Лабораторная работа №6.

Мандатное разграничение прав в Linux

Дьяконова С.Ф., НКАбд-01-22

Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux.

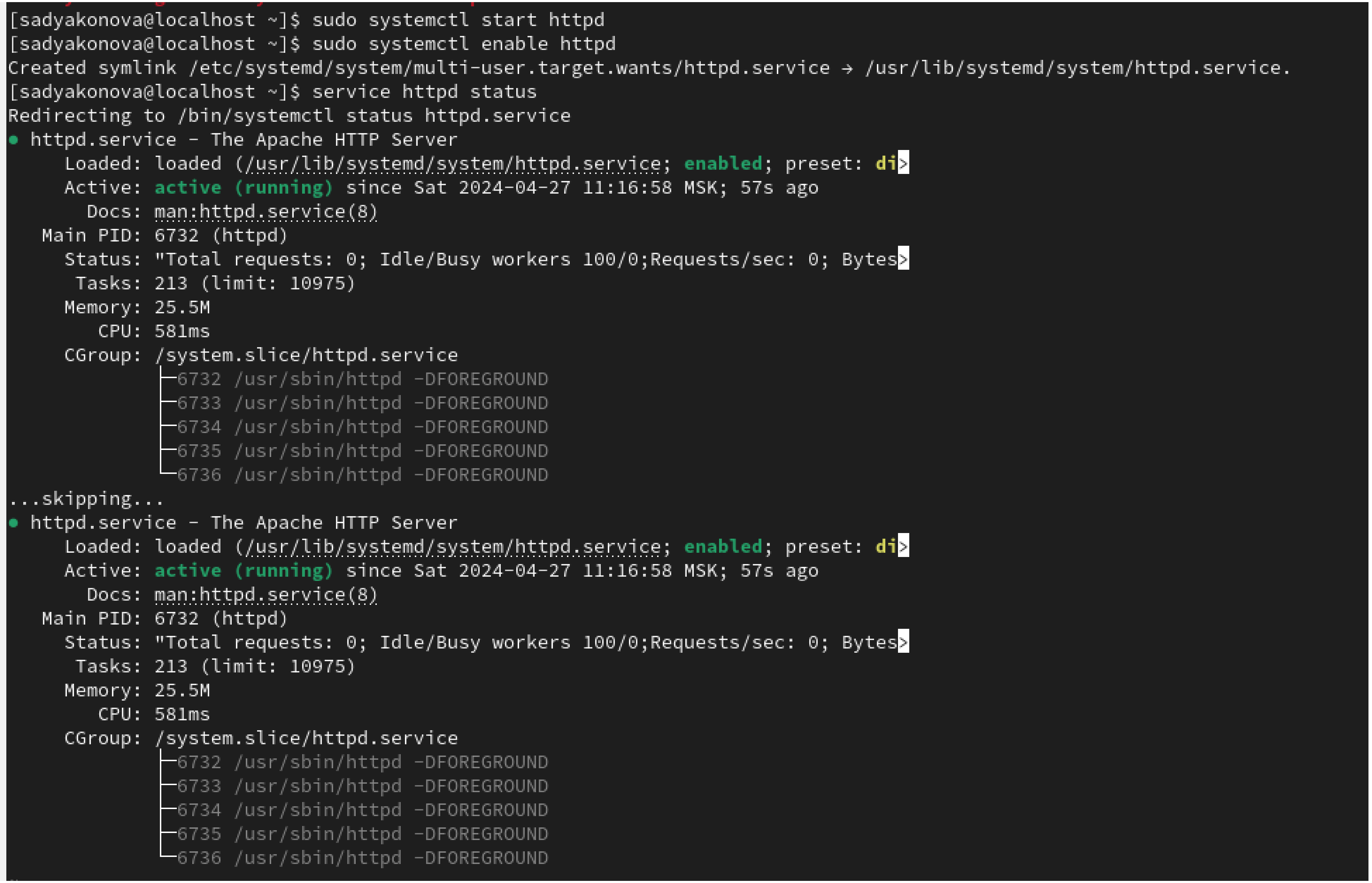
Проверить работу SELinx на практике совместно с веб-сервером Apache.

Выполнение лабораторной работы

Selinux

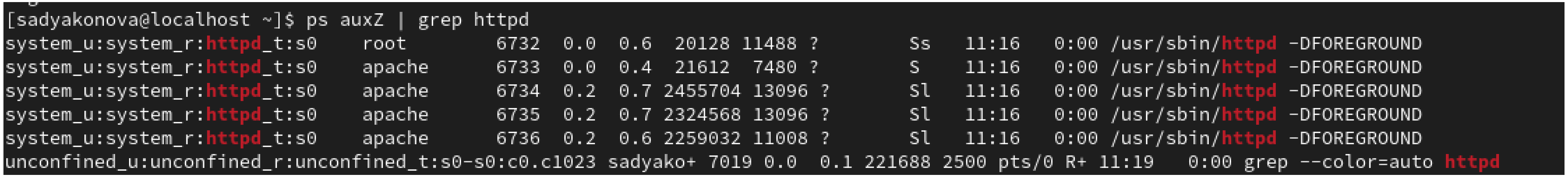
alt text

Проверка работы



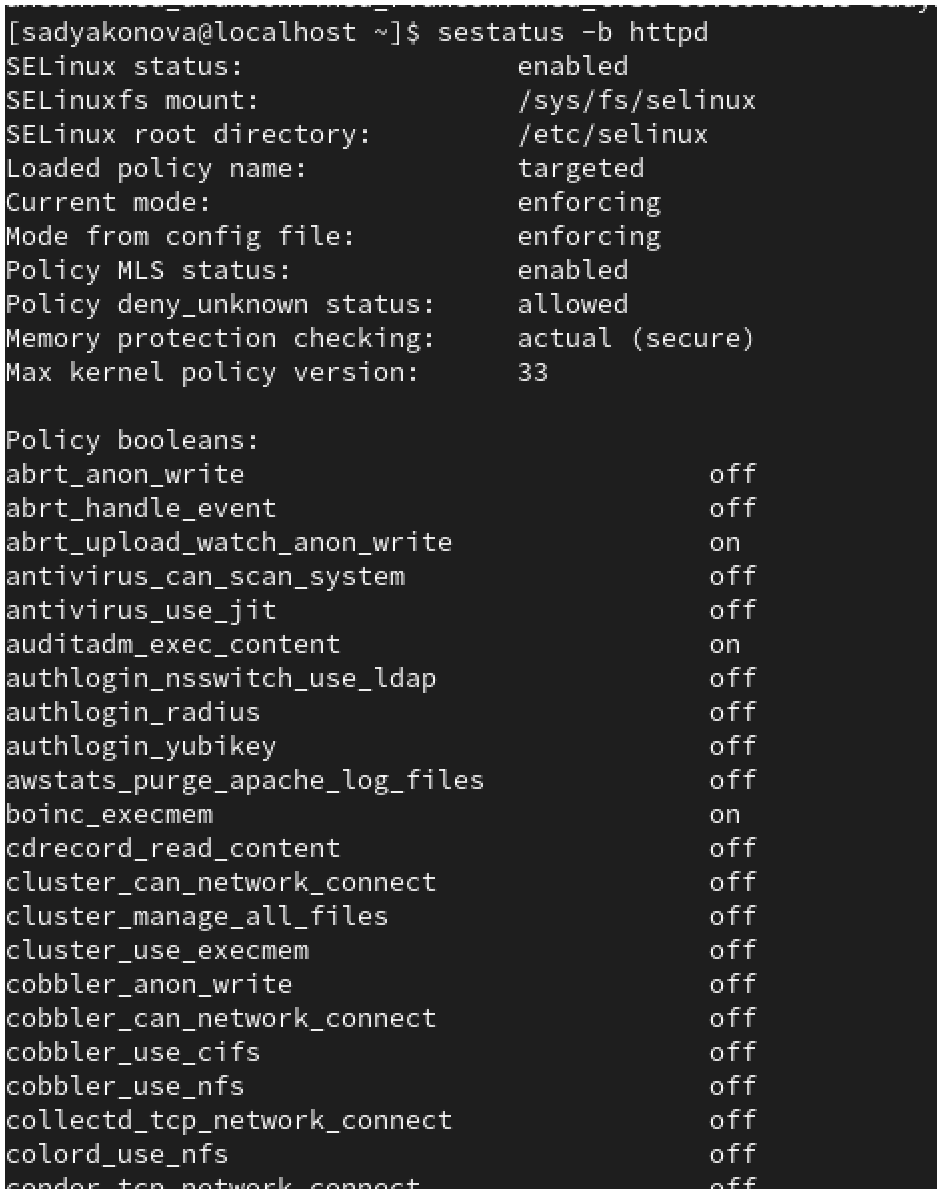
```
[sadyakonova@localhost ~]$ sudo systemctl start httpd
[sadyakonova@localhost ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[sadyakonova@localhost ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: di>
     Active: active (running) since Sat 2024-04-27 11:16:58 MSK; 57s ago
       Docs: man:httpd.service(8)
   Main PID: 6732 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes>
      Tasks: 213 (limit: 10975)
     Memory: 25.5M
        CPU: 581ms
     CGroup: /system.slice/httpd.service
             ├─6732 /usr/sbin/httpd -DFOREGROUND
             ├─6733 /usr/sbin/httpd -DFOREGROUND
             ├─6734 /usr/sbin/httpd -DFOREGROUND
             ├─6735 /usr/sbin/httpd -DFOREGROUND
             └─6736 /usr/sbin/httpd -DFOREGROUND
...skipping...
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: di>
     Active: active (running) since Sat 2024-04-27 11:16:58 MSK; 57s ago
       Docs: man:httpd.service(8)
   Main PID: 6732 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes>
      Tasks: 213 (limit: 10975)
     Memory: 25.5M
        CPU: 581ms
     CGroup: /system.slice/httpd.service
             ├─6732 /usr/sbin/httpd -DFOREGROUND
             ├─6733 /usr/sbin/httpd -DFOREGROUND
             ├─6734 /usr/sbin/httpd -DFOREGROUND
             ├─6735 /usr/sbin/httpd -DFOREGROUND
             └─6736 /usr/sbin/httpd -DFOREGROUND
```

Состояние переключателей



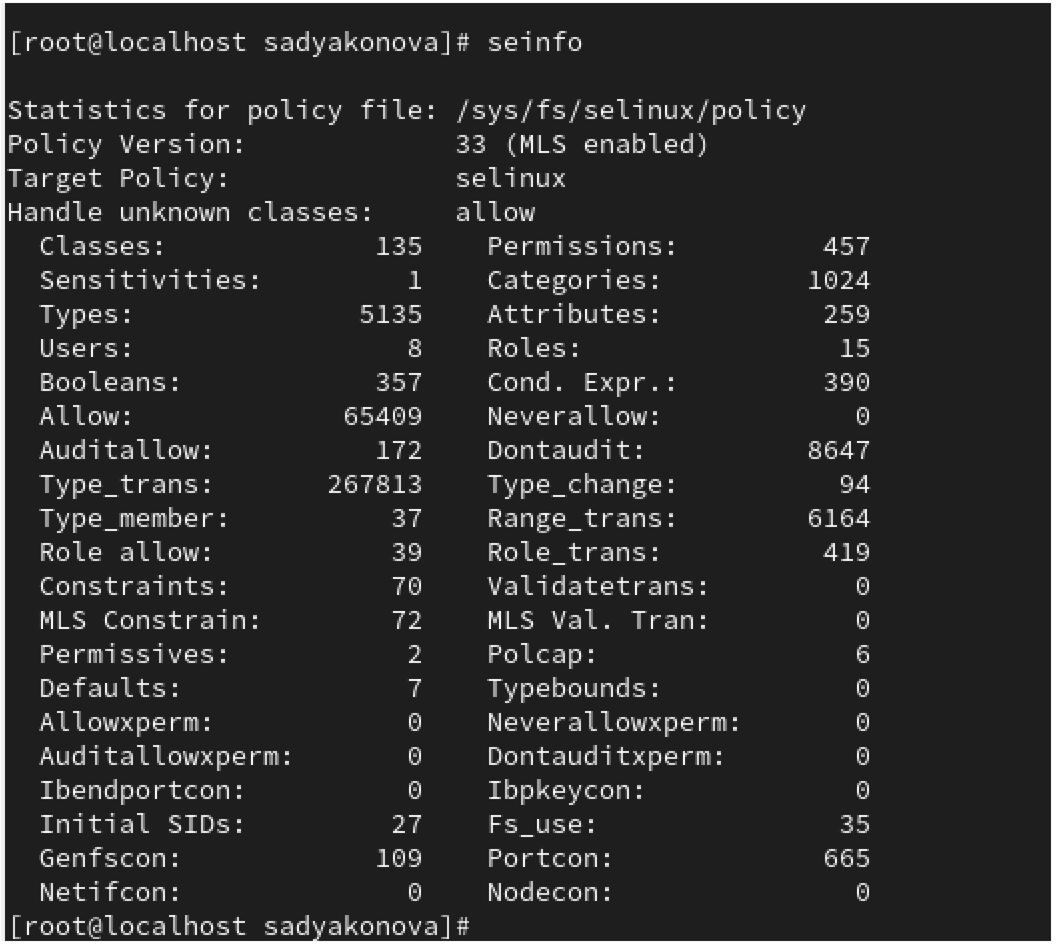
```
[sadyakonova@localhost ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root        6732  0.0  0.6  20128 11488 ?        Ss   11:16   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      6733  0.0  0.4  21612  7480 ?        S    11:16   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      6734  0.2  0.7 2455704 13096 ?       Sl   11:16   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      6735  0.2  0.7 2324568 13096 ?       Sl   11:16   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      6736  0.2  0.6 2259032 11008 ?       Sl   11:16   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 sadyako+ 7019 0.0  0.1 221688 2500 pts/0 R+ 11:19   0:00 grep --color=auto httpd
```

Состояние переключателей



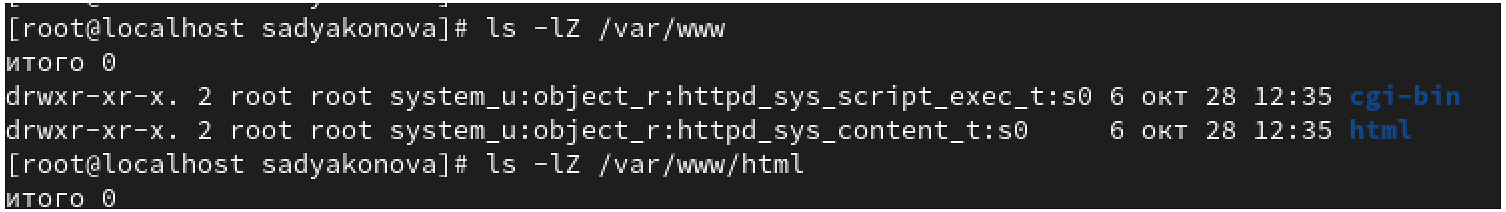
```
[sadyakonova@localhost ~]$ sestatus -b httpd
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
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
cluster_manage_all_files                    off
cluster_use_execmem                         off
cobbler_anon_write                          off
cobbler_can_network_connect                 off
cobbler_use_cifs                            off
cobbler_use_nfs                             off
collectd_tcp_network_connect                off
colord_use_nfs                              off
condor_tcp_network_connect                  off
```

Статистика



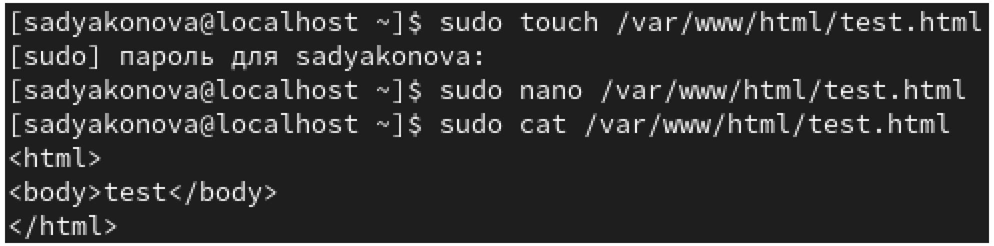
```
[root@localhost sadyakonova]# seinfo

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
[root@localhost sadyakonova]#
```

Тип файлов, круг пользователей



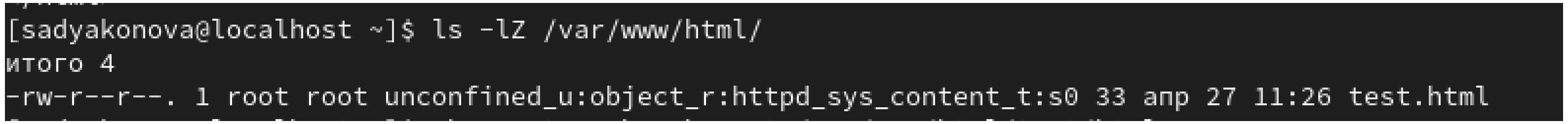
```
[root@localhost sadyakonova]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 окт 28 12:35 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 окт 28 12:35 html
[root@localhost sadyakonova]# ls -lZ /var/www/html
итого 0
```

Файл



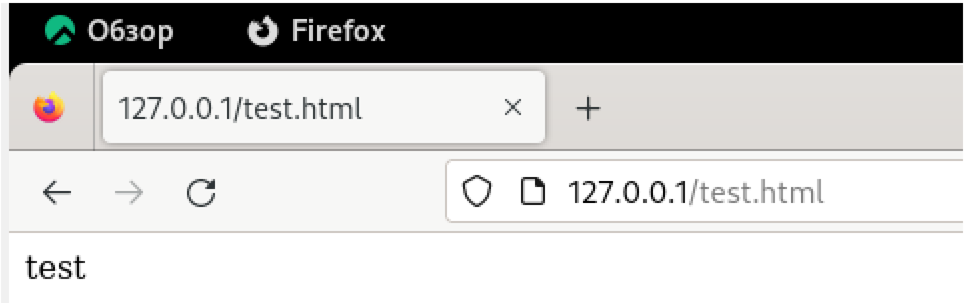
```
[sadyakonova@localhost ~]$ sudo touch /var/www/html/test.html
[sudo] пароль для sadyakonova:
[sadyakonova@localhost ~]$ sudo nano /var/www/html/test.html
[sadyakonova@localhost ~]$ sudo cat /var/www/html/test.html
<html>
<body>test</body>
</html>
```

Контекст файла



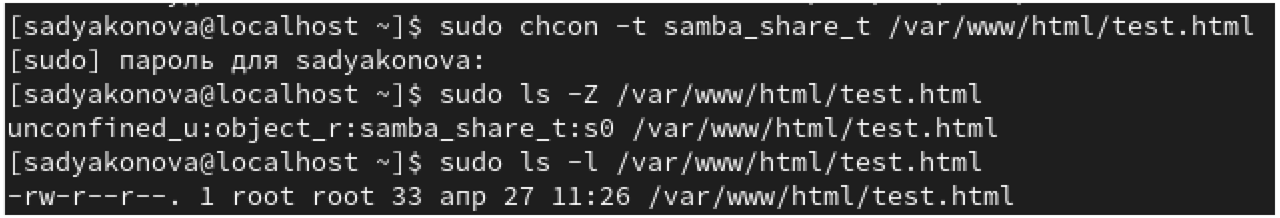
```
[sadyakonova@localhost ~]$ ls -lZ /var/www/html/
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 апр 27 11:26 test.html
```

Состояние переключателей



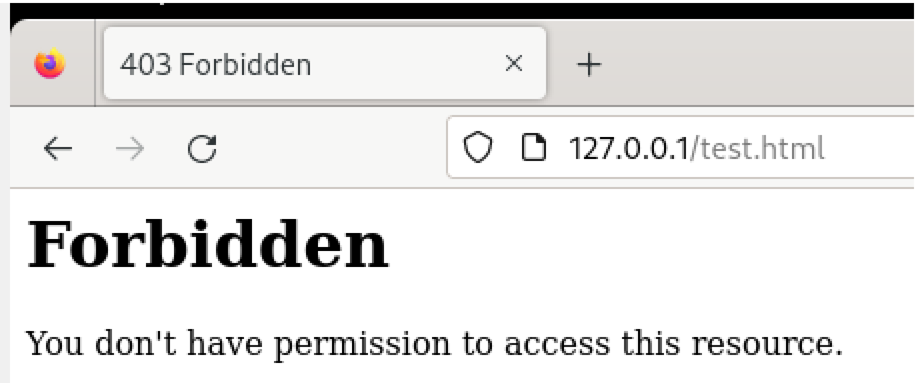
test

Изменение контекста



```
[sadyakonova@localhost ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[sudo] пароль для sadyakonova:
[sadyakonova@localhost ~]$ sudo ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[sadyakonova@localhost ~]$ sudo ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 апр 27 11:26 /var/www/html/test.html
```

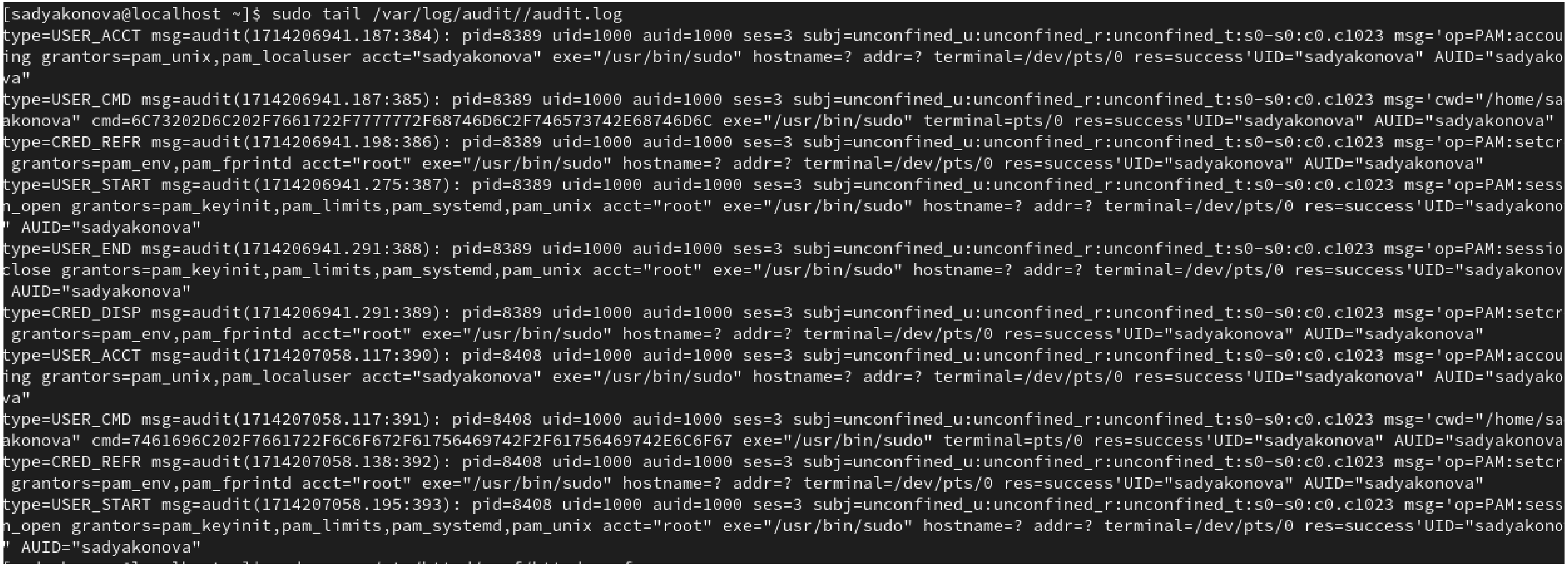
Отказ в доступе



Forbidden

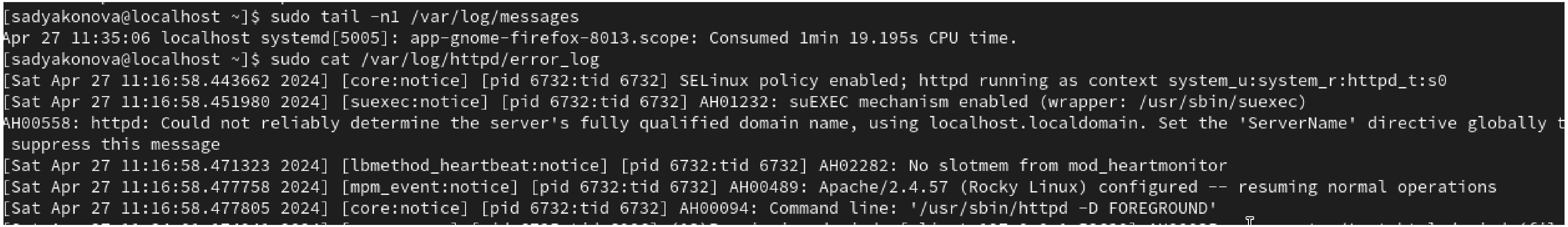
You don't have permission to access this resource.

Лог-файл



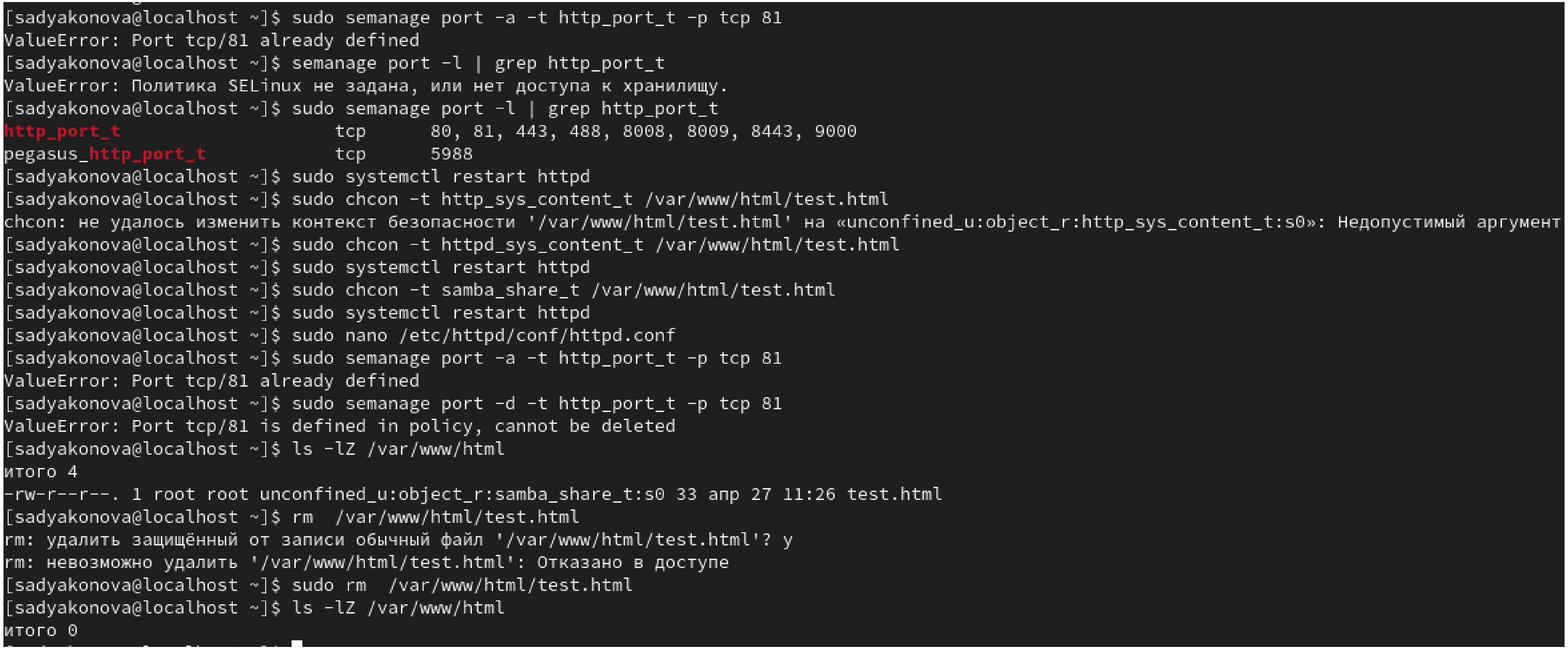
```
[sadyakonova@localhost ~]$ sudo tail /var/log/audit//audit.log
type=USER_ACCT msg=audit(1714206941.187:384): pid=8389 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:accou
ing grantors=pam_unix,pam_localuser acct="sadyakonova" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="sadyakonova" AUID="sadyako
va"
type=USER_CMD msg=audit(1714206941.187:385): pid=8389 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='cwd="/home/sa
akonova" cmd=6C73202D6C202F7661722F7777772F68746D6C2F746573742E68746D6C exe="/usr/bin/sudo" terminal=pts/0 res=success'UID="sadyakonova" AUID="sadyakonova"
type=CRED_REFR msg=audit(1714206941.198:386): pid=8389 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcr
 grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="sadyakonova" AUID="sadyakonova"
type=USER_START msg=audit(1714206941.275:387): pid=8389 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:sess
n_open grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="sadyakono
" AUID="sadyakonova"
type=USER_END msg=audit(1714206941.291:388): pid=8389 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:sessio
close grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="sadyakonov
 AUID="sadyakonova"
type=CRED_DISP msg=audit(1714206941.291:389): pid=8389 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcr
 grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="sadyakonova" AUID="sadyakonova"
type=USER_ACCT msg=audit(1714207058.117:390): pid=8408 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:accou
ing grantors=pam_unix,pam_localuser acct="sadyakonova" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="sadyakonova" AUID="sadyako
va"
type=USER_CMD msg=audit(1714207058.117:391): pid=8408 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='cwd="/home/sa
akonova" cmd=7461696C202F7661722F6C6F672F61756469742F2F61756469742E6C6F67 exe="/usr/bin/sudo" terminal=pts/0 res=success'UID="sadyakonova" AUID="sadyakonova
type=CRED_REFR msg=audit(1714207058.138:392): pid=8408 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcr
 grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="sadyakonova" AUID="sadyakonova"
type=USER_START msg=audit(1714207058.195:393): pid=8408 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:sess
n_open grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="sadyakono
" AUID="sadyakonova"
```

Перезапуск сервера



```
[sadyakonova@localhost ~]$ sudo tail -n1 /var/log/messages
Apr 27 11:35:06 localhost systemd[5005]: app-gnome-firefox-8013.scope: Consumed 1min 19.195s CPU time.
[sadyakonova@localhost ~]$ sudo cat /var/log/httpd/error_log
[Sat Apr 27 11:16:58.443662 2024] [core:notice] [pid 6732:tid 6732] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Apr 27 11:16:58.451980 2024] [suexec:notice] [pid 6732:tid 6732] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using localhost.localdomain. Set the 'ServerName' directive globally t
 suppress this message
[Sat Apr 27 11:16:58.471323 2024] [lbmethod_heartbeat:notice] [pid 6732:tid 6732] AH02282: No slotmem from mod_heartmonitor
[Sat Apr 27 11:16:58.477758 2024] [mpm_event:notice] [pid 6732:tid 6732] AH00489: Apache/2.4.57 (Rocky Linux) configured -- resuming normal operations
[Sat Apr 27 11:16:58.477805 2024] [core:notice] [pid 6732:tid 6732] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
```

Конец)



```
[sadyakonova@localhost ~]$ sudo semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[sadyakonova@localhost ~]$ semanage port -l | grep http_port_t
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[sadyakonova@localhost ~]$ sudo 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
[sadyakonova@localhost ~]$ sudo systemctl restart httpd
[sadyakonova@localhost ~]$ sudo chcon -t http_sys_content_t /var/www/html/test.html
chcon: не удалось изменить контекст безопасности '/var/www/html/test.html' на «unconfined_u:object_r:http_sys_content_t:s0»: Недопустимый аргумент
[sadyakonova@localhost ~]$ sudo chcon -t httpd_sys_content_t /var/www/html/test.html
[sadyakonova@localhost ~]$ sudo systemctl restart httpd
[sadyakonova@localhost ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[sadyakonova@localhost ~]$ sudo systemctl restart httpd
[sadyakonova@localhost ~]$ sudo nano /etc/httpd/conf/httpd.conf
[sadyakonova@localhost ~]$ sudo semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[sadyakonova@localhost ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[sadyakonova@localhost ~]$ ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 33 апр 27 11:26 test.html
[sadyakonova@localhost ~]$ rm  /var/www/html/test.html
rm: удалить защищённый от записи обычный файл '/var/www/html/test.html'? y
rm: невозможно удалить '/var/www/html/test.html': Отказано в доступе
[sadyakonova@localhost ~]$ sudo rm  /var/www/html/test.html
[sadyakonova@localhost ~]$ ls -lZ /var/www/html
итого 0
```

Выводы

Я развила навыки администрирования ОС Linux, получила первое практическое знакомство с технологией SELinux.

Спасибо за внимание!