

# Знакомство с SELinux

---

Кашкин Иван Евгеньевич

12 октября, 2024, Москва, Россия

Российский Университет Дружбы

Народов

# Цели и задачи

---

SELinux или Security Enhanced Linux — это улучшенный механизм управления доступом, разработанный Агентством национальной безопасности США (АНБ США) для предотвращения злонамеренных вторжений. Он реализует принудительную (или мандатную) модель управления доступом (англ. Mandatory Access Control, MAC) поверх существующей дискреционной (или избирательной) модели (англ. Discretionary Access Control, DAC), то есть разрешений на чтение, запись, выполнение.

Apache – это свободное программное обеспечение для размещения веб-сервера. Он хорошо показывает себя в работе с масштабными проектами, поэтому заслуженно считается одним из самых популярных веб-серверов. Кроме того, Apache очень гибок в плане настройки, что даёт возможность реализовать все особенности размещаемого веб-ресурса.

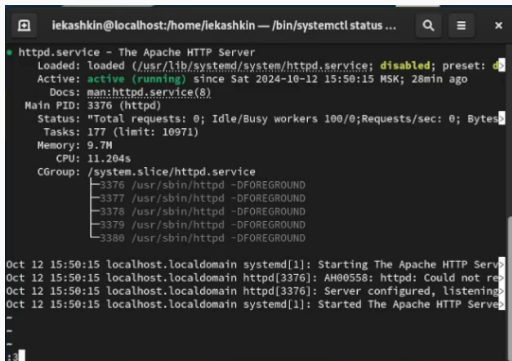
## Цель лабораторной работы

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

# **Выполнение лабораторной работы**

---

# Запуск HTTP-сервера

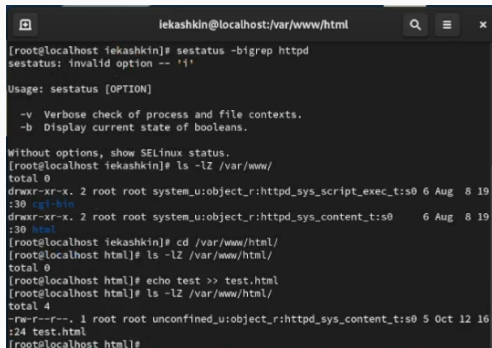
A terminal window titled 'iekashkin@localhost:/home/iekashkin — /bin/systemctl status ...'. It displays the status of the 'httpd.service'. The service is 'active (running)' since Saturday, 2024-10-12 15:50:15 MSK, 28 minutes ago. It shows the main PID as 3376 (httpd) and lists several child processes (3376-3380) running '/usr/sbin/httpd -DFOREGROUND'. At the bottom, there are log messages from 'systemd[1]' showing the service starting and listening on port 80.

```
iekashkin@localhost:/home/iekashkin — /bin/systemctl status ...
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
   Active: active (running) since Sat 2024-10-12 15:50:15 MSK; 28min ago
     Docs: man:httpd.service(8)
   Main PID: 3376 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0"
   Tasks: 177 (limit: 10971)
  Memory: 9.7M
    CPU: 11.204s
   CGroup: /system.slice/httpd.service
           └─3376 /usr/sbin/httpd -DFOREGROUND
             └─3377 /usr/sbin/httpd -DFOREGROUND
               └─3378 /usr/sbin/httpd -DFOREGROUND
                 └─3379 /usr/sbin/httpd -DFOREGROUND
                   └─3380 /usr/sbin/httpd -DFOREGROUND

Oct 12 15:50:15 localhost.localdomain systemd[1]: Starting The Apache HTTP Server:
Oct 12 15:50:15 localhost.localdomain httpd[3376]: AH00558: httpd: Could not re
Oct 12 15:50:15 localhost.localdomain httpd[3376]: Server configured, listening
Oct 12 15:50:15 localhost.localdomain systemd[1]: Started The Apache HTTP Server
-
-
:~
```

Figure 1: запуск http

# Создание HTML-файла



```
iekashkin@localhost:/var/www/html
[root@localhost iekashkin]# sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

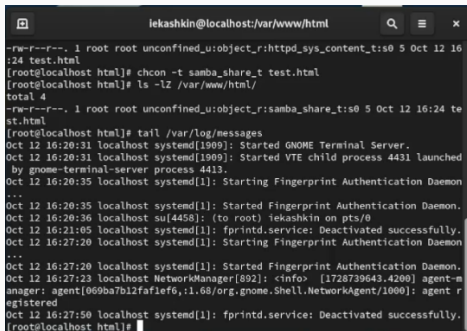
    -v Verbose check of process and file contexts.
    -b Display current state of booleans.

Without options, show SELinux status.
[root@localhost iekashkin]# ls -lZ /var/www/
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Aug 8 19
:30 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Aug 8 19
:30 html
[root@localhost iekashkin]# cd /var/www/html/
[root@localhost html]# ls -lZ /var/www/html/
total 0
[root@localhost html]# echo test >> test.html
[root@localhost html]# ls -lZ /var/www/html/
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 5 Oct 12 16
:24 test.html
[root@localhost html]#
```

Figure 2: создание html-файла и доступ по http



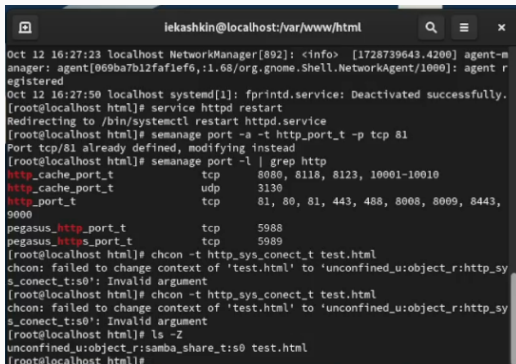
# Изменение контекста безопасности

A terminal window titled 'iekashkin@localhost:/var/www/html' with search, menu, and close icons. It displays a series of commands and system logs. The commands executed are: 'chcon -t samba\_share\_t test.html', 'ls -lZ /var/www/html/', and 'tail /var/log/messages'. The output shows the file permissions for 'test.html' and the system logs for the 'messages' file. The logs indicate that the 'Fingerprint Authentication Daemon' was started and deactivated successfully, and the 'NetworkManager' agent was registered.

```
iekashkin@localhost:/var/www/html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 5 Oct 12 16:24 test.html
[root@localhost html]# chcon -t samba_share_t test.html
[root@localhost html]# ls -lZ /var/www/html/
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 5 Oct 12 16:24 test.html
[root@localhost html]# tail /var/log/messages
Oct 12 16:20:31 localhost systemd[1909]: Started GNOME Terminal Server.
Oct 12 16:20:31 localhost systemd[1909]: Started VTE child process 4431 launched by gnome-terminal-server process 4413.
Oct 12 16:20:35 localhost systemd[1]: Starting Fingerprint Authentication Daemon
...
Oct 12 16:20:35 localhost systemd[1]: Started Fingerprint Authentication Daemon.
Oct 12 16:20:36 localhost su[4458]: (to root) iekashkin on pts/0
Oct 12 16:21:05 localhost systemd[1]: fprintd.service: Deactivated successfully.
Oct 12 16:27:20 localhost systemd[1]: Starting Fingerprint Authentication Daemon
...
Oct 12 16:27:20 localhost systemd[1]: Started Fingerprint Authentication Daemon.
Oct 12 16:27:23 localhost NetworkManager[892]: <info> [1728739643.4200] agent-manager: agent[069ba7b12faf1ef6,1.68/org.gnome.Shell.NetworkAgent/1000]: agent registered
Oct 12 16:27:50 localhost systemd[1]: fprintd.service: Deactivated successfully.
[root@localhost html]#
```

Figure 3: ошибка доступа после изменения контекста

# Переключение порта и восстановление контекста безопасности



```
iekashkin@localhost:/var/www/html
Oct 12 16:27:23 localhost NetworkManager[892]: <info> [1728739643.4200] agent-m
anager: agent[069ba7b12faf1ef6,1.68/org.gnome.Shell.NetworkAgent/1000]: agent r
egistered
Oct 12 16:27:50 localhost systemd[1]: fprintd.service: Deactivated successfully.
[root@localhost html]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@localhost html]# semanage port -a -t http_port_t -p tcp 81
Port tcp/81 already defined, modifying instead
[root@localhost html]# semanage port -l | grep http
http_cache_port_t      tcp      8080, 8118, 8123, 10001-10010
http_cache_port_t      udp      3130
http_port_t            tcp      81, 80, 81, 443, 488, 8008, 8009, 8443,
9000
pegasus_http_port_t    tcp      5988
pegasus_https_port_t   tcp      5989
[root@localhost html]# chcon -t http_sys_connect_t test.html
chcon: failed to change context of 'test.html' to 'unconfined_u:object_r:http_sy
s_connect_t:s0': Invalid argument
[root@localhost html]# chcon -t http_sys_connect_t test.html
chcon: failed to change context of 'test.html' to 'unconfined_u:object_r:http_sy
s_connect_t:s0': Invalid argument
[root@localhost html]# ls -Z
unconfined_u:object_r:samba_share_t:s0 test.html
[root@localhost html]#
```

Figure 4: доступ по http на 81 порт

## **Выводы**

---

## Результаты выполнения лабораторной работы

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