

Знакомство с SELinux

Альсид Мона НФИбд-03-18¹

27 ноября 2021 г., Москва, Россия

¹российский Университет Дружбы Народов

Цели и задачи

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

Выполнения лабораторной работы

```
[root@mona alseedmona]# 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@mona alseedmona]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@mona alseedmona]# 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 Sat 2021-11-27 15:05:26 MSK; 1h 49min ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 1420 (httpd)
    Status: "Total requests: 0; Current requests/sec: 0; Current traffic:  0 B/sec"
    CGroup: /system.slice/httpd.service
            └─1420 /usr/sbin/httpd -DFOREGROUND
              └─1421 /usr/sbin/httpd -DFOREGROUND
                └─1422 /usr/sbin/httpd -DFOREGROUND
                  └─1423 /usr/sbin/httpd -DFOREGROUND
                    └─1424 /usr/sbin/httpd -DFOREGROUND
                      └─1425 /usr/sbin/httpd -DFOREGROUND

Nov 27 15:05:16 mona.localdomain systemd[1]: Starting The Apache HTTP Server...
Nov 27 15:05:21 mona.localdomain httpd[1420]: AH00558: httpd: Could not reliably determine the...age
Nov 27 15:05:26 mona.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@mona alseedmona]#
```

Figure 1: запуск http

```
na html# ls -lZ /var/www
get access var/www: No such file or directory
na html# ls -lZ /var/www
-r-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
-r-x. root root system_u:object_r:httpd_sys_content_t:s0 html
na html# touch test.html
na html# echo "test" >> test.html
na html# ls -lZ /var/www/html/test.html
-r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
na html# chcon -t samba_share_t /var/www/html/test.html
failed to change context of '/var/www/html/test.html' to 'unconfined_u:object_r:samba_share_t:s0':
Invalid argument
na html# ls -lZ /var/www/html/test.html
-r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
na html# ls -l /var/www/html/test.html
-r--. 1 root root 39 Nov 27 18:06 /var/www/html/test.html
na html# _
```



Figure 2: создание html-файла и доступ по http

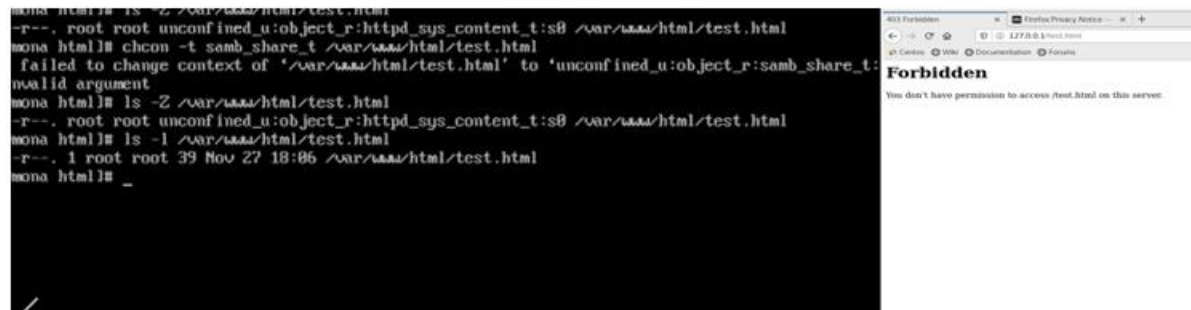


Figure 3: ошибка доступа после изменения контекста

```
[root@mona html]# 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@mona html]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@mona html]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@mona html]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'?
[root@mona html]#
```

Figure 4: доступ по http на 81 порт

Выводы

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