

# Лабораторная работа № 6

---

Ли Тимофей Александрович, НФИбд-01-18

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

# Выполнение лабораторной работы

Для начала я, зайдя в root, установил apache, задал servername в конфигурационном файле и отключил пакетный фильтр. (рис. @fig:001):

```
[tim@10 ~]$ su root
Пароль:
[root@10 tim]# yum install httpd
CentOS Linux 8 - AppStream                629 B/s | 4.3 kB      00:07
CentOS Linux 8 - AppStream                5.2 MB/s | 8.1 MB      00:01
CentOS Linux 8 - BaseOS                  8.9 kB/s | 3.9 kB      00:00
CentOS Linux 8 - BaseOS                  5.7 MB/s | 3.5 MB      00:00
CentOS Linux 8 - Extras                  2.9 kB/s | 1.5 kB      00:00
Зависимости разрешены.
=====
Пакет      Архитектура  Версия      Репозиторий      Размер
=====
Установка:
httpd      x86_64 2.4.37-43.module_el8.5.0+1022+b541f3b1_appstream 1.4 M
```

```
[root@10 conf]# echo "ServerName test.ru" >> httpd.conf
[root@10 conf]# cat httpd.conf
#
# This is the main Apache HTTP server configuration file. It contains the
# configuration directives that give the server its instructions.
# See <URL:http://httpd.apache.org/docs/2.4/> for detailed information.
# In particular, see
# <URL:http://httpd.apache.org/docs/2.4/mod/directives.html>
# for a discussion of each configuration directive.
#
# See the httpd.conf(5) man page for more information on this configuration
```

```
[root@10 conf]# cd
[root@10 ~]# iptables -F
[root@10 ~]# iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
Bad argument 'iptables'
Try 'iptables -h' or 'iptables --help' for more information.
[root@10 ~]# iptables -P INPUT ACCEPT
[root@10 ~]# iptables -P OUTPUT ACCEPT
```

Рис. 1: подготовка

# Выполнение лабораторной работы

Убедился, что SELinux работает в нужном режиме. Нашел apache в списке процессов: (рис. @fig:002)

```
[root@10 ~]# getenforce
Enforcing
[root@10 ~]# 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@10 ~]# ps auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 3973 0.0  0.1 12136 1160 pts/0 R+ 02:22   0:00 grep --color=auto httpd
[root@10 ~]# ps -eZ | grep httpd
[root@10 ~]# sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

  -v  Verbose check of process and file contexts.
  -b  Display current state of booleans.

Without options, show SELinux status.
[root@10 ~]# sestatus | grep httpd
[root@10 ~]# seinfo
bash: seinfo: команда не найдена...
Установить пакет «setools-console», предоставляющий команду «seinfo»? [N/y] y
```

Рис. 2: выполненные действия

# Выполнение лабораторной работы

посмотрел состояние переключателей SELinux: (рис. @fig:003)

```
[root@10 ~]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          31 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow
Classes:                 132
Sensitivities:           1
Types:                   4959
Users:                   8
Booleans:                340
Allow:                   112885
Auditallow:              166
Type_trans:              253398
Type_member:             35
Role_allow:              38
Constraints:             72
MLS Constrain:           72
Permissives:             0
Defaults:                7
Allowxperm:              0
Auditallowxperm:         0
Ibendportcon:            0
Initial SIDs:            27
Genfscon:                106
Netifcon:                0
Permissions:             463
Categories:             1024
Attributes:              255
Roles:                   14
Cond. Expr.:             389
Neverallow:              0
Dontaudit:               10362
Type_change:             87
Range_trans:             6015
Role_trans:              423
Validatetrans:           0
MLS Val. Tran:           0
Polcap:                  5
Typebounds:              0
Neverallowxperm:         0
Dontauditxperm:          0
Ibpkeycon:               0
Fs_use:                  33
Portcon:                 640
Nodecon:                 0

[root@10 ~]# sestatus -bigrep httpd
sestatus: invalid option -- 'i'

[root@10 ~]# 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_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
httpd_read_user_content    off
httpd_run_ipa              off
```

Рис. 3: выполненные действия

# Выполнение лабораторной работы

Определил типы файлов и поддиректорий в `www` и `www/html`.  
Создал файл `test.html`: (рис. @fig:004)

```
[root@10 ~]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 12 07:58 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ноя 12 07:58 html
[root@10 ~]# ls -lZ /var/www/html
итого 0
[root@10 ~]# echo "<html>\n<body>test</body>\n</html>" > /var/www/html/test.html
[root@10 ~]# cat /var/www/html/test.html
<html>\n<body>test</body>\n</html>
[root@10 ~]# gedit /var/www/html/test.html
No protocol specified

(gedit:5021): dbind-WARNING **: 03:20:00.253: Could not open X display

(gedit:5021): GLib-GIO-CRITICAL **: 03:20:00.438: g_dbus_proxy_new_sync: assertion 'G_IS_DBUS_CONNECTION (connection)' failed

(gedit:5021): dconf-WARNING **: 03:20:00.615: failed to commit changes to dconf: Соединение закрыто

(gedit:5021): dconf-WARNING **: 03:20:00.629: failed to commit changes to dconf: Соединение закрыто
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)

(gedit:5021): dconf-WARNING **: 03:20:01.654: failed to commit changes to dconf: Соединение закрыто

(gedit:5021): dconf-WARNING **: 03:20:01.659: failed to commit changes to dconf: Соединение закрыто

(gedit:5021): dconf-WARNING **: 03:20:01.659: failed to commit changes to dconf: Соединение закрыто

** (gedit:5021): WARNING **: 03:20:53.422: Set document metadata failed: Установка атрибута metadata::gedit-spell-language не поддерживается

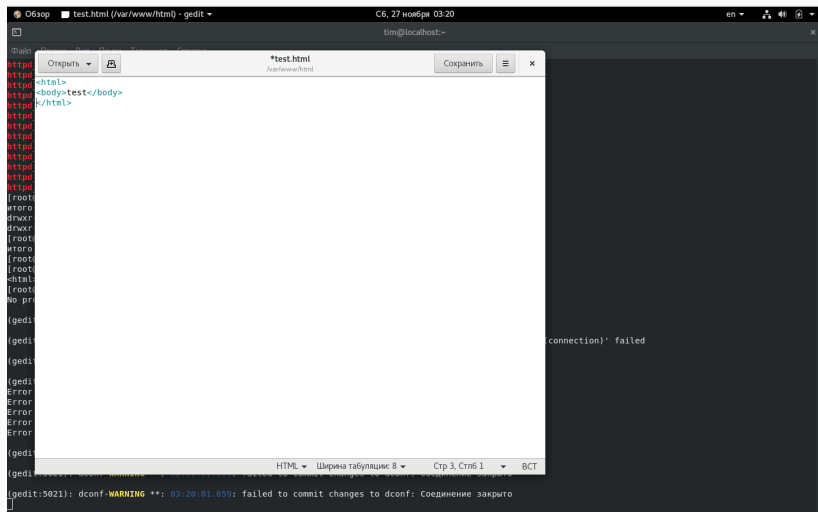
** (gedit:5021): WARNING **: 03:20:53.426: Set document metadata failed: Установка атрибута metadata::gedit-encoding не поддерживается

** (gedit:5021): WARNING **: 03:20:55.950: Set document metadata failed: Установка атрибута metadata::gedit-position не поддерживается

(gedit:5021): dconf-WARNING **: 03:20:56.152: failed to commit changes to dconf: Соединение закрыто
[root@10 ~]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
```

# Выполнение лабораторной работы

Получившийся файл: (рис. @fig:005)



# Выполнение лабораторной работы

Затем, не смог отобразить файл через браузер. Проверил контекст файла и попробовал его изменить (получил сообщение об ошибке). Посмотрел лог-файл: (рис. @fig:006)

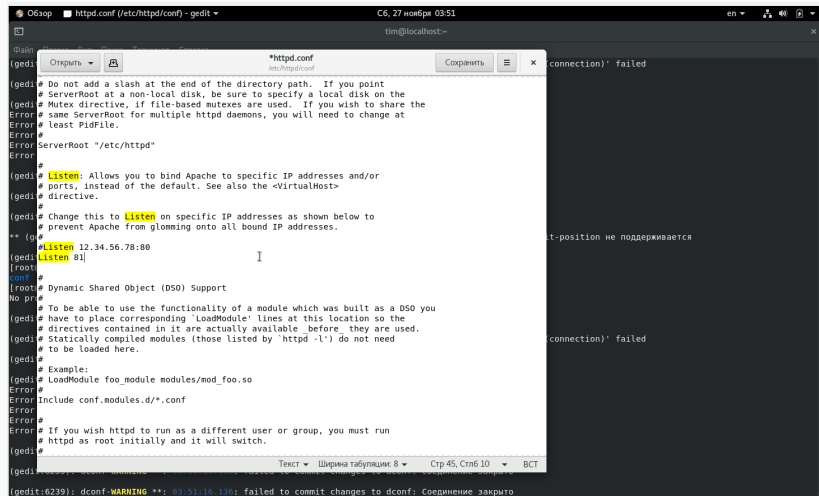
```
[root@10 ~]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@10 ~]# man httpd_selinux
Нет справочной страницы для httpd_selinux
[root@10 ~]# chcon -t samba_share_t /var/www/html/test.html
chcon: невозможно получить доступ к 't': Нет такого файла или каталога
chcon: не удалось изменить контекст безопасности '/var/www/html/test.html' на «unconfined_u:object_r:samba_share_t:s0»: Недопустимый аргумент
[root@10 ~]# http://127.0.0.1/test.html
bash: http://127.0.0.1/test.html: Нет такого файла или каталога
[root@10 ~]# wget http://127.0.0.1/test.html
--2021-11-27 03:47:25--  ftp://http://127.0.0.1/test.html
=> «test.html»
Распознаётся http (http)... ошибка: Неизвестное имя или служба.
wget: не удалось разрешить адрес «http»
[root@10 ~]# wget https://127.0.0.1/test.html
--2021-11-27 03:47:50--  ftp://https://127.0.0.1/test.html
=> «test.html»
Распознаётся https (https)... ошибка: Неизвестное имя или служба.
wget: не удалось разрешить адрес «https»
[root@10 ~]# wget 127.0.0.1/test.html
--2021-11-27 03:47:58--  http://127.0.0.1/test.html
Подключение к 127.0.0.1:80... ошибка: В соединении отказано.
[root@10 ~]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 ноя 27 03:20 /var/www/html/test.html
[root@10 ~]# tail /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@10 ~]# tail /var/log/messages
Nov 27 03:49:02 10 rsyslogd[1017]: [origin software="rsyslogd" swVersion="8.1911.0-7.el8_4.2" x-pid="1017" x-info="https://www.rsyslog.com"] rsyslogd was HUPe
d
```

Рис. 6: выполненные действия



# Выполнение лабораторной работы

Попробовал запустить веб-сервер на прослушивание порта 81, изменив файл httpd.conf: (рис. @fig:007)



```
Обзор  httpd.conf (/etc/httpd/conf) - gedit  C6, 27 ноября 03:51  en  tim@localhost:~  
tim@localhost:~  
(gedit) *httpd.conf  
(gedit) # 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  
(gedit) # Mutex directive, if file-based mutexes are used.  If you wish to share the  
Error # same ServerRoot for multiple httpd daemons, you will need to change at  
Error # least PidFile.  
Error #  
Error ServerRoot "/etc/httpd"  
Error #  
(gedit) # Listen: Allows you to bind Apache to specific IP addresses and/or  
# ports, instead of the default.  See also the <VirtualHost>  
(gedit) # directive.  
#  
(gedit) # Change this to Listen on specific IP addresses as shown below to  
# prevent Apache from glomming onto all bound IP addresses.  
** (g  
(gedit) #Listen 12.34.56.78:80  
(gedit) #Listen 81  
(gedit) [root  
conf  
[root #  
No pr # Dynamic Shared Object (DSO) Support  
#  
# To be able to use the functionality of a module which was built as a DSO you  
(gedit) # have to place corresponding 'LoadModule' lines at this location so the  
# directives contained in it are actually available before they are used.  
(gedit) # Statically compiled modules (those listed by 'httpd -l') do not need  
# to be loaded here.  
(gedit) #  
# Example:  
(gedit) # LoadModule foo_module modules/mod_foo.so  
Error #  
Error Include conf.modules.d/*.conf  
Error #  
Error # If you wish httpd to run as a different user or group, you must run  
# httpd as root initially and it will switch.  
(gedit) #  
(gedit) #  
Text  Ширина таблицы: 8  Стр 45, Стлб 10  ВСТ  
(gedit) dconf-WARNING **: 03:51:10.130: failed to commit changes to dconf: Соединение закрыто
```

# Выполнение лабораторной работы

Не смог запустить веб-сервер, проанализировал лог-файлы.  
Выполнил команды semanage и убедился, что порт 81 есть в списках: (рис. @fig:008)

```
[root@10 ~]# gedit /etc/httpd/conf/httpd.conf
No protocol specified

(gedit:6239): dbind-WARNING **: 03:51:15.344: Could not open X display

(gedit:6239): GLib-GIO-CRITICAL **: 03:51:15.469: g_dbus_proxy_new_sync: assertion 'G_IS_DBUS_CONNECTION (connection)' failed

(gedit:6239): dconf-WARNING **: 03:51:15.518: failed to commit changes to dconf: Соединение закрыто

(gedit:6239): dconf-WARNING **: 03:51:15.523: failed to commit changes to dconf: Соединение закрыто
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)

(gedit:6239): dconf-WARNING **: 03:51:16.136: failed to commit changes to dconf: Соединение закрыто

(gedit:6239): dconf-WARNING **: 03:51:16.136: failed to commit changes to dconf: Соединение закрыто

(gedit:6239): dconf-WARNING **: 03:51:16.136: failed to commit changes to dconf: Соединение закрыто

** (gedit:6239): WARNING **: 03:51:58.145: Set document metadata failed: Установка атрибута metadata::gedit-spell-language не поддерживается
** (gedit:6239): WARNING **: 03:51:58.200: Set document metadata failed: Установка атрибута metadata::gedit-encoding не поддерживается
** (gedit:6239): WARNING **: 03:52:00.226: Set document metadata failed: Установка атрибута metadata::gedit-position не поддерживается

(gedit:6239): dconf-WARNING **: 03:52:00.432: failed to commit changes to dconf: Соединение закрыто
[root@10 ~]# apache
bash: apache: команда не найдена...
[root@10 ~]# tail -nl /var/log/messages
tail: неверное число строк: «l»
[root@10 ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@10 ~]# 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@10 ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
```

# Выполнение лабораторной работы

Вернул контекст файлу test.html, исправил обратно конфигурационный файл, попытался удалить привязку к порту 81 и удалил файл test.html: (рис. @fig:009)

```
[root@10 ~]# gedit /etc/httpd/conf/httpd.conf
No protocol specified

(gedit:6348): dbind-WARNING **: 03:55:49.766: Could not open X display
(gedit:6348): GLib-GIO-CRITICAL **: 03:55:49.901: g_dbus_proxy_new_sync: assertion 'G_IS_DBUS_CONNECTION (connection)' failed
(gedit:6348): dconf-WARNING **: 03:55:50.039: failed to commit changes to dconf: Соединение закрыто
(gedit:6348): dconf-WARNING **: 03:55:50.061: failed to commit changes to dconf: Соединение закрыто
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)
(gedit:6348): dconf-WARNING **: 03:55:50.836: failed to commit changes to dconf: Соединение закрыто
(gedit:6348): dconf-WARNING **: 03:55:50.841: failed to commit changes to dconf: Соединение закрыто
(gedit:6348): dconf-WARNING **: 03:55:50.841: failed to commit changes to dconf: Соединение закрыто
** (gedit:6348): WARNING **: 03:56:00.512: Set document metadata failed: Установка атрибута metadata::gedit-spell-language не поддерживается
** (gedit:6348): WARNING **: 03:56:00.563: Set document metadata failed: Установка атрибута metadata::gedit-encoding не поддерживается
** (gedit:6348): WARNING **: 03:56:02.215: Set document metadata failed: Установка атрибута metadata::gedit-position не поддерживается
(gedit:6348): dconf-WARNING **: 03:56:02.376: failed to commit changes to dconf: Соединение закрыто
[root@10 ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@10 ~]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@10 ~]#
```

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux1. Проверил работу SELinux на практике совместно с веб-сервером Apache.