Лабораторная работа №6.

Мандатное разграничение прав в Linux

Стариков Данила Андреевич

27 апреля 2024

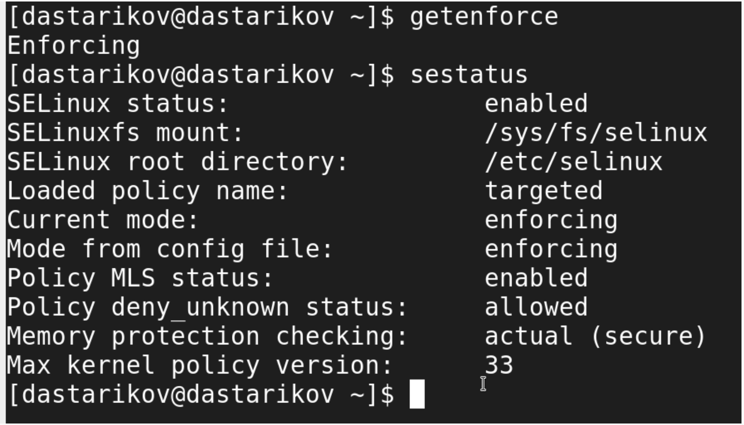
Цели и задачи

Цели и задачи

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

Выполнение

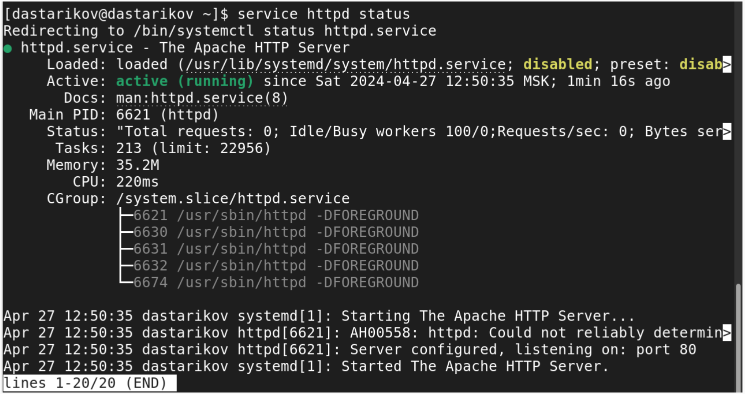
Выполнение



```
[dastarikov@dastarikov ~]$ getenforce
Enforcing
[dastarikov@dastarikov ~]$ 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
[dastarikov@dastarikov ~]$ 
```

Рис. 1: Проверка режима работы SELinux.

Выполнение

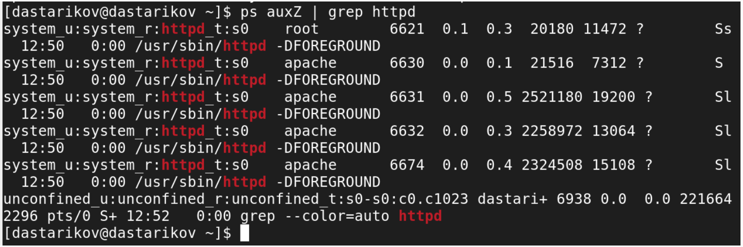


```
[dastarikov@dastarikov ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disab>
     Active: active (running) since Sat 2024-04-27 12:50:35 MSK; 1min 16s ago
       Docs: man:httpd.service(8)
   Main PID: 6621 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes ser>
      Tasks: 213 (limit: 22956)
     Memory: 35.2M
        CPU: 220ms
     CGroup: /system.slice/httpd.service
             ├─6621 /usr/sbin/httpd -DFOREGROUND
             ├─6630 /usr/sbin/httpd -DFOREGROUND
             ├─6631 /usr/sbin/httpd -DFOREGROUND
             ├─6632 /usr/sbin/httpd -DFOREGROUND
             └─6674 /usr/sbin/httpd -DFOREGROUND

Apr 27 12:50:35 dastarikov systemd[1]: Starting The Apache HTTP Server...
Apr 27 12:50:35 dastarikov httpd[6621]: AH00558: httpd: Could not reliably determin>
Apr 27 12:50:35 dastarikov httpd[6621]: Server configured, listening on: port 80
Apr 27 12:50:35 dastarikov systemd[1]: Started The Apache HTTP Server.
lines 1-20/20 (END)
```

Рис. 2: Проверка режима работы httpd.

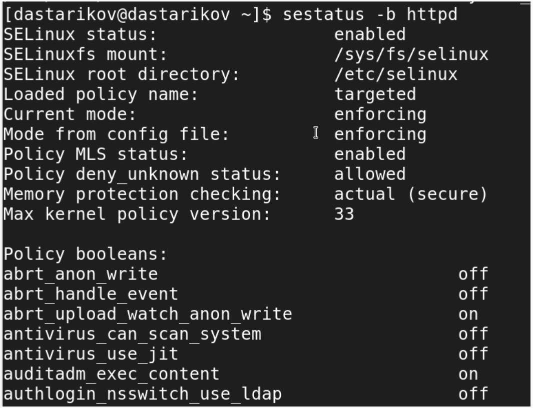
Выполнение



```
[dastarikov@dastarikov ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root        6621  0.1  0.3  20180 11472 ?        Ss
  12:50   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      6630  0.0  0.1  21516  7312 ?        S
  12:50   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      6631  0.0  0.5 2521180 19200 ?       Sl
  12:50   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      6632  0.0  0.3 2258972 13064 ?       Sl
  12:50   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      6674  0.0  0.4 2324508 15108 ?       Sl
  12:50   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 dastari+ 6938 0.0  0.0 221664
2296 pts/0 S+ 12:52   0:00 grep --color=auto httpd
[dastarikov@dastarikov ~]$ 
```

Рис. 3: Список всех связанных с httpd процессов.

Выполнение

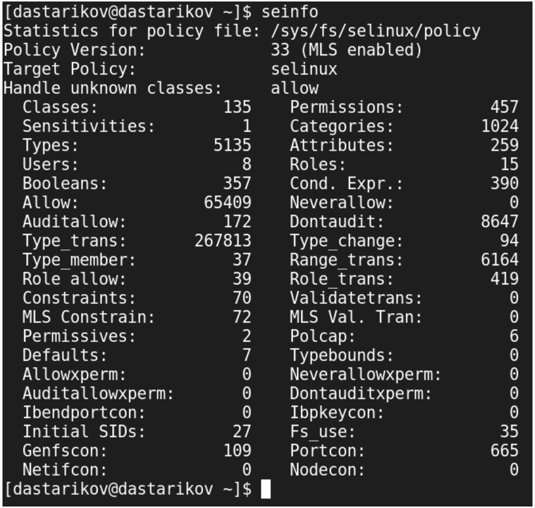


```
[dastarikov@dastarikov ~]$ sestatus -b httpd
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
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
```

Рис. 4: Фрагмент справки текущих состояний httpd.

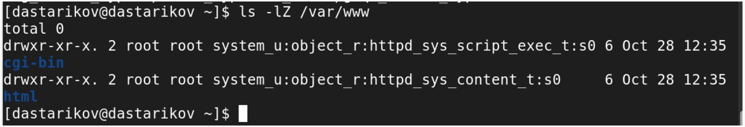
Выполнение



```
[dastarikov@dastarikov ~]$ 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
[dastarikov@dastarikov ~]$
```

Рис. 5: Статистика по политике httpd.

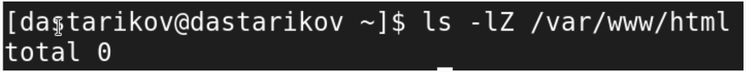
Выполнение



```
[dastarikov@dastarikov ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Oct 28 12:35
cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 Oct 28 12:35
html
[dastarikov@dastarikov ~]$
```

Рис. 6: Информация о содержимом каталога /var/www .

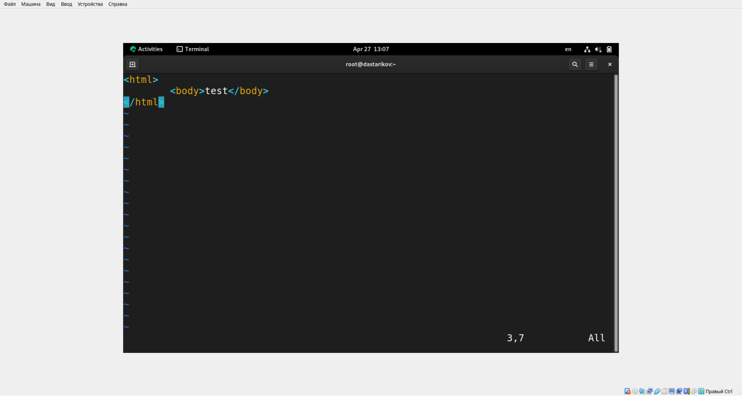
Выполнение



```
[dastarikov@dastarikov ~]$ ls -lZ /var/www/html
total 0
```

Рис. 7: Информация о содержимом каталога /var/www/html .

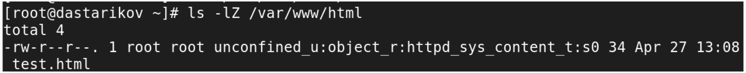
Выполнение



```
<html>
        <body>test</body>
</html>
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
                                                  3,7           All
```

Рис. 8: Создание файла test.html.

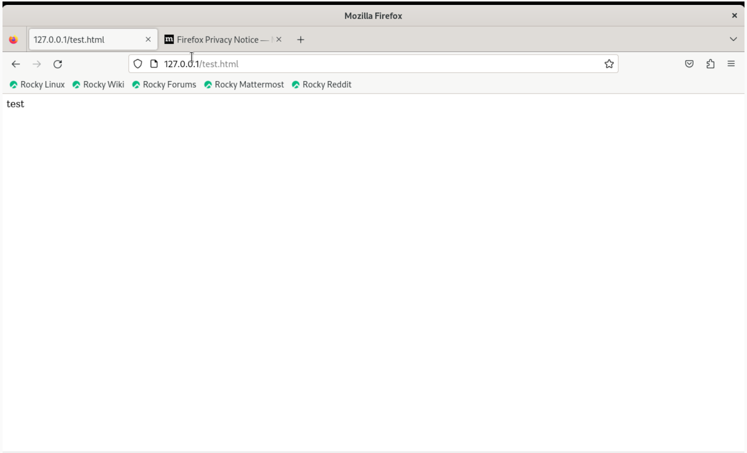
Выполнение



```
[root@dastarikov ~]# ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 Apr 27 13:08
 test.html
```

Рис. 9: Проверка контекста test.html.

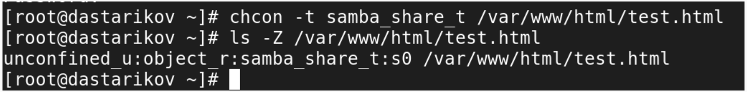
Выполнение



test

Рис. 10: Открытие файла через веб-браузер.

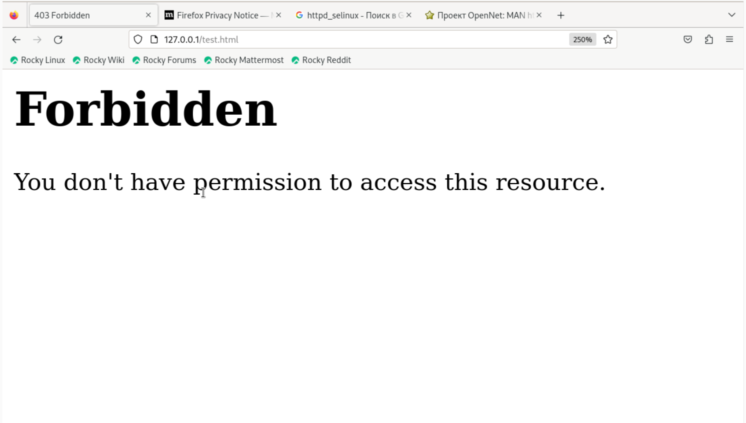
Выполнение



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

Рис. 11: Изменение контекста файла test.html.

Выполнение

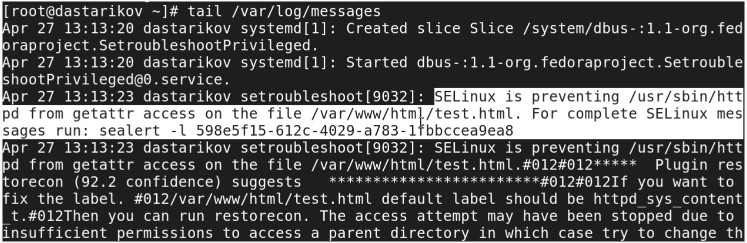


Forbidden

You don't have permission to access this resource.

Рис. 12: Попытка открытия файла через веб-браузер.

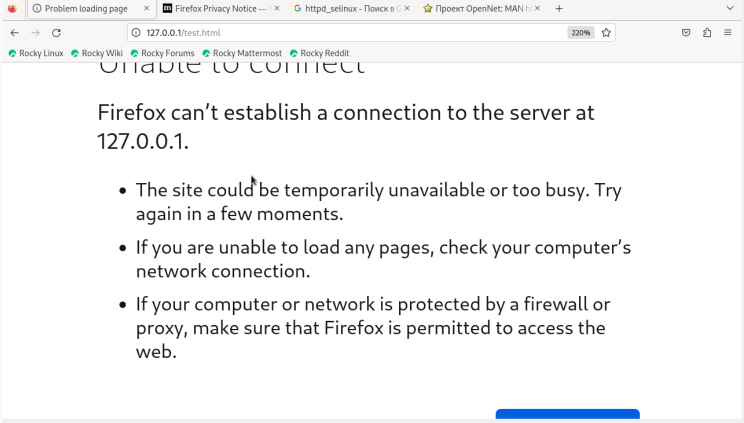
Выполнение



```
[root@dastarikov ~]# tail /var/log/messages
Apr 27 13:13:20 dastarikov systemd[1]: Created slice Slice /system/dbus-:1.1-org.fed
oraproject.SetroubleshootPrivileged.
Apr 27 13:13:20 dastarikov systemd[1]: Started dbus-:1.1-org.fedoraproject.Setrouble
shootPrivileged@0.service.
Apr 27 13:13:23 dastarikov setroubleshoot[9032]: SELinux is preventing /usr/sbin/htt
pd from getattr access on the file /var/www/html/test.html. For complete SELinux mes
sages run: sealert -l 598e5f15-612c-4029-a783-1fbbccea9ea8
Apr 27 13:13:23 dastarikov setroubleshoot[9032]: SELinux is preventing /usr/sbin/htt
pd from getattr access on the file /var/www/html/test.html.#012#012*****  Plugin res
torecon (92.2 confidence) suggests   ************************#012#012If you want to
fix the label. #012/var/www/html/test.html default label should be httpd_sys_content
_t.#012Then you can run restorecon. The access attempt may have been stopped due to
insufficient permissions to access a parent directory in which case try to change th
```

Рис. 13: Просмотр логов веб-сервера.

Выполнение



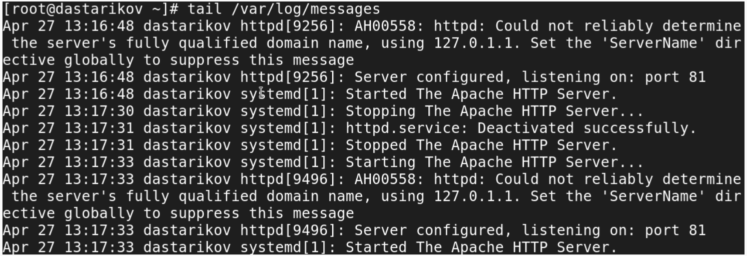
Unable to connect

Firefox can’t establish a connection to the server at 127.0.0.1.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer’s network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Рис. 14: Ошибка при попытке открытия файла через веб-браузер.

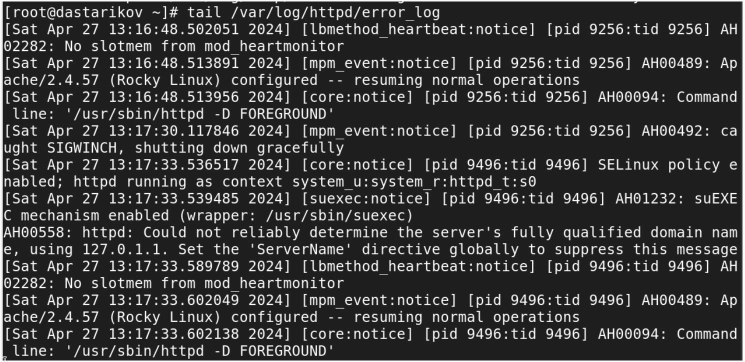
Выполнение



```
[root@dastarikov ~]# tail /var/log/messages
Apr 27 13:16:48 dastarikov httpd[9256]: AH00558: httpd: Could not reliably determine
 the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' dir
ective globally to suppress this message
Apr 27 13:16:48 dastarikov httpd[9256]: Server configured, listening on: port 81
Apr 27 13:16:48 dastarikov systemd[1]: Started The Apache HTTP Server.
Apr 27 13:17:30 dastarikov systemd[1]: Stopping The Apache HTTP Server...
Apr 27 13:17:31 dastarikov systemd[1]: httpd.service: Deactivated successfully.
Apr 27 13:17:31 dastarikov systemd[1]: Stopped The Apache HTTP Server.
Apr 27 13:17:33 dastarikov systemd[1]: Starting The Apache HTTP Server...
Apr 27 13:17:33 dastarikov httpd[9496]: AH00558: httpd: Could not reliably determine
 the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' dir
ective globally to suppress this message
Apr 27 13:17:33 dastarikov httpd[9496]: Server configured, listening on: port 81
Apr 27 13:17:33 dastarikov systemd[1]: Started The Apache HTTP Server.
```

Рис. 15: Просмотр /var/log/messages.

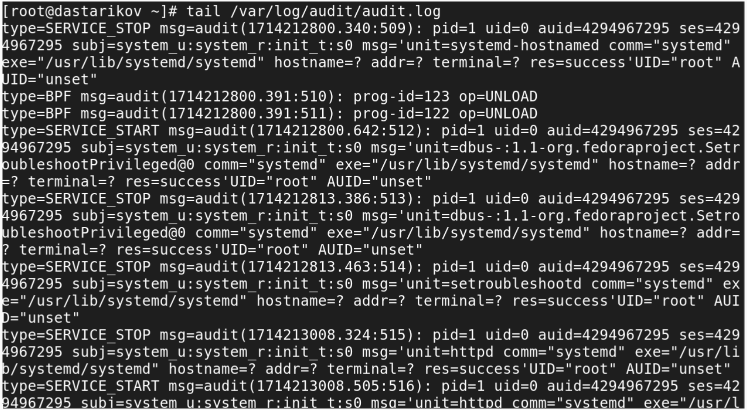
Выполнение



```
[root@dastarikov ~]# tail /var/log/httpd/error_log
[Sat Apr 27 13:16:48.502051 2024] [lbmethod_heartbeat:notice] [pid 9256:tid 9256] AH
02282: No slotmem from mod_heartmonitor
[Sat Apr 27 13:16:48.513891 2024] [mpm_event:notice] [pid 9256:tid 9256] AH00489: Ap
ache/2.4.57 (Rocky Linux) configured -- resuming normal operations
[Sat Apr 27 13:16:48.513956 2024] [core:notice] [pid 9256:tid 9256] AH00094: Command
 line: '/usr/sbin/httpd -D FOREGROUND'
[Sat Apr 27 13:17:30.117846 2024] [mpm_event:notice] [pid 9256:tid 9256] AH00492: ca
ught SIGWINCH, shutting down gracefully
[Sat Apr 27 13:17:33.536517 2024] [core:notice] [pid 9496:tid 9496] SELinux policy e
nabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Apr 27 13:17:33.539485 2024] [suexec:notice] [pid 9496:tid 9496] AH01232: suEXE
C mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain nam
e, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
[Sat Apr 27 13:17:33.589789 2024] [lbmethod_heartbeat:notice] [pid 9496:tid 9496] AH
02282: No slotmem from mod_heartmonitor
[Sat Apr 27 13:17:33.602049 2024] [mpm_event:notice] [pid 9496:tid 9496] AH00489: Ap
ache/2.4.57 (Rocky Linux) configured -- resuming normal operations
[Sat Apr 27 13:17:33.602138 2024] [core:notice] [pid 9496:tid 9496] AH00094: Command
 line: '/usr/sbin/httpd -D FOREGROUND'
```

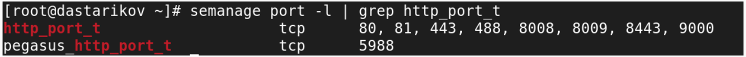
Рис. 16: Просмотр /var/log/httpd/error_log.

Выполнение



```
[root@dastarikov ~]# tail /var/log/audit/audit.log
type=SERVICE_STOP msg=audit(1714212800.340:509): pid=1 uid=0 auid=4294967295 ses=429
4967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-hostnamed comm="systemd"
exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" A
UID="unset"
type=BPF msg=audit(1714212800.391:510): prog-id=123 op=UNLOAD
type=BPF msg=audit(1714212800.391:511): prog-id=122 op=UNLOAD
type=SERVICE_START msg=audit(1714212800.642:512): pid=1 uid=0 auid=4294967295 ses=42
94967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-:1.1-org.fedoraproject.Setr
oubleshootPrivileged@0 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr
=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1714212813.386:513): pid=1 uid=0 auid=4294967295 ses=429
4967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-:1.1-org.fedoraproject.Setro
ubleshootPrivileged@0 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=
? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1714212813.463:514): pid=1 uid=0 auid=4294967295 ses=429
4967295 subj=system_u:system_r:init_t:s0 msg='unit=setroubleshootd comm="systemd" ex
e="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUI
D="unset"
type=SERVICE_STOP msg=audit(1714213008.324:515): pid=1 uid=0 auid=4294967295 ses=429
4967295 subj=system_u:system_r:init_t:s0 msg='unit=httpd comm="systemd" exe="/usr/li
b/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1714213008.505:516): pid=1 uid=0 auid=4294967295 ses=42
94967295 subj=system_u:system_r:init_t:s0 msg='unit=httpd comm="systemd" exe="/usr/l
```

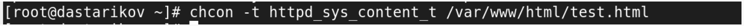
Рис. 17: Просмотр /var/log/audit/audit.log.



```
[root@dastarikov ~]# 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
```

Рис. 18: Настройка прослушивания порта 81.

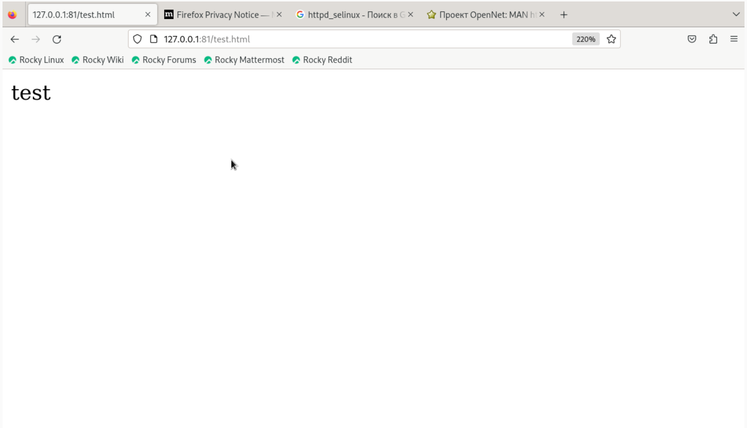
Выполнение



```
[root@dastarikov ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
```

Рис. 19: Возвращение нужного контекста файлу test.html.

Выполнение



test

Рис. 20: Открытие файла через веб-браузер на порте 81.

Итог

Итог

- В рамках лабораторной работы развили навыки администрирования ОС Linux, получили первое практическое знакомство с технологией SELinux и проверили работу SELinux на практике совместно с веб-сервером Apache.