

Знакомство с SELinux

Абузярова Лейла Дамилевна НБИбд-01-19

15 октября, 2022, Москва, Россия

Российский Университет Дружбы Народов

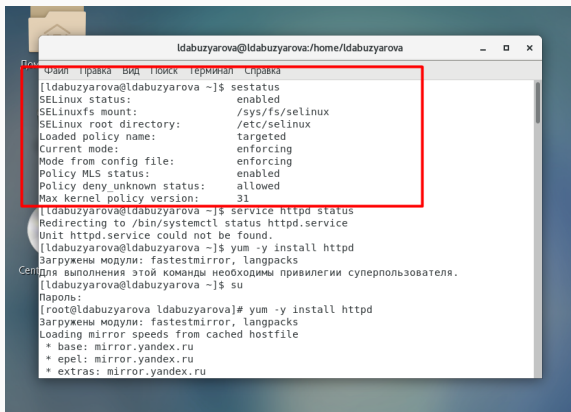
Цели и задачи

Цель лабораторной работы

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

Выполнение лабораторной работы

Запуск HTTP-сервера



The screenshot shows a terminal window titled 'ldabuzyarova@ldabuzyarova:/home/ldabuzyarova'. The terminal output is as follows:

```
ldabuzyarova@ldabuzyarova ~]$ 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
Max kernel policy version: 31

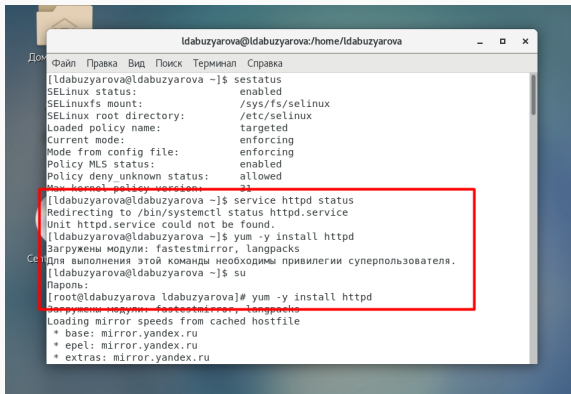
ldabuzyarova@ldabuzyarova ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
Unit httpd.service could not be found.

ldabuzyarova@ldabuzyarova ~]$ yum -y install httpd
Загружены модули: fastestmirror, langpacks
Для выполнения этой команды необходимы привилегии суперпользователя.
ldabuzyarova@ldabuzyarova ~]$ su
Пароль:
[root@ldabuzyarova ldabuzyarova]# yum -y install httpd
Загружены модули: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
* base: mirror.yandex.ru
* epel: mirror.yandex.ru
* extras: mirror.yandex.ru
```

A red rectangle highlights the output of the `sestatus` command.

Figure 1: Подготовка к работе

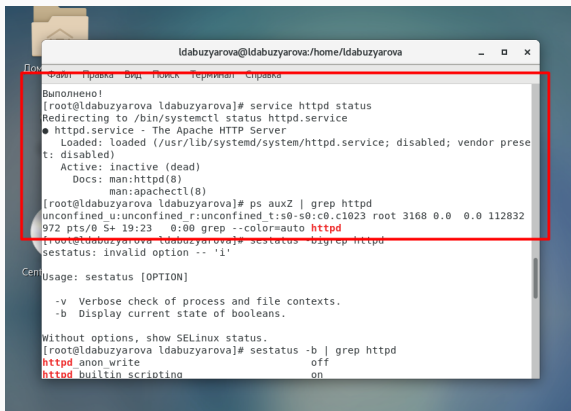
Запуск HTTP-сервера



```
ldabuzyarova@ldabuzyarova: /home/ldabuzyarova
[ldabuzyarova@ldabuzyarova ~]$ 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
Max kernel policy version: 31
[ldabuzyarova@ldabuzyarova ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
Unit httpd.service could not be found.
[ldabuzyarova@ldabuzyarova ~]$ yum -y install httpd
Заручены модули: fastestmirror, langpacks
Для выполнения этой команды необходимы привилегии суперпользователя.
[ldabuzyarova@ldabuzyarova ~]$ su
Пароль:
[root@ldabuzyarova ldabuzyarova]# yum -y install httpd
Заручены модули: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
* base: mirror.yandex.ru
* epel: mirror.yandex.ru
* extras: mirror.yandex.ru
```

Figure 2: Установка пакета httpd

Запуск HTTP-сервера



```
ldabuzyarova@ldabuzyarova:/home/ldabuzyarova
Помощь Файл Правка Вид Поиск Терминал Справка
Выполнено!
[root@ldabuzyarova ldabuzyarova]# 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; vendor prese
t: disabled)
   Active: inactive (dead)
     Docs: man:httpd(8)
          man:apachectl(8)
[root@ldabuzyarova ldabuzyarova]# ps auxZ | grep httpd
unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 root 3168 0.0  0.0 112832
972 pts/0 S+ 19:23  0:00 grep --color=auto httpd
[root@ldabuzyarova ldabuzyarova]# sestatus -bigrep httpd
sestatus: invalid option -- 'i'

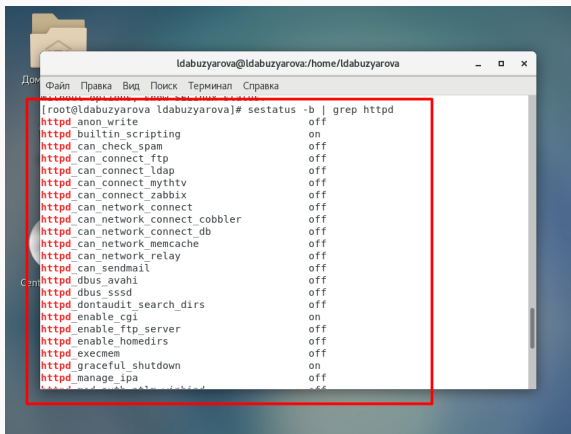
CentOS
Usage: sestatus [OPTION]

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

Without options, show SELinux status.
[root@ldabuzyarova ldabuzyarova]# sestatus -b | grep httpd
httpd anon write                                off
httpd builtin scripting                          on
```

Figure 3: Проверка службы

Запуск HTTP-сервера

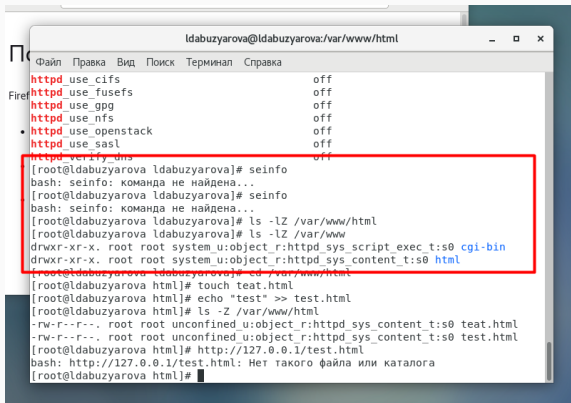


A terminal window titled 'ldabuzyarova@ldabuzyarova:/home/ldabuzyarova' displays the command 'sestatus -b | grep httpd'. The output lists various SELinux booleans for the httpd process, with 'httpd_anon_write' and 'httpd_enable_cgi' set to 'on', and all others to 'off'. A red rectangle highlights the output of the command.

```
(root@ldabuzyarova ldabuzyarova)# sestatus -b | grep httpd
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_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_avaahi                                    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                              on
httpd_manage_ipa                                     off
httpd_manage_etc_hosts                               off
```

Figure 4: Переключатели SELinux для http

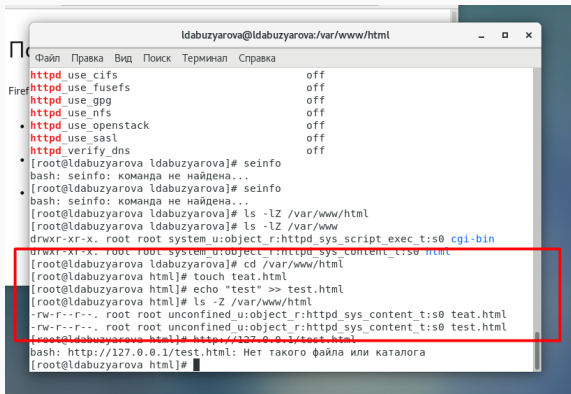
Проверка контекста файлов



```
ldabuzyarova@ldabuzyarova: /var/www/html
Файл  Правка  Вид  Поиск  Терминал  Справка
httpd_use_cifs                                off
httpd_use_fusefs                              off
httpd_use_gpg                                 off
httpd_use_nfs                                 off
• httpd_use_openstack                         off
httpd_use_sasl                                off
httpd_verify_dns                             off
[root@ldabuzyarova ldabuzyarova]# seinfo
bash: seinfo: команда не найдена...
[root@ldabuzyarova ldabuzyarova]# seinfo
bash: seinfo: команда не найдена...
[root@ldabuzyarova ldabuzyarova]# ls -lZ /var/www/html
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[root@ldabuzyarova ldabuzyarova]# cd /var/www/html
[root@ldabuzyarova html]# touch test.html
[root@ldabuzyarova html]# echo "test" >> test.html
[root@ldabuzyarova html]# ls -lZ /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@ldabuzyarova html]# http://127.0.0.1/test.html
bash: http://127.0.0.1/test.html: Нет такого файла или каталога
[root@ldabuzyarova html]#
```

Figure 5: Определение типа файлов в директориях

Создание html-файла



The screenshot shows a terminal window titled 'ldabuzyarova@ldabuzyarova: /var/www/html'. The terminal output includes the following commands and their results:

```
ldabuzyarova@ldabuzyarova: /var/www/html
httpd use_cifs off
httpd use_fusefs off
httpd use_gpg off
httpd use_nfs off
httpd use_openstack off
httpd use_sasl off
httpd verify_dns off
[root@ldabuzyarova ldabuzyarova]# seinfo
bash: seinfo: команда не найдена...
[root@ldabuzyarova ldabuzyarova]# seinfo
bash: seinfo: команда не найдена...
[root@ldabuzyarova ldabuzyarova]# ls -lZ /var/www/html
[root@ldabuzyarova ldabuzyarova]# ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[root@ldabuzyarova ldabuzyarova]# cd /var/www/html
[root@ldabuzyarova html]# touch test.html
[root@ldabuzyarova html]# echo "test" >> test.html
[root@ldabuzyarova html]# ls -lZ /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@ldabuzyarova html]# http://127.0.0.1/test.html
bash: http://127.0.0.1/test.html: Нет такого файла или каталога
[root@ldabuzyarova html]#
```

A red rectangle highlights the commands from `cd /var/www/html` to `http://127.0.0.1/test.html`, which are the steps for creating and filling the HTML file.

Figure 6: Создание и заполнение html-файла

Работа с html-файлом

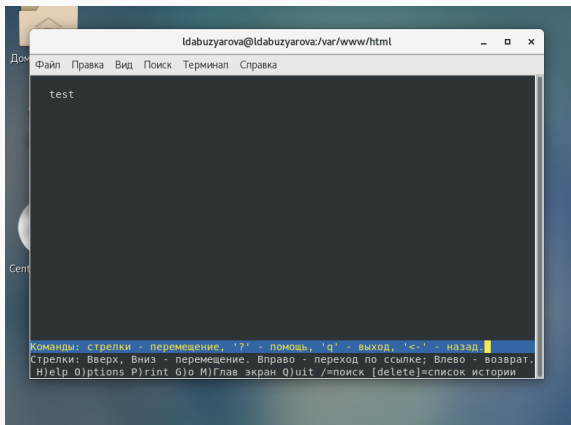
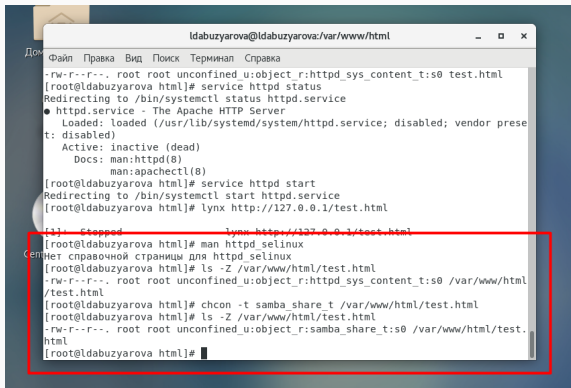


Figure 7: Проверка содержимого файла

Изменение контекста безопасности



The image shows a terminal window titled 'ldabuzyarova@ldabuzyarova:/var/www/html'. The terminal output shows the following commands and their results:

```
ldabuzyarova@ldabuzyarova:/var/www/html
- - -
File Edit View Search Terminal Help
[root@ldabuzyarova html]# 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; vendor prese
   Active: inactive (dead)
     Docs: man:httpd(8)
          man:apachectl(8)
[root@ldabuzyarova html]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@ldabuzyarova html]# lynx http://127.0.0.1/test.html
[!] Stopped lynx http://127.0.0.1/test.html
[root@ldabuzyarova html]# man httpd_selinux
Нет справочной страницы для httpd_selinux
[root@ldabuzyarova html]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html
/test.html
[root@ldabuzyarova html]# chcon -t samba_share_t /var/www/html/test.html
[root@ldabuzyarova html]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.
html
[root@ldabuzyarova html]#
```

A red rectangle highlights the last four lines of the terminal output, which show the file's context being changed to 'samba_share_t' and the subsequent 'ls' command output.

Figure 8: Проверка и изменение контекста файла

Изменение контекста безопасности

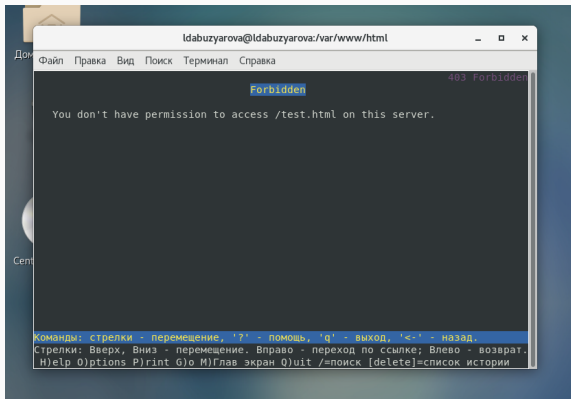
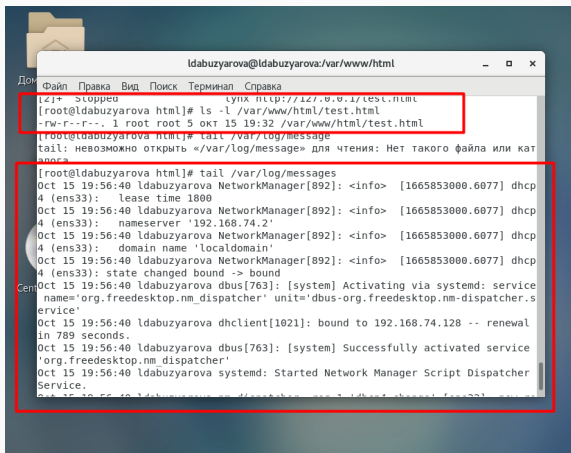


Figure 9: Ошибка доступа после изменения контекста

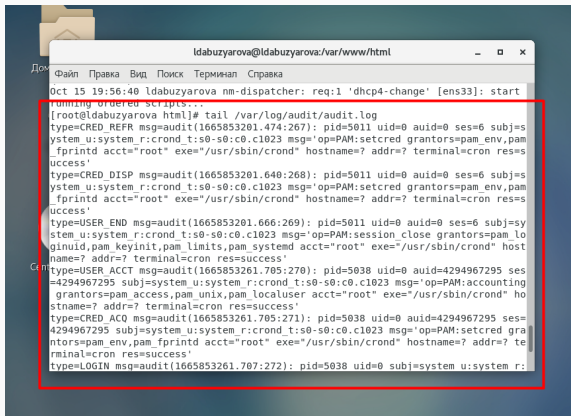
Последствия изменения контекста



```
ldabuzyarova@ldabuzyarova:/var/www/html
Файл Правка Вид Поиск Терминал Справка
[12]+  stopped lynx http://127.0.0.1/test.html
[root@ldabuzyarova html]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 5 окт 15 19:32 /var/www/html/test.html
[root@ldabuzyarova html]# tail /var/log/message
tail: невозможно открыть /var/log/message для чтения: Нет такого файла или каталога
[root@ldabuzyarova html]# tail /var/log/messages
Oct 15 19:56:40 ldabuzyarova NetworkManager[892]: <info> [1665853000.6077] dhcp
4 (ens33): lease time 1800
Oct 15 19:56:40 ldabuzyarova NetworkManager[892]: <info> [1665853000.6077] dhcp
4 (ens33): nameserver '192.168.74.2'
Oct 15 19:56:40 ldabuzyarova NetworkManager[892]: <info> [1665853000.6077] dhcp
4 (ens33): domain name 'localdomain'
Oct 15 19:56:40 ldabuzyarova NetworkManager[892]: <info> [1665853000.6077] dhcp
4 (ens33): state changed bound -> bound
Oct 15 19:56:40 ldabuzyarova dbus[763]: [system] Activating via systemd: service
name='org.freedesktop.nm_dispatcher' unit='dbus-org.freedesktop.nm_dispatcher.s
ervice'
Oct 15 19:56:40 ldabuzyarova dhclient[1021]: bound to 192.168.74.128 -- renewal
in 789 seconds.
Oct 15 19:56:40 ldabuzyarova dbus[763]: [system] Successfully activated service
'org.freedesktop.nm_dispatcher'
Oct 15 19:56:40 ldabuzyarova systemd: Started Network Manager Script Dispatcher
Service.
```

Figure 10: Лог ошибок

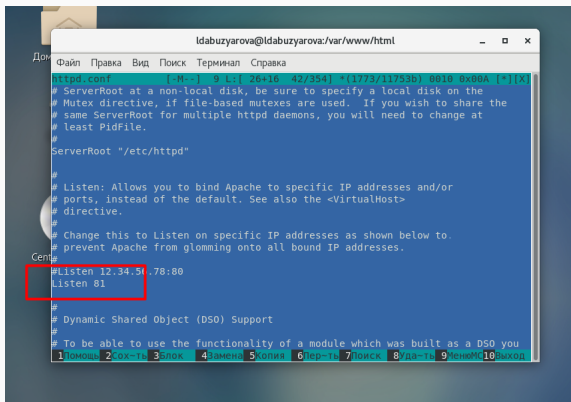
Последствия изменения контекста



```
ldabuzyarova@ldabuzyarova:/var/www/html
Файл Правка Вид Поиск Терминал Справка
Oct 15 19:56:40 ldabuzyarova nm-dispatcher: req:1 'dhcp4-change' [ens33]: start
running ordered scripts...
[root@ldabuzyarova html]# tail /var/log/audit/audit.log
type=CRED_REFR msg=audit(1665853201.474:267): pid=5011 uid=0 auid=0 ses=6 subj=s
ystem_u:system_r:cron_d_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam
_fprintd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=s
uccess'
type=CRED_DISP msg=audit(1665853201.640:268): pid=5011 uid=0 auid=0 ses=6 subj=s
ystem_u:system_r:cron_d_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam
_fprintd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=s
uccess'
type=USER_END msg=audit(1665853201.666:269): pid=5011 uid=0 auid=0 ses=6 subj=sy
stem_u:system_r:cron_d_t:s0-s0:c0.c1023 msg='op=PAM:session close grantors=pam_lo
ginuid,pam_keyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" host
name=? addr=? terminal=cron res=success'
type=USER ACCT msg=audit(1665853261.705:270): pid=5038 uid=0 auid=4294967295 ses
=4294967295 subj=system_u:system_r:cron_d_t:s0-s0:c0.c1023 msg='op=PAM:accounting
grantors=pam_access,pam_unix,pam_localuser acct="root" exe="/usr/sbin/crond" ho
stname=? addr=? terminal=cron res=success'
type=CRED_ACQ msg=audit(1665853261.705:271): pid=5038 uid=0 auid=4294967295 ses=
4294967295 subj=system_u:system_r:cron_d_t:s0-s0:c0.c1023 msg='op=PAM:setcred gra
ntors=pam_env,pam_fprintd acct="root" exe="/usr/sbin/crond" hostname=? addr=? te
rminial=cron res=success'
type=LOGIN msg=audit(1665853261.707:272): pid=5038 uid=0 subj=system_u:system_r:
```

Figure 11: Лог ошибок

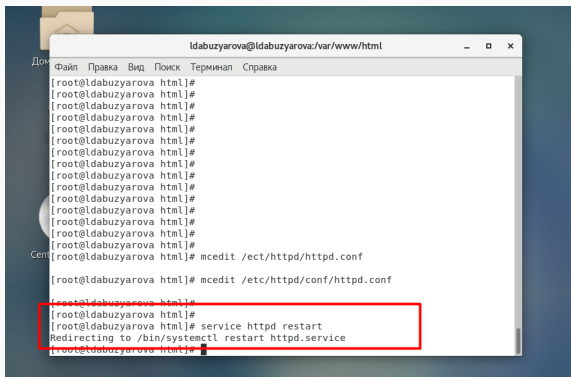
Переключение порта и восстановление контекста без-опасности



```
ldabuzyarova@ldabuzyarova:var/www/html
Файл Правка Вид Поиск Терминал Справка
httpd.conf
# 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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#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
```

Figure 12: Переключение порта

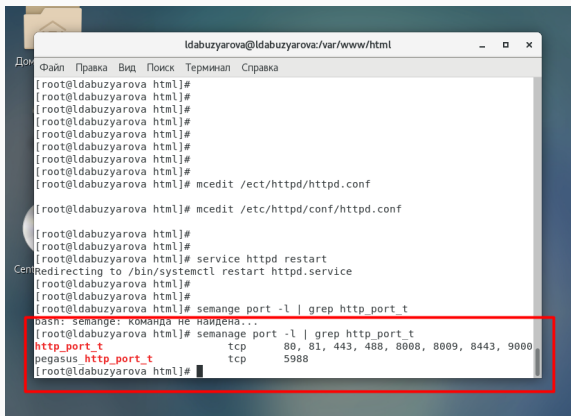
Переключение порта и восстановление контекста безопасности



```
ldabuzyarova@ldabuzyarova: /var/www/html
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]# mcedit /etc/httpd/httpd.conf
[root@ldabuzyarova html]# mcedit /etc/httpd/conf/httpd.conf
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@ldabuzyarova html]#
```

Figure 13: Проверка на сбой

Переключение порта и восстановление контекста без-опасности



```
ldabuzyarova@ldabuzyarova: /var/www/html
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]# mcedit /etc/httpd/httpd.conf
[root@ldabuzyarova html]# mcedit /etc/httpd/conf/httpd.conf
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]# semanage port -l | grep http_port t
bash: semange: команда не найдена...
[root@ldabuzyarova html]# 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@ldabuzyarova html]#
```

Figure 14: Проверка списка портов

Переключение порта и восстановление контекста без-опасности

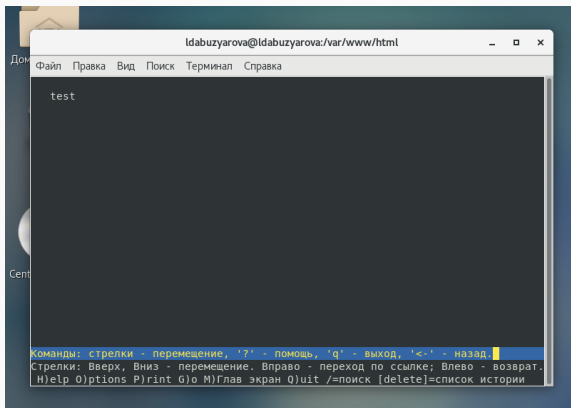
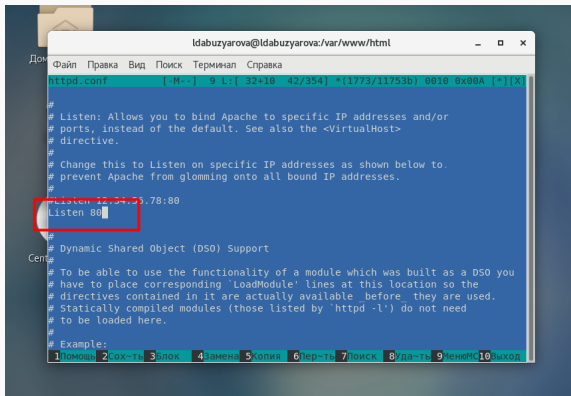


Figure 15: Содержимое файла

Переключение порта и восстановление контекста без-опасности

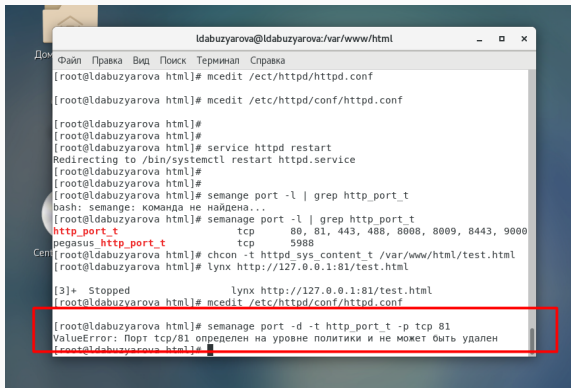


```
ldabuzyarova@ldabuzyarova:/var/www/html
Файл  Правка  Вид  Поиск  Терминал  Справка
httpd.conf  [-M--]  9  L: [ 32+10  42/354]  *(1773/11753b)  0010  0x00A  *}[X]

#
# 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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
Listen 12.34.56.78:80
Listen 80
#
#
# 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
# to be loaded here.
#
# Example:
# LoadModule ssl_module modules/mod_ssl.so
```

Figure 16: Повторное переключение порта

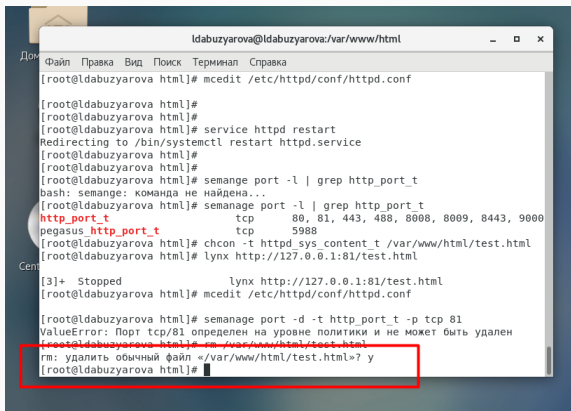
Удаление 81 порта



```
ldabuzyarova@ldabuzyarova:/var/www/html
Домашний
Файл Правка Вид Поиск Терминал Справка
[root@ldabuzyarova html]# mcedit /ect/httpd/httpd.conf
[root@ldabuzyarova html]# mcedit /etc/httpd/conf/httpd.conf
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]# semanage port -l | grep http_port_t
bash: semanage: команда не найдена...
[root@ldabuzyarova html]# 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
CentOS [root@ldabuzyarova html]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@ldabuzyarova html]# lynx http://127.0.0.1:81/test.html
[3]+  Stopped                  lynx http://127.0.0.1:81/test.html
[root@ldabuzyarova html]# mcedit /etc/httpd/conf/httpd.conf
[root@ldabuzyarova html]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@ldabuzyarova html]#
```

Figure 17: Неудачная попытка удалить 81 порт

Удаление файла



```
ldabuzyarova@ldabuzyarova:var/www/html
Файл Правка Вид Поиск Терминал Справка
[root@ldabuzyarova html]# mcedit /etc/httpd/conf/httpd.conf

[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@ldabuzyarova html]#
[root@ldabuzyarova html]#
[root@ldabuzyarova html]# semange port -l | grep http_port_t
bash: semange: команда не найдена...
[root@ldabuzyarova html]# semange 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@ldabuzyarova html]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@ldabuzyarova html]# lynx http://127.0.0.1:81/test.html
[3]+  Stopped                  lynx http://127.0.0.1:81/test.html
[root@ldabuzyarova html]# mcedit /etc/httpd/conf/httpd.conf

[root@ldabuzyarova html]# semange port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@ldabuzyarova html]# rm -f /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
[root@ldabuzyarova html]#
```

Figure 18: Удаление файла

Выводы

В процессе выполнения лабораторной работы мною были получены базовые навыки работы с технологией seLinux.