

# Мандатное разграничение прав в Linux

---

Венчаков Никита Юрьевич<sup>1</sup>

10 октября, 2022

<sup>1</sup>Российский университет дружбы народов, Москва, Россия

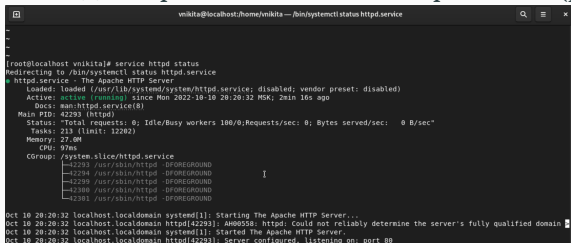
- Венчаков Никита Юрьевич
- студент 4 курса
- Студенческий билет: 1032196697
- группа НБИбд-01-19
- Российский университет дружбы народов
- venchakov2001@gmail.com

## Цель работы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux1. Проверил работу SELinx на практике совместно с веб-сервером Apache.

# Выполнение лабораторной работы

1. Обратился с помощью браузера к веб-серверу, запущенному на компьютере, и убедился, что последний работает: `service httpd status` (рис.Nº1)



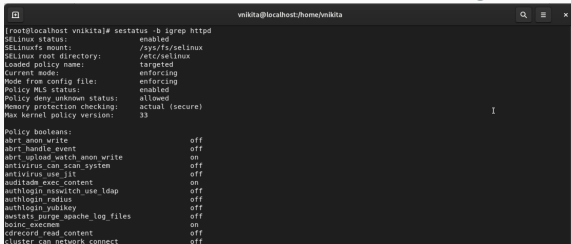
```
vnikita@localhost: /home/vnikita - /bin/systemctl status httpd.service

[root@localhost vnikita]# 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 Mon 2022-10-10 20:20:32 MSK; 2min 16s ago
     Docs: man:httpd.service(8)
   Main PID: 42293 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
   Tasks: 213 (limit: 12202)
  Memory: 27.0M
     CPU: 97ms
   CGroup: /system.slice/httpd.service
           └─42293 /usr/sbin/httpd -DFOREGROUND
             └─4294 /usr/sbin/httpd -DFOREGROUND
             └─4299 /usr/sbin/httpd -DFOREGROUND
             └─4300 /usr/sbin/httpd -DFOREGROUND
             └─4301 /usr/sbin/httpd -DFOREGROUND

Oct 10 20:20:32 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 10 20:20:32 localhost.localdomain httpd[42293]: AH00558: httpd: Could not reliably determine the server's fully qualified domain
Oct 10 20:20:32 localhost.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 10 20:20:32 localhost.localdomain httpd[42293]: Server configured, listening on: port 80
```

# Состояние переключателей SELinux для Apache

## 2. Посмотрел текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b | grep httpd`



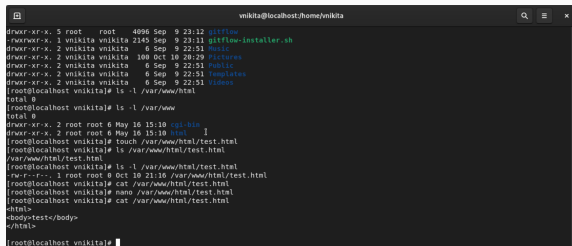
```
[root@localhost vnika]# sestatus -b | grep httpd
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            targeted
Current mode:                  enforcing
Mode from config file:         enforcing
Policy MLS status:             enabled
Policy deny unknown status:    allowed
Memory protection checking:    actual (secure)
Max kernel policy version:    33

Policy booleans:
abrt_anon_write                off
abrt_handle_event              off
abrt_upload_watch_anon_write   on
antivirus_can_scan_system      off
antivirus_use_jit              off
auditd_execcontent             on
authlogin_nsswitch_use_ldap     off
authlogin_radius               off
authlogin_yubikey              off
avstats_purge_apache_log_files off
boinc_execcnt                  on
cdrecd_read_content            off
cluster_can_network_connect    off
```

(рис.№2)

# Создание тестового html файла

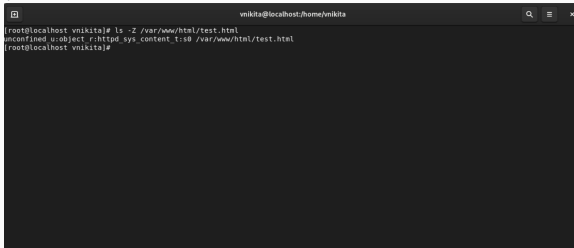
3. Создал от имени суперпользователя html-файл /var/www/html/test.html следующего содержания:  
test



```
vnikita@localhost:~/home/vnikita
dnvr-xr-x. 5 root root 4096 Sep 9 23:12 gitflow
dnvr-xr-x. 1 vnikita vnikita 2145 Sep 9 23:11 gitflow-installer.sh
dnvr-xr-x. 2 vnikita vnikita 6 Sep 9 22:51 Music
dnvr-xr-x. 2 vnikita vnikita 100 Oct 10 20:29 Pictures
dnvr-xr-x. 2 vnikita vnikita 6 Sep 9 22:51 Public
dnvr-xr-x. 2 vnikita vnikita 6 Sep 9 22:51 Templates
dnvr-xr-x. 2 vnikita vnikita 6 Sep 9 22:51 Videos
[root@localhost vnikita]# ls -l /var/www/html
total 0
[root@localhost vnikita]# ls -l /var/www
total 0
dnvr-xr-x. 2 root root 6 May 16 15:10 cgi-bin
dnvr-xr-x. 2 root root 6 May 16 15:10 html
[root@localhost vnikita]# touch /var/www/html/test.html
[root@localhost vnikita]# ls /var/www/html/test.html
/var/www/html/test.html
[root@localhost vnikita]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 0 Oct 10 21:16 /var/www/html/test.html
[root@localhost vnikita]# cat /var/www/html/test.html
[root@localhost vnikita]# nano /var/www/html/test.html
[root@localhost vnikita]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@localhost vnikita]#
```

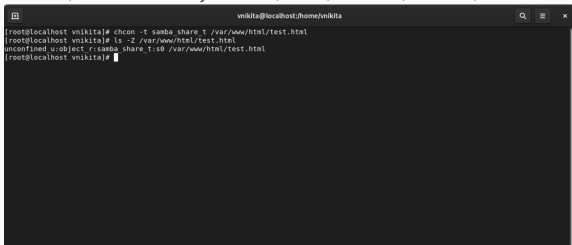
(рис.№3)

4. Обратился к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедился, что файл был успешно отображён. (рис.Nº4)

A terminal window with a dark background and light text. The title bar at the top reads 'vnikita@localhost/home/vnikita'. The terminal shows a sequence of commands and their outputs: the user enters 'ls -Z /var/www/html/test.html', the system responds with 'unconfined u:object r:httpd\_sys\_content\_t:s0 /var/www/html/test.html', and the user then enters a second prompt.

```
vnikita@localhost/home/vnikita
[root@localhost vnikita]# ls -Z /var/www/html/test.html
unconfined u:object r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@localhost vnikita]#
```

5. Изменил контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на любой другой, к которому процесс `httpd` не должен иметь доступа, например, на `samba_share_t`: `chcon -t samba_share_t /var/www/html/test.html`, `ls -Z /var/www/html/test.html`

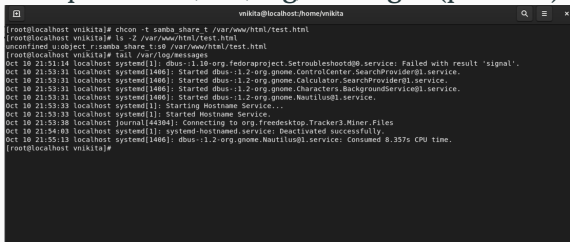


```
vnikita@localhost:~/home/vnikita
[root@localhost vnikita]# chcon -t samba_share_t /var/www/html/test.html
[root@localhost vnikita]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@localhost vnikita]#
```

(рис.№5)



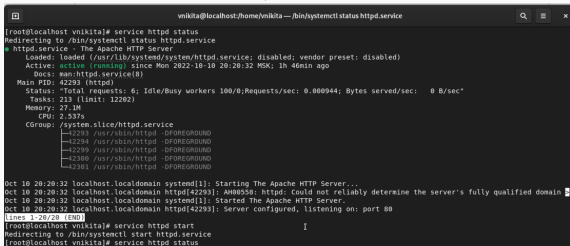
6. Проанализировал ситуацию команду `ls -l /var/www/html/test.html` Просмотрел log-файлы веб-сервера Apache. Также просмотрел системный лог-файл: `tail /var/log/messages` (рис.№6)

A screenshot of a terminal window with a dark background. The title bar shows the user 'vnikita' at 'localhost/home/vnikita'. The terminal displays a series of commands and their outputs. The first command is 'chcon -t samba\_share\_t /var/www/html/test.html'. The second is 'ls -l /var/www/html/test.html', which shows file permissions and ownership. The third command is 'tail /var/log/messages', which displays a log of system events, including the start of various dbus services and the connection to org.freedesktop.Tracker3.Miner.Files.

```
[root@localhost vnikita]# chcon -t samba_share_t /var/www/html/test.html
[root@localhost vnikita]# ls -l /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@localhost vnikita]# tail /var/log/messages
Oct 10 21:51:14 localhost systemd[1]: dbus-1.10-org.fedoraproject.Setroubleshootd@0.service: Failed with result 'signal'.
Oct 10 21:53:31 localhost systemd[1406]: Started dbus-1.2-org.gnome.ControlCenter.SearchProvider@1.service.
Oct 10 21:53:31 localhost systemd[1406]: Started dbus-1.2-org.gnome.Calculator.SearchProvider@1.service.
Oct 10 21:53:31 localhost systemd[1406]: Started dbus-1.2-org.gnome.Characters.BackgroundService@1.service.
Oct 10 21:53:31 localhost systemd[1406]: Started dbus-1.2-org.gnome.Nautilus@1.service.
Oct 10 21:53:33 localhost systemd[1]: Starting Hostname Service...
Oct 10 21:53:33 localhost systemd[1]: Started Hostname Service.
Oct 10 21:53:38 localhost journal[44304]: Connecting to org.freedesktop.Tracker3.Miner.Files
Oct 10 21:54:03 localhost systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Oct 10 21:55:13 localhost systemd[1406]: dbus-1.2-org.gnome.Nautilus@1.service: Consumed 8.357s CPU time.
[root@localhost vnikita]#
```

# Перезапуск веб-сервера

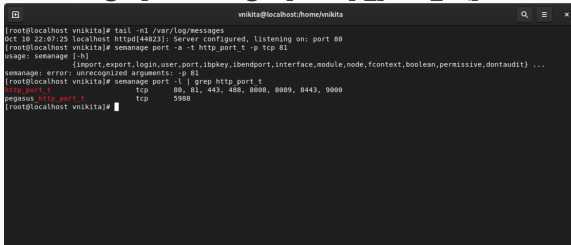
## 7. Выполнил перезапуск веб-сервера Apache(рис.№7)



```
vnikita@localhost:/home/vnikita — /bin/systemctl status httpd.service
[root@localhost vnikita]# 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 Mon 2022-10-10 20:20:32 MSK; 1h 46min ago
     Docs: man:httpd.service(8)
   Main PID: 42293 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0.000944; Bytes served/sec: 0 B/sec"
   Tasks: 213 (limit: 12202)
  Memory: 27.1M
    CPU: 2.537s
   CGroup: /system.slice/httpd.service
           └─42298 /usr/sbin/httpd -DFOREGROUND
           └─42294 /usr/sbin/httpd -DFOREGROUND
           └─42299 /usr/sbin/httpd -DFOREGROUND
           └─42300 /usr/sbin/httpd -DFOREGROUND
           └─42301 /usr/sbin/httpd -DFOREGROUND

Oct 10 20:20:32 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 10 20:20:32 localhost.localdomain httpd[42293]: AH00558: httpd: Could not reliably determine the server's fully qualified domain
Oct 10 20:20:32 localhost.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 10 20:20:32 localhost.localdomain httpd[42293]: Server configured, listening on: port 80
(lines 1-26/28 (END))
[root@localhost vnikita]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@localhost vnikita]# service httpd status
```

8. Выполнил команду `semanage port -a -t http_port_t -p tcp 81` После этого проверьте список портов командой `semanage port -l | grep http_port_t` (рис.Nº8)



```
vnikita@localhost:~/home/vnikita
[root@localhost vnikita]# tail -n1 /var/log/messages
Oct 10 22:07:25 localhost httpd[44823]: Server configured, listening on: port 80
[root@localhost vnikita]# semmanage port -a -t http_port_t -p tcp 81
usage: semmanage [-h]
                    {import,export,login,user,port,ibpkey,ibendport,interface,module,node,fcontext,boolean,permissive,dontaudit} ...
                    -p 81
semmanage: error: unrecognized arguments: -p 81
[root@localhost vnikita]# semmanage port -l | grep http_port_t
http_port_t      tcp      80, 81, 443, 488, 8080, 8089, 8443, 9000
pegasus http_port_t      tcp      5988
[root@localhost vnikita]#
```

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux1. Проверил работу SELinux на практике совместно с веб-сервером Apache.