

Мандатное разграничение прав в Linux

Бансимба Клодели Дъегра НПИбд-02-22¹

27 апреля 2024, Москва, Россия

¹Российский Университет Дружбы Народов

Информация

- Бансимба Клодели Дьегра
- Студент, НПИбд-02-22
- Российский университет дружбы народов
- 1032215651@pfur.ru



Цели и задачи работы

Цель лабораторной работы

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

Процесс выполнения лабораторной работы

Запуск http

Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing

```
claudeybansimba@claudey:~$ /bin/systemctl status httpd.service

[claudeybansimba@claudey ~]$ getenforce
Enforcing
[claudeybansimba@claudey ~]$ 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
[claudeybansimba@claudey ~]$
[claudeybansimba@claudey ~]$ 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; preset: disabled)
   Active: inactive (dead)
   Docs: man:httpd.service(8)

[1]• Stopped service httpd status
[claudeybansimba@claudey ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service

[claudeybansimba@claudey ~]$
[claudeybansimba@claudey ~]$ 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; preset: disabled)
   Active: active (running) since Sat 2024-04-27 17:23:49 MSK; 4s ago
   Docs: man:httpd.service(8)
  Main PID: 34920 (httpd)
   Status: "Started, listening on: port 80"
    Tasks: 213 (limit: 23033)
   Memory: 35.5M
      CPU: 136ms
   CGroup: /system.slice/httpd.service
           └─34920 /usr/sbin/httpd -DFOREGROUND
             └─34920 /usr/sbin/httpd -DFOREGROUND
               └─34920 /usr/sbin/httpd -DFOREGROUND
```

Рис. 1: запуск http

Посмотрели текущее состояние переключателей SELinux для Apache

```
[3]+ Stopped service httpd status
[claudelybansimba@claudely ~]$ ps auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 claudel+ 34874 0.0 0.2 23622
0 8760 pts/1 T 17:23 0:00 /bin/systemctl status httpd.service
system_u:system_r:httpd_t:s0 root 34920 0.0 0.3 20332 11604 ? Ss
17:23 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 34928 0.0 0.1 21668 7432 ? S
17:23 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 34929 0.0 0.4 2455800 15220 ? Sl
17:23 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 34930 0.0 0.4 2259128 17264 ? Sl
17:23 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 34931 0.0 0.4 2259128 15224 ? Sl
17:23 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 claudel+ 35168 0.0 0.2 23622
0 8992 pts/1 T 17:23 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 claudel+ 35222 0.0 0.2 23622
0 8972 pts/1 T 17:26 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 claudel+ 35242 0.0 0.0 22166
4 2296 pts/1 S+ 17:27 0:00 grep --color=auto httpd
[claudelybansimba@claudely ~]$
[claudelybansimba@claudely ~]$
[claudelybansimba@claudely ~]$ 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.
[claudelybansimba@claudely ~]$
```

Рис. 2: переключатели SELinux для http

переключатели SELinux для http

Посмотрели статистику по политике с помощью команды seinfo

```
[claudelybansimba@claudely ~]$  
[claudelybansimba@claudely ~]$ 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:                65009 Neverallow:      0  
Auditallow:           170 Dontaudit:      8572  
Type_trans:           265337 Type_change:    87  
Type_member:           35  Range_trans:   6164  
Role allow:           38  Role_trans:    420  
Constraints:          70  Validatetrans: 0  
MLS Constrains:       72  MLS Val. Tran: 0  
Permissives:          2   Polcap:         6  
Defaults:             7   Typebounds:     0  
Allowxperm:           0   Neverallowxperm: 0  
Auditallowxperm:      0   Dontauditxperm: 0  
Ibendportcon:         0   Ibpkeycon:       0  
Initial SIDs:         27  Fs_use:         35  
Genfscon:             109 Portcon:         660  
Netifcon:             0   Nodecon:         0  
[claudelybansimba@claudely ~]$  
[claudelybansimba@claudely ~]$ ls -lZ /var/www  
total 0  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Oct 28 12:35  
  cgi-bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Oct 28 12:35  
  html  
[claudelybansimba@claudely ~]$  
[claudelybansimba@claudely ~]$
```

Рис. 3: переключатели SELinux для http

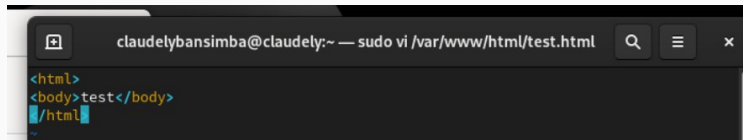
создание html-файла и доступ по http

создание html-файла и доступ по http

```
[claudelybansimba@claudely ~]$  
[claudelybansimba@claudely ~]$ ls -lZ /var/www  
total 0  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Oct 28 12:35  
  cgi-bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 Oct 28 12:35  
  html  
[claudelybansimba@claudely ~]$  
[claudelybansimba@claudely ~]$ ls -lZ /var/www/html  
total 0  
[claudelybansimba@claudely ~]$  
[claudelybansimba@claudely ~]$  
[claudelybansimba@claudely ~]$  
[claudelybansimba@claudely ~]$  
[claudelybansimba@claudely ~]$ sudo touch /var/www/html/test.html  
[sudo] password for claudelybansimba:  
[claudelybansimba@claudely ~]$ sudo vi /var/www/html/test.html  
[claudelybansimba@claudely ~]$
```

Рис. 4: создание html-файла и доступ по http

создание html-файла и доступ по http

A screenshot of a terminal window with a dark background. The title bar at the top shows the user 'claudelybansimba' at host 'claudely', with the command 'sudo vi /var/www/html/test.html' and search, menu, and close icons. The terminal content shows the first three lines of an HTML document: '<html>', '<body>test</body>', and '/html' with a blue cursor at the end of the third line.

```
claudelybansimba@claudely:~ — sudo vi /var/www/html/test.html
<html>
<body>test</body>
/html
```

Рис. 5: создание html-файла и доступ по http

успешно отображён

успешно отображён

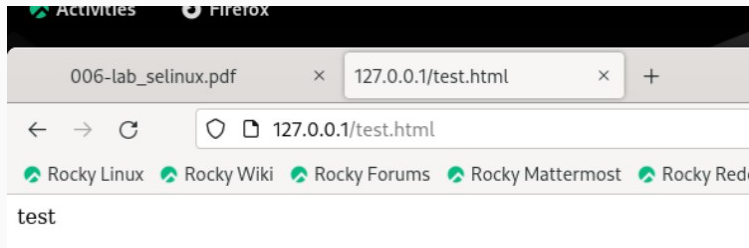
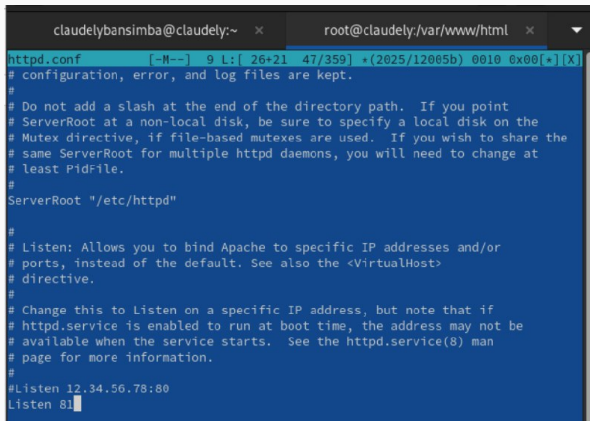


Рис. 6: успешно отображён

Рис. 7: лог ошибок

переключение порта

Для этого в файле `/etc/httpd/httpd.conf` найдите строчку `Listen 80` и замените её на `Listen 81`.



```
claudelybansimba@claudely:~ x root@claudely:/var/www/html x
httpd.conf [-M--] 9 L: [ 26+21 47/359] *(2025/12005b) 0010 0x00[*] [X]
# 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 a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 81
```

Рис. 8: переключение порта

переключение порта

попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test`

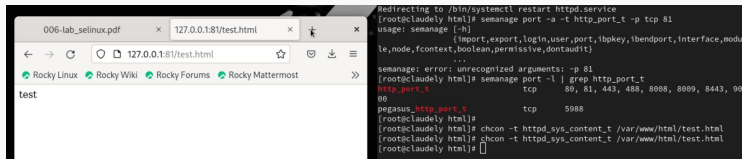


Рис. 9: доступ по http на 81 порт

Выводы по проделанной работе

В процессе выполнения лабораторной работы мною были получены базовые навыки работы с технологией seLinux.