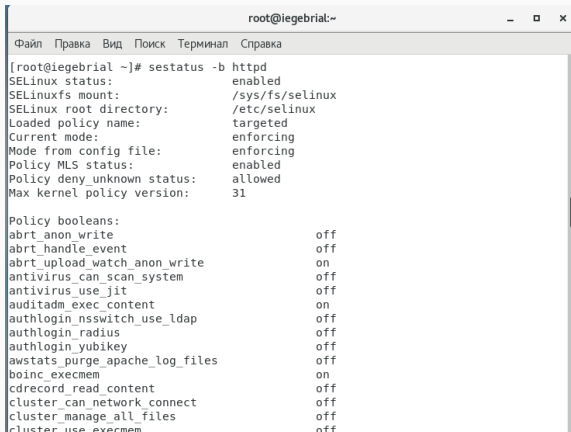
Нашёл веб-сервер Apache в списке процессов, определил его контекст безопасности. (рис. 3)



```
root@iegebrial:~  
[root@iegebrial ~]# ps auxZ | grep httpd  
system_u:system_r:httpd_t:s0 root 3327 0.2 0.4 224084 5008 ? S  
s 14:56 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3332 0.0 0.3 226168 3096 ? S  
14:56 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3333 0.0 0.3 226168 3096 ? S  
14:56 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3334 0.0 0.3 226168 3096 ? S  
14:56 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3335 0.0 0.3 226168 3096 ? S  
14:56 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3336 0.0 0.3 226168 3096 ? S  
14:56 0:00 /usr/sbin/httpd -DFOREGROUND  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 3368 0.0 0.0 112836  
972 pts/0 S+ 14:57 0:00 grep --color=auto httpd  
[root@iegebrial ~]#
```

Figure 3: Контекст безопасности

Посмотрел текущее состояние переключателей SELinux для Apache. (рис. 4)

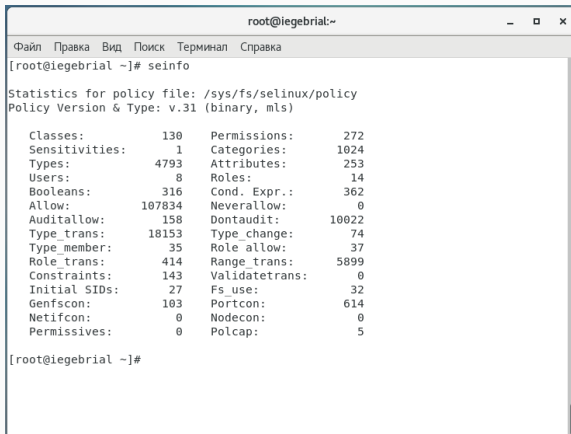


```
root@iegebrial:~  
[root@iegebrial ~]# sestatus -b httpd  
SELinux status:                enabled  
SELinuxfs mount:                /sys/fs/selinux  
SELinux root directory:         /etc/selinux  
Loaded policy name:              targeted  
Current mode:                   enforcing  
Mode from config file:          enforcing  
Policy MLS status:              enabled  
Policy deny_unknown status:     allowed  
Max kernel policy version:      31  
  
Policy booleans:  
abrt_anon_write                  off  
abrt_handle_event                off  
abrt_upload_watch_anon_write     on  
antivirus_can_scan_system        off  
antivirus_use_jit                off  
auditadm_exec_content            on  
authlogin_nsswitch_use_ldap      off  
authlogin_radius                 off  
authlogin_yubikey                off  
awstats_purge_apache_log_files  off  
boinc_execmem                    on  
cdrecord_read_content            off  
cluster_can_network_connect      off  
cluster_manage_all_files         off  
cluster_use_execmem              off
```

Figure 4: Просмотр состояния переключателей SELinux для Apache



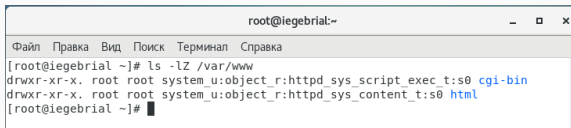
Посмотрел статистику по политике с помощью команды seinfo (рис. 5)



```
root@iegebrial:~  
Файл Правка Вид Поиск Терминал Справка  
[root@iegebrial ~]# 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  
  
[root@iegebrial ~]#
```

Figure 5: Просмотр статистики по политике с помощью команды seinfo

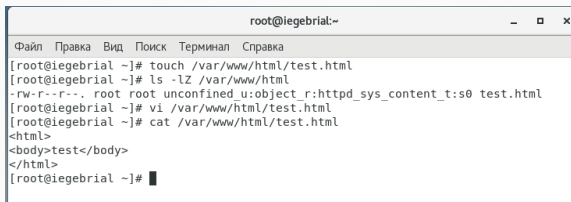
Определил тип файлов и поддиректорий, находящихся в директории /var/www (рис. 6)



```
root@iegebrial:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[root@iegebrial ~]# 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@iegebrial ~]#
```

**Figure 6:** Определение типа файлов и поддиректорий, находящихся в директории /var/www

Создал html-файл /var/www/html/test.html. (рис. 7)



```
root@iegebrial:~  
Файл Правка Вид Поиск Терминал Справка  
[root@iegebrial ~]# touch /var/www/html/test.html  
[root@iegebrial ~]# ls -lZ /var/www/html  
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html  
[root@iegebrial ~]# vi /var/www/html/test.html  
[root@iegebrial ~]# cat /var/www/html/test.html  
<html>  
<body>test</body>  
</html>  
[root@iegebrial ~]#
```

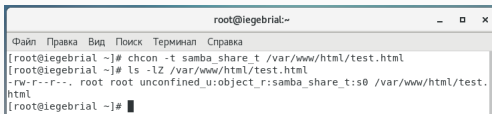
Figure 7: Создание html-файла и проверка его контекста

Обратился к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html` . (рис. 8)



Figure 8: Проверка html-файла в браузере

Изменил контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на любой другой (рис. 9)



```
root@iegebrial:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[root@iegebrial ~]# chcon -t samba_share_t /var/www/html/test.html  
[root@iegebrial ~]# ls -lZ /var/www/html/test.html  
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html  
[root@iegebrial ~]#
```

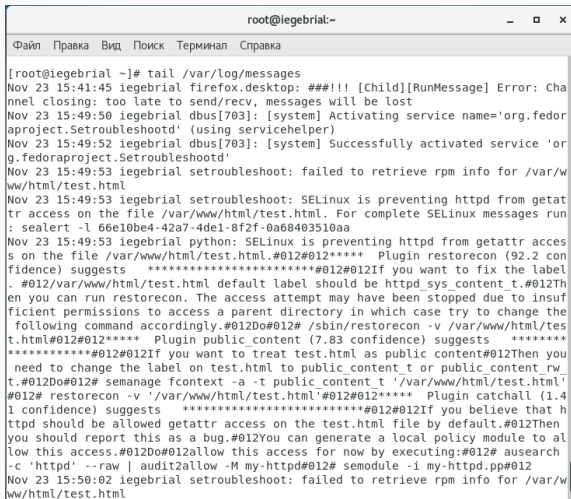
Figure 9: Изменение контекста файла `/var/www/html/test.html` и его проверка

Попробовал ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html` (рис. 10)



Figure 10: Проверка html-файла в браузере

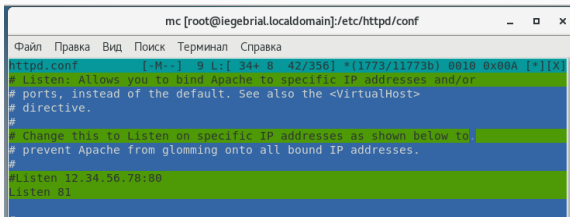
## Просмотрел log-файлы веб-сервера Apache. (рис. 11)



```
root@iegebrial:~  
Файл Правка Вид Поиск Терминал Справка  
[root@iegebrial ~]# tail /var/log/messages  
Nov 23 15:41:45 iegebrial firefox.desktop: ###!!! [Child][RunMessage] Error: Cha  
nnel closing: too late to send/recvd, messages will be lost  
Nov 23 15:49:50 iegebrial dbus[703]: [system] Activating service name='org.fedor  
aproject.Setroubleshootd' (using servicehelper)  
Nov 23 15:49:52 iegebrial dbus[703]: [system] Successfully activated service 'or  
g.fedoraproject.Setroubleshootd'  
Nov 23 15:49:53 iegebrial setroubleshoot: failed to retrieve rpm info for /var/w  
ww/html/test.html  
Nov 23 15:49:53 iegebrial setroubleshoot: SELinux is preventing httpd from getat  
tr access on the file /var/www/html/test.html. For complete SELinux messages run  
: sealert -l 66e10be4-42a7-4de1-8f2f-0a68403510aa  
Nov 23 15:49:53 iegebrial python: SELinux is preventing httpd from getattr acces  
s on the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 con  
fidence) suggests *****#012#012If you want to fix the label  
. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Th  
en you can run restorecon. The access attempt may have been stopped due to insuf  
ficient permissions to access a parent directory in which case try to change the  
following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/tes  
t.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 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# restorecon -v '/var/www/html/test.html'#012#012***** Plugin catchall (1.4  
1 confidence) suggests *****#012#012If you believe that h  
ttpd should be allowed getattr access on the test.html file by default.#012Then  
you should report this as a bug.#012You can generate a local policy module to al  
low 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 23 15:50:02 iegebrial setroubleshoot: failed to retrieve rpm info for /var/w  
ww/html/test.html
```

Figure 11: Проверка логи /var/log/messages

Открыл файл /etc/httpd/httpd.conf нашёл строчку Listen 80 и заменил её на Listen 81. (рис. 12)



```
mc [root@iegebril.localdomain]:/etc/httpd/conf
Файл Правка Вид Поиск Терминал Справка
httpd.conf [-M-~] 9 L:[ 34+ 8 42/356] *(1773/11773b) 0010 0x00A [X]
# 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
#
```

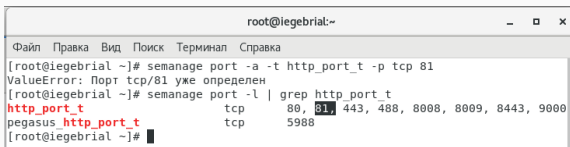
Figure 12: Замена порта прослушивание TCP

Проанализировал лог-файлы. (рис. 13)

```
[root@iegebrial ~]# tail -n1 /var/log/messages
Nov 23 16:01:08 iegebrial systemd: Started The Apache HTTP Server.
[root@iegebrial ~]# cat /var/log/httpd/error_log
```

Figure 13: Анализ лог-файлы

Выполнил команду `semanage port -a -t http_port_t -p tcp 81`. После этого проверил список портов командой. (рис. 14)

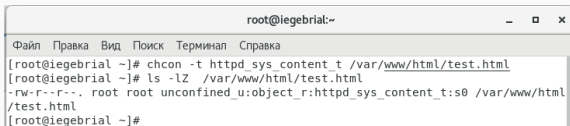


```
root@iegebrial:~  
Файл Правка Вид Поиск Терминал Справка  
[root@iegebrial ~]# semanage port -a -t http_port_t -p tcp 81  
ValueError: Порт tcp/81 уже определен  
[root@iegebrial ~]# semanage port -l | grep http_port_t  
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000  
pegasus_http_port_t  tcp      5988  
[root@iegebrial ~]#
```

Figure 14: Добавление порта 81 и проверка список портов



Вернул контекст `httpd_sys_content_t` к файлу `/var/www/html/ test.html` (рис. 15)



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

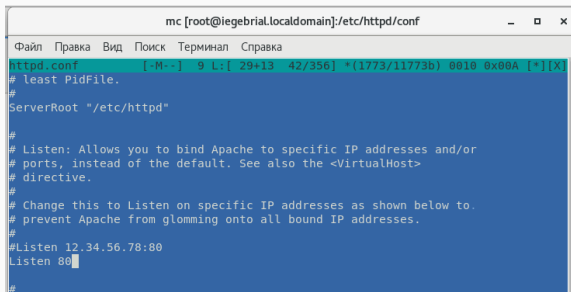
Figure 15: Возвращение контекста файла

Попробовал получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html` (рис. 16)



Figure 16: Попытка получения доступа к файлу через веб-сервер

Исправил обратно конфигурационный файл apache, вернув Listen 80.(рис. 17)



```
mc [root@iegebrial.localdomain]:/etc/httpd/conf
Файл Правка Вид Поиск Терминал Справка
httpd.conf [-M--] 9 L:[ 29+13 42/356] *(1773/11773b) 0010 0x00A [*][X]
# 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
#
```

Figure 17: Исправления обратно конфигурационный файл apache

Удалил привязку `http_port_t` к 81 порту и удалил файл `/var/www/html/test.html`. (рис. 18)

A terminal window titled 'root@iegebrial:/etc/httpd/conf' with standard window controls. The terminal shows a sequence of commands and their outputs. First, the user runs 'semanage port -d -t http\_port\_t -p tcp 81', which results in a 'ValueError' message stating that the port is defined in the policy and cannot be removed. Next, the user runs 'rm /var/www/html/test.html', which prompts for confirmation to delete the file. The user responds with 'y', and the command completes successfully.

```
root@iegebrial:/etc/httpd/conf
Файл Правка Вид Поиск Терминал Справка
[root@iegebrial 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@iegebrial conf]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
[root@iegebrial conf]#
```

Figure 18: Удаление привязки `http_port_t` к 81 порту и файла `/var/www/html/test.html`

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinux на практике совместно с веб-сервером Apache.

Спасибо за внимание