

# Лабораторная работа № 6.

---

Серегин Д.А.

14 октября 2023

Российский университет дружбы народов, Москва, Россия

## Цель работы

---

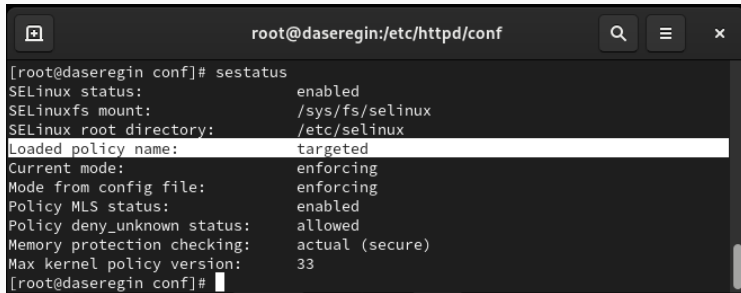
Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache.

## Выполнение работы

---

Перед выполнением лабораторной работы я подготовил виртуальную машину в соответствии с указаниями к лабораторной работе

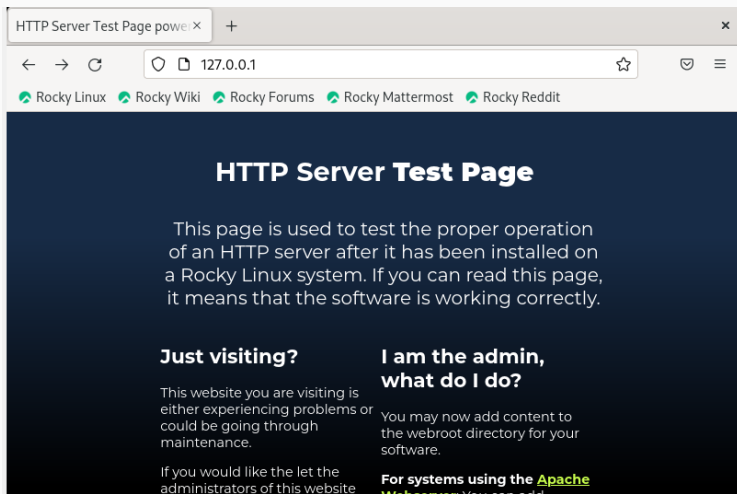
1. Вошел в систему с полученными учётными данными и убедился, что SELinux работает в режиме enforcing политики targeted.

A terminal window titled 'root@daseregin:/etc/httpd/conf' with search, menu, and close icons in the title bar. The terminal shows the command 'sestatus' being executed, displaying the following SELinux configuration details:

```
[root@daseregin 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@daseregin conf]#
```

Рис. 1: Режим и политика SELinux

2. Проверил работу веб-сервера с помощью браузера, убедившись, что он успешно работает.



### 3. Нашел процесс веб-сервера Apache в списке процессов.

```
[root@daseregin init.d]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root      40639  0.0  0.5  20116 11360 ?
Ss  21:20   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    40640  0.0  0.3  21600  7380 ?
S   21:20   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    40641  0.0  0.6 1210508 13008 ?
Sl  21:20   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    40642  0.0  0.5 1079372 10960 ?
Sl  21:20   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    40643  0.0  0.5 1079372 10960 ?
Sl  21:20   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root  41120  0.0  0.1 221796
2296 pts/0  S+  21:25   0:00 grep --color=auto httpd
[root@daseregin init.d]#
```

Рис. 3: Процесс веб-сервера Apache



4. Проверил текущее состояние переключателей SELinux для Apache с использованием команды `sestatus -bigrep httpd`.

```
[root@daseregin init.d]# 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_manage_courier_spool 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_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
```

5. Получил статистику по политике с помощью команды `seinfo` и определил множество пользователей, ролей и типов.

```
[root@daseregin init.d]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:                  135      Permissions:              457
Sensitivities:            1        Categories:              1024
Types:                    5100     Attributes:               258
Users:                    8         Roles:                    14
Booleans:                 353      Cond. Expr.:             384
Allow:                    65000    Neverallow:               0
Auditallow:               170      Dontaudit:               8572
Type_trans:               265341   Type_change:              87
Type_member:              35       Range_trans:             6164
Role_allow:               38       Role_trans:              420
Constraints:              70       Validatetrans:            0
MLS Constrain:            72       MLS Val. Tran:            0
Permissives:              2        Polcap:                   6
Defaults:                 7        Typebounds:               0
Allowxperm:               0        Neverallowxperm:          0
Auditallowxperm:          0        Dontauditxperm:           0
```

6. Определил тип файлов и поддиректорий в директории `/var/www` с помощью команды `ls -lZ /var/www`.

```
[root@daseregin init.d]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 23:
21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 May 16 23:
21 html
```

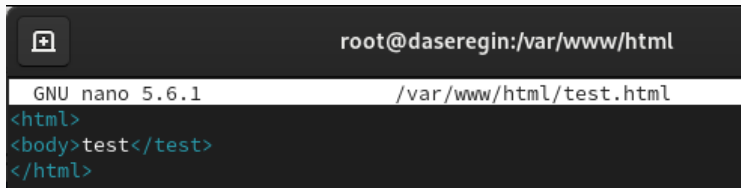
Рис. 6: Типы файлов

7. Определил тип файлов в директории `/var/www/html` с помощью команды `ls -lZ /var/www/html`. Как видим папка пуста.

```
[root@daseregin init.d]# ls -lZ /var/www/html
total 0
```

Рис. 7: Типы файлов

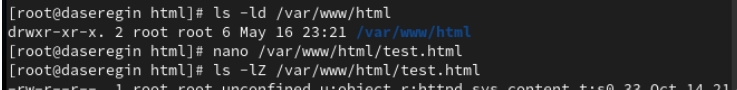
9. Создал от имени суперпользователя файл `/var/www/html/test.html` с указанным содержанием.



```
root@daseregin:/var/www/html
GNU nano 5.6.1 /var/www/html/test.html
<html>
<body>test</body>
</html>
```

Рис. 9: Файл test.html

10. Проверил контекст созданного файла, внес контекст, присваиваемый по умолчанию новым файлам в директории `/var/www/html`



```
[root@daseregin html]# ls -ld /var/www/html
drwxr-xr-x. 2 root root 6 May 16 23:21 /var/www/html
[root@daseregin html]# nano /var/www/html/test.html
[root@daseregin html]# ls -lZ /var/www/html/test.html
-rw-r--r-- 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct 14 21:14
```

11. Обратился к файлу через веб-сервер, введя в браузере соответствующий адрес, и убедился, что файл был успешно отображён.

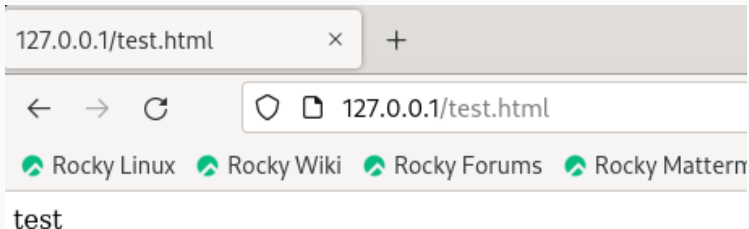


Рис. 11: Отображение файла

12. Изучил справку `man httpd_selinux` и сопоставил контексты файлов для `httpd`. Проверил контекст файла с помощью команды `ls -Z /var/www/html/test.html`.

```
[root@daseregin html]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

13. Изменил контекст файла `/var/www/html/test.html` на другой, к которому процессу `httpd` не должен иметь доступа, и проверил изменение контекста.
14. Попытался снова получить доступ к файлу через веб-сервер и убедился, что была выдана ошибка “Forbidden”.

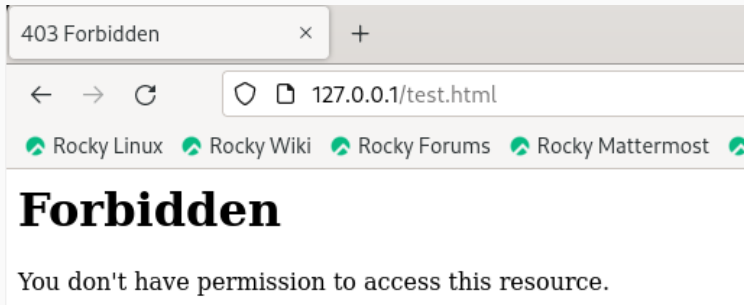
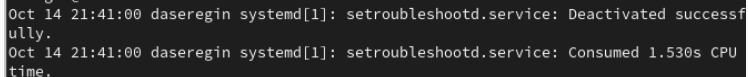


Рис. 13: Ошибка доступа

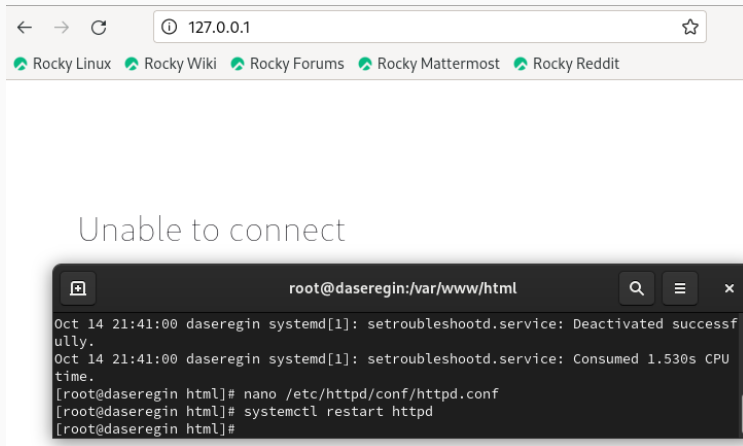
15. Проанализировал ситуацию и выяснил, что файл не был отображен, несмотря на права доступа, изучив логи веб-сервера и системные логи.

A screenshot of a terminal window displaying system logs. The logs show two entries from 'daseregin systemd[1]' regarding the 'setroubleshootd.service'. The first entry states 'Deactivated successfully.' and the second entry states 'Consumed 1.530s CPU time.'

```
Oct 14 21:41:00 daseregin systemd[1]: setroubleshootd.service: Deactivated successfully.  
Oct 14 21:41:00 daseregin systemd[1]: setroubleshootd.service: Consumed 1.530s CPU time.
```

Рис. 14: Логи веб-сервера

16. Попытался запустить веб-сервер Apache на прослушивание TCP-порта 81 и выяснил, что возник сбой. Так как порт не является стандартным.





17. Проанализировал логи и выяснил причину сбоя при попытке изменения порта прослушивания.

```
Oct 14 21:46:01 daseregin systemd[1]: Stopping The Apache HTTP Server...
Oct 14 21:46:02 daseregin systemd[1]: httpd.service: Deactivated successfully.
Oct 14 21:46:02 daseregin systemd[1]: Stopped The Apache HTTP Server.
Oct 14 21:46:02 daseregin systemd[1]: httpd.service: Consumed 1.242s CPU time.
Oct 14 21:46:02 daseregin systemd[1]: Starting The Apache HTTP Server...
Oct 14 21:46:02 daseregin systemd[1]: Started The Apache HTTP Server.
Oct 14 21:46:02 daseregin httpd[42141]: Server configured, listening on: port 81
```

Рис. 16: Логи Apache

18. Проанализировал логи веб-сервера Apache и системные логи, определив, где появились новые записи.

19. Выполнил команду `semanage port -a -t http_port_t -p tcp 81` и убедился, что порт 81 добавлен.

```
[root@daseregin html]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@daseregin html]# semanage port -l | grep http_port_t
http_port_t          tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
```

Рис. 17: Добавления порта 81 в разрешенные

20. Попытался снова запустить веб-сервер Apache и убедился, что он запустился успешно.

21. Вернул контекст файла `/var/www/html/test.html` к исходному, предварительно изменив его на `samba_share_t`.
22. Изменил обратно конфигурационный файл Apache, вернув порт прослушивания к 80.
23. Удалил привязку `http_port_t` к порту 81.
24. Удалил файл `/var/www/html/test.html`.

## Вывод

---

В результате выполнения работы я развил свои навыки администрирования Linux, смог настроить SELinux, а также поработать с веб-сервисом Apache.