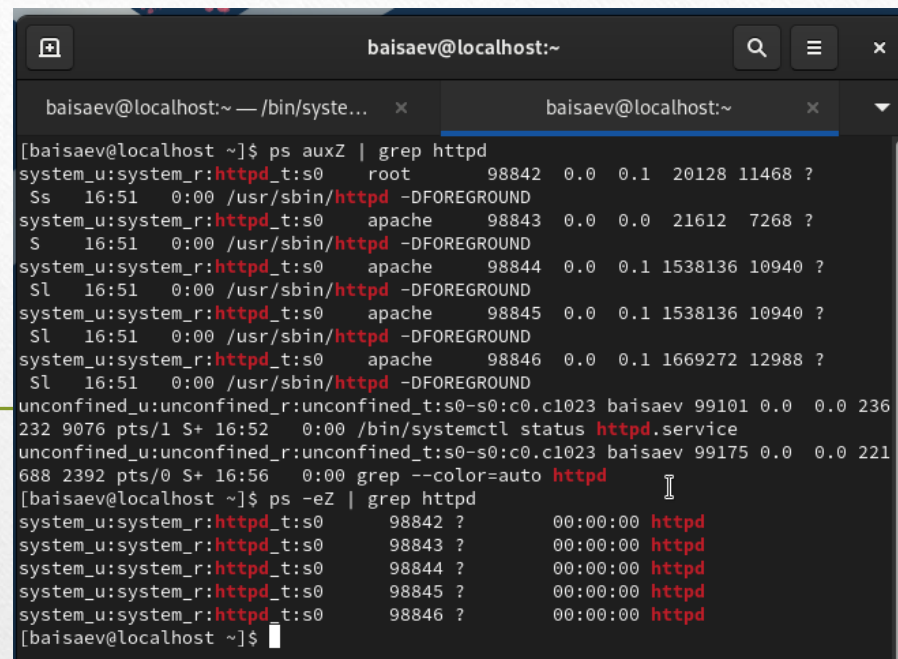


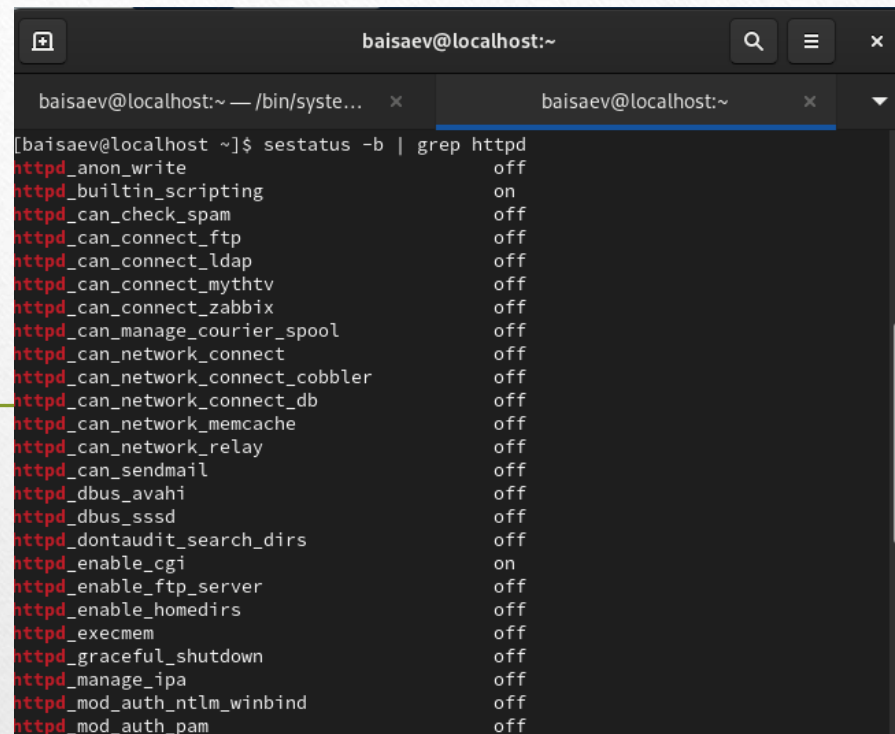

```
baisaev@localhost:~ — /bin/systemctl status httpd.service
[baiaev@localhost ~]$ getenforce
Enforcing
[baiaev@localhost ~]$ sestatus
SELinux status:                enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:              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
[baiaev@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; enabled; preset: disabled)
   Active: active (running) since Sat 2024-04-27 16:51:48 +04; 45s ago
     Docs: man:httpd.service(8)
   Main PID: 98842 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served: 0"
   Tasks: 213 (limit: 65577)
  Memory: 23.2M
    CPU: 85ms
   CGroup: /system.slice/httpd.service
           └─98842 /usr/sbin/httpd -DFOREGROUND
```

Рис. 1: Запуск и проверка веб-сервера

A terminal window titled 'baisaev@localhost:~' with two tabs. The first tab shows the command 'ps auxZ | grep httpd' and its output, which lists several httpd processes with their full SELinux contexts. The second tab shows the command 'ps -eZ | grep httpd' and its output, which shows the same processes with abbreviated SELinux contexts. The terminal output is as follows:

```
[baisaev@localhost ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 98842 0.0 0.1 20128 11468 ?
Ss 16:51 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 98843 0.0 0.0 21612 7268 ?
S 16:51 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 98844 0.0 0.1 1538136 10940 ?
Sl 16:51 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 98845 0.0 0.1 1538136 10940 ?
Sl 16:51 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 98846 0.0 0.1 1669272 12988 ?
Sl 16:51 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 baisaev 99101 0.0 0.0 236
232 9076 pts/1 S+ 16:52 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 baisaev 99175 0.0 0.0 221
688 2392 pts/0 S+ 16:56 0:00 grep --color=auto httpd
[baisaev@localhost ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0 98842 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 98843 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 98844 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 98845 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 98846 ? 00:00:00 httpd
[baisaev@localhost ~]$
```

Рис. 2: Контекст безопасности веб-сервера



A terminal window titled 'baisaev@localhost:~' showing the output of the command 'sestatus -b | grep httpd'. The output lists various SELinux booleans for the httpd process, with most set to 'off' and a few to 'on'.

SELinux Boolean	Status
httpd_anon_write	off
httpd_built_in_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
httpd_mod_auth_ntlm_winbind	off
httpd_mod_auth_pam	off

Рис. 3: Состояние переключателей SELinux


```
baisaev@localhost:~  
[baisaev@localhost ~]$ seinfo  
Statistics for policy file: /sys/fs/selinux/policy  
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 Constrain: 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  
[baisaev@localhost ~]$
```

Рис. 4: Статистика по политике

```
[baisaev@localhost ~]$ 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 13
:35 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 окт 28 13
:35 html
[baisaev@localhost ~]$ ls -lZ /var/www/html
итого 0
[baisaev@localhost ~]$
```

Рис. 5: Определение типа файлов и папок

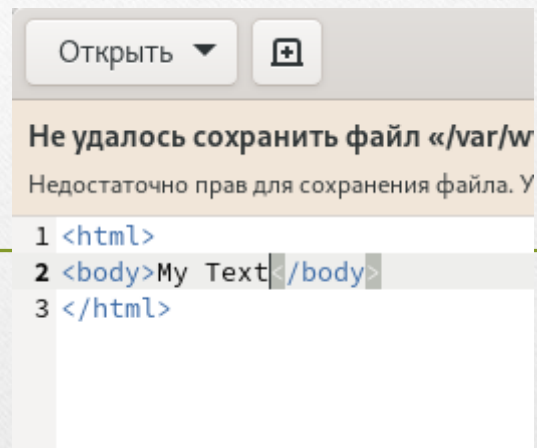


Рис. 6: test.html

```
[root@localhost ~]# ps auxZ | grep myfile.html  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 100374 0.0 0.0 22182  
4 2404 pts/0 S+ 17:42 0:00 grep --color=auto myfile.html  
[root@localhost ~]#
```

Рис. 7: Контекст файла

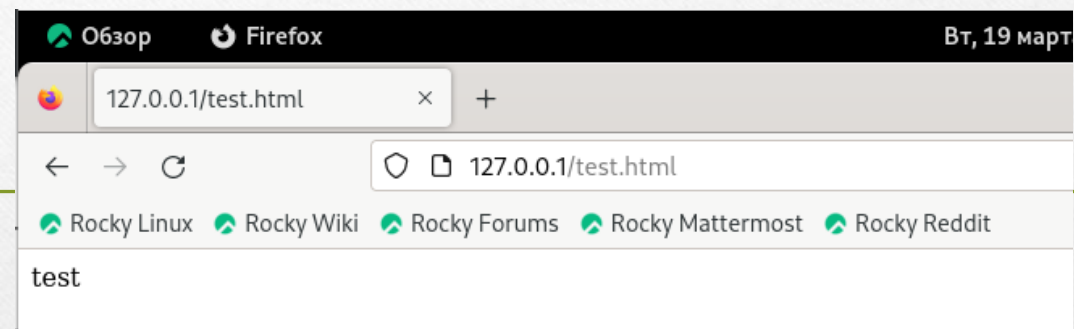


Рис. 8: Проверка в браузере


```
[root@localhost ~]# man httpd
[root@localhost ~]# man selinux
[root@localhost ~]# ls -Z /var/www/html/myfile.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/myfile.html
[root@localhost ~]#
```

Рис. 9: Изучение man, проверка контекста


```
[root@localhost ~]# tail /var/log/messages
Apr 27 17:29:08 localhost cupsd[896]: REQUEST localhost - - "POST / HTTP/1.1" 20
0 186 Renew-Subscription successful-ok
Apr 27 17:31:46 localhost systemd[2077]: dbus-:1.2-org.gnome.gedit@6.service: Co
nsumed 5.422s CPU time.
Apr 27 17:43:25 localhost systemd[2077]: Started dbus-:1.2-org.gnome.gedit@7.ser
vice.
Apr 27 17:43:26 localhost gnome-shell[2184]: meta_window_set_stack_position_no_s
ync: assertion 'window->stack_position >= 0' failed
Apr 27 17:43:39 localhost systemd[2077]: Started dbus-:1.2-org.gnome.gedit@8.ser
vice.
Apr 27 17:43:39 localhost gnome-shell[2184]: meta_window_set_stack_position_no_s
ync: assertion 'window->stack_position >= 0' failed
Apr 27 17:45:28 localhost systemd[2077]: Started dbus-:1.2-org.gnome.gedit@9.ser
vice.
Apr 27 17:45:29 localhost gnome-shell[2184]: meta_window_set_stack_position_no_s
ync: assertion 'window->stack_position >= 0' failed
Apr 27 17:45:42 localhost systemd[2077]: Started Application launched by gnome-s
hell.
Apr 27 17:45:45 localhost rtkit-daemon[748]: Successfully made thread 100628 of
process 100494 (/usr/lib64/firefox/firefox) owned by '1000' RT at priority 10.
[root@localhost ~]#
```

Рис. 10: Изменение контекста


```
# 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

#
# Dynamic Shared Object (DSO) Support
```

Рис. 12: Смена порта


```
[baisaev@localhost ~]$ sudo service httpd restart  
[sudo] пароль для baisaev:  
Попробуйте ещё раз.  
[sudo] пароль для baisaev:  
Redirecting to /bin/systemctl restart httpd.service  
[baisaev@localhost ~]$
```

Рис. 13: Сбой веб-сервера


```
[baisaev@localhost ~]$ tail -n1 /var/log/messages  
tail: невозможно открыть '/var/log/messages' для чтения: Отказано в доступе  
[baisaev@localhost ~]$ cat /var/log/httpd/error_log  
cat: /var/log/httpd/error_log: Отказано в доступе  
[baisaev@localhost ~]$ cat /var/log/httpd/error_log  
cat: /var/log/httpd/error_log: Отказано в доступе  
[baisaev@localhost ~]$ cat /var/log/httpd/error_log
```

Рис. 14: Проверка лог-файлов


```
[baisaev@localhost ~]$ tail -n1 /var/log/messages
tail: невозможно открыть '/var/log/messages' для чтения: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/error_log
cat: /var/log/httpd/error_log: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/error_log
cat: /var/log/httpd/error_log: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/error_log
cat: /var/log/httpd/error_log: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/access_log
cat: /var/log/httpd/access_log: Отказано в доступе
[baisaev@localhost ~]$
```

Рис. 15: Проверка лог-файлов


```
[baisaev@localhost ~]$ tail -n1 /var/log/messages
tail: невозможно открыть '/var/log/messages' для чтения: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/error_log
cat: /var/log/httpd/error_log: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/error_log
cat: /var/log/httpd/error_log: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/error_log
cat: /var/log/httpd/error_log: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/access_log
cat: /var/log/httpd/access_log: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/audit.log
cat: /var/log/httpd/audit.log: Отказано в доступе
[baisaev@localhost ~]$
```

Рис. 16: Проверка лог-файлов


```
[baisaev@localhost ~]$ cat /var/log/httpd/error_log
cat: /var/log/httpd/error_log: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/access_log
cat: /var/log/httpd/access_log: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/audit.log
cat: /var/log/httpd/audit.log: Отказано в доступе
[baisaev@localhost ~]$ semanage port -a -t http_port_t t tcp 81
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[baisaev@localhost ~]$ semanage port -l | grep httpd restart
grep: restart: Нет такого файла или каталога
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[baisaev@localhost ~]$ sudo service httpd restart
[sudo] пароль для baisaev:
Redirecting to /bin/systemctl restart httpd.service
```

Рис. 17: Добавление порта 81 в список


```
[baisaev@localhost ~]$ chcon -t httpd_sys_content_t /var/www/html/myfile.html  
[baisaev@localhost ~]$ sudo service httpd restart  
Redirecting to /bin/systemctl restart httpd.service  
[baisaev@localhost ~]$
```

Рис. 18: Возвращение контекста и перезапуск веб-сервера


```
#  
# Change this to Listen on a  
# httpd.service is enabled to  
# available when the service  
# page for more information.  
#  
#Listen 12.34.56.78:80  
Listen 80  
  
#  
# Dynamic Shared Object (DSO)  
#
```

Рис. 19: Смена порта на 80


```
[baisaev@localhost ~]$ semanage port -d -t http_port_t -p tcp 81
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[baisaev@localhost ~]$ rm /var/www/html/myfile.html
rm: удалить защищённый от записи пустой обычный файл '/var/www/html/myfile.html'
? y
rm: невозможно удалить '/var/www/html/myfile.html': Отказано в доступе
[baisaev@localhost ~]$
```

Рис. 20: Удаление привязки к 81 порту и удаление html-файла

Выводы

Я развил навыки администрирования ОС Linux, познакомился с технологией SELinux, поработал с веб-сервером Apache