

# Лабораторная работа №6

## Мандатное разграничение прав в Linux

---

Ильин А.В.

14 октября 2023

Российский университет дружбы народов, Москва, Россия

# Информация

---

- Ильин Андрей Владимирович
- НФИбд-01-20
- 1032201656
- Российский Университет Дружбы Народов
- 1032201656@pfur.ru
- <https://github.com/av-ilin>



# **Вводная часть**

---

- Приобрести необходимые в современном научном сообществе навыки администрирования систем и информационной безопасности.

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

1. Настроить и запустить сервер Apache.
2. Исследовать влияние различных параметров на работу сервера.

- Rocky Linux
- Git
- VirtualBox



## **Выполнение работы**

---

# Проверка SELinux. Статус веб-сервера

```
aviljin login: aviljin
Password:
Last login: Sat Oct 14 16:24:16 on tty1
[aviljin@aviljin ~]$ getenforce
Enforcing
[aviljin@aviljin ~]$ 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
[aviljin@aviljin ~]$
```

Рис. 1: Проверка SELinux

```
[aviljin@aviljin ~]$ sudo service httpd start
[sudo] password for aviljin:
Redirecting to /bin/systemctl start httpd.service
[aviljin@aviljin ~]$ 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 2023-10-14 16:39:13 MSK; 11s ago
     Docs: man:httpd.service(8)
   Main PID: 1398 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/s"
     Tasks: 213 (limit: 17404)
    Memory: 37.8M
       CPU: 55ms
    CGroup: /system.slice/httpd.service
            └─1398 /usr/sbin/httpd -DFOREGROUND
              └─1391 /usr/sbin/httpd -DFOREGROUND
                └─1392 /usr/sbin/httpd -DFOREGROUND
                  └─1393 /usr/sbin/httpd -DFOREGROUND
                    └─1395 /usr/sbin/httpd -DFOREGROUND

Oct 14 16:39:13 aviljin systemd[1]: Starting The Apache HTTP Server...
Oct 14 16:39:13 aviljin systemd[1]: Started The Apache HTTP Server.
Oct 14 16:39:13 aviljin httpd[1398]: Server configured, listening on: port 80
```

Рис. 2: Статус веб-сервера

# Контекст безопасности. Переключатели SELinux

```
aviljin@aviljin ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      1390  0.0  0.4 28168 11416 ?        Ss   16:39   0:00 /
usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  1391  0.0  0.2 21600 7120 ?        S    16:39   0:00 /
usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  1392  0.0  0.3 1538124 18064 ?      Sl   16:39   0:00 /
usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  1393  0.0  0.5 1669260 17000 ?      Sl   16:39   0:00 /
usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  1395  0.0  0.5 1538124 17000 ?      Sl   16:39   0:00 /
usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1823 aviljin 1612  0.0  0.0 3076 2824 tty1 S+  16:40
0:00 grep --color=auto httpd
aviljin@aviljin ~]$ _
```

Рис. 3: Контекст безопасности Apache

```
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_avalahi off
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_homedirs off
httpd_execmem off
httpd_graceful_shutdown off
httpd_manage_ipa off
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ipa off
httpd_run_preupgrade off
httpd_run_stickshift off
httpd_serve_cobbler_files off
httpd_setrlimit off
httpd_ssl_exec off
httpd_sys_script_anon_write off
httpd_tmp_exec off
httpd_tty_comm off
httpd_unified off
httpd_use_cifs off
httpd_use_fusefs off
httpd_use_gpg off
httpd_use_nfs off
httpd_use_openscryptoki off
httpd_use_openstack off
httpd_use_sasl off
httpd_verify_dns off
aviljin@aviljin ~]$ _
```

Рис. 4: Переключатели SELinux для Apache

# Статистика по политике. Тип файлов и поддиректорий Apache

```
[aviljin@aviljin ~]$ 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: 1824
Types: 5857 Attributes: 253
Users: 8 Roles: 14
Booleans: 348 Cond. Expr.: 378
Allow: 63159 Neverallow: 8
Auditallow: 163 Dontaudit: 8417
Type_trans: 249586 Type_change: 87
Type_member: 35 Range_trans: 6161
Role_allow: 37 Role_trans: 418
Constraints: 78 Validate_trans: 8
MLS Constrains: 72 MLS Val. Tran: 8
Permissives: 2 Polcap: 6
Defaults: 7 Typebounds: 8
Allowexecperm: 8 Neverallowexecperm: 8
Auditallowexecperm: 8 Dontauditexecperm: 8
lbenportcom: 8 lbpkeycom: 8
Initial SIDs: 27 Fs_use: 35
Genfscom: 189 Portcom: 668
Netifcom: 8 Nodecom: 8
[aviljin@aviljin ~]$ _
```

Рис. 5: Статистика по политике

```
[aviljin@aviljin ~]$ ls -lZ /var/www
total 8
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
[aviljin@aviljin ~]$ ls -lZ /var/www/html
total 8
[aviljin@aviljin ~]$ ls -alF /var/www
total 4
drwxr-xr-x. 4 root root 33 Oct 14 16:28 ./
drwxr-xr-x. 28 root root 4896 Oct 14 16:28 ../
drwxr-xr-x. 2 root root 6 May 16 23:21 cgi-bin/
drwxr-xr-x. 2 root root 6 May 16 23:21 html/
[aviljin@aviljin ~]$
```

Рис. 6: Тип файлов и поддиректорий Apache

# Создание html.test

```
root@aviljin aviljin# cat /var/www/html/test.html
<html>
  <body>
    test
  </body>
</html>
root@aviljin aviljin# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
root@aviljin aviljin# lynx http://127.0.0.1:80/test.html
```

Рис. 7: Создание html.test



Рис. 8: Просмотр <http://127.0.0.1/test.html>  
(1)

# Изменение контекст файла test.html

```
root@aviljin aviljin# chcon -t samba_share_t /var/www/html/test.html
root@aviljin aviljin# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
root@aviljin aviljin# exit
exit
```

**Рис. 9:** Изменение контекст файла test.html



**Рис. 10:** Просмотр <http://127.0.0.1/test.html>  
(2)

# Изменение httpd.conf на прослушивание TCP-порта 81

```
# 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
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available before they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
include conf.modules.d/*/*.conf
```

47,9 7%

Рис. 11: Изменение httpd.conf на прослушивание TCP-порта 81

```
(root@aviljin aviljin)# tail -n5 /var/log/messages
Oct 14 17:15:53 aviljin systemd[1]: httpd.service: Deactivated successfully.
Oct 14 17:15:53 aviljin systemd[1]: Stopped The Apache HTTP Server.
Oct 14 17:15:53 aviljin systemd[1]: Starting The Apache HTTP Server...
Oct 14 17:15:53 aviljin httpd[2856]: Server configured, listening on: port 81
Oct 14 17:15:53 aviljin systemd[1]: Started The Apache HTTP Server.
(root@aviljin aviljin)# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
(root@aviljin aviljin)# semanage port -l | grep http_port_t
http_port_t tcp 80, 81, 443, 488, 8080, 8089, 8443, 9080
pegasus_http_port_t tcp 5988
(root@aviljin aviljin)# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
(root@aviljin aviljin)# chcon -t httpd_sys_content_t /var/www/html/test.html
(root@aviljin aviljin)# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
(root@aviljin aviljin)#
```

Рис. 12: Добавление порта 81 в список портов

## Результаты

---



- Нам удалось развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache. Также мы настроили и запустили сервер Apache. Исследовали влияние различных параметров на работу сервера.

**Спасибо за внимание!**