

# Отчет по лабораторной работе №6

---

Дерябина Мария

2021

RUDN University, Moscow, Russian Federation

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

# Выполнение. Изучение политики и контекста SELinux

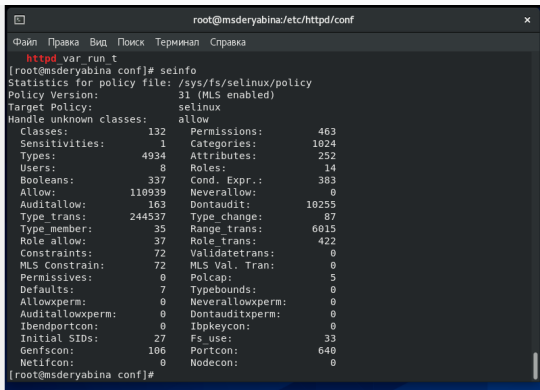
Вошла в систему и убедилась, что SELinux работает в режиме enforcing политики targeted. Запустила веб-сервер Apache. Нашла веб-сервер в списке процессов. Его контекст безопасности - “system\_u:system\_r:httpd\_t:s0”

```
[root@msderyabina conf]# ps -eZ | grep httpd
system_u:system_r:httpd_t:s0      32930 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      32931 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      32932 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      32933 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      32934 ?        00:00:00 httpd
```

**Figure 1:** Контекст безопасности веб-сервера Apache

# Выполнение. Изучение политики и контекста SELinux

Посмотрела статистику по политике. Количество пользователей - 8, ролей - 14, типов - 4934



```
root@msderyabina:/etc/httpd/conf
Файл Правка Вид Поиск Терминал Справка
httpd_var_run_t
[root@msderyabina conf]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version: 31 (MLS enabled)
Target Policy: selinux
Handle unknown classes: allow
Classes: 132 Permissions: 463
Sensitivities: 1 Categories: 1024
Types: 4934 Attributes: 252
Users: 8 Roles: 14
Booleans: 337 Cond. Expr.: 383
Allow: 110939 Neverallow: 0
Auditallow: 163 Dontaudit: 10255
Type_trans: 244537 Type_change: 87
Type_member: 35 Range_trans: 6015
Role allow: 37 Role_trans: 422
Constraints: 72 Validatetrans: 0
MLS Constraint: 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: 33
Genfscon: 106 Portcon: 640
Netifcon: 0 Nodecon: 0
[root@msderyabina conf]#
```

Figure 2: Статистика по политике SELinux

# Выполнение. Изучение политики и контекста SELinux

Определила тип поддиректорий, находящихся в директории /var/www. Тип каталога cgi-bin - httpd\_sys\_script\_exec\_t, тип каталога html - httpd\_sys\_content\_t

```
[root@msderyabina conf]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 12 07:58 cg
i-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ноя 12 07:58 ht
ml
[root@msderyabina conf]# ls -lZ /var/www/html
итого 0
[root@msderyabina conf]# ls -lZ /var/www/html
```

**Figure 3:** Типы поддиректорий в директории /var/www

## Выполнение. Изучение политики и контекста SELinux

От имени суперпользователя создала файл test.html. Контекст созданного файла - `unconfined_u:object_r:httpd_sys_content_t:s0`. Так как по умолчанию пользователи CentOS являются свободными от типа, созданному файлу test.html был сопоставлен пользователь `unconfined_u`. Роль `object_r` используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. Тип `httpd_sys_content_t` позволяет процессу `httpd` получить доступ к файлу. Благодаря наличию последнего типа можно получить доступ к файлу при обращении к нему через браузер

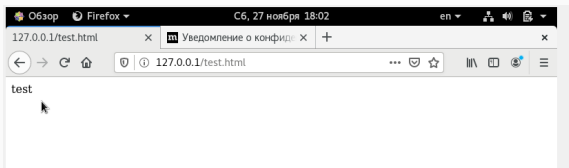
A terminal window showing the command 'ls -lZ' and its output. The output line for 'test.html' shows the SELinux context 'unconfined\_u:object\_r:httpd\_sys\_content\_t:s0'.

```
[root@msderyabina html]# ls -lZ
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 ноя 27 17:54 test.html
[root@msderyabina html]#
[root@msderyabina html]#
```

**Figure 4:** Контекст файла test.html

# Выполнение. Изучение политики и контекста SELinux

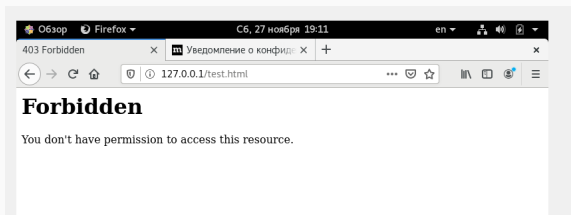
Обратилась к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`



**Figure 5:** Доступ к файлу `test.html` через браузер

## Выполнение. Изучение политики и контекста SELinux

Изменила контекст файла `test.html` на `samba_share_t`, к которому процесс `httpd` не должен иметь доступа. Снова попробовала получить доступ к файлу через браузер, получила сообщение об ошибке. В системном логе появилась информация о необходимости сменить тип файла `test.html`, чтобы демон `httpd` мог к нему обращаться

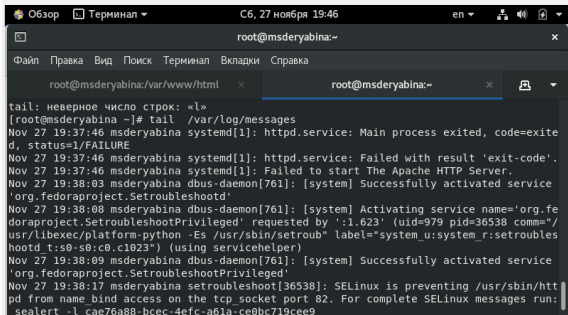


**Figure 6:** Сообщение об ошибке после смены контекста



# Выполнение. Изменение ТСП-порта

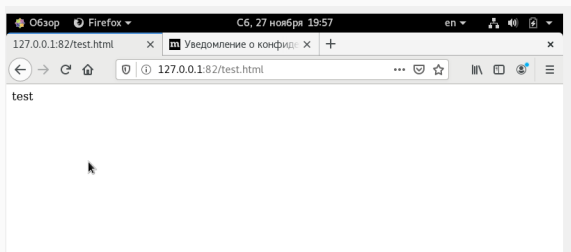
В соответствии с новой политикой, порт 81 входит в список портов по умолчанию, поэтому я изменила порт с 80 на 82 в файле `/etc/httpd/conf/httpd.conf`. При перезапуске веб-сервера произошел сбой. В файле `/var/log/messages` появилась запись о запрете доступа через порт 82 и необходимости изменить тип порта. В файле `/var/log/audit/audit.log` появилась запись о неудачной попытке запуска веб-сервера



```
Обзор Терминал C6, 27 ноября 19:46 en
root@msderyabina:~
Файл Правка Вид Поиск Терминал Вкладки Справка
root@msderyabina:/var/www/html root@msderyabina:~
tail: неверное число строк: «1»
[root@msderyabina ~]# tail /var/log/messages
Nov 27 19:37:46 msderyabina systemd[1]: httpd.service: Main process exited, code=exited, status=1/FAILURE
Nov 27 19:37:46 msderyabina systemd[1]: httpd.service: Failed with result 'exit-code'.
Nov 27 19:37:46 msderyabina systemd[1]: Failed to start The Apache HTTP Server.
Nov 27 19:38:03 msderyabina dbus-daemon[761]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Nov 27 19:38:08 msderyabina dbus-daemon[761]: [system] Activating service name='org.fedoraproject.SetroubleshootPrivileged' requested by ':1.623' (uid=979 pid=36538 comm="/usr/libexec/platform-python -Es /usr/sbin/setroub label=system_u:system_r:setroubleshootd t:s0-s0:c0.c1023") (using servicehelper)
Nov 27 19:38:09 msderyabina dbus-daemon[761]: [system] Successfully activated service 'org.fedoraproject.SetroubleshootPrivileged'
Nov 27 19:38:17 msderyabina setroubleshoot[36538]: SELinux is preventing /usr/sbin/httpd from name_bind access on the tcp_socket port 82. For complete SELinux messages run:
sealert -l cae76a88-bcec-4efc-a61a-ce0bc719cee9
```

## Выполнение. Изменение TCP-порта

Добавила порт 82 к списку портов `http_port_t`. После этого удалось запустить веб-сервер. Вернула контекст `httpd_sys_content__t` к файлу `/var/www/html/ test.html` и попробовала получить доступ к файлу через веб-сервер, введя в браузере `http://127.0.0.1:82/test.html`



**Figure 8:** Доступ к файлу `test.html` через 82 порт

- Я развила навыки администрирования ОС Linux.
- Получила практическое знакомство с технологией SELinux.
- Проверила работу SELinux на практике совместно с веб-сервером Apache.