

Отчёт по лабораторной работе №6

Мандатное разграничение прав в Linux

Венчаков Никита НБИбд-01-19

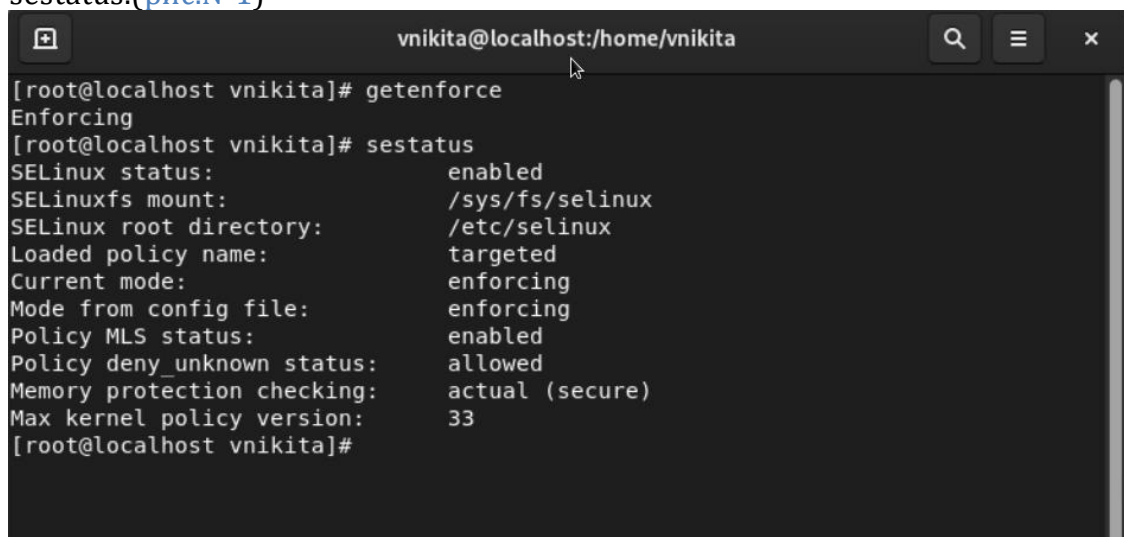
Содержание

Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinux на практике совместно с веб-сервером Apache.

Выполнение лабораторной работы

1. Вошел в систему с полученными учётными данными и убедился, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.[\(рис.№1\)](#)



```
vnikita@localhost:/home/vnikita
[root@localhost vnikita]# getenforce
Enforcing
[root@localhost vnikita]# 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
[root@localhost vnikita]#
```

2. Обратился с помощью браузера к веб-серверу, запущенному на компьютере, и убедился, что последний работает: `service httpd status` (рис.№2)

```
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
             └─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
```

3. Нашел веб-сервер Apache в списке процессов, определите его контекст безопасности. Использовал команду `ps auxZ | grep httpd` (рис.№3)

```
vnikita@localhost:/home/vnikita

Memory: 27.0M
CPU: 97ms
CGroup: /system.slice/httpd.service
└─42293 /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

[root@localhost vnikita]# ps auxZ | grep httpd
system u:system_r:httpd_t:s0 root 42293 0.0 0.5 20064 11536 ? Ss 20:20 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system_r:httpd_t:s0 apache 42294 0.0 0.3 21516 6964 ? S 20:20 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system_r:httpd_t:s0 apache 42299 0.0 0.5 1079216 11020 ? Sl 20:20 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system_r:httpd_t:s0 apache 42300 0.0 0.5 1079216 11032 ? Sl 20:20 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system_r:httpd_t:s0 apache 42301 0.0 0.6 1210352 13080 ? Sl 20:20 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 42676 0.0 0.1 221668 2228 pts/0 S+ 20:25 0:00 grep --color=auto httpd
[root@localhost vnikita]#
```

4. Посмотрел текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` (рис.№4)

```
vnikita@localhost:/home/vnikita

[root@localhost vnikita]# sestatus -b igrep 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
auditadm_exec_content on
authlogin_nsswitch_use_ldap off
authlogin_radius off
authlogin_yubikey off
awstats_purge_apache_log_files off
boinc_execmem on
cdrecord_read_content off
cluster_can_network_connect off
```

5. Посмотрел статистику по политике с помощью команды seinfo.(рис.№5)

```
vnikita@localhost:/home/vnikita
[root@localhost vnikita]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow
Classes:                 133      Permissions:      454
Sensitivities:           1        Categories:       1024
Types:                   4995     Attributes:       254
Users:                   8         Roles:           14
Booleans:                347      Cond. Expr.:     382
Allow:                   63727    Neverallow:      0
Auditallow:              163      Dontaudit:       8391
Type_trans:              251060   Type_change:     87
Type_member:              35       Range_trans:     5958
Role_allow:              38        Role_trans:      418
Constraints:              72       Validatetrans:   0
MLS Constrain:           72        MLS Val. Tran:   0
Permissives:             0         Polcap:          5
Defaults:                 7        Typebounds:      0
Allowxperm:              0         Neverallowxperm: 0
Auditallowxperm:         0         Dontauditxperm:  0
Ibendportcon:            0         Ibpkeycon:       0
Initial SIDs:            27         Fs_use:          33
Genfscon:                106       Portcon:         651
Netifcon:                 0         Nodecon:         0
[root@localhost vnikita]#
```

6. Определил тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www(рис.№6)

```
[root@localhost vnikita]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 May 16 15:10 html
[root@localhost vnikita]#
```

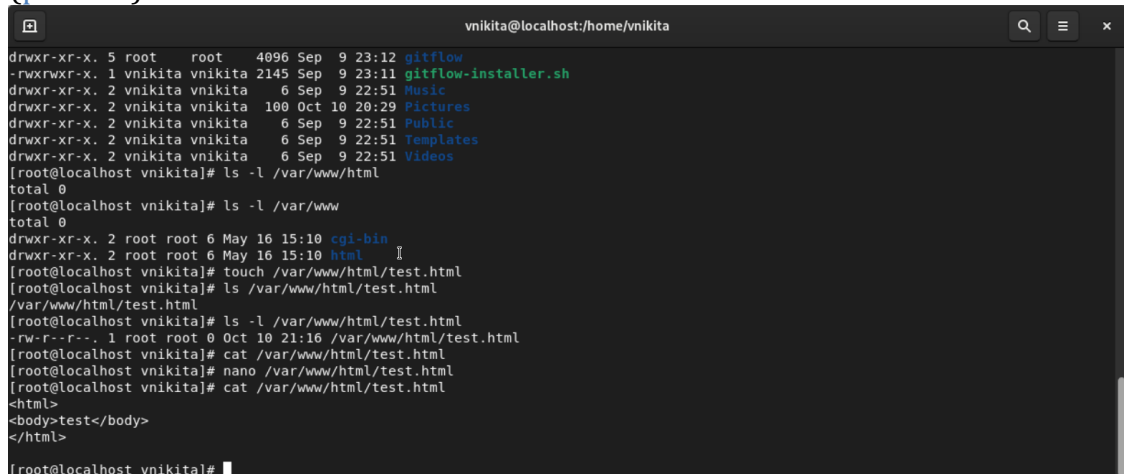
7. Определил тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html (рис.№7)

```
vnikita@localhost:/home/vnikita
Handle unknown classes:  allow
Classes:                 133      Permissions:      454
Sensitivities:           1        Categories:       1024
Types:                   4995     Attributes:       254
Users:                   8         Roles:           14
Booleans:                347      Cond. Expr.:     382
Allow:                   63727    Neverallow:      0
Auditallow:              163      Dontaudit:       8391
Type_trans:              251060   Type_change:     87
Type_member:              35       Range_trans:     5958
Role_allow:              38        Role_trans:      418
Constraints:              72       Validatetrans:   0
MLS Constrain:           72        MLS Val. Tran:   0
Permissives:             0         Polcap:          5
Defaults:                 7        Typebounds:      0
Allowxperm:              0         Neverallowxperm: 0
Auditallowxperm:         0         Dontauditxperm:  0
Ibendportcon:            0         Ibpkeycon:       0
Initial SIDs:            27         Fs_use:          33
Genfscon:                106       Portcon:         651
Netifcon:                 0         Nodecon:         0
[root@localhost vnikita]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 May 16 15:10 html
[root@localhost vnikita]#
```

8. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html.
9. Создал от имени суперпользователя html-файл /var/www/html/test.html следующего содержания:

test

(рис.№8)



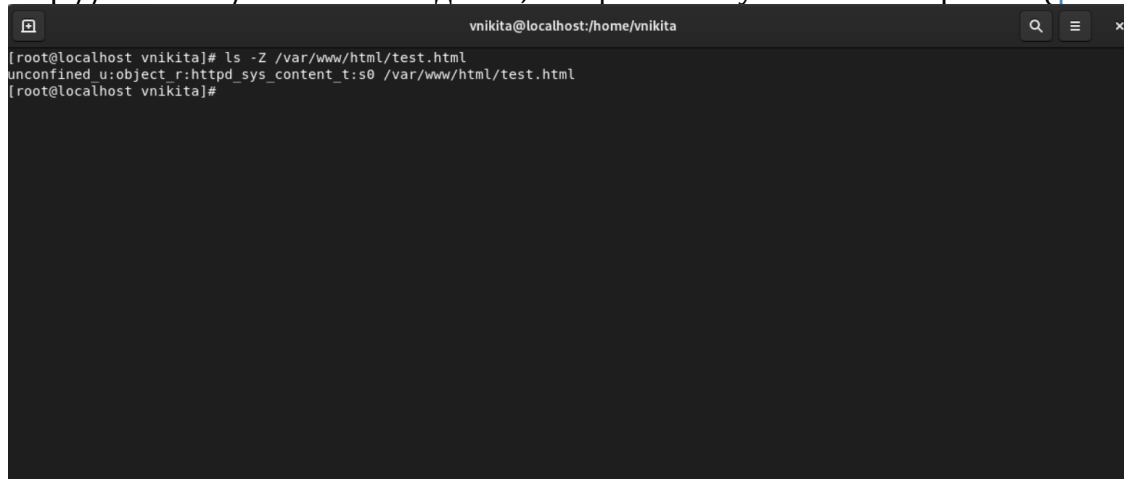
```
vnikita@localhost:/home/vnikita
drwxr-xr-x. 5 root root 4096 Sep  9 23:12 gitflow
-rwxrwxr-x. 1 vnikita vnikita 2145 Sep  9 23:11 gitflow-installer.sh
drwxr-xr-x. 2 vnikita vnikita  6 Sep  9 22:51 Music
drwxr-xr-x. 2 vnikita vnikita 100 Oct 10 20:29 Pictures
drwxr-xr-x. 2 vnikita vnikita  6 Sep  9 22:51 Public
drwxr-xr-x. 2 vnikita vnikita  6 Sep  9 22:51 Templates
drwxr-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
drwxr-xr-x. 2 root root 6 May 16 15:10 cgi-bin
drwxr-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]#
```

10. Проверил контекст созданного файла. (рис.№9)



```
vnikita@localhost:/home/vnikita
[root@localhost vnikita]# matchpathcon -V /var/www/html
/var/www/html verified.
[root@localhost vnikita]#
```

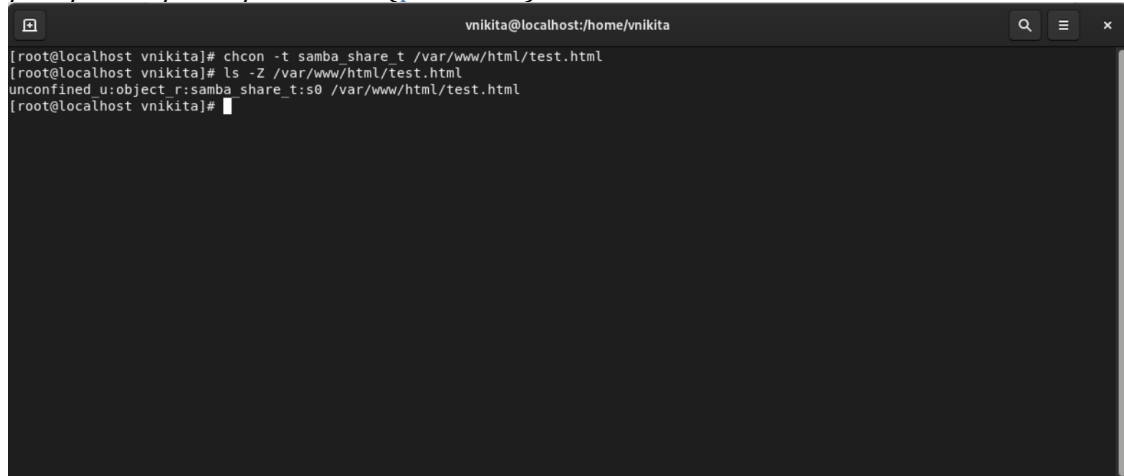
11. Обратился к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Убедился, что файл был успешно отображён. (рис.№10)



```
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]#
```

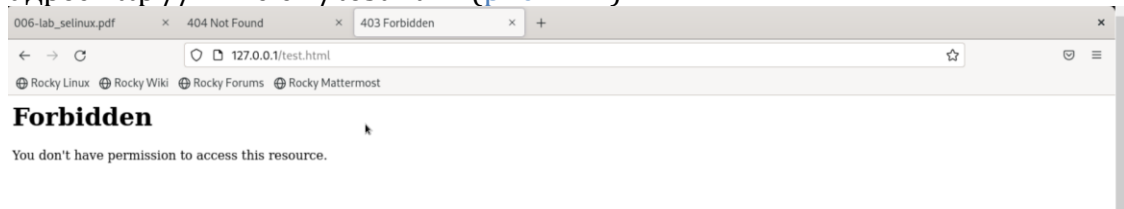
12. Изучил справку man httpd_selinux и выясните, какие контексты файлов определены для httpd.

13. 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` (рис.№11)

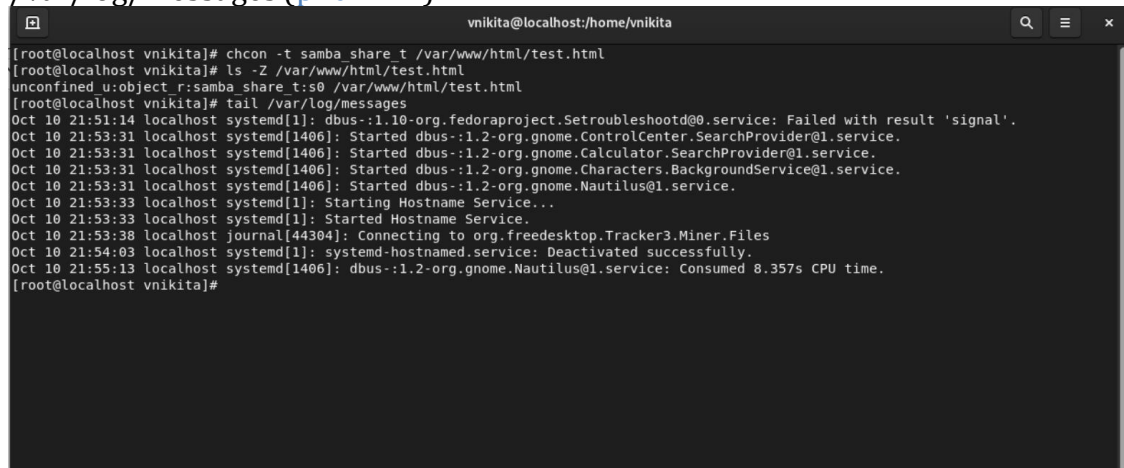


```
vnikita@localhost:~/home/vnikita
[root@localhost vnikita]# chcon -t samba_share_t /var/www/html/test.html
[root@localhost vnikita]# ls -Z /var/www/html/test.html
unconfined u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@localhost vnikita]#
```

14. Попробовал ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. (рис.№12)



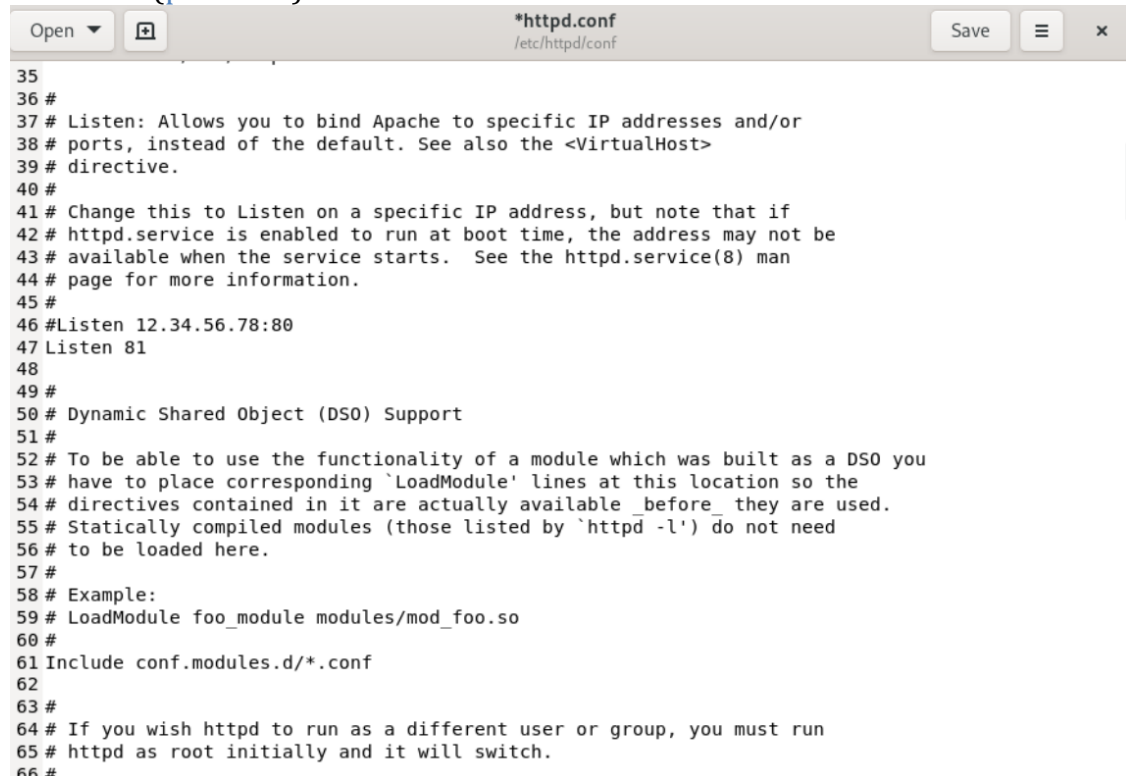
15. Проанализировал ситуацию командой `ls -l /var/www/html/test.html` Просмотрел log-файлы веб-сервера Apache. Также просмотрел системный лог-файл: `tail /var/log/messages` (рис.№12)



```
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]# 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]#
```

16. Попробовал запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле `/etc/httpd/httpd.conf` найдите строчку `Listen 80` и заменил её на

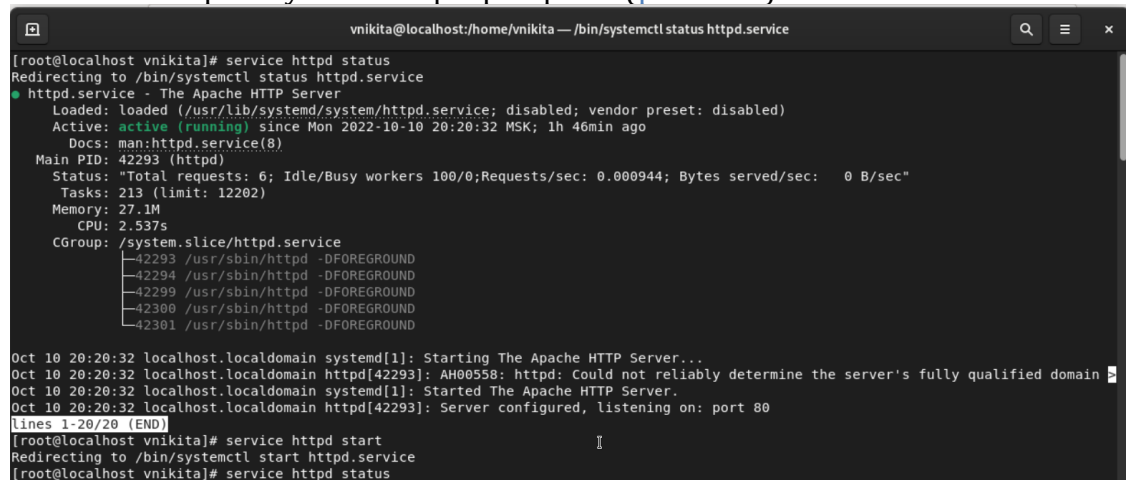
Listen 81. (рис.№13)



```
*httpd.conf
/etc/httpd.conf

35
36 #
37 # Listen: Allows you to bind Apache to specific IP addresses and/or
38 # ports, instead of the default. See also the <VirtualHost>
39 # directive.
40 #
41 # Change this to Listen on a specific IP address, but note that if
42 # httpd.service is enabled to run at boot time, the address may not be
43 # available when the service starts. See the httpd.service(8) man
44 # page for more information.
45 #
46 #Listen 12.34.56.78:80
47 Listen 81
48
49 #
50 # Dynamic Shared Object (DSO) Support
51 #
52 # To be able to use the functionality of a module which was built as a DSO you
53 # have to place corresponding 'LoadModule' lines at this location so the
54 # directives contained in it are actually available _before_ they are used.
55 # Statically compiled modules (those listed by 'httpd -l') do not need
56 # to be loaded here.
57 #
58 # Example:
59 # LoadModule foo_module modules/mod_foo.so
60 #
61 Include conf.modules.d/*.conf
62
63 #
64 # If you wish httpd to run as a different user or group, you must run
65 # httpd as root initially and it will switch.
66 #
```

17. Выполнил перезапуск веб-сервера Apache(рис.№13)



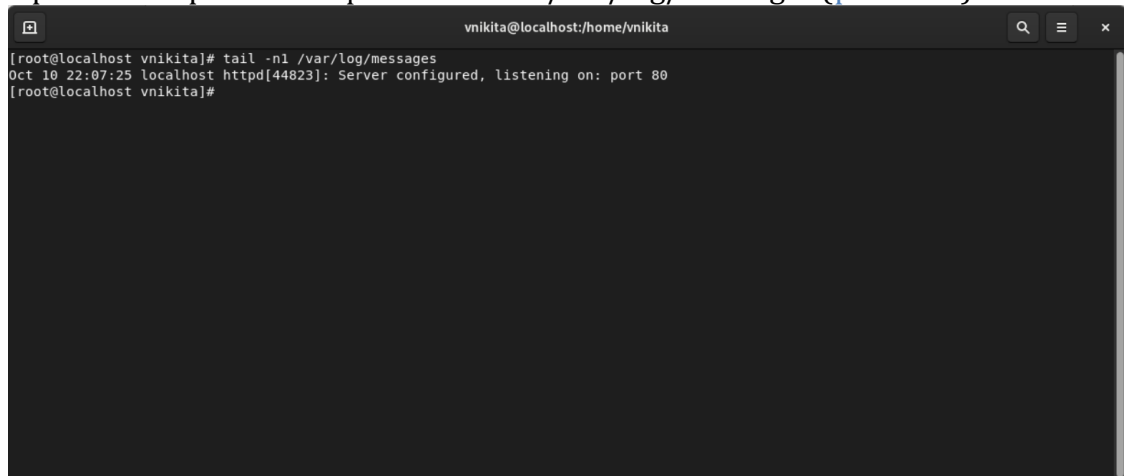
```
vnikita@localhost:~/home/vnikita — /bin/systemctl status httpd.service

[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: 6; 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
            └─42293 /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 1-20/20 (END)

[root@localhost vnikita]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@localhost vnikita]# service httpd status
```

18. Проанализировал лог-файлы: `tail -nl /var/log/messages` (рис.№14)



```
vnikita@localhost:/home/vnikita
[root@localhost vnikita]# tail -nl /var/log/messages
Oct 10 22:07:25 localhost httpd[44823]: Server configured, listening on: port 80
[root@localhost vnikita]#
```

19. 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.№15)



```
vnikita@localhost:/home/vnikita
[root@localhost vnikita]# tail -nl /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} ...
semmanage: error: unrecognized arguments: -p 81
[root@localhost vnikita]# semmanage 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@localhost vnikita]#
```

20. Попробовал запустить веб-сервер Apache ещё раз.
21. Вернул контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`: `chcon -t httpd_sys_content_t /var/www/html/test.html` После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`.
22. Исправил обратно конфигурационный файл `apache`, вернув `Listen 80`.
23. Удалил привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81` и проверил, что порт 81 удалён.

24. Удалил файл /var/www/html/test.html: `rm /var/www/html/test.html` (рис.№16)

A terminal window titled 'vnikita@localhost:/home/vnikita' showing a series of commands and their outputs. The commands are: 'chcon -t httpd_sys_content_t /var/www/html/test.html', 'semanage port -d -t http_port_t -p tcp 81', and 'rm /var/www/html/test.html'. The outputs are: 'ValueError: Port tcp/81 is defined in policy, cannot be deleted', 'rm: remove regular file '/var/www/html/test.html'? y', and a final prompt. The terminal has a dark background with light-colored text.

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

Вывод

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