

Отчет по лабораторной работе №6

Мандатное разграничение прав

Гисматуллин Артём Вадимович НПИбд-01-22

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	20
	Список литературы	21

Список иллюстраций

3.1	Командная строка. Проверка работоспособности сервера	7
3.2	Командная строка. Веб-сервер запущен в процессе	8
3.3	Командная строка. Текущее состояние переключателей	9
3.4	Командная строка. Статистика о политике	10
3.5	Командная строка. Информация о директории и файле	11
3.6	Браузер. Проверка отображения файла	12
3.7	Командная строка. Изменение контекста файла	13
3.8	Браузер. Попытка посетить сайт	14
3.9	Командная строка. Просмотр ошибок	15
3.10	Командная строка. Изменение конфигурационного файла	16
3.11	Браузер. Попытка соединения	17
3.12	Командная строка. Просмотр ошибок	17
3.13	Командная строка. Проверка изменений	18
3.14	Командная строка. Повторный запуск сервера	18
3.15	Командная строка. Удаление	19

Список таблиц

1 Цель работы

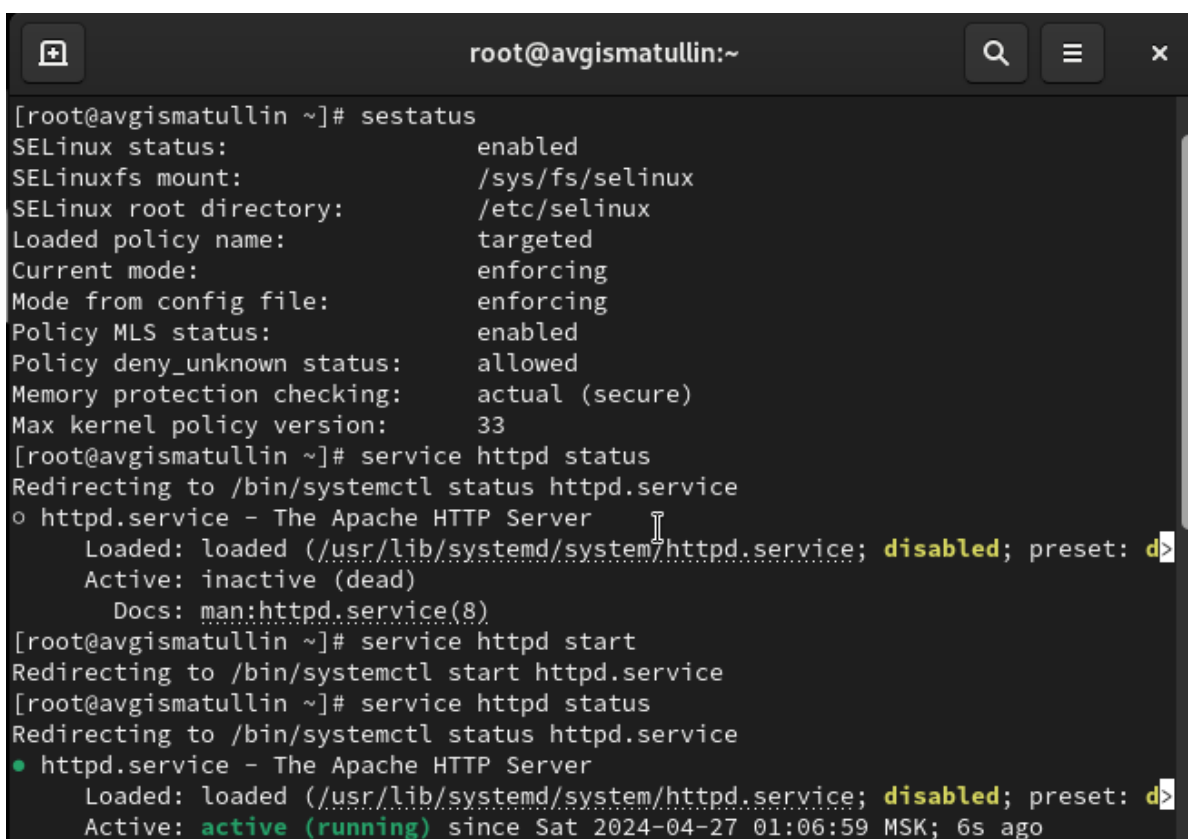
- Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1.
- Проверить работу SELinx на практике совместно с веб-сервером Apache.

2 Задание

Последовательно выполнять все пункты, занося ответы и замечания в отчет.

3 Выполнение лабораторной работы

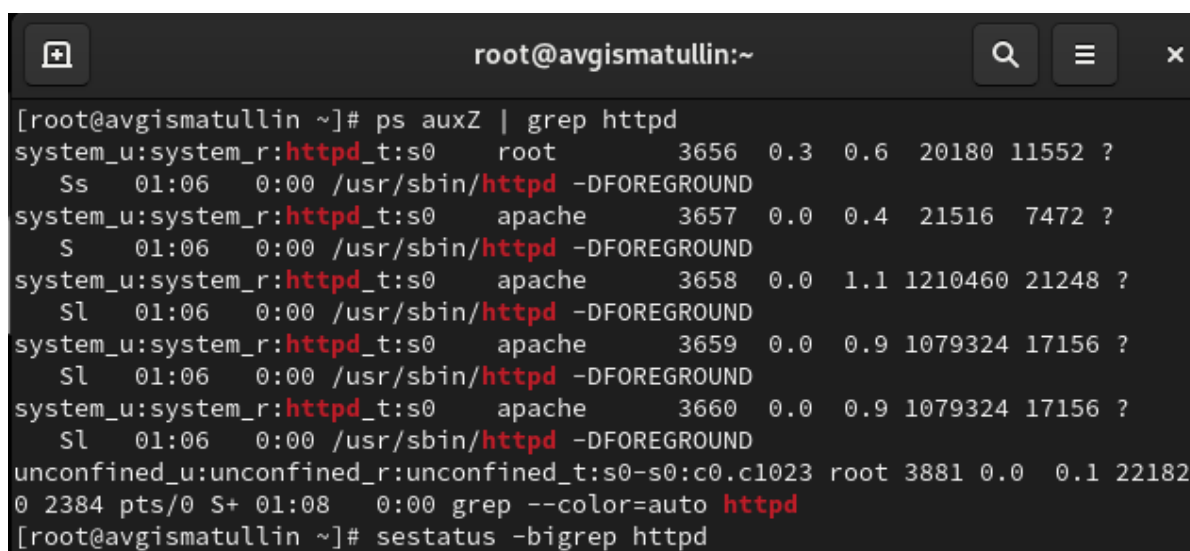
1. После выполнения всех требований для данной лабораторной работы, обратимся к веб-серверу и убедимся, что он у нас успешно работает (команда `service httpd status`) (рис. 3.1)



```
root@avgismatullin:~  
[root@avgismatullin ~]# 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@avgismatullin ~]# 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; preset: d>  
   Active: inactive (dead)  
   Docs: man:httpd.service(8)  
[root@avgismatullin ~]# service httpd start  
Redirecting to /bin/systemctl start httpd.service  
[root@avgismatullin ~]# 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; preset: d>  
   Active: active (running) since Sat 2024-04-27 01:06:59 MSK; 6s ago
```

Рис. 3.1: Командная строка. Проверка работоспособности сервера

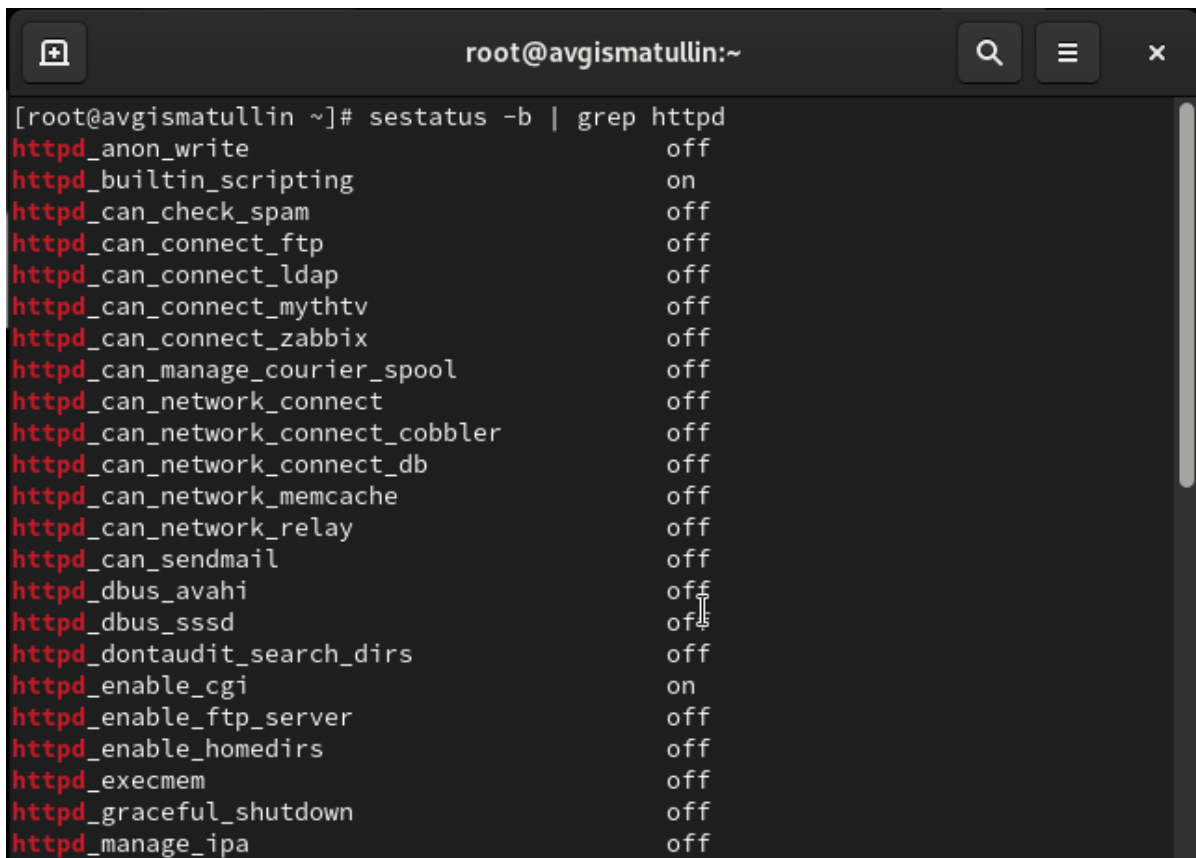
2. Найдем веб-сервер Apache списке процессов и убедимся, что он доступен только для суперпользователей (рис. 3.2)



```
root@avgismatullin:~  
[root@avgismatullin ~]# ps auxZ | grep httpd  
system_u:system_r:httpd_t:s0 root 3656 0.3 0.6 20180 11552 ?  
Ss 01:06 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3657 0.0 0.4 21516 7472 ?  
S 01:06 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3658 0.0 1.1 1210460 21248 ?  
Sl 01:06 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3659 0.0 0.9 1079324 17156 ?  
Sl 01:06 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3660 0.0 0.9 1079324 17156 ?  
Sl 01:06 0:00 /usr/sbin/httpd -DFOREGROUND  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 3881 0.0 0.1 22182  
0 2384 pts/0 S+ 01:08 0:00 grep --color=auto httpd  
[root@avgismatullin ~]# sestatus -bigrep httpd
```

Рис. 3.2: Командная строка. Веб-сервер запущен в процессе

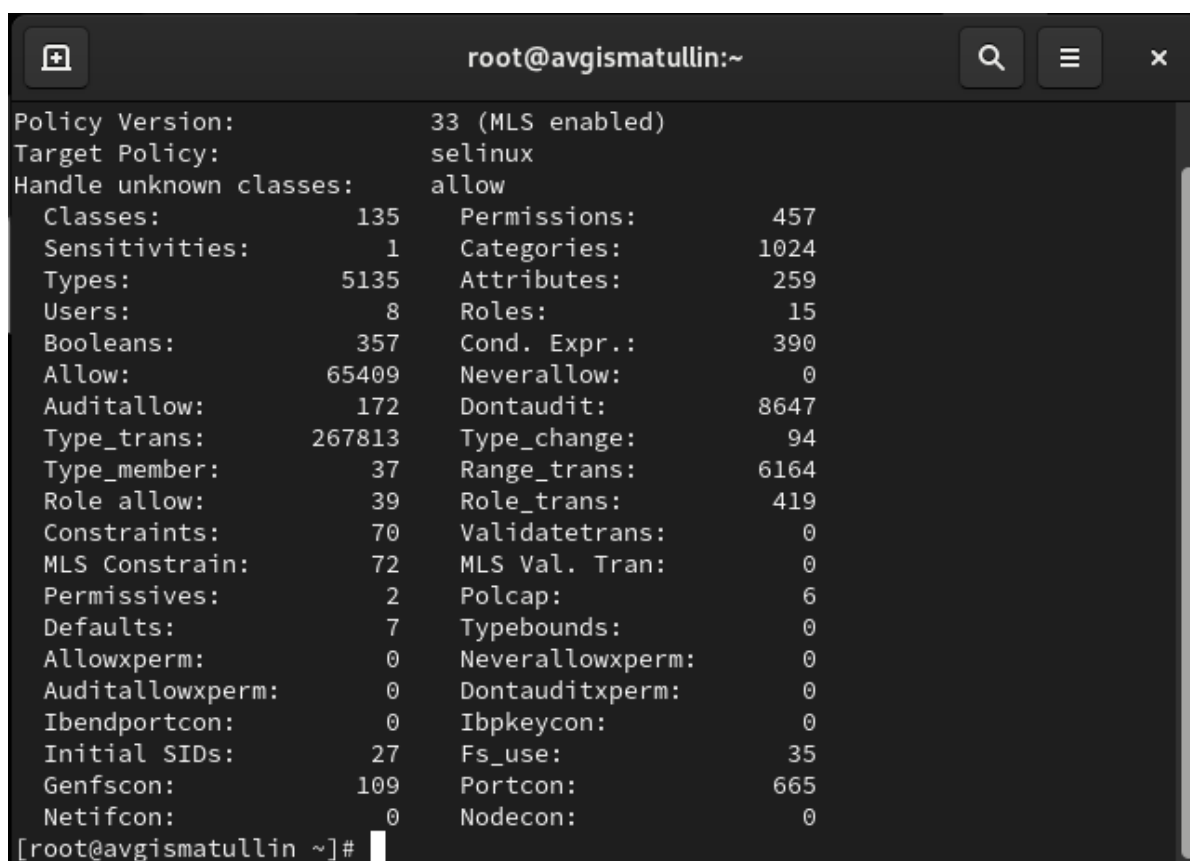
3. Далее командой `sestatus -b | grep` посмотрим текущее состояние переключателей SELinux для Apache (рис. 3.3)



```
[root@avgismatullin ~]# 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_manage_courier_spool 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
```

Рис. 3.3: Командная строка. Текущее состояние переключателей

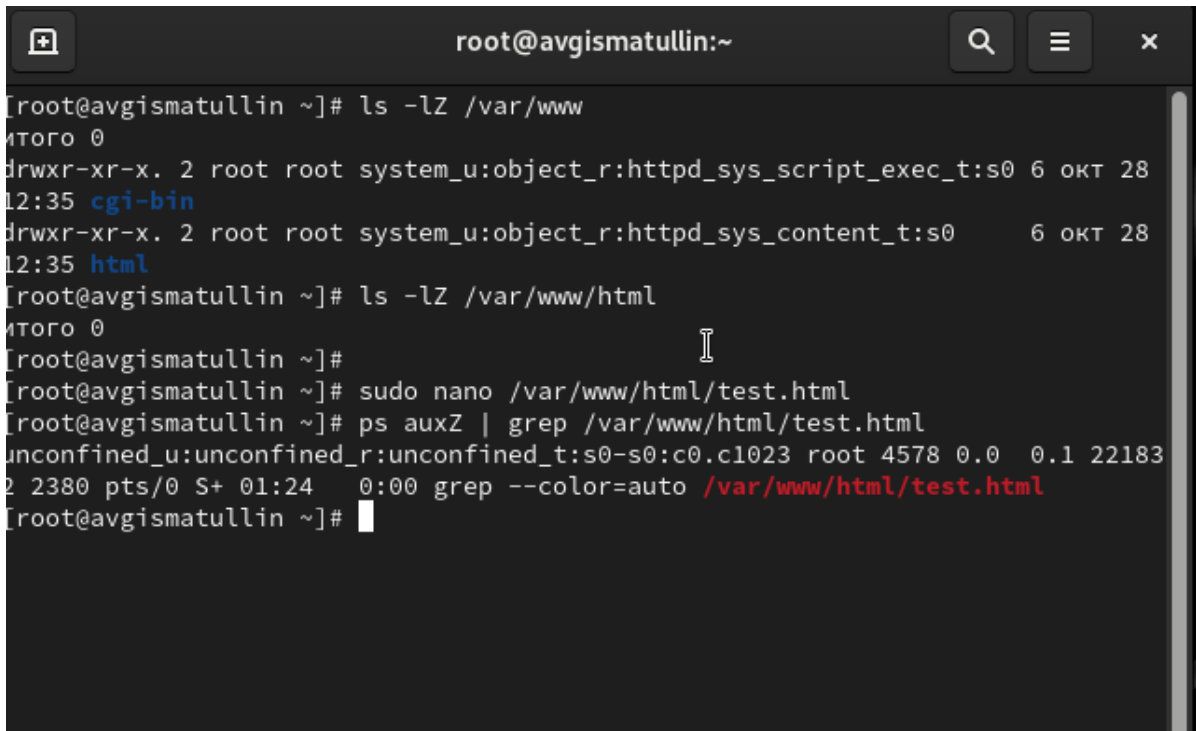
4. После этого при помощи команды `seinfo` посмотрим статистику по политике, определим множество пользователей, ролей и типов (рис. 3.4)

A terminal window titled 'root@avgismatullin:~' with search, menu, and close icons in the title bar. It displays the output of the 'seinfo' command, showing SELinux policy statistics. The output is organized into two columns. The first column lists various SELinux components and their counts, while the second column lists other components and their counts. The prompt '[root@avgismatullin ~]#' is visible at the bottom.

```
Policy Version:      33 (MLS enabled)
Target Policy:      selinux
Handle unknown classes:  allow
Classes:            135      Permissions:          457
Sensitivities:      1       Categories:          1024
Types:              5135     Attributes:           259
Users:              8       Roles:                15
Booleans:           357     Cond. Expr.:         390
Allow:              65409    Neverallow:           0
Auditallow:         172     Dontaudit:           8647
Type_trans:         267813   Type_change:          94
Type_member:        37      Range_trans:         6164
Role allow:         39      Role_trans:          419
Constraints:        70      Validatetrans:        0
MLS Constrains:     72      MLS Val. Tran:        0
Permissives:        2       Polcap:               6
Defaults:           7       Typebounds:           0
Allowxperm:         0       Neverallowxperm:      0
Auditallowxperm:    0       Dontauditxperm:       0
Ibendportcon:       0       Ibpkeycon:            0
Initial SIDs:       27      Fs_use:               35
Genfscon:           109     Portcon:              665
Netifcon:           0       Nodecon:              0
[root@avgismatullin ~]#
```

Рис. 3.4: Командная строка. Статистика о политике

5. Затем определим тип файлов в директории `/var/www` и `/var/www/html`, создадим файл `test.html` с выводом в теле слова “test” и проверим его контекст (рис. 3.5)



```
root@avgismatullin:~  
[root@avgismatullin ~]# ls -lZ /var/www  
итого 0  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 окт 28  
12:35 cgi-bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 окт 28  
12:35 html  
[root@avgismatullin ~]# ls -lZ /var/www/html  
итого 0  
[root@avgismatullin ~]#  
[root@avgismatullin ~]# sudo nano /var/www/html/test.html  
[root@avgismatullin ~]# ps auxZ | grep /var/www/html/test.html  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 4578 0.0 0.1 22183  
2 2380 pts/0 S+ 01:24 0:00 grep --color=auto /var/www/html/test.html  
[root@avgismatullin ~]#
```

Рис. 3.5: Командная строка. Информация о директории и файле

6. После этого Зайдем по локальному адресу и проверим работоспособность сервера (рис. 3.6)

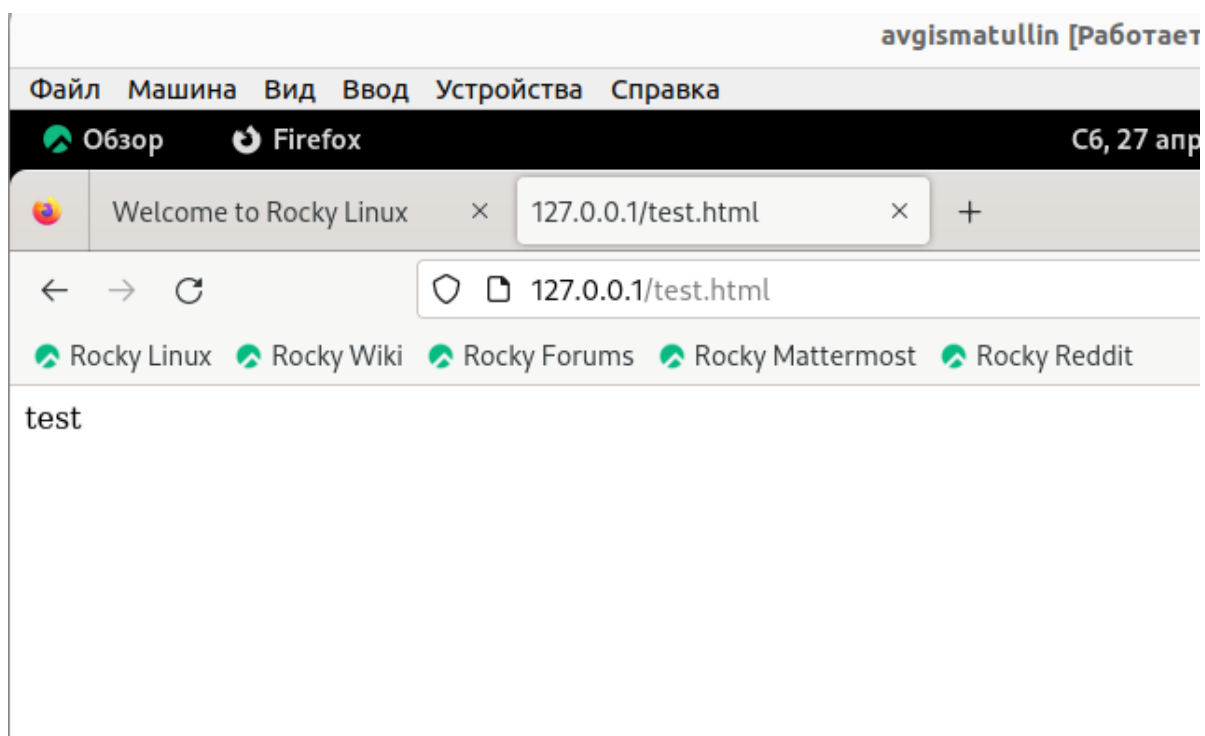
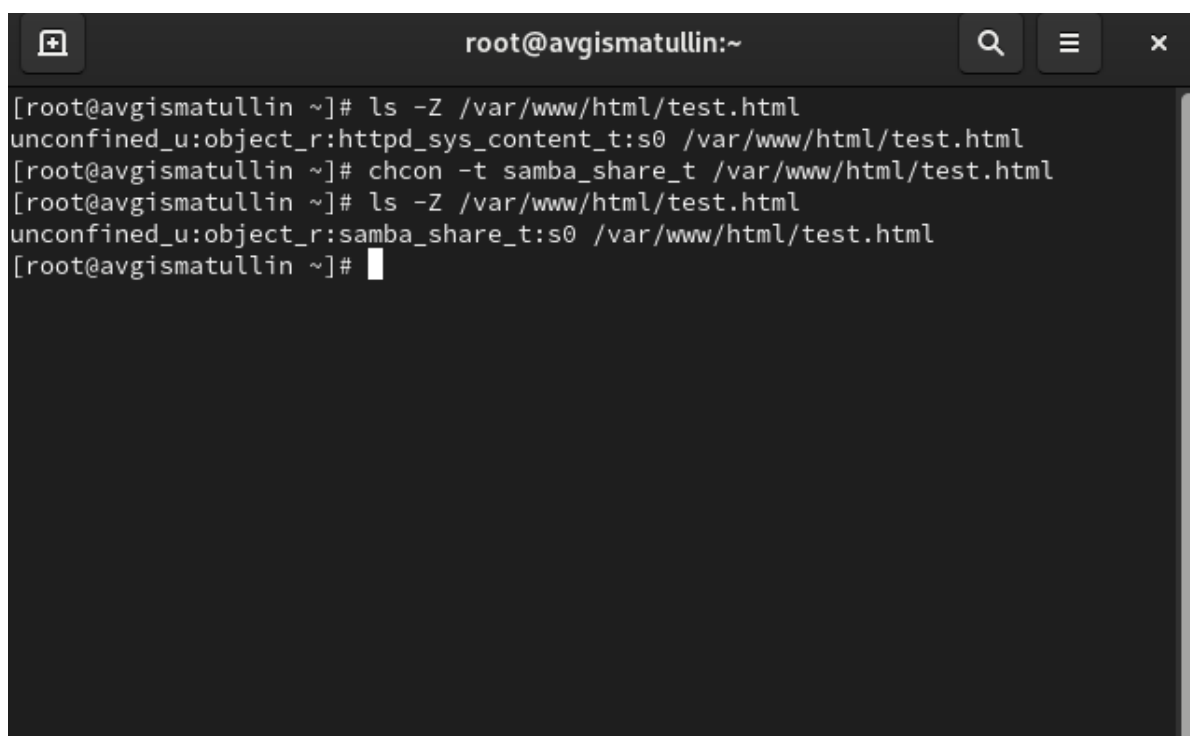


Рис. 3.6: Браузер. Проверка отображения файла

7. Мы можем успешно изменять контекст файла командой `chcon`. Сделаем это, прописав `samba_share_t` (рис. 3.7)

A terminal window titled 'root@avgismatullin:~' with search, menu, and close icons in the title bar. The terminal shows the following commands and output:

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

Рис. 3.7: Командная строка. Изменение контекста файла

8. Как видим, доступ к файлу через веб-сервер мы потеряли (рис. 3.8)

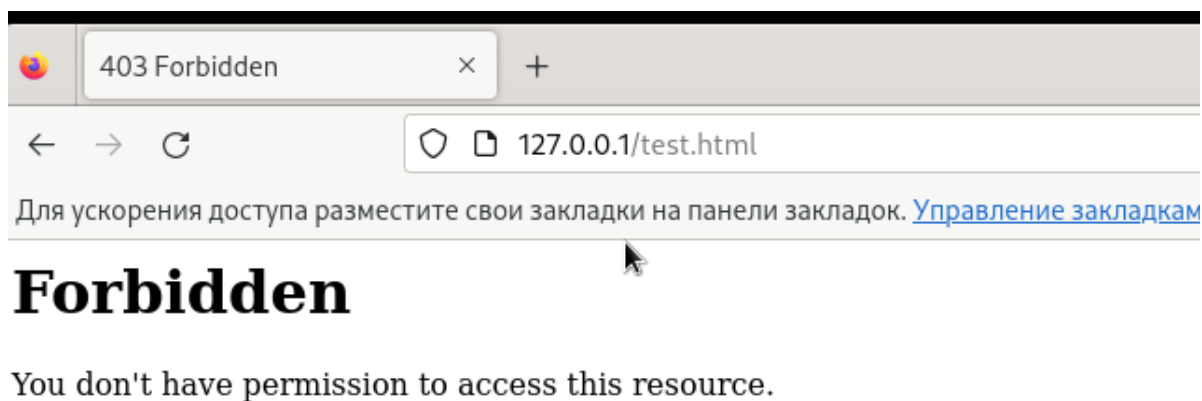
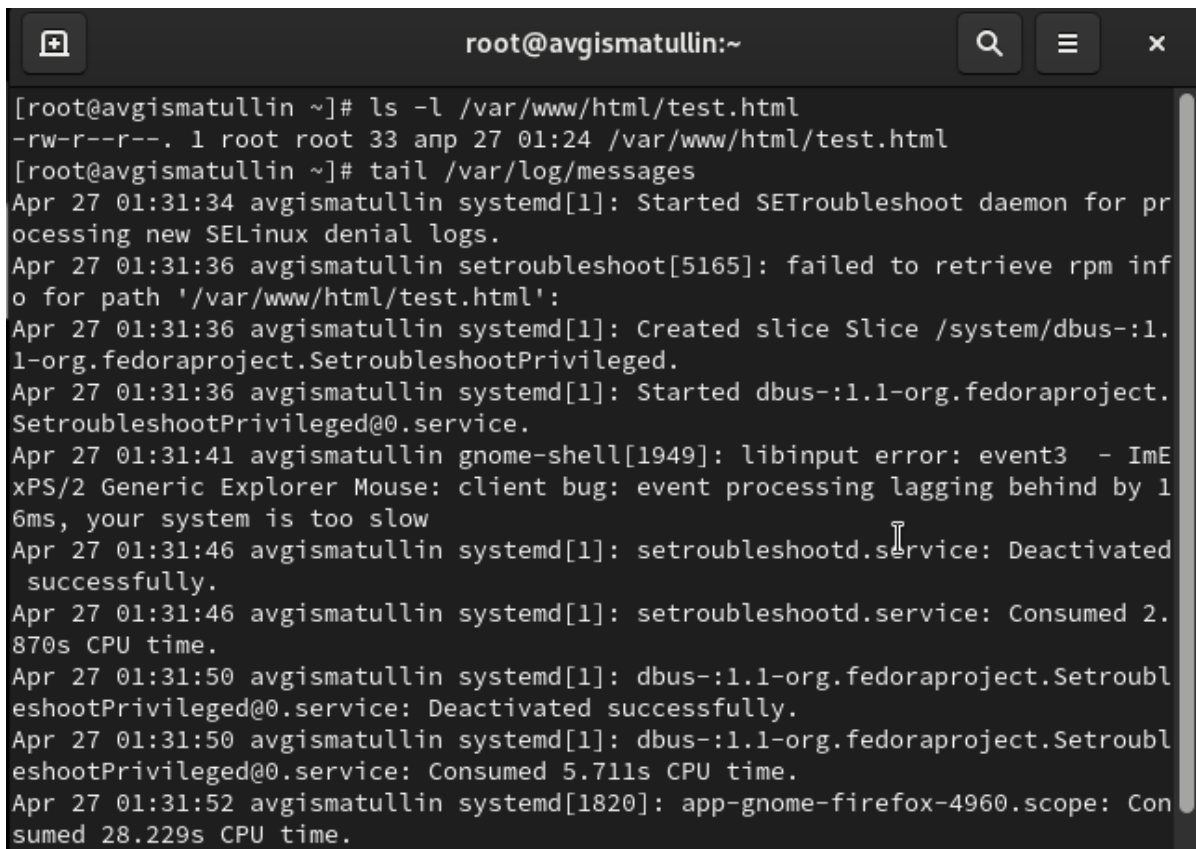


Рис. 3.8: Браузер. Попытка посетить сайт

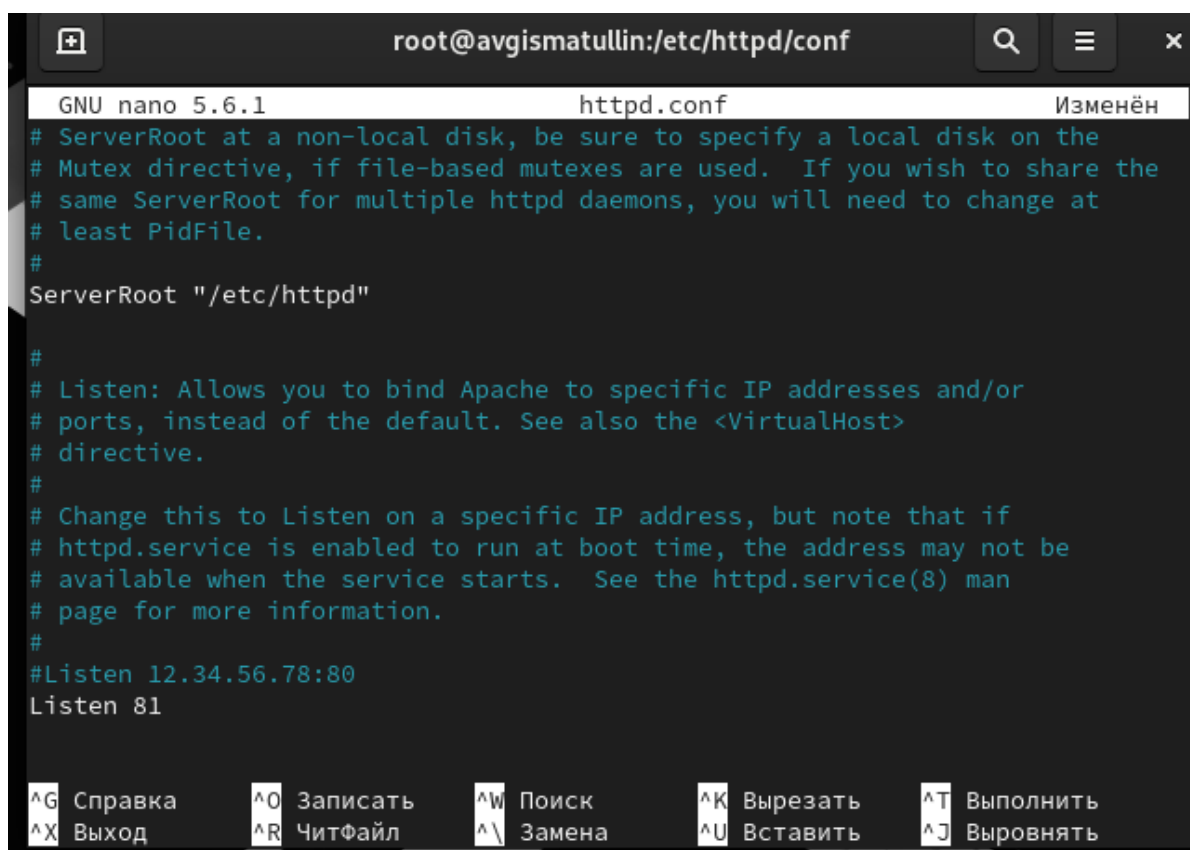
9. Проанализируем атрибуты файла, а также log-файлы веб-сервера. Оказалось, что там запущены setroubleshootd процессы (рис. 3.9)

A terminal window titled 'root@avgismatullin:~' with search, menu, and close icons in the title bar. The terminal displays the output of 'ls -l /var/www/html/test.html' and 'tail /var/log/messages'. The logs show the startup of the SELinux denial logs, the setroubleshoot daemon, and the dbus service. It also includes a libinput error message about event processing lagging behind by 16ms, and CPU time consumption for the setroubleshootd and dbus services.

```
root@avgismatullin:~  
[root@avgismatullin ~]# ls -l /var/www/html/test.html  
-rw-r--r--. 1 root root 33 anp 27 01:24 /var/www/html/test.html  
[root@avgismatullin ~]# tail /var/log/messages  
Apr 27 01:31:34 avgismatullin systemd[1]: Started SETroubleshoot daemon for processing new SELinux denial logs.  
Apr 27 01:31:36 avgismatullin setroubleshoot[5165]: failed to retrieve rpm info for path '/var/www/html/test.html':  
Apr 27 01:31:36 avgismatullin systemd[1]: Created slice Slice /system/dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged.  
Apr 27 01:31:36 avgismatullin systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service.  
Apr 27 01:31:41 avgismatullin gnome-shell[1949]: libinput error: event3 - ImExPS/2 Generic Explorer Mouse: client bug: event processing lagging behind by 16ms, your system is too slow  
Apr 27 01:31:46 avgismatullin systemd[1]: setroubleshootd.service: Deactivated successfully.  
Apr 27 01:31:46 avgismatullin systemd[1]: setroubleshootd.service: Consumed 2.870s CPU time.  
Apr 27 01:31:50 avgismatullin systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated successfully.  
Apr 27 01:31:50 avgismatullin systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Consumed 5.711s CPU time.  
Apr 27 01:31:52 avgismatullin systemd[1820]: app-gnome-firefox-4960.scope: Consumed 28.229s CPU time.
```

Рис. 3.9: Командная строка. Просмотр ошибок

10. Попробуем запустить веб-сервер на прослушивание TCP-порта 81, а не 80, как было ранее, изменив соответствующий параметр в конфигурационном файле (рис. 3.10)



The screenshot shows a terminal window with the title bar "root@avgismatullin:/etc/httpd/conf". The nano text editor is open, editing the file "httpd.conf". The editor's status bar at the top indicates "GNU nano 5.6.1", the filename "httpd.conf", and the state "Изменён" (Changed). The content of the file is as follows:

```
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used.  If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"
#
# 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 a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts.  See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 81
```

The bottom of the window displays the nano editor's keyboard shortcuts in Russian:

^G Справка	^O Записать	^W Поиск	^K Вырезать	^T Выполнить
^X Выход	^R ЧитФайл	^_\ Замена	^U Вставить	^J Выровнять

Рис. 3.10: Командная строка. Изменение конфигурационного файла

11. Обнаружилось, что доступ к сайту мы потеряли. Сервер не готов прослушивать нас на этом порте (рис. 3.11)

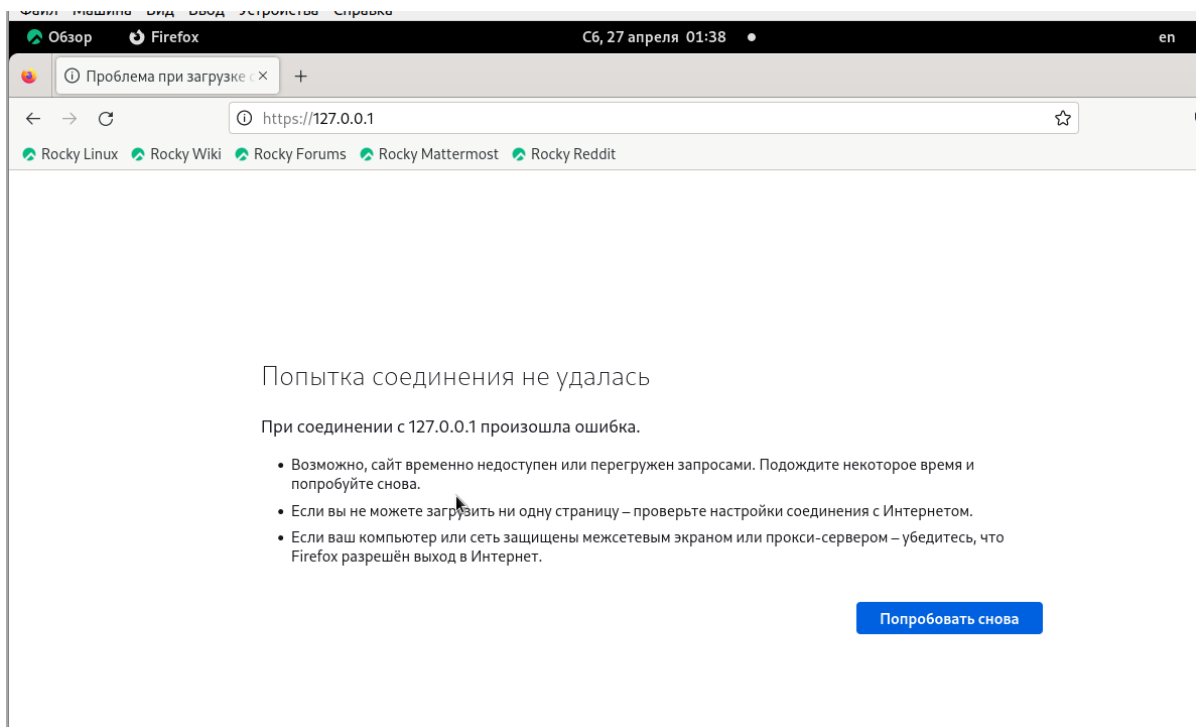


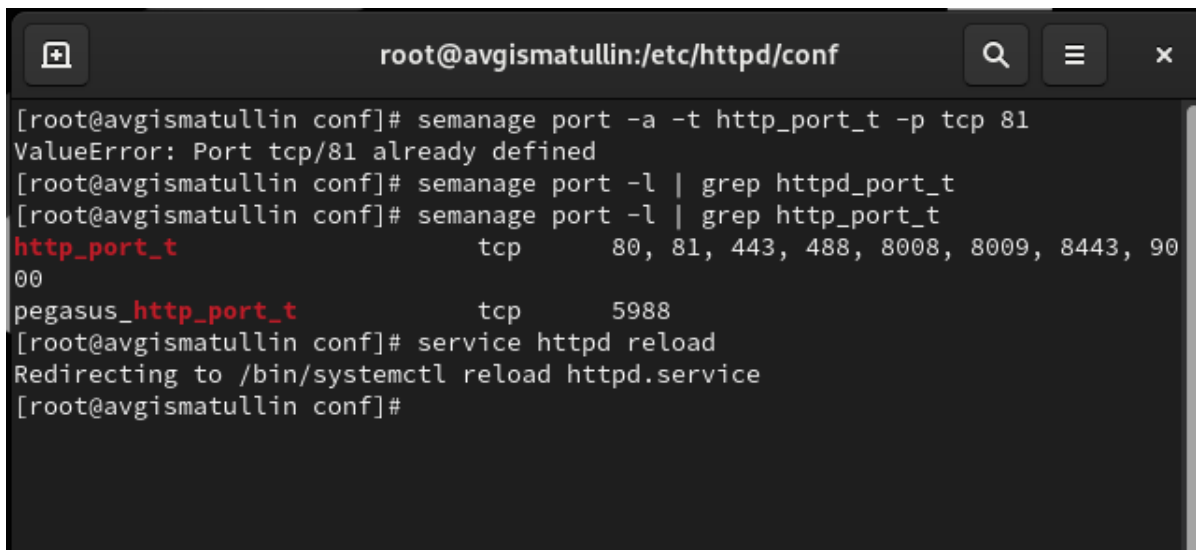
Рис. 3.11: Браузер. Попытка соединения

12. Проанализируем ошибки, посмотрим лог файлы и проследим за полученными запросами серверу (рис. 3.12)

```
[root@avgismatullin conf]# sudo cat /var/log/httpd/access_log
127.0.0.1 - - [27/Apr/2024:01:15:22 +0300] "GET / HTTP/1.1" 403 7620 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [27/Apr/2024:01:15:27 +0300] "GET /icons/poweredby.png HTTP/1.1" 200 15443 "http://127.0.0.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [27/Apr/2024:01:15:27 +0300] "GET /poweredby.png HTTP/1.1" 200 5714 "http://127.0.0.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [27/Apr/2024:01:15:28 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [27/Apr/2024:01:26:01 +0300] "GET /test.html HTTP/1.1" 200 33 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [27/Apr/2024:01:31:30 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
[root@avgismatullin conf]#
```

Рис. 3.12: Командная строка. Просмотр ошибок

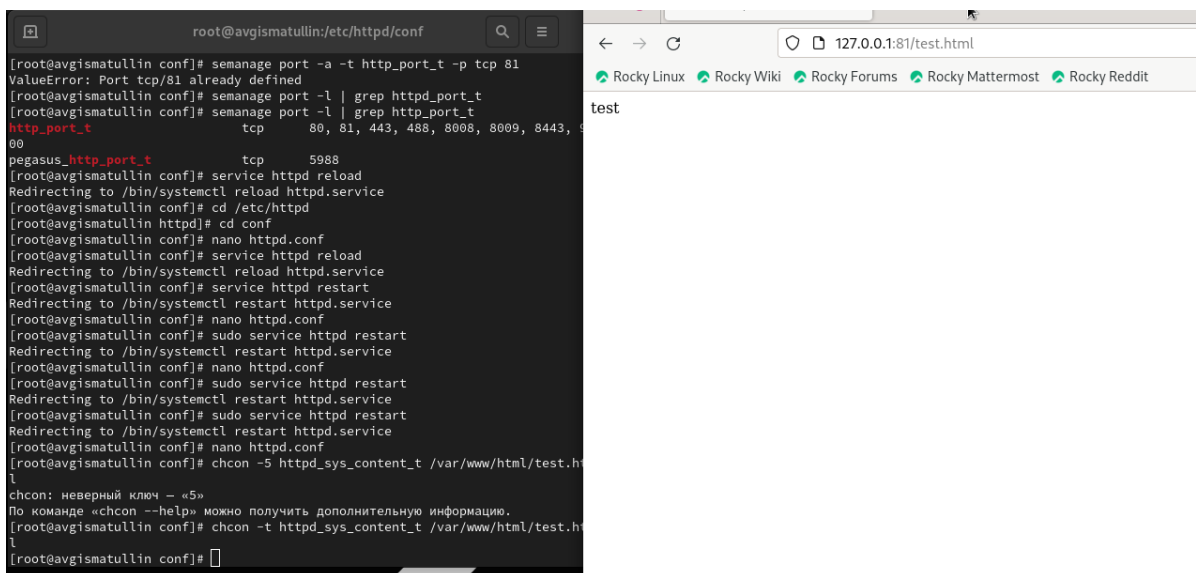
13. Выполним команду `semanage port -a -t http_port_t -p tcp 81` и проверим изменения (рис. 3.13)



```
root@avgismatullin:/etc/httpd/conf
[root@avgismatullin conf]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@avgismatullin conf]# semanage port -l | grep httpd_port_t
[root@avgismatullin conf]# semanage 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@avgismatullin conf]# service httpd reload
Redirecting to /bin/systemctl reload httpd.service
[root@avgismatullin conf]#
```

Рис. 3.13: Командная строка. Проверка изменений

14. Перезапустим сервер и попробуем запустить его после изменения контекста обратно, а также указания порта 81 (рис. 3.14)



```
root@avgismatullin:/etc/httpd/conf
[root@avgismatullin conf]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@avgismatullin conf]# semanage port -l | grep httpd_port_t
[root@avgismatullin conf]# semanage 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@avgismatullin conf]# service httpd reload
Redirecting to /bin/systemctl reload httpd.service
[root@avgismatullin conf]# cd /etc/httpd
[root@avgismatullin httpd]# cd conf
[root@avgismatullin conf]# nano httpd.conf
[root@avgismatullin conf]# service httpd reload
Redirecting to /bin/systemctl reload httpd.service
[root@avgismatullin conf]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@avgismatullin conf]# nano httpd.conf
[root@avgismatullin conf]# sudo service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@avgismatullin conf]# nano httpd.conf
[root@avgismatullin conf]# sudo service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@avgismatullin conf]# nano httpd.conf
[root@avgismatullin conf]# chcon -t httpd_sys_content_t /var/www/html/test.html
chcon: неверный ключ - «5»
По команде «chcon --help» можно получить дополнительную информацию.
[root@avgismatullin conf]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@avgismatullin conf]#
```

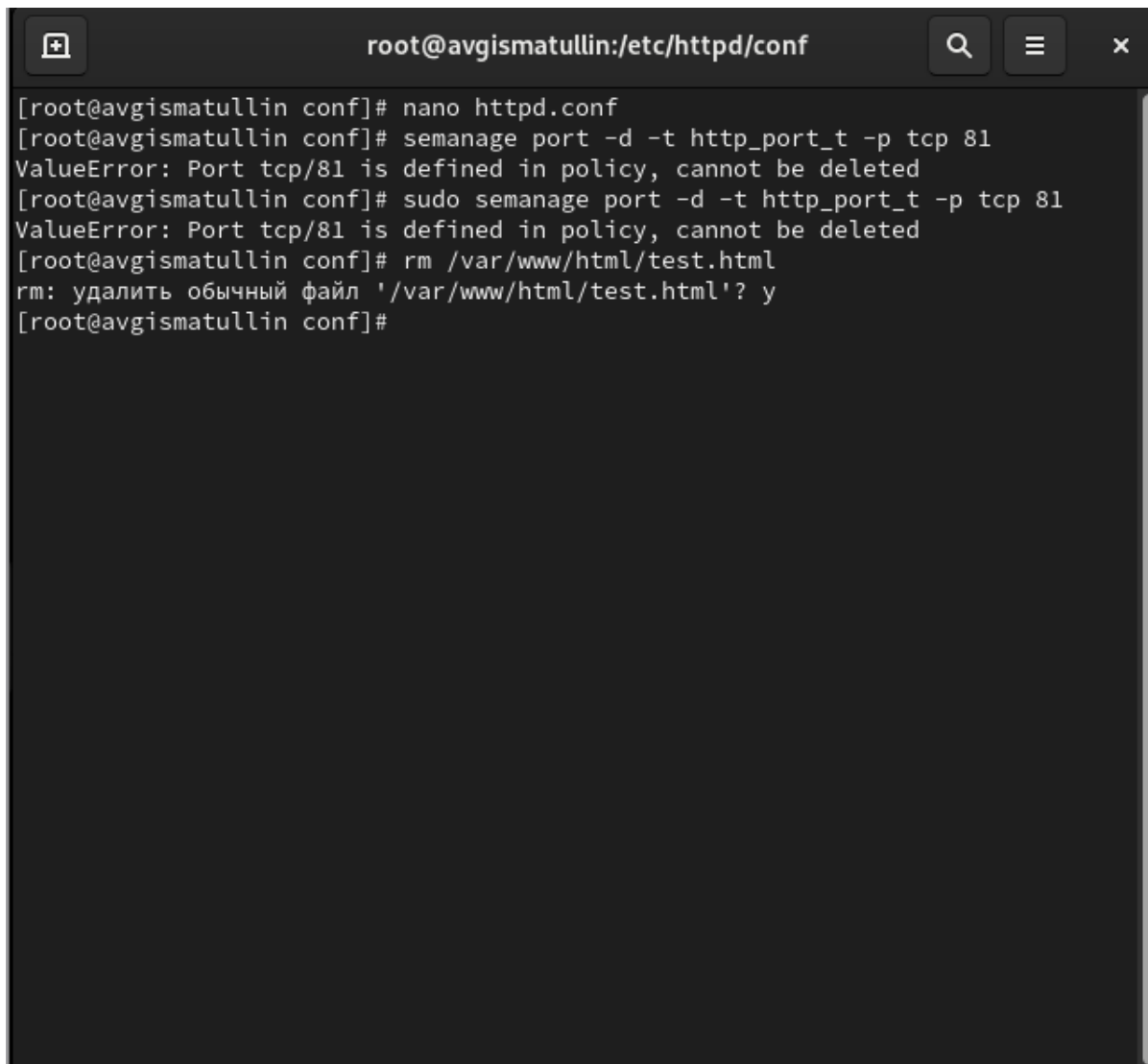
127.0.0.1:81/test.html

Rocky Linux Rocky Wiki Rocky Forums Rocky Mattermost Rocky Reddit

test

Рис. 3.14: Командная строка. Повторный запуск сервера

15. Удалим привязку контекста файла к порту 81, а также сам html файлов (рис. 3.15)

A terminal window titled 'root@avgismatullin:/etc/httpd/conf' with search, menu, and close buttons. It shows a series of commands and their outputs: 'nano httpd.conf' is executed; 'semanage port -d -t http_port_t -p tcp 81' is executed and returns 'ValueError: Port tcp/81 is defined in policy, cannot be deleted'; 'sudo semanage port -d -t http_port_t -p tcp 81' is executed and returns the same error; 'rm /var/www/html/test.html' is executed and returns 'rm: удалить обычный файл '/var/www/html/test.html'? y'; the prompt returns to the root user.

```
[root@avgismatullin conf]# nano httpd.conf
[root@avgismatullin conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@avgismatullin conf]# sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@avgismatullin conf]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@avgismatullin conf]#
```

Рис. 3.15: Командная строка. Удаление

4 Выводы

В ходе выполнения данной лабораторной работы были развиты навыки администрирования ОС Linux, а также проверена работа SELinux на практике совместно с веб-сервером Apache.

Список литературы

1. Теория разграничения прав пользователей
2. Разрешения доступа к файлам