Лабораторная работа №6

Основы информационной безопасности

Астраханцева А. А.

27 апреля 2024

Российский университет дружбы народов, Москва, Россия

Докладчик

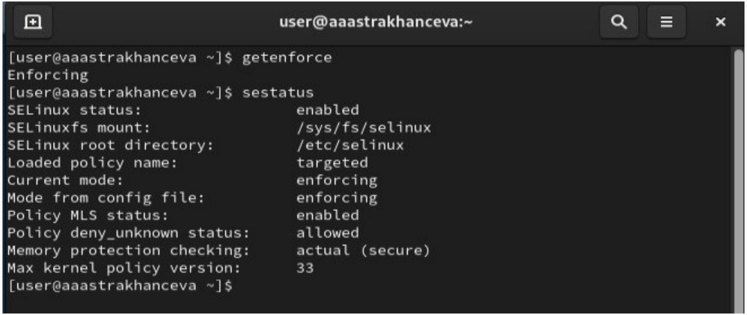
- Астраханцева Анастасия Александровна
- студентка НКАбд-01-22
- Студ. билет: 1132226437
- Российский университет дружбы народов
- https://anastasiia7205.github.io/

Цель работы

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

Выполнение лабораторной работы

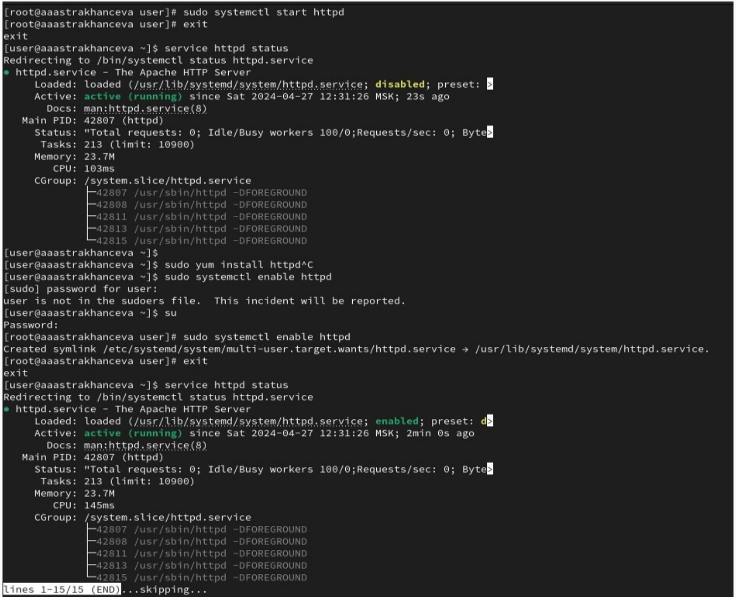
Проверка работы SELinux



```
[user@aaastrakhanceva ~]$ getenforce
Enforcing
[user@aaastrakhanceva ~]$ 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
[user@aaastrakhanceva ~]$
```

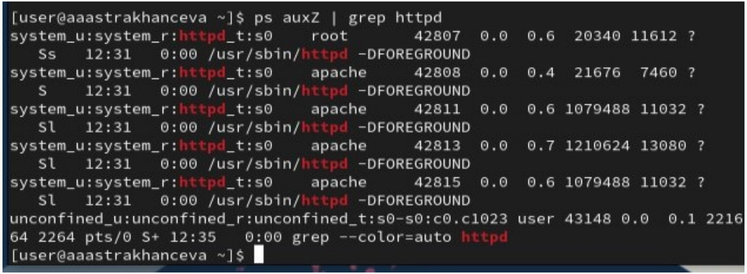
Рис. 1: Проверка работы SELinux

Проверка работы веб-сервера



```
[root@aaastrakhanceva user]# sudo systemctl start httpd
[root@aaastrakhanceva user]# exit
exit
[user@aaastrakhanceva ~]$ 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: >
     Active: active (running) since Sat 2024-04-27 12:31:26 MSK; 23s ago
       Docs: man:httpd.service(8)
   Main PID: 42807 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Byte>
      Tasks: 213 (limit: 10900)
     Memory: 23.7M
        CPU: 103ms
     CGroup: /system.slice/httpd.service
             ├─42807 /usr/sbin/httpd -DFOREGROUND
             ├─42808 /usr/sbin/httpd -DFOREGROUND
             ├─42811 /usr/sbin/httpd -DFOREGROUND
             ├─42813 /usr/sbin/httpd -DFOREGROUND
             └─42815 /usr/sbin/httpd -DFOREGROUND
[user@aaastrakhanceva ~]$
[user@aaastrakhanceva ~]$ sudo yum install httpd^C
[user@aaastrakhanceva ~]$ sudo systemctl enable httpd
[sudo] password for user:
user is not in the sudoers file.  This incident will be reported.
[user@aaastrakhanceva ~]$ su
Password:
[root@aaastrakhanceva user]# sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@aaastrakhanceva user]# exit
exit
[user@aaastrakhanceva ~]$ 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: d>
     Active: active (running) since Sat 2024-04-27 12:31:26 MSK; 2min 0s ago
       Docs: man:httpd.service(8)
   Main PID: 42807 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Byte>
      Tasks: 213 (limit: 10900)
     Memory: 23.7M
        CPU: 145ms
     CGroup: /system.slice/httpd.service
             ├─42807 /usr/sbin/httpd -DFOREGROUND
             ├─42808 /usr/sbin/httpd -DFOREGROUND
             ├─42811 /usr/sbin/httpd -DFOREGROUND
             ├─42813 /usr/sbin/httpd -DFOREGROUND
             └─42815 /usr/sbin/httpd -DFOREGROUND
lines 1-15/15 (END)...skipping...
```

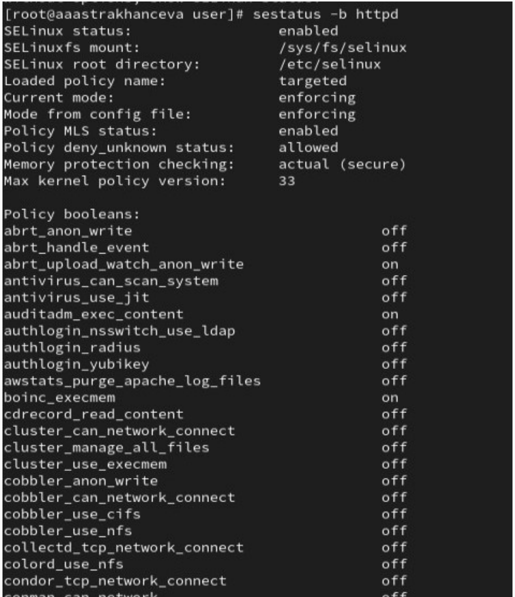
Контекст безопасности веб-сервера Apache



```
[user@aaastrakhanceva ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root       42807  0.0  0.6  20340 11612 ?
   Ss   12:31   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     42808  0.0  0.4  21676  7460 ?
   S    12:31   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     42811  0.0  0.6 1079488 11032 ?
   Sl   12:31   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     42813  0.0  0.7 1210624 13080 ?
   Sl   12:31   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     42815  0.0  0.6 1079488 11032 ?
   Sl   12:31   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 user 43148 0.0  0.1 2216
64 2264 pts/0 S+ 12:35   0:00 grep --color=auto httpd
[user@aaastrakhanceva ~]$ 
```

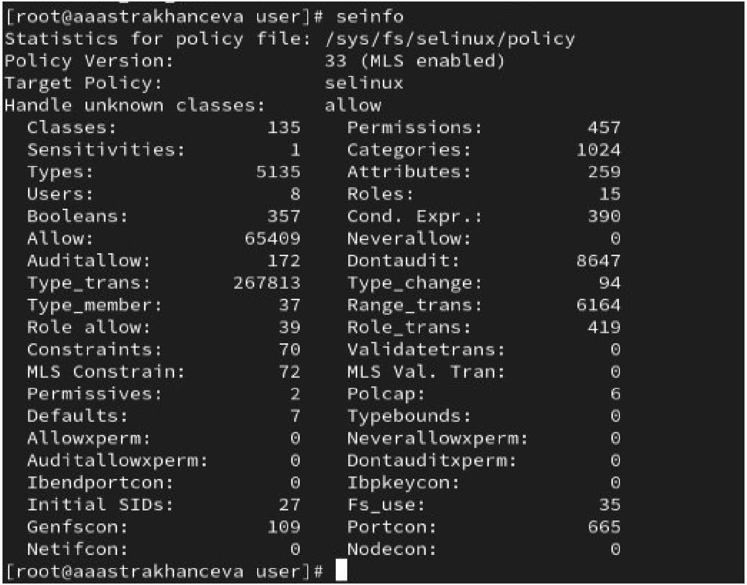
Рис. 3: Контекст безопасности веб-сервера Apache

Текущее состояние переключателей SELinux для Apache



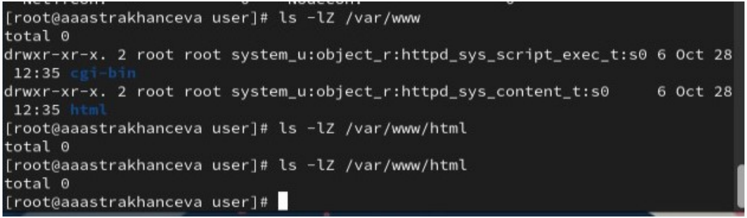
```
[root@aaastrakhanceva user]# sestatus -b httpd
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing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

Статистика по политике



```
[root@aaastrakhanceva user]# 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@aaastrakhanceva user]#
```

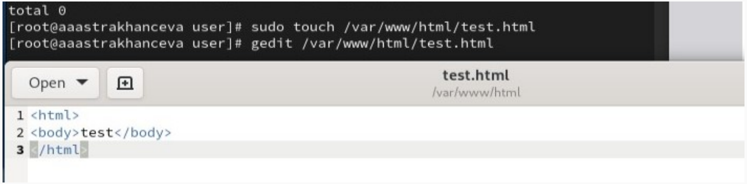
Типы файлов в дирректриях /var/www и /var/www/html



```
[root@aaastrakhanceva user]# 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
[root@aaastrakhanceva user]# ls -lZ /var/www/html
total 0
[root@aaastrakhanceva user]# ls -lZ /var/www/html
total 0
[root@aaastrakhanceva user]# 
```

Рис. 6: Типы файлов в дирректриях /var/www и /var/www/html

Создание html-файла

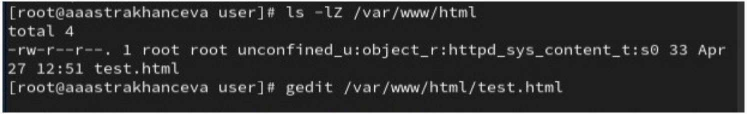


```
total 0
[root@aaastrakhanceva user]# sudo touch /var/www/html/test.html
[root@aaastrakhanceva user]# gedit /var/www/html/test.html
```

```
<html>
<body>test</body>
</html>
```

Рис. 7: Создание html-файла

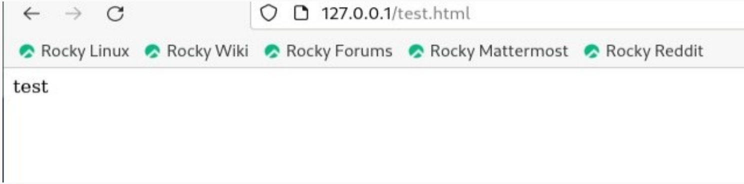
Контекст файла /var/www/html



```
[root@aaastrakhanceva user]# ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Apr
27 12:51 test.html
[root@aaastrakhanceva user]# gedit /var/www/html/test.html
```

Рис. 8: Контекст файла /var/www/html

Файл /var/www/html

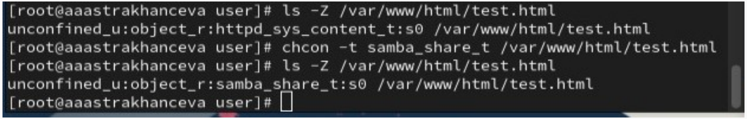


127.0.0.1/test.html

test

Рис. 9: Файл /var/www/html

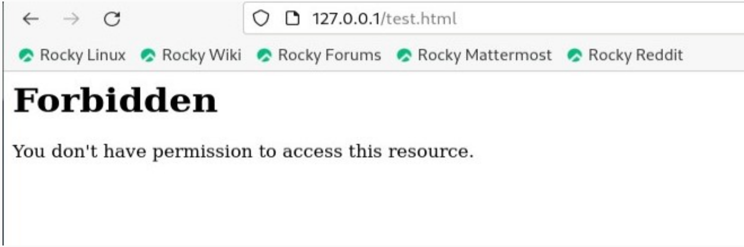
Изменение контекста файла /var/www/html/test.html



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

Рис. 10: Изменение контекста файла /var/www/html/test.html

Сообщение об ошибке

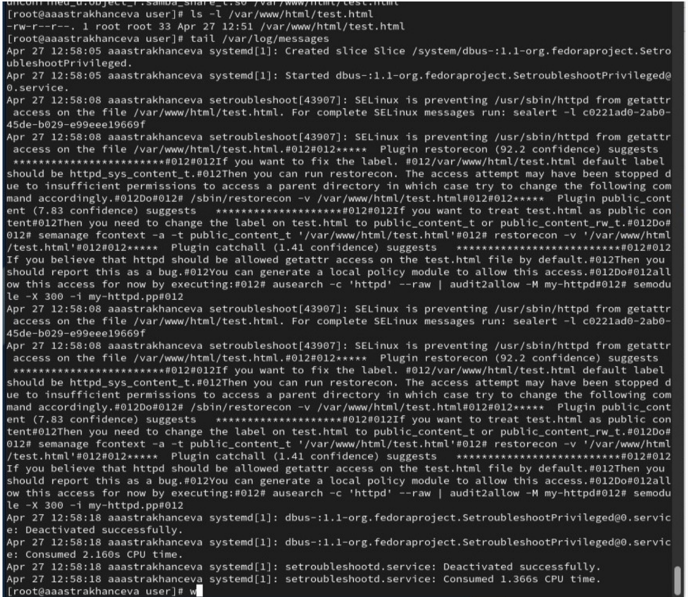


Forbidden

You don't have permission to access this resource.

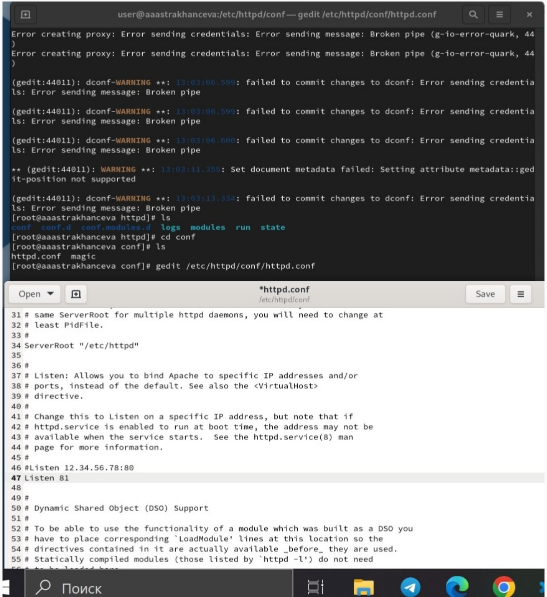
Рис. 11: Сообщение об ошибке

Просмотр log-файлов



```
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@aaastrakhanceva user]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 Apr 27 12:51 /var/www/html/test.html
[root@aaastrakhanceva user]# tail /var/log/messages
Apr 27 12:58:05 aaastrakhanceva systemd[1]: Created slice Slice /system/dbus-:1.1-org.fedoraproject.Setro
ubleshootPrivileged.
Apr 27 12:58:05 aaastrakhanceva systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@
0.service.
Apr 27 12:58:08 aaastrakhanceva setroubleshoot[43907]: SELinux is preventing /usr/sbin/httpd from getattr
 access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l c0221ad0-2ab0-
45de-b029-e99eee19669f
Apr 27 12:58:08 aaastrakhanceva setroubleshoot[43907]: SELinux is preventing /usr/sbin/httpd from getattr
 access on the file /var/www/html/test.html.#012#012*****  Plugin restorecon (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 d
ue to insufficient permissions to access a parent directory in which case try to change the following com
mand accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012*****  Plugin public_cont
ent (7.83 confidence) suggests   *********************#012#012If you want to treat test.html as public con
tent#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
/test.html'#012#012*****  Plugin catchall (1.41 confidence) suggests   **************************#012#012
If you believe that httpd should be allowed getattr access on the test.html file by default.#012Then you
should report this as a bug.#012You can generate a local policy module to allow this access.#012Do#012all
ow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodu
le -X 300 -i my-httpd.pp#012
Apr 27 12:58:08 aaastrakhanceva setroubleshoot[43907]: SELinux is preventing /usr/sbin/httpd from getattr
 access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l c0221ad0-2ab0-
45de-b029-e99eee19669f
Apr 27 12:58:08 aaastrakhanceva setroubleshoot[43907]: SELinux is preventing /usr/sbin/httpd from getattr
 access on the file /var/www/html/test.html.#012#012*****  Plugin restorecon (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 d
ue to insufficient permissions to access a parent directory in which case try to change the following com
mand accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012*****  Plugin public_cont
ent (7.83 confidence) suggests   *********************#012#012If you want to treat test.html as public con
tent#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
/test.html'#012#012*****  Plugin catchall (1.41 confidence) suggests   **************************#012#012
If you believe that httpd should be allowed getattr access on the test.html file by default.#012Then you
should report this as a bug.#012You can generate a local policy module to allow this access.#012Do#012all
ow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodu
le -X 300 -i my-httpd.pp#012
Apr 27 12:58:18 aaastrakhanceva systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.servic
e: Deactivated successfully.
Apr 27 12:58:18 aaastrakhanceva systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.servic
e: Consumed 2.160s CPU time.
Apr 27 12:58:18 aaastrakhanceva systemd[1]: setroubleshootd.service: Deactivated successfully.
Apr 27 12:58:18 aaastrakhanceva systemd[1]: setroubleshootd.service: Consumed 1.366s CPU time.
[root@aaastrakhanceva user]# w
```

Просмотр log-файлов

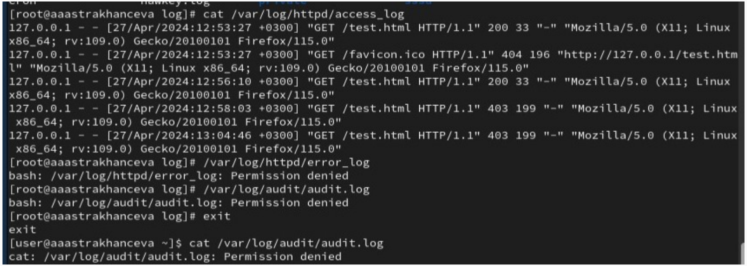


user@aaastrakhanceva:/etc/httpd/conf — gedit /etc/httpd/conf/httpd.conf

```
Error creating proxy: Error sending credentials: Error sending message: Broken pipe (g-io-error-quark, 44
)
Error creating proxy: Error sending credentials: Error sending message: Broken pipe (g-io-error-quark, 44
)

(gedit:44011): dconf-WARNING **: 13:03:06.599: failed to commit changes to dconf: Error sending credentia
ls: Error sending message: Broken pipe

(gedit:44011): dconf-WARNING **: 13:03:06.599: failed to commit changes to dconf: Error sending credentia
ls: Error sending message: Broken pipe

(gedit:44011): dconf-WARNING **: 13:03:06.600: failed to commit changes to dconf: Error sending credentia
ls: Error sending message: Broken pipe

** (gedit:44011): WARNING **: 13:03:11.355: Set document metadata failed: Setting attribute metadata::ged
it-position not supported

(gedit:44011): dconf-WARNING **: 13:03:13.334: failed to commit changes to dconf: Error sending credentia
ls: Error sending message: Broken pipe
[root@aaastrakhanceva httpd]# ls
conf  conf.d  conf.modules.d  logs  modules  run  state
[root@aaastrakhanceva httpd]# cd conf
[root@aaastrakhanceva conf]# ls
httpd.conf  magic
[root@aaastrakhanceva conf]# gedit /etc/httpd/conf/httpd.conf
```

```
# 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

#
# 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
```

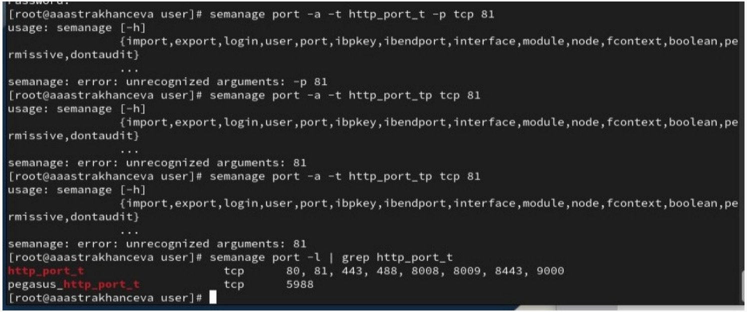
Просмотр файлов /var/log/messages, /var/log/http/error_log



```
[root@aaastrakhanceva log]# cat /var/log/httpd/access_log
127.0.0.1 - - [27/Apr/2024:12:53:27 +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/2024:12:53:27 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.htm
l" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [27/Apr/2024:12:56:10 +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/2024:12:58:03 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux
 x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [27/Apr/2024:13:04:46 +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@aaastrakhanceva log]# /var/log/httpd/error_log
bash: /var/log/httpd/error_log: Permission denied
[root@aaastrakhanceva log]# /var/log/audit/audit.log
bash: /var/log/audit/audit.log: Permission denied
[root@aaastrakhanceva log]# exit
exit
[user@aaastrakhanceva ~]$ cat /var/log/audit/audit.log
cat: /var/log/audit/audit.log: Permission denied
```

Рис. 14: Просмотр файлов /var/log/messages, /var/log/http/error_log

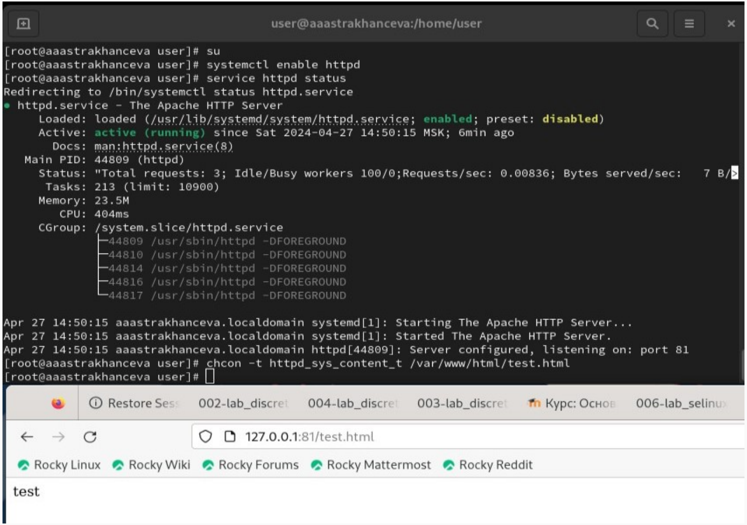
Добавление порта 81



```
[root@aaastrakhanceva user]# semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]
                {import,export,login,user,port,ibpkey,ibendport,interface,module,node,fcontext,boolean,pe
rmissive,dontaudit}
                ...
semanage: error: unrecognized arguments: -p 81
[root@aaastrakhanceva user]# semanage port -a -t http_port_tp tcp 81
usage: semanage [-h]
                {import,export,login,user,port,ibpkey,ibendport,interface,module,node,fcontext,boolean,pe
rmissive,dontaudit}
                ...
semanage: error: unrecognized arguments: 81
[root@aaastrakhanceva user]# semanage port -a -t http_port_tp tcp 81
usage: semanage [-h]
                {import,export,login,user,port,ibpkey,ibendport,interface,module,node,fcontext,boolean,pe
rmissive,dontaudit}
                ...
semanage: error: unrecognized arguments: 81
[root@aaastrakhanceva user]# 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@aaastrakhanceva user]# 
```

Рис. 15: Добавление порта 81

Зпапуск веб-сервера Apache

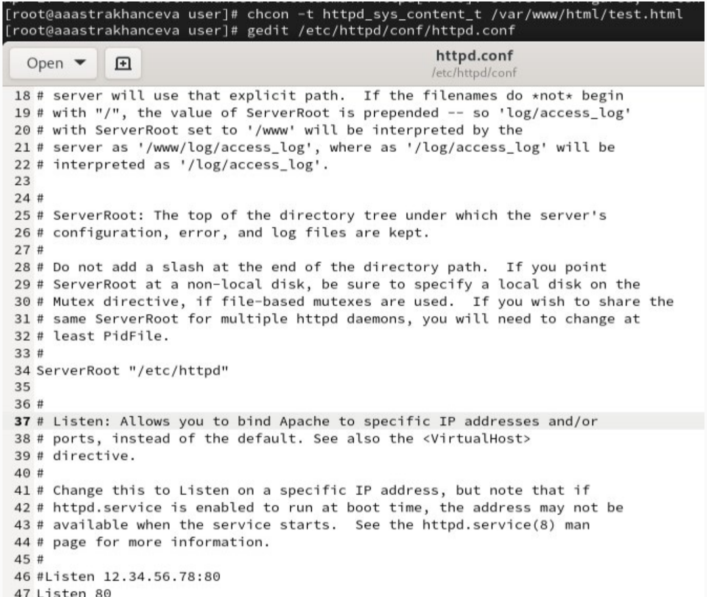


```
[root@aaastrakhanceva user]# su
[root@aaastrakhanceva user]# systemctl enable httpd
[root@aaastrakhanceva user]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
     Active: active (running) since Sat 2024-04-27 14:50:15 MSK; 6min ago
       Docs: man:httpd.service(8)
   Main PID: 44809 (httpd)
     Status: "Total requests: 3; Idle/Busy workers 100/0;Requests/sec: 0.00836; Bytes served/sec:   7 B/>
      Tasks: 213 (limit: 10900)
     Memory: 23.5M
        CPU: 404ms
     CGroup: /system.slice/httpd.service
             ├─44809 /usr/sbin/httpd -DFOREGROUND
             ├─44810 /usr/sbin/httpd -DFOREGROUND
             ├─44814 /usr/sbin/httpd -DFOREGROUND
             ├─44816 /usr/sbin/httpd -DFOREGROUND
             └─44817 /usr/sbin/httpd -DFOREGROUND

Apr 27 14:50:15 aaastrakhanceva.localdomain systemd[1]: Starting The Apache HTTP Server...
Apr 27 14:50:15 aaastrakhanceva.localdomain systemd[1]: Started The Apache HTTP Server.
Apr 27 14:50:15 aaastrakhanceva.localdomain httpd[44809]: Server configured, listening on: port 81
[root@aaastrakhanceva user]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@aaastrakhanceva user]# 
```

test

Рис. 16: Зпапуск веб-сервера Apache

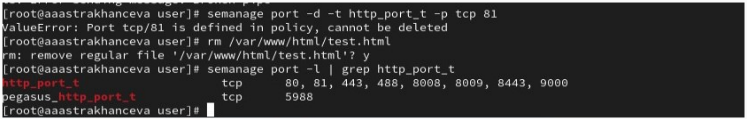
Исправление конфигурационного файла apache



```
[root@aaastrakhanceva user]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@aaastrakhanceva user]# gedit /etc/httpd/conf/httpd.conf
```

```
# server will use that explicit path.  If the filenames do *not* begin
# with "/", the value of ServerRoot is prepended -- so 'log/access_log'
# with ServerRoot set to '/www' will be interpreted by the
# server as '/www/log/access_log', where as '/log/access_log' will be
# interpreted as '/log/access_log'.

#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path.  If you point
# 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 80
```

Удаление привязки к порту 81 и файла /var/www/html/test.html:



```
[root@aaastrakhanceva user]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@aaastrakhanceva user]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@aaastrakhanceva user]# 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@aaastrakhanceva user]# 
```

Рис. 18: Удаление привязки к порту 81 и файла /var/www/html/test.html:

Выводы

В ходе выполения ЛР№6 я развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux1. Прверила работу SELinx на практике совместно с веб-сервером Apache.

Спасибо за внимание