

# Отчет по лабораторной работе №6

Панкратьев Александр Владимирович

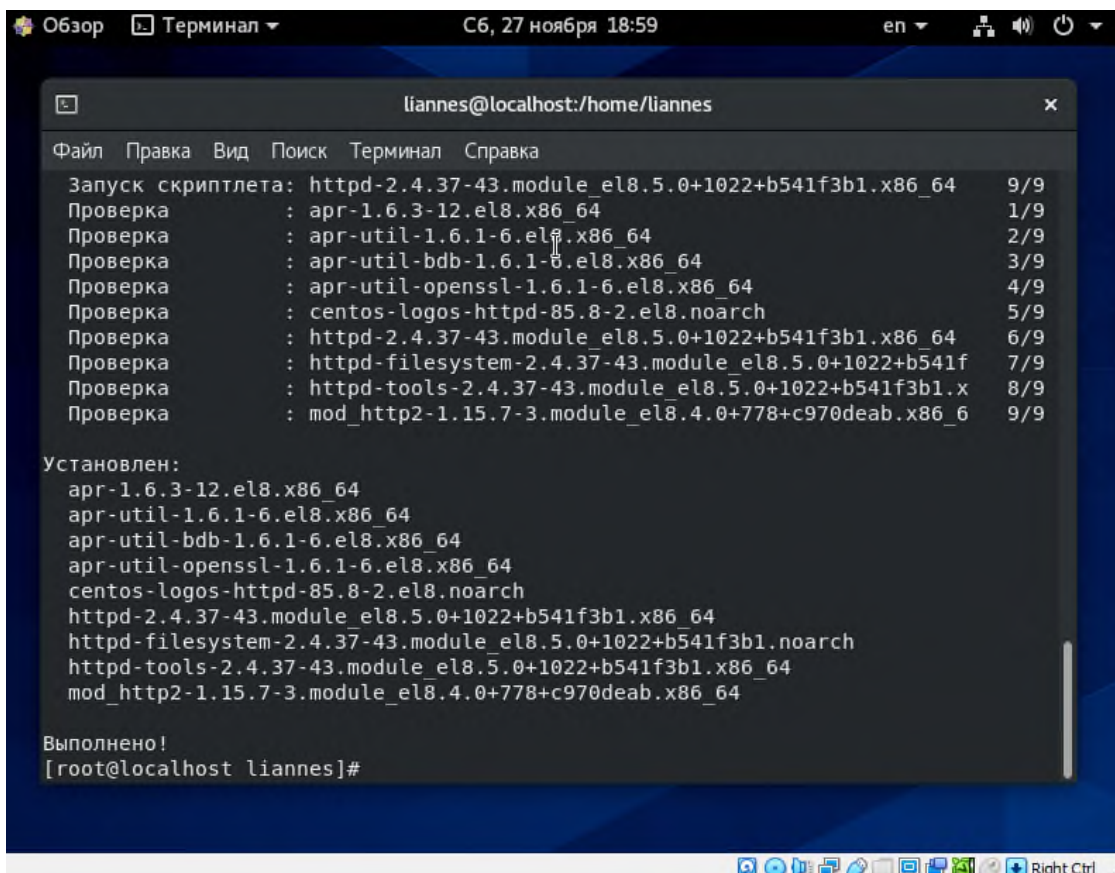
2021

## Цель работы

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

## Выполнение лабораторной работы

Для выполнения работы, установил httpd (рис. -@fig:001).



```
Обзор Терминал C6, 27 ноября 18:59 en
liannes@localhost:/home/liannes
Файл Правка Вид Поиск Терминал Справка
Запуск скриплетта: httpd-2.4.37-43.module_el8.5.0+1022+b541f3b1.x86_64 9/9
Проверка : apr-1.6.3-12.el8.x86_64 1/9
Проверка : apr-util-1.6.1-6.el8.x86_64 2/9
Проверка : apr-util-bdb-1.6.1-6.el8.x86_64 3/9
Проверка : apr-util-openssl-1.6.1-6.el8.x86_64 4/9
Проверка : centos-logos-httpd-85.8-2.el8.noarch 5/9
Проверка : httpd-2.4.37-43.module_el8.5.0+1022+b541f3b1.x86_64 6/9
Проверка : httpd-filesystem-2.4.37-43.module_el8.5.0+1022+b541f3b1.x86_64 7/9
Проверка : httpd-tools-2.4.37-43.module_el8.5.0+1022+b541f3b1.x86_64 8/9
Проверка : mod_http2-1.15.7-3.module_el8.4.0+778+c970deab.x86_64 9/9

Установлен:
apr-1.6.3-12.el8.x86_64
apr-util-1.6.1-6.el8.x86_64
apr-util-bdb-1.6.1-6.el8.x86_64
apr-util-openssl-1.6.1-6.el8.x86_64
centos-logos-httpd-85.8-2.el8.noarch
httpd-2.4.37-43.module_el8.5.0+1022+b541f3b1.x86_64
httpd-filesystem-2.4.37-43.module_el8.5.0+1022+b541f3b1.noarch
httpd-tools-2.4.37-43.module_el8.5.0+1022+b541f3b1.x86_64
mod_http2-1.15.7-3.module_el8.4.0+778+c970deab.x86_64

Выполнено!
[root@localhost liannes]#
```

Установка httpd

## Выполнение лабораторной работы

Следующим действием посмотреть httpd.conf (рис. -@fig:002).

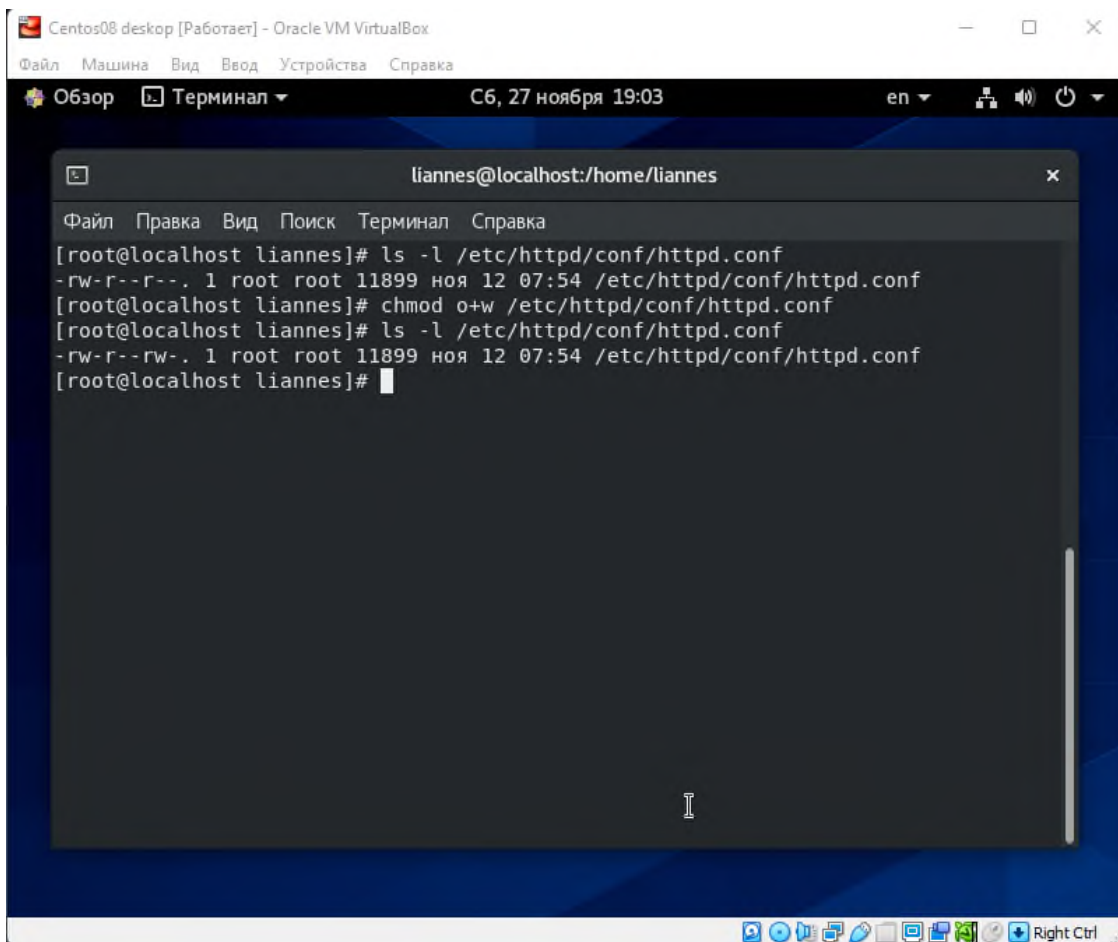
```
liannes@localhost:/home/liannes
Файл Правка Вид Поиск Терминал Справка
GNU nano 2.9.8 /etc/httpd/conf/httpd.conf

# This is the main Apache HTTP server configuration file. It contains the
# configuration directives that give the server its instructions.
# See <URL:http://httpd.apache.org/docs/2.4/> for detailed information.
# In particular, see
# <URL:http://httpd.apache.org/docs/2.4/mod/directives.html>
# for a discussion of each configuration directive.
#
# See the httpd.conf(5) man page for more information on this configuration,
# and httpd.service(8) on using and configuring the httpd service.
#
# Do NOT simply read the instructions in here without understanding
# what they do. They're here only as hints or reminders. If you are unsure
# consult the online docs. You have been warned.
#
# Configuration and logfile names: If the filenames you specify for many
# of the server's control files begin with "/" (or "drive:/" for Win32), the
# server will use that explicit path. If the filenames do *not* begin
# with "/", the value of ServerRoot is prepended -- so 'log/access_log'
[ Read 356 lines ]
^G Помощь ^O Записать ^W Поиск ^K Вырезать ^J Выводить ^C ТекПозиц
^X Выход ^R ЧитФайл ^\ Замена ^U Отмен. выр ^T Словарь ^_ К строке
```

*Просмотр httpd.conf*

## Выполнение лабораторной работы

Дальше от имени root добавил значения ServerName в httpd.conf (рис. -@fig:003, -@fig:004).

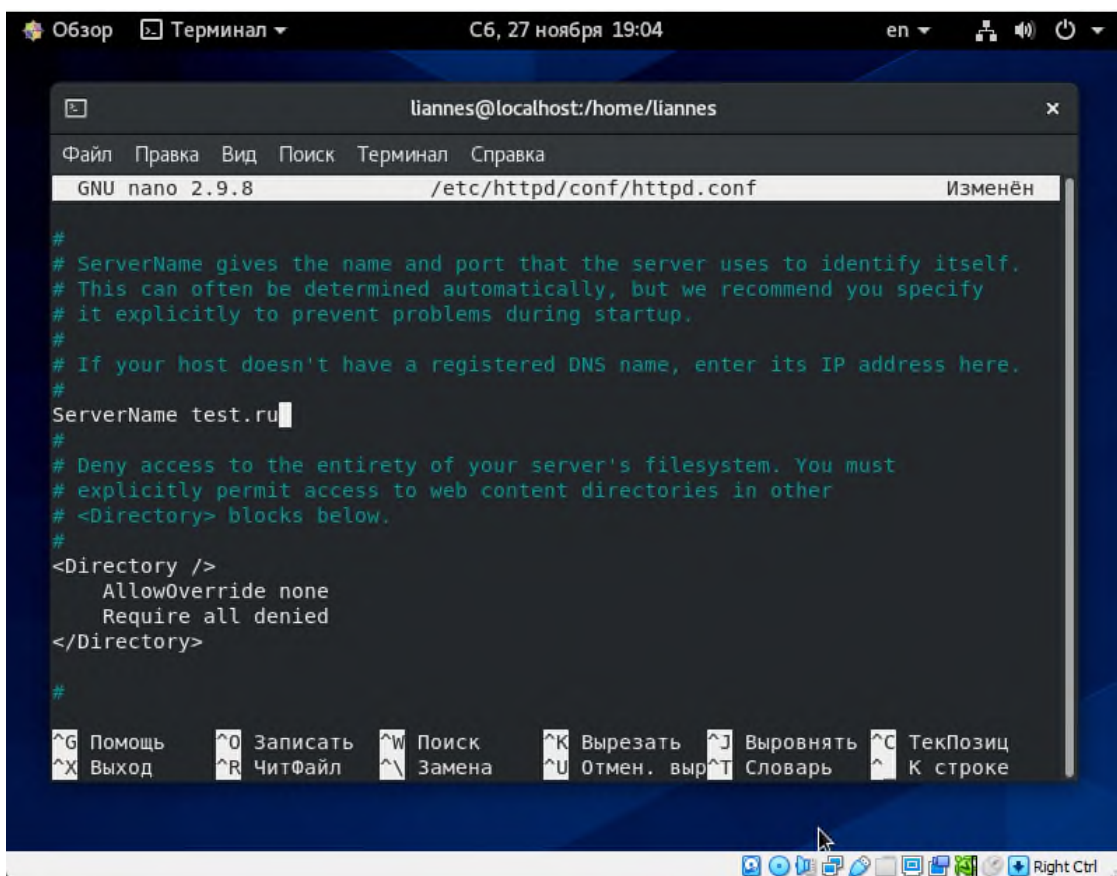


The screenshot shows a virtual machine window titled "Centos08 desktop [Работает] - Oracle VM VirtualBox". The interface includes a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". Below the menu is a toolbar with "Обзор", "Терминал", and a clock showing "Сб, 27 ноября 19:03". The language is set to "en". A terminal window is open, titled "liannes@localhost:/home/liannes". It has a menu bar with "Файл", "Правка", "Вид", "Поиск", "Терминал", and "Справка". The terminal output shows the following commands and results:

```
liannes@localhost:/home/liannes
[root@localhost liannes]# 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 liannes]# chmod o+w /etc/httpd/conf/httpd.conf
[root@localhost liannes]# 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 liannes]#
```

The terminal window has a scrollbar on the right side. The desktop background is blue. The taskbar at the bottom contains various icons and a "Right Ctrl" button.

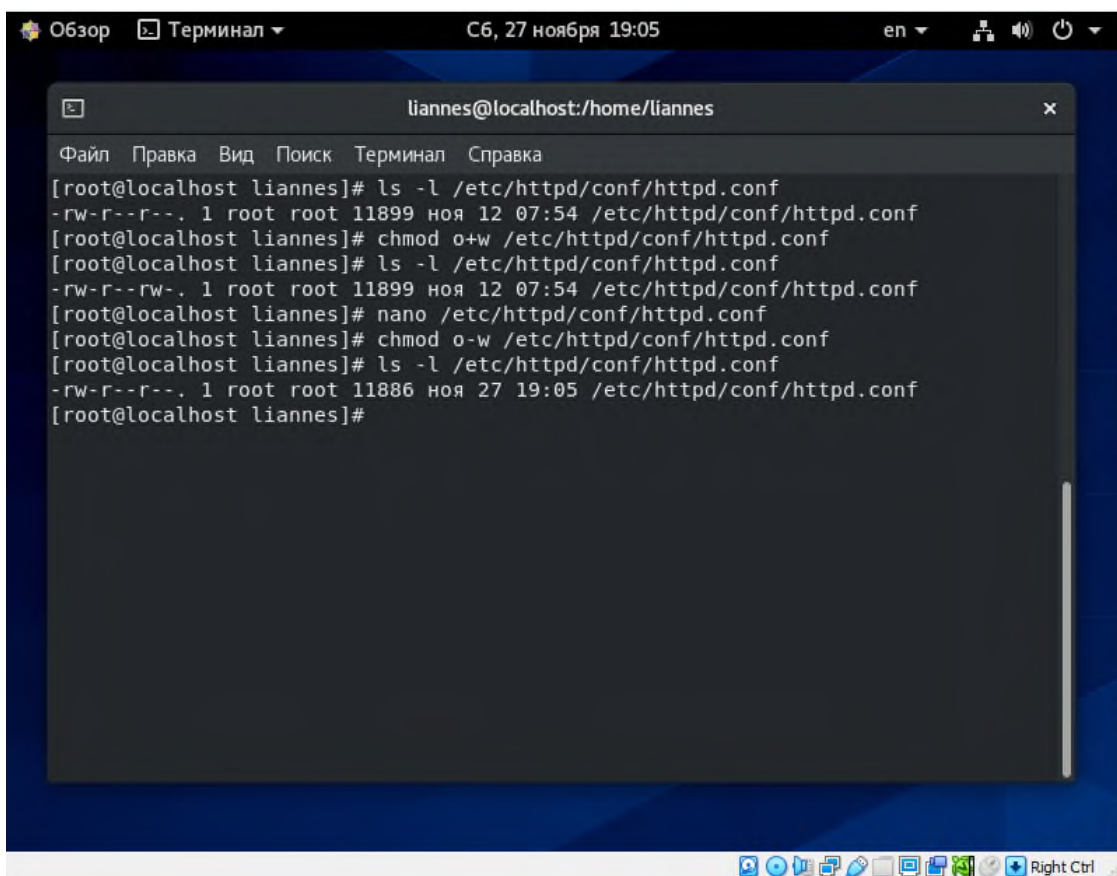
*Изменения разрешения*



*Успешное добавление ServerName*

## Выполнение лабораторной работы

Вернул разрешения обратно (рис. -@fig:005)

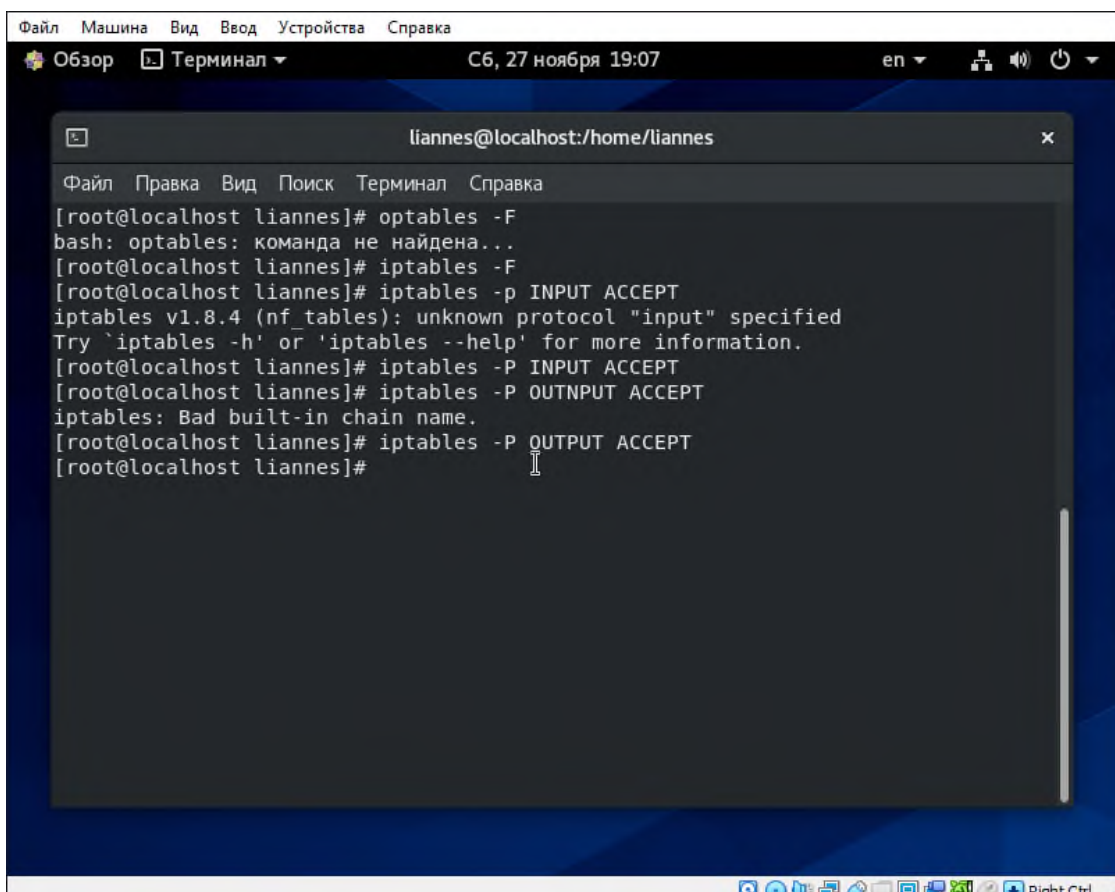


*Возврат разрешения*

## Выполнение лабораторной работы

Отключил фильтры iptables (рис. -@fig:006).





The screenshot shows a terminal window titled "liannes@localhost:/home/liannes". The terminal output is as follows:

```
Файл  Правка  Вид  Поиск  Терминал  Справка
[root@localhost liannes]# optables -F
bash: optables: команда не найдена...
[root@localhost liannes]# iptables -F
[root@localhost liannes]# iptables -p INPUT ACCEPT
iptables v1.8.4 (nf_tables): unknown protocol "input" specified
Try `iptables -h' or 'iptables --help' for more information.
[root@localhost liannes]# iptables -P INPUT ACCEPT
[root@localhost liannes]# iptables -P OUTNPUT ACCEPT
iptables: Bad built-in chain name.
[root@localhost liannes]# iptables -P OUTPUT ACCEPT
[root@localhost liannes]#
```

*Отключения фильтров*

## **Выполнение лабораторной работы**

Дальше запустил сервис httpd (рис. -@fig:007)

The screenshot shows a virtual machine window titled "Centos08 desktop [Работает] - Oracle VM VirtualBox". Inside the VM, a terminal window is open with the title "liannes@localhost:/home/liannes". The terminal shows the following commands and output:

```
[root@localhost liannes]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@localhost liannes]# 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 19:08:12 MSK; 1min 15s ago
     Docs: man:httpd.service(8)
   Main PID: 4104 (httpd)
   Status: "Running, listening on: port 80"
   Tasks: 213 (limit: 11260)
   Memory: 16.7M
   CGroup: /system.slice/httpd.service
           └─4104 /usr/sbin/httpd -DFOREGROUND
             └─4106 /usr/sbin/httpd -DFOREGROUND
               └─4107 /usr/sbin/httpd -DFOREGROUND
                 └─4110 /usr/sbin/httpd -DFOREGROUND
                   └─4111 /usr/sbin/httpd -DFOREGROUND
```

Below the service status, there are three lines of system logs:

```
ноя 27 19:08:11 localhost.localdomain systemd[1]: Starting The Apache HTTP Serv>
ноя 27 19:08:12 localhost.localdomain systemd[1]: Started The Apache HTTP Serve>
ноя 27 19:08:12 localhost.localdomain httpd[4104]: Server configured, listening>
```

The terminal window has a menu bar with "Файл", "Правка", "Вид", "Поиск", "Терминал", and "Справка". The status bar at the bottom of the terminal shows "lines 1-18/18 (END)".

*Запуск httpd*

## Выполнение лабораторной работы

Следующим этапом нахожу список процессов от httpd (рис. -@fig:008).

```
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  Сб, 27 ноября 19:10  en  [иконки]

liannes@localhost:/home/liannes
Файл  Правка  Вид  Поиск  Терминал  Справка
├─4104 /usr/sbin/httpd -DFOREGROUND
├─4106 /usr/sbin/httpd -DFOREGROUND
├─4107 /usr/sbin/httpd -DFOREGROUND
├─4110 /usr/sbin/httpd -DFOREGROUND
└─4111 /usr/sbin/httpd -DFOREGROUND

ноя 27 19:08:11 localhost.localdomain systemd[1]: Starting The Apache HTTP Serv
ноя 27 19:08:12 localhost.localdomain systemd[1]: Started The Apache HTTP Serve
ноя 27 19:08:12 localhost.localdomain httpd[4104]: Server configured, listening>

[root@localhost liannes]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 4104 0.0 0.6 273852 11168 ?
Ss 19:08 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 4106 0.0 0.4 289860 8404 ?
S 19:08 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 4107 0.0 0.6 1478796 12192 ?
Sl 19:08 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 4110 0.0 0.5 1347668 10152 ?
Sl 19:08 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 4111 0.0 0.5 1347668 10152 ?
Sl 19:08 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 4427 0.0 0.0 12136 1
048 pts/0 R+ 19:10 0:00 grep --color=auto httpd
[root@localhost liannes]#
```

*Список процессов httpd*

## Выполнение лабораторной работы

Использовал команду `sestatus` для того, чтобы посмотреть состояние переключателей для Apache (рис. -@fig:009).



```
liannes@localhost:~$ sestatus -b | grep httpd
httpd_anon_write off
httpd_builtin_scripting on
httpd_can_check_spam off
httpd_can_connect_ftp off
httpd_can_connect_ldap off
httpd_can_connect_mythtv off
httpd_can_connect_zabbix off
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_avahi 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
```

*Состояние переключателей httpd*

## Выполнение лабораторной работы

Дальше посмотреть статистику политики (рис. -@fig:010).

```
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  C6, 27 ноября 19:14  en  [system icons]

liannes@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

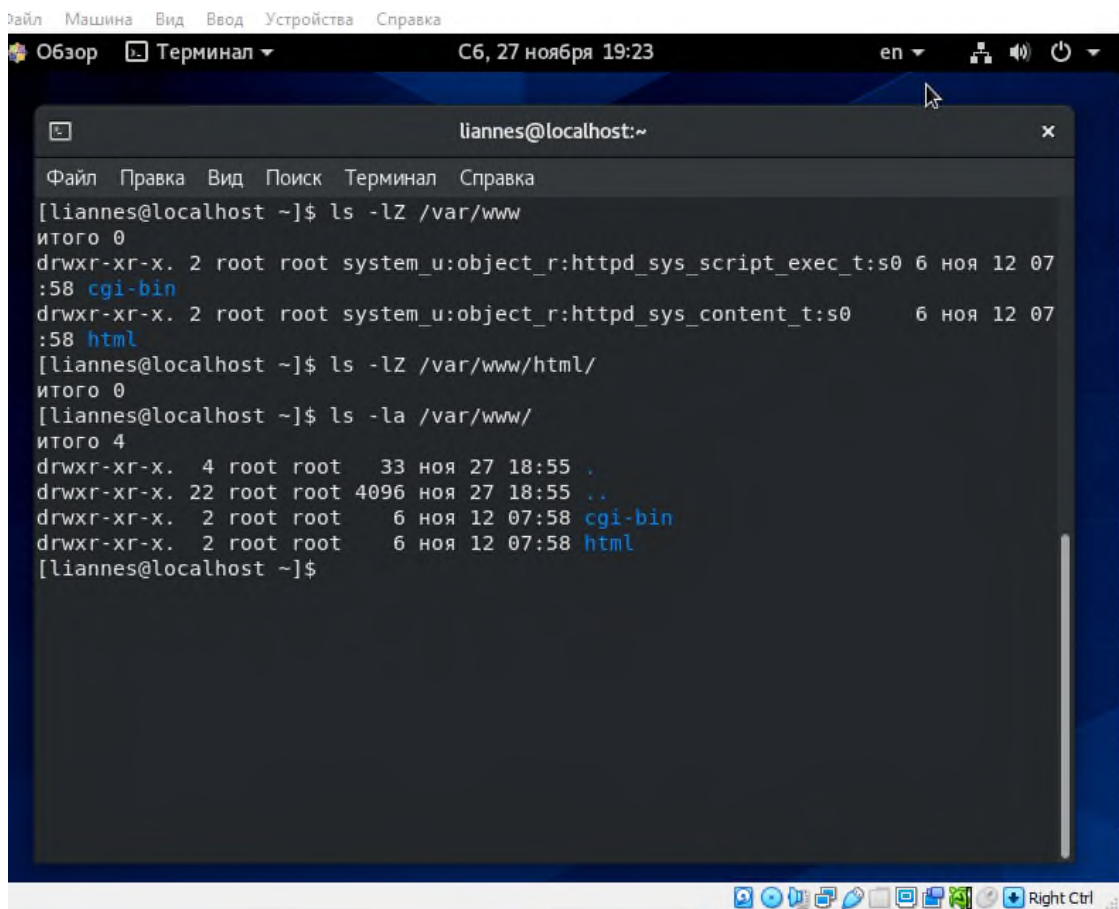
Classes:          132      Permissions:        464
Sensitivities:    1        Categories:         1024
Types:            4970     Attributes:         255
Users:            8        Roles:              14
Booleans:         338     Cond. Expr.:       386
Allow:            112639   Neverallow:         0
Auditallow:       166     Dontaudit:          10363
Type_trans:       252800  Type_change:        87
Type_member:      35      Range_trans:        5781
Role allow:       38      Role_trans:         421
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:              34
Genfscon:         107     Portcon:             646
Netifcon:         0       Nodecon:             0

[liannes@localhost ~]$
```

*Статистику политики*

## Выполнение лабораторной работы

Следом определил файлы в директории /var/www и /var/www/html (рис. -@fig:011)



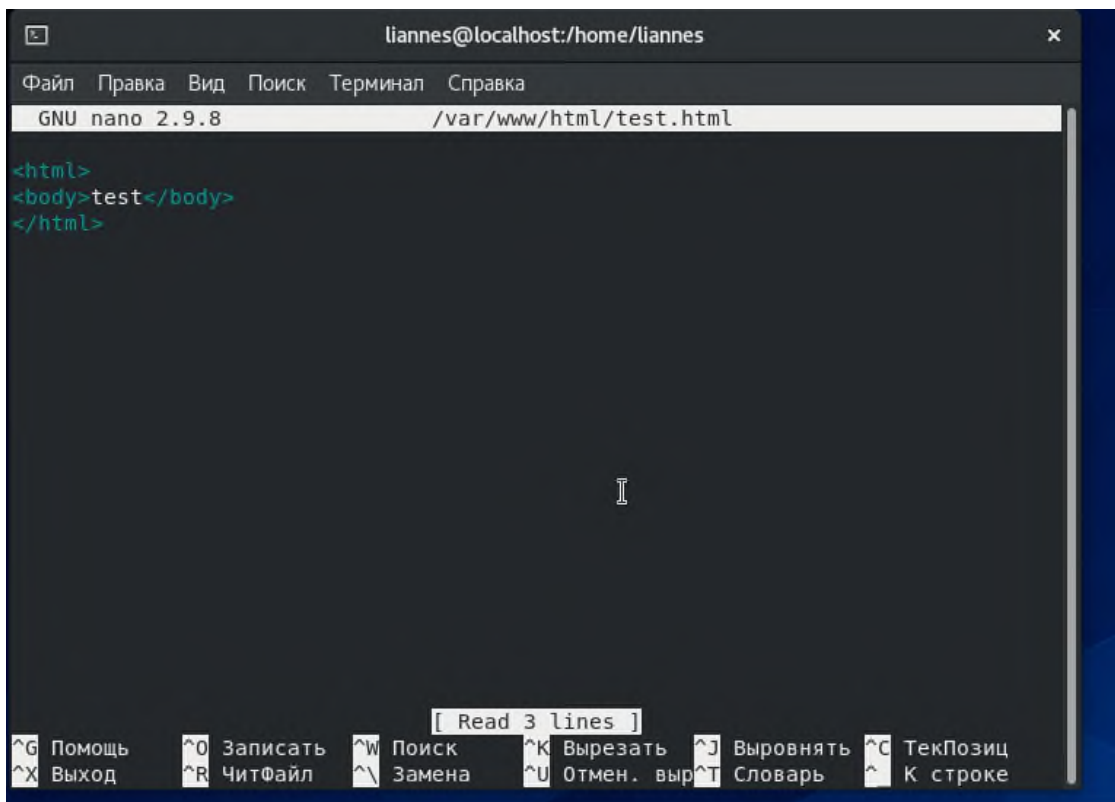
The screenshot shows a terminal window titled "liannes@localhost:~" with a menu bar containing "Файл", "Правка", "Вид", "Поиск", "Терминал", and "Справка". The terminal displays the following commands and output:

```
[liannes@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
[liannes@localhost ~]$ ls -lZ /var/www/html/
итого 0
[liannes@localhost ~]$ ls -la /var/www/
итого 4
drwxr-xr-x. 4 root root 33 ноя 27 18:55 .
drwxr-xr-x. 22 root root 4096 ноя 27 18:55 ..
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
[liannes@localhost ~]$
```

*Файлы в директориях*

## Выполнение лабораторной работы

Создал файл test.html в директории /var/www/html/ с содержанием (рис. -@fig:012)



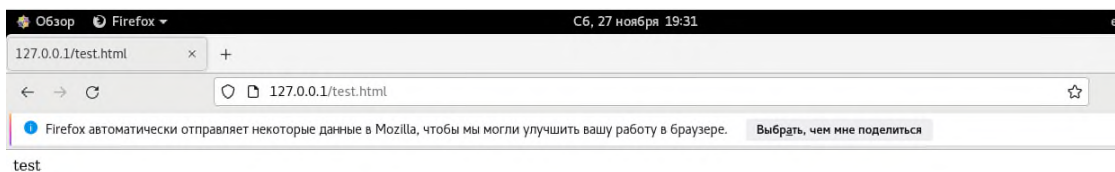
```
liannes@localhost:/home/liannes
Файл  Правка  Вид  Поиск  Терминал  Справка
GNU nano 2.9.8 /var/www/html/test.html
<html>
<body>test</body>
</html>

[ Read 3 lines ]
^G Помощь  ^O Записать  ^W Поиск    ^K Вырезать  ^J Выводить  ^C ТекПозиц
^X Выход    ^R ЧитФайл  ^\ Замена   ^U Отмен. выр ^T Словарь  ^_ К строке
```

Текст файлы

## Выполнение лабораторной работы

Открыл браузер и перешел по пути <http://127.0.0.1/test.html> и увидел там текст (рис. - @fig:013)

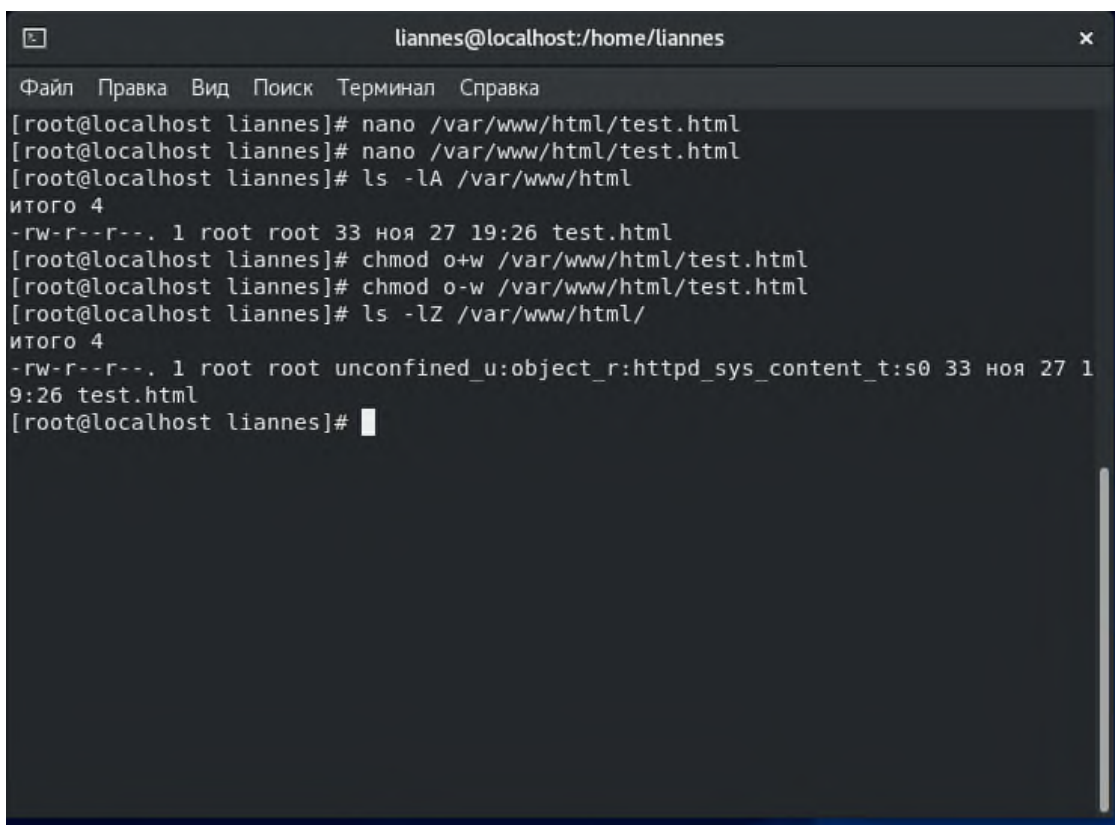


##

## Выполнение лабораторной работы

Проверил контекст test.html (рис. -@fig:014) Присутствует `unconfined_u`, потому что был создан мной;

Роль `object_r` используется по умолчанию

A terminal window titled 'liannes@localhost:/home/liannes' with a menu bar containing 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal shows a series of commands and their outputs. The user runs 'nano /var/www/html/test.html' twice. Then 'ls -lA /var/www/html' shows a file 'test.html' with permissions '-rw-r--r--', owned by root, created on Nov 27 at 19:26. The user then runs 'chmod o+w /var/www/html/test.html' and 'chmod o-w /var/www/html/test.html'. A final 'ls -lZ /var/www/html/' shows the file with SELinux context 'unconfined\_u:object\_r:httpd\_sys\_content\_t:s0'.

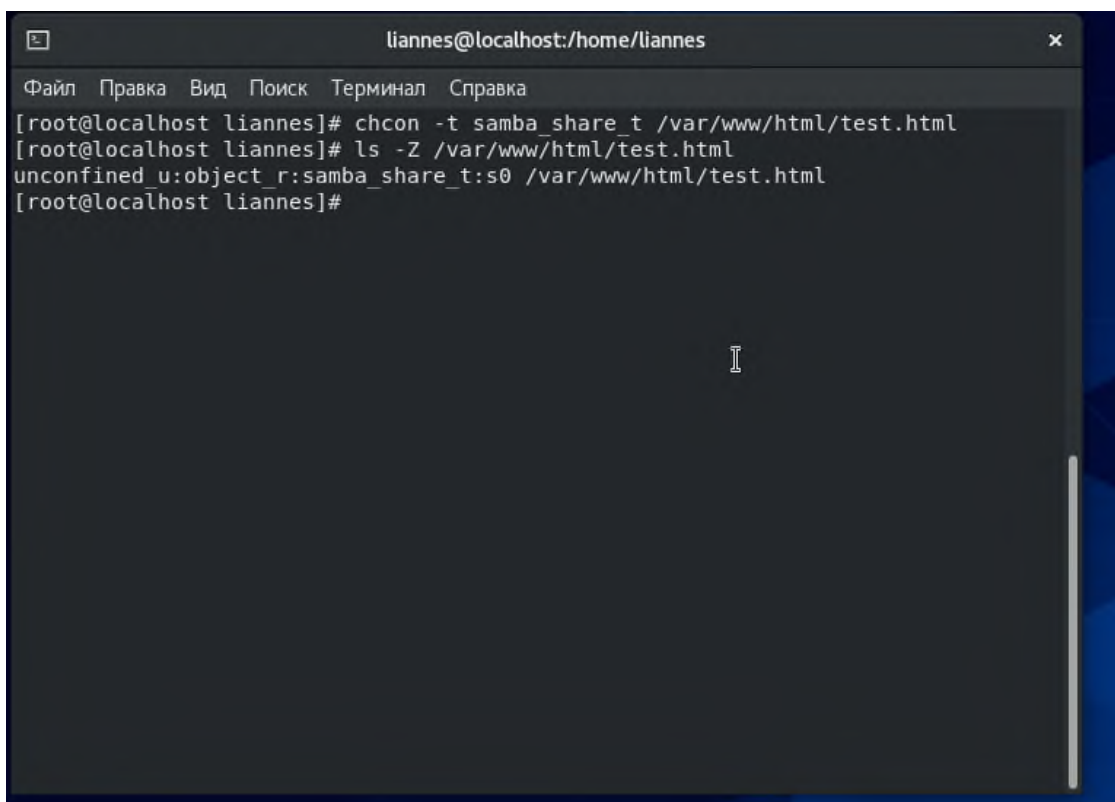
```
liannes@localhost:/home/liannes
Файл  Правка  Вид  Поиск  Терминал  Справка
[root@localhost liannes]# nano /var/www/html/test.html
[root@localhost liannes]# nano /var/www/html/test.html
[root@localhost liannes]# ls -lA /var/www/html
итого 4
-rw-r--r--. 1 root root 33 ноя 27 19:26 test.html
[root@localhost liannes]# chmod o+w /var/www/html/test.html
[root@localhost liannes]# chmod o-w /var/www/html/test.html
[root@localhost liannes]# ls -lZ /var/www/html/
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 ноя 27 1
9:26 test.html
[root@localhost liannes]#
```

*Контекст*

## Выполнение лабораторной работы

Изменил контекст файла test.html на samba\_share\_t (рис. -@fig:015)



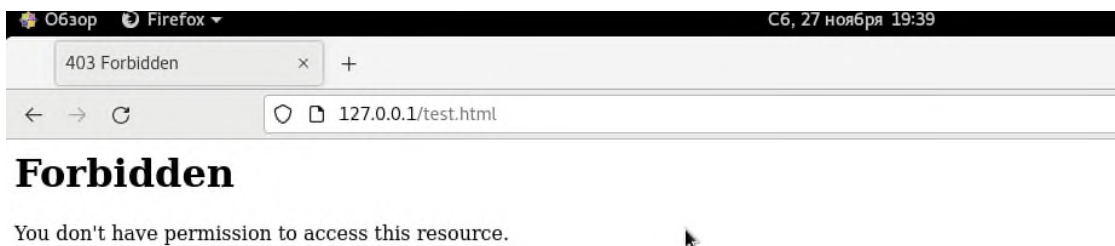


```
liannes@localhost:/home/liannes
Файл Правка Вид Поиск Терминал Справка
[root@localhost liannes]# chcon -t samba_share_t /var/www/html/test.html
[root@localhost liannes]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@localhost liannes]#
```

*Контекст*

## Выполнение лабораторной работы

Обновил страницу браузера и увидел ошибку (рис. -@fig:016)



*Содержимое страницы*

## Выполнение лабораторной работы

Просмотрел файл log/messages (рис. -@fig:017)

```
liannes@localhost:/home/liannes
Файл Правка Вид Поиск Терминал Справка
[liannes@localhost ~]$ tails /var/log/messages
bash: tails: команда не найдена...
Аналогичная команда: 'tail'
[liannes@localhost ~]$ tail /var/log/messages
tail: невозможно открыть '/var/log/messages' для чтения: Отказано в доступе
[liannes@localhost ~]$ su
Пароль:
[root@localhost liannes]# tail /var/log/messages
Nov 27 19:39:12 localhost setroubleshoot[8001]: SELinux is preventing /usr/sbin/httpd from get
attr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l
bcead8d0-04da-4738-b7d2-8c1ec2474ac1
Nov 27 19:39:12 localhost setroubleshoot[8001]: SELinux is preventing /usr/sbin/httpd from get
attr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 confide
nce) suggests *****#012#012If you want to fix the label. #012/var/www/htm
l/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. The a
ccess attempt may have been stopped due to insufficient permissions to access a parent directo
ry in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon
-v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggests **
*****#012#012If you want to treat test.html as public content#012Then you need to
change the label on test.html to public_content_t or public_content_rw_t.#012Do#012# semanage
fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/t
est.html'#012#012***** Plugin catchall (1.41 confidence) suggests *****
*#012#012If you believe that httpd should be allowed getattr access on the test.html file by d
efault.#012Then you should report this as a bug.#012You can generate a local policy module to
allow this access.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd' -
-r raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Nov 27 19:39:14 localhost setroubleshoot[8001]: failed to retrieve rpm info for /var/www/html/
test.html
```

Лог messages

## Выполнение лабораторной работы

Изменил tcp порт на 81 (рис. -@fig:018)

```
liannes@localhost:/home/liannes
Файл Правка Вид Поиск Терминал Справка
GNU nano 2.9.8 /etc/httpd/conf/httpd.conf

# 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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#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

[ Wrote 355 lines ]
^G Помощь ^O Записать ^W Поиск ^K Вырезать ^J Выворнять ^C ТекПозиц
^X Выход ^R ЧитФайл ^\ Замена ^U Отмен. вырез ^T Словарь ^_ К строке
```

Смена порта

## Выполнение лабораторной работы

Запустил httpd и все получилось удачно, тк как 81 входит в политеку SeLinux (рис. -@fig:019)

Перезапуск httpd

## Выполнение лабораторной работы

Посмотрел логи файлов access\_log и error\_log, и не нашел ничего не криминального (рис. -@fig:020, -@fig:021)

Содержимое access\_log

Содержимое error\_log

## Выполнение лабораторной работы

Добавил в политику порт 81 и проверил на корректность (рис. -@fig:022)

Проверка портов

## Выполнение лабораторной работы

Перезапустил httpd и все прошло успешно (рис. -@fig:023)

Проверка портов

## Выполнение лабораторной работы

Поменял порт на 82 и получил ошибку, потому что он не в ходит в политеку SeLinux (рис. -@fig:024)

Ошибка запуска

## Выводы

В результате выполнения познакомился с SeLinux и развил навыки владения ОС Linux