

# **Отчёт по лабораторной работе №6**

Попов Олег Павлович

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>3</b>	<b>Выводы</b>	<b>15</b>

# List of Tables

# List of Figures

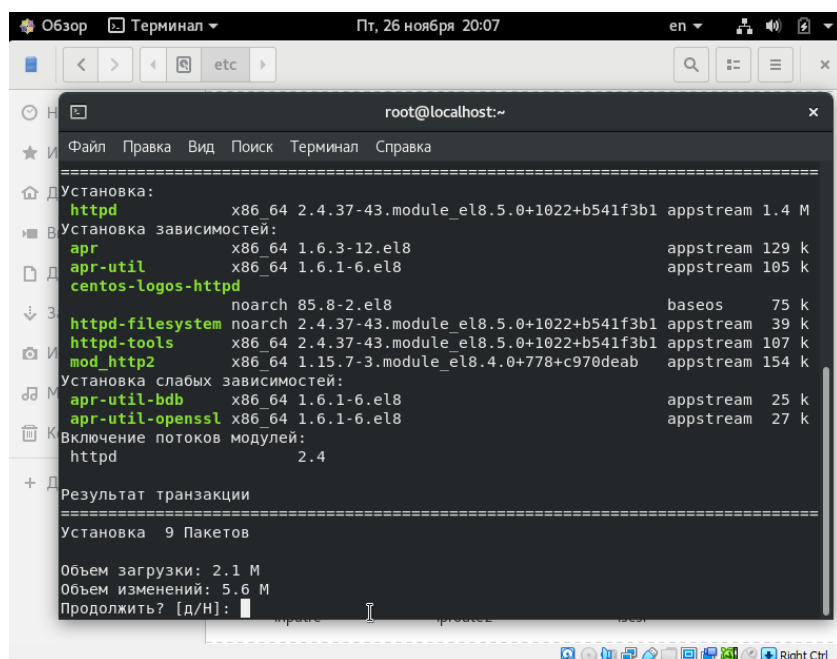
2.1	Установка httpd . . . . .	6
2.2	Строка ServerName . . . . .	7
2.3	Изменение прав доступа для перезаписи ServerName . .	7
2.4	Перезапись ServerName . . . . .	8
2.5	Возвращаем изначальные права доступа . . . . .	8
2.6	Разрешение на INPUT и OUTPUT . . . . .	8

# 1 Цель работы

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

## 2 Выполнение лабораторной работы

За кадром:



```
root@localhost:~#
=====
Установка:
  httpd                x86_64 2.4.37-43.module_el8.5.0+1022+b541f3b1 appstream 1.4 M
Установка зависимостей:
  apr                  x86_64 1.6.3-12.el8                        appstream 129 k
  apr-util              x86_64 1.6.1-6.el8                        appstream 105 k
  centos-logos-httpd    noarch 85.8-2.el8                        baseos    75 k
  httpd-filesystem      noarch 2.4.37-43.module_el8.5.0+1022+b541f3b1 appstream  39 k
  httpd-tools           x86_64 2.4.37-43.module_el8.5.0+1022+b541f3b1 appstream 107 k
  mod_http2             x86_64 1.15.7-3.module_el8.4.0+778+c970deab appstream 154 k
Установка слабых зависимостей:
  apr-util-bdb          x86_64 1.6.1-6.el8                        appstream  25 k
  apr-util-openssl      x86_64 1.6.1-6.el8                        appstream  27 k
Включение потоков модулей:
  httpd                  2.4
=====
Результат транзакции
=====
Установка  9 Пакетов

Объем загрузки: 2.1 М
Объем изменений: 5.6 М
Продолжить? [д/н]:
```

Figure 2.1: Установка httpd

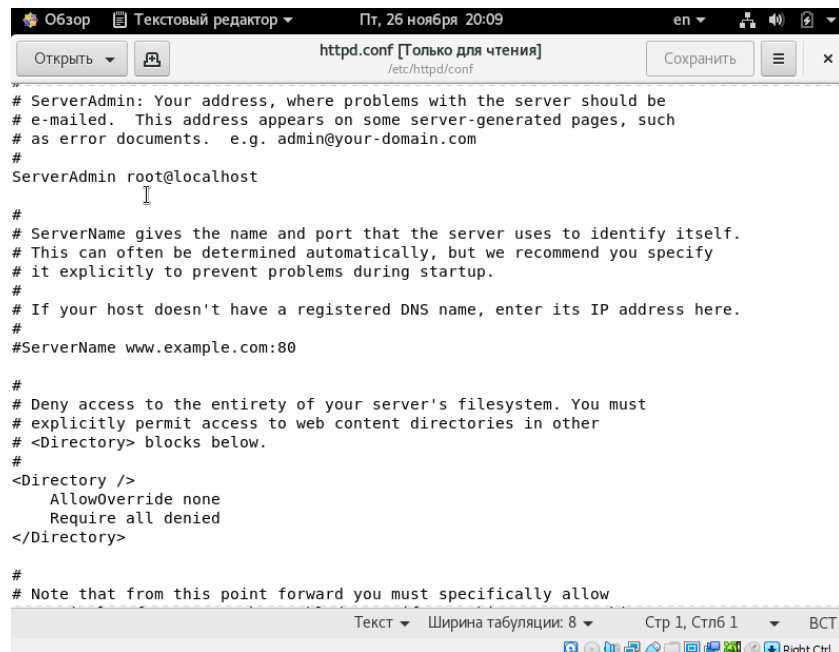


Figure 2.2: Строка ServerName

```
[root@localhost ~]# ls -l /etc/httpd/conf/httpd.conf
-rw-r--r--. 1 root root 11899 ноя 12 07:54 /etc/httpd/conf/httpd.conf
[root@localhost ~]# chmod o+w /etc/httpd/conf/httpd.conf
[root@localhost ~]# ls -l /etc/httpd/conf/httpd.conf
-rw-r--rw-. 1 root root 11899 ноя 12 07:54 /etc/httpd/conf/httpd.conf
[root@localhost ~]#
```

Figure 2.3: Изменение прав доступа для перезаписи ServerName

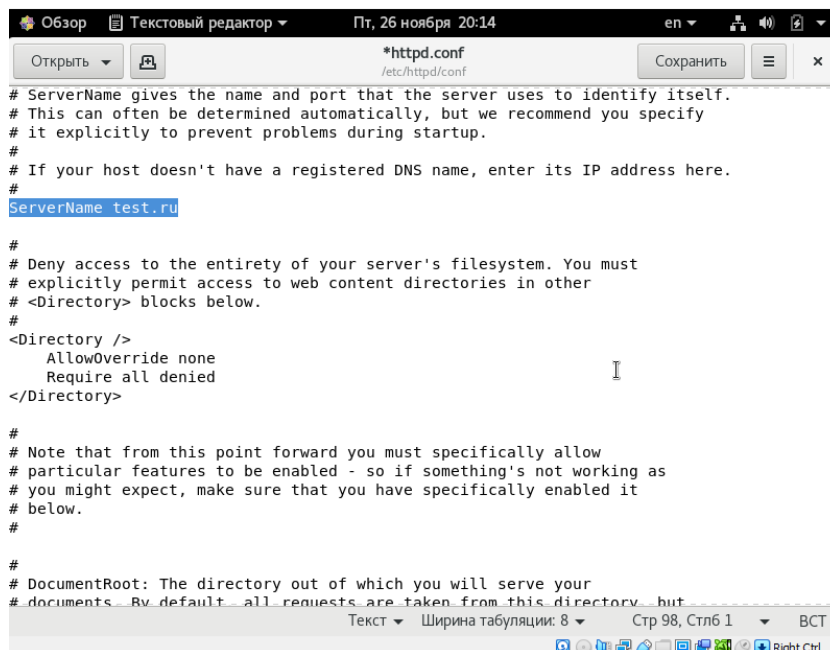


Figure 2.4: Перезапись ServerName

```
[root@localhost ~]# lsmod /etc/httpd/conf/httpd.conf
Usage: lsmod
[root@localhost ~]# ls -l /etc/httpd/conf/httpd.conf
-rw-r--r--. 1 root root 11899 ноя 12 07:54 /etc/httpd/conf/httpd.conf
[root@localhost ~]# chmod o+w /etc/httpd/conf/httpd.conf
[root@localhost ~]# ls -l /etc/httpd/conf/httpd.conf
-rw-r--rw-. 1 root root 11899 ноя 12 07:54 /etc/httpd/conf/httpd.conf
[root@localhost ~]# chmod o-w /etc/httpd/conf/httpd.conf
[root@localhost ~]# ls -l /etc/httpd/conf/httpd.conf
-rw-r--r--. 1 root root 11887 ноя 26 20:15 /etc/httpd/conf/httpd.conf
[root@localhost ~]#
```

Figure 2.5: Возвращаем изначальные права доступа

```
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -P INPUT ACCEPT
[root@localhost ~]# iptables -P OUTPUT ACCEPT
[root@localhost ~]#
```

Figure 2.6: Разрешение на INPUT и OUTPUT

Выполнение работы:



The first screenshot shows the terminal output for starting the httpd service and checking its status. The service is successfully started and is running on port 80. The second screenshot shows the output of the `ps auxZ | grep httpd` command, displaying the process details for the httpd service, including the user, system, and process information.

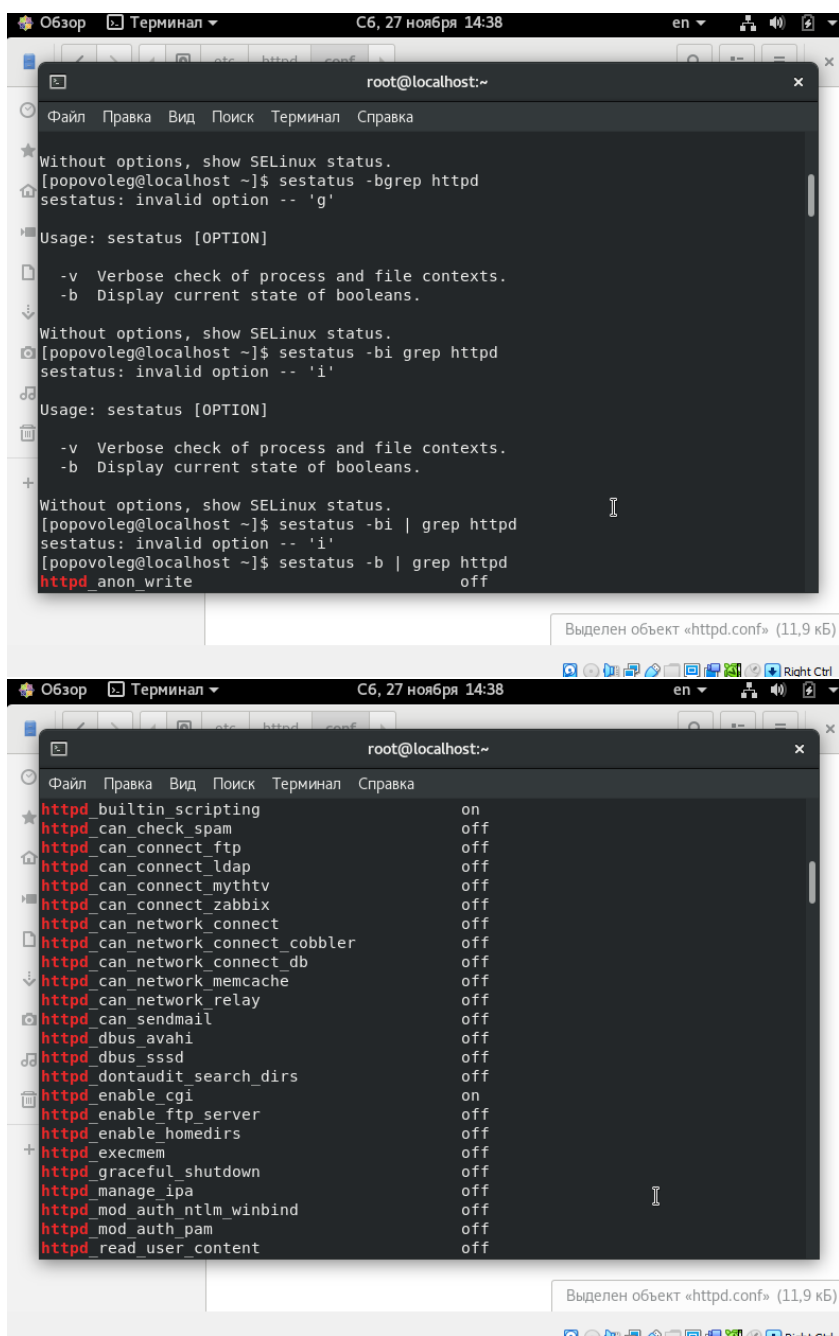
```
root@localhost:~  
[popovoleg@localhost ~]$ service httpd start  
Redirecting to /bin/systemctl start httpd.service  
[popovoleg@localhost ~]$ service httpd status  
service поддерживает только базовые действия LSB (start, stop, restart, try-restart, reload, force-reload, status). Для выполнения других действий следует обратиться к помощи systemctl.  
[popovoleg@localhost ~]$ 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: enabled)  
   Active: active (running) since Sat 2021-11-27 13:41:58 MSK; 14s ago  
     Docs: man:httpd.service(8)  
  Main PID: 3091 (httpd)  
    Status: "Running, listening on: port 80"  
    Tasks: 213 (limit: 4812)  
   Memory: 20.9M  
    CGroup: /system.slice/httpd.service  
           └─3091 /usr/sbin/httpd -DFOREGROUND  
             └─3099 /usr/sbin/httpd -DFOREGROUND  
               └─3104 /usr/sbin/httpd -DFOREGROUND  
                 └─3105 /usr/sbin/httpd -DFOREGROUND  
                   └─3106 /usr/sbin/httpd -DFOREGROUND  
[popovoleg@localhost ~]$ ps auxZ | grep httpd  
system_u:system_r:httpd_t:s0 root 3091 0.2 1.3 273828 11304 ?
```

Выделен объект «httpd.conf» (11,9 кБ)

```
root@localhost:~  
Ss 13:41 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3099 0.0 1.0 289832 8508 ?  
S 13:41 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3104 0.0 1.2 1347640 10176 ?  
Sl 13:41 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3105 0.0 1.2 1478768 10176 ?  
Sl 13:41 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3106 0.0 1.2 1347640 10176 ?  
Sl 13:41 0:00 /usr/sbin/httpd -DFOREGROUND  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 popovoleg 3378 0.0 0.1 121  
36 1100 pts/0 R+ 13:42 0:00 grep --color=auto httpd  
[popovoleg@localhost ~]$ ps -eZ | grep httpd  
system_u:system_r:httpd_t:s0 3091 ? 00:00:00 httpd  
system_u:system_r:httpd_t:s0 3099 ? 00:00:00 httpd  
system_u:system_r:httpd_t:s0 3104 ? 00:00:00 httpd  
system_u:system_r:httpd_t:s0 3105 ? 00:00:00 httpd  
system_u:system_r:httpd_t:s0 3106 ? 00:00:00 httpd  
[popovoleg@localhost ~]$ sestatus -bigrep httpd  
sestatus: invalid option -- 'i'  
  
Usage: sestatus [OPTION]  
-v Verbose check of process and file contexts.  
-b Display current state of booleans.
```

Выделен объект «httpd.conf» (11,9 кБ)

Отсюда видим, что контекст Apache - system\_u:system\_r:httpd\_t:s0



Обзор Терминал C6, 27 ноября 14:38 en

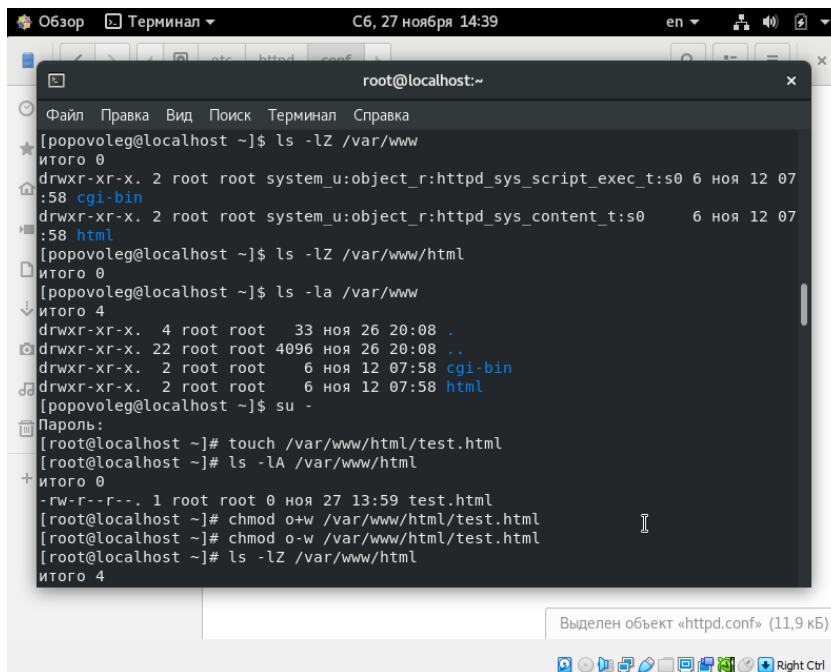
```
root@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
★ httpd_run_ipa off  
★ httpd_run_preupgrade off  
★ httpd_run_stickshift off  
★ httpd_serve_cobbler_files off  
★ httpd_setrlimit off  
★ httpd_ssi_exec off  
★ httpd_sys_script_anon_write off  
★ httpd_tmp_exec off  
★ httpd_tty_comm off  
★ httpd_unified off  
★ httpd_use_cifs off  
★ httpd_use_fusefs off  
★ httpd_use_gpg off  
★ httpd_use_nfs off  
★ httpd_use_opencryptoki off  
★ httpd_use_openstack off  
★ httpd_use_sasl off  
★ httpd_verify_dns off  
+ [popovoleg@localhost ~]$ seinfo  
bash: seinfo: команда не найдена...  
Установить пакет «setools-console», предоставляющий команду «seinfo»? [N/y] y  
* Ожидание в очереди...
```

Выделен объект «httpd.conf» (11,9 кБ)

Обзор Терминал C6, 27 ноября 14:39 en Right Ctrl

```
root@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
★ Statistics for policy file: /sys/fs/selinux/policy  
★ Policy Version: 31 (MLS enabled)  
★ Target Policy: selinux  
★ Handle unknown classes: allow  
Classes: 132 Permissions: 463  
Sensitivities: 1 Categories: 1024  
Types: 4959 Attributes: 255  
Users: 8 Roles: 14  
Booleans: 340 Cond. Expr.: 389  
Allow: 112885 Neverallow: 0  
Auditallow: 166 Dontaudit: 10362  
Type_trans: 253398 Type_change: 87  
Type_member: 35 Range_trans: 6015  
Role_allow: 38 Role_trans: 423  
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: 640  
Netifcon: 0 Nodecon: 0
```

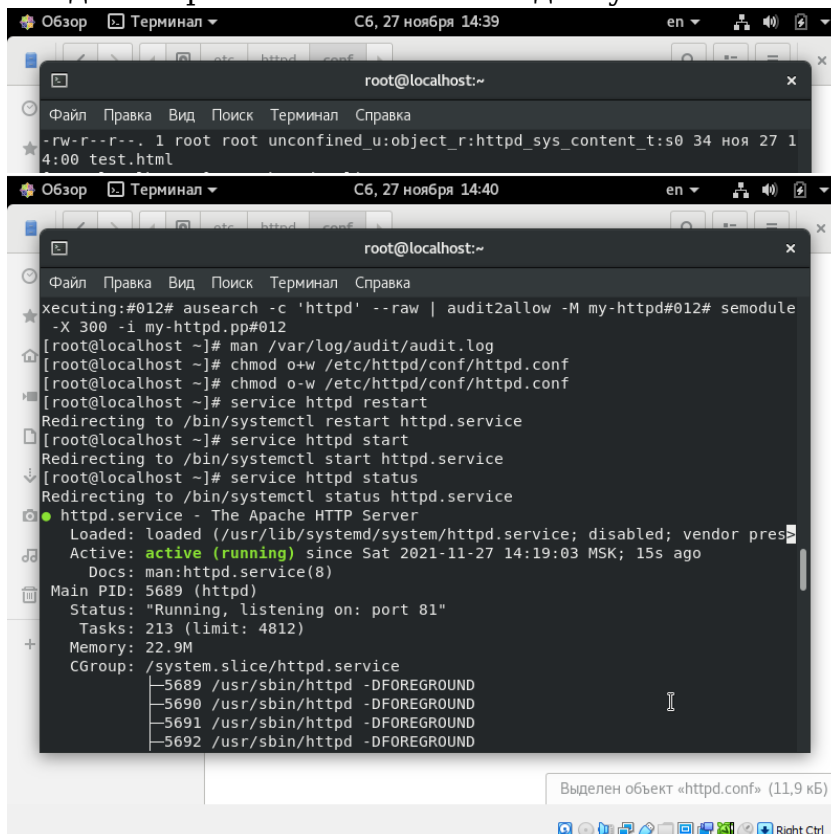
Выделен объект «httpd.conf» (11,9 кБ)



```
root@localhost:~  
[porovoleg@localhost ~]$ ls -lZ /var/www  
итого 0  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 12 07  
:58 cgi-bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ноя 12 07  
:58 html  
[porovoleg@localhost ~]$ ls -lZ /var/www/html  
итого 0  
[porovoleg@localhost ~]$ ls -la /var/www  
итого 4  
drwxr-xr-x. 4 root root 33 ноя 26 20:08 .  
drwxr-xr-x. 22 root root 4096 ноя 26 20:08 ..  
drwxr-xr-x. 2 root root 6 ноя 12 07:58 cgi-bin  
drwxr-xr-x. 2 root root 6 ноя 12 07:58 html  
[porovoleg@localhost ~]$ su -  
Пароль:  
[root@localhost ~]# touch /var/www/html/test.html  
[root@localhost ~]# ls -la /var/www/html  
итого 0  
-rw-r--r--. 1 root root 0 ноя 27 13:59 test.html  
[root@localhost ~]# chmod o+w /var/www/html/test.html  
[root@localhost ~]# chmod o-w /var/www/html/test.html  
[root@localhost ~]# ls -lZ /var/www/html  
итого 4
```

Выделен объект «httpd.conf» (11,9 кБ)

В папке www не было файлов, только две директории: http и cgi-bin.  
Создание файлов в папке html доступно только пользователю root.



```
root@localhost:~  
[root@localhost ~]# touch /var/www/html/test.html  
[root@localhost ~]# ls -la /var/www/html  
итого 0  
-rw-r--r--. 1 root root 0 ноя 27 13:59 test.html  
[root@localhost ~]# su -  
Пароль:  
[root@localhost ~]# xecuting:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule  
-X 300 -i my-httpd.pp#012  
[root@localhost ~]# man /var/log/audit/audit.log  
[root@localhost ~]# chmod o+w /etc/httpd/conf/httpd.conf  
[root@localhost ~]# chmod o-w /etc/httpd/conf/httpd.conf  
[root@localhost ~]# service httpd restart  
Redirecting to /bin/systemctl restart httpd.service  
[root@localhost ~]# service httpd start  
Redirecting to /bin/systemctl start httpd.service  
[root@localhost ~]# 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 pres  
Active: active (running) since Sat 2021-11-27 14:19:03 MSK; 15s ago  
Docs: man:httpd.service(8)  
Main PID: 5689 (httpd)  
Status: "Running, listening on: port 81"  
Tasks: 213 (limit: 4812)  
Memory: 22.9M  
CGroup: /system.slice/httpd.service  
├─5689 /usr/sbin/httpd -DFOREGROUND  
├─5690 /usr/sbin/httpd -DFOREGROUND  
├─5691 /usr/sbin/httpd -DFOREGROUND  
└─5692 /usr/sbin/httpd -DFOREGROUND
```

Выделен объект «httpd.conf» (11,9 кБ)



```
root@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
ноя 27 14:28:51 localhost.localdomain systemd[1]: Started The Apache HTTP Server  
ноя 27 14:28:51 localhost.localdomain httpd[6686]: Server configured, listening  
[root@localhost ~]# ls -Z /var/www/html/test.html  
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html  
[root@localhost ~]# chmod o+w /etc/httpd/conf/httpd.conf  
[root@localhost ~]# chmod o-w /etc/httpd/conf/httpd.conf  
[root@localhost ~]# semanage port -d -t http_port_t -p tcp 81  
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален  
[root@localhost ~]# service httpd restart  
Redirecting to /bin/systemctl restart httpd.service  
[root@localhost ~]# 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: enabled)  
   Active: active (running) since Sat 2021-11-27 14:35:49 MSK; 9s ago  
     Docs: man:httpd.service(8)  
   Main PID: 7407 (httpd)  
    Status: "Running, listening on: port 80"  
   Tasks: 213 (limit: 4812)  
  Memory: 37.6M  
   CGroup: /system.slice/httpd.service  
           └─7407 /usr/sbin/httpd -DFOREGROUND  
             └─7408 /usr/sbin/httpd -DFOREGROUND  
               └─7409 /usr/sbin/httpd -DFOREGROUND
```

Выделен объект «httpd.conf» (11,9 кБ)

“Порт tcp/81 определен на уровне политики” - об этом недопонимании говорилось ранее.

## **3 Выводы**

В результате выполнения работы мы познакомились с SELinux и развили навыки администрирования ОС Linux.