

Лабораторная работа №9

Презентация

Устинова В. В.

31 октября 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Устинова Виктория Вадимовна
- студент НПИбд-01-24
- Российский университет дружбы народов

Получить навыки работы с контекстом безопасности и политиками SELinux.

1. Продемонстрируйте навыки по управлению режимами SELinux (см. раздел 9.4.1).
2. Продемонстрируйте навыки по восстановлению контекста безопасности SELinux (см. раздел 9.4.2).
3. Настройте контекст безопасности для нестандартного расположения файлов веб-службы (см. раздел 9.4.3).
4. Продемонстрируйте навыки работы с переключателями SELinux (см. раздел 9.4.4).

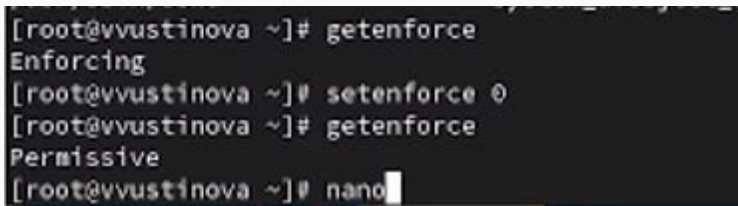
Просмотрите текущую информацию о состоянии SELinux

```
[root@vvustinova ~]# sestatus -v
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

Process contexts:
Current context:              unconfined_u:unconfined_r:unconfined_t:s0-s
```

Рис. 1: переходим в андмин. и смотрим информацию, селинукс активен и работает нормально

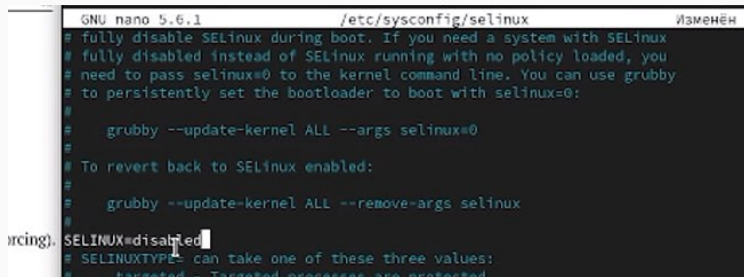
Посмотрите, в каком режиме работает SELinux, измените режим работы SELinux на разрешающий (Permissive)

A terminal window with a black background and white text. The prompt is [root@vvustinova ~]#. The first command is 'getenforce', which outputs 'Enforcing'. The second command is 'setenforce 0'. The third command is 'getenforce', which outputs 'Permissive'. The fourth command is 'nano', followed by a cursor.

```
[root@vvustinova ~]# getenforce
Enforcing
[root@vvustinova ~]# setenforce 0
[root@vvustinova ~]# getenforce
Permissive
[root@vvustinova ~]# nano
```

Рис. 2: SELinux работает в режиме enforcing, мы переключили его на Permissive

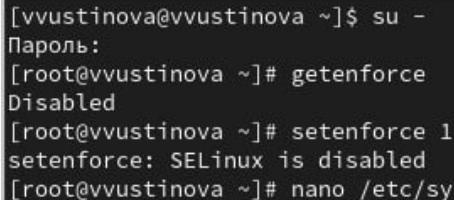
В файле `/etc/sysconfig/selinux` с помощью редактора установите disabled



```
GNU nano 5.6.1 /etc/sysconfig/selinux изменён
# fully disable SELinux during boot. If you need a system with SELinux
# fully disabled instead of SELinux running with no policy loaded, you
# need to pass selinux=0 to the kernel command line. You can use grubby
# to persistently set the bootloader to boot with selinux=0:
#
#   grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubby --update-kernel ALL --remove-args selinux
#
rcing). SELINUX=disabled
# SELINUXTYPE can take one of these three values:
#   targeted - Targeted processes are protected
```

Рис. 3: заменяем enforcing на disabled и перезапускаем систему

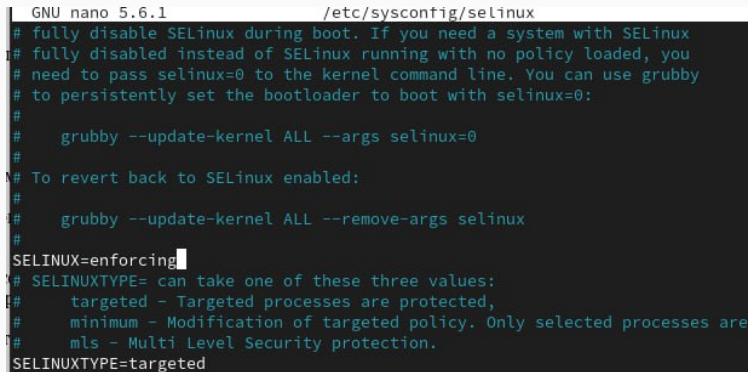
После перезагрузки, посмотрите статус SELinux, попробуйте переключить режим работы SELinux

A terminal window with a dark background. The prompt is [vvustinova@vvustinova ~]\$ and the user has entered 'su -'. The prompt changes to [root@vvustinova ~]#. The user enters 'getenforce', and the output is 'Disabled'. The user then enters 'setenforce 1', and the output is 'setenforce: SELinux is disabled'. Finally, the user enters 'nano /etc/sysconfig/selinux', and the prompt returns to [root@vvustinova ~]#.

```
[vvustinova@vvustinova ~]$ su -  
Пароль:  
[root@vvustinova ~]# getenforce  
Disabled  
[root@vvustinova ~]# setenforce 1  
setenforce: SELinux is disabled  
[root@vvustinova ~]# nano /etc/sysconfig/selinux
```

Рис. 4: Статус стал: disabled, не удастся переключить на режим работы потому что она отключена

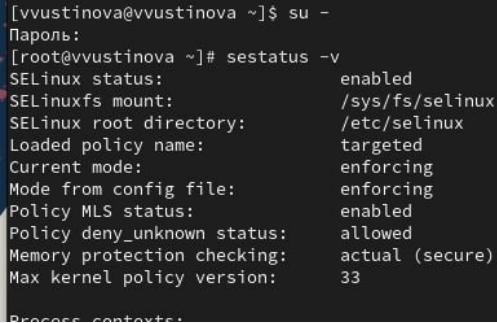
Откройте файл `/etc/sysconfig/selinux` с помощью редактора и установите enforcing



```
GNU nano 5.6.1 /etc/sysconfig/selinux
# fully disable SELinux during boot. If you need a system with SELinux
# fully disabled instead of SELinux running with no policy loaded, you
# need to pass selinux=0 to the kernel command line. You can use grubby
# to persistently set the bootloader to boot with selinux=0:
#
#   grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubby --update-kernel ALL --remove-args selinux
#
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Рис. 5: Снова меняем, только теперь на enforcing

После перезагрузки, убедитесь, что система работает в принудительном режиме (enforcing) использования SELinux.

A terminal window showing the command 'su -' to switch to root, followed by 'sestatus -v' to display SELinux status. The output shows that SELinux is enabled, the policy is targeted, and the current mode is enforcing.

```
[vvustinova@vvustinova ~]$ su -  
Пароль:  
[root@vvustinova ~]# sestatus -v  
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  
Process contexts:
```

Рис. 6: Она активна и работает в принудительном режиме все верно

Использование restorecon для восстановления контекста безопасности

Посмотрите контекст безопасности файла /etc/hosts, Скопируйте файл /etc/hosts в домашний каталог, Проверьте контекст файла ~/hosts

```
[root@vvustinova ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@vvustinova ~]# cp /etc/hosts ~/
[root@vvustinova ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
```

Рис. 7: у файла есть метка контекста net_conf_t., после копирования(что считается созданием нового файла) контекст стал admin_home_t.

Попытайтесь перезаписать существующий файл hosts из домашнего каталога в каталог /etc, убедитесь, что тип контекста по-прежнему установлен на admin_home_t

```
unconfined_u:object_r:admin_home_t:s0 /etc/hosts  
[root@vvustinova ~]# mv ~/hosts /etc  
mv: переписать '/etc/hosts'? y  
[root@vvustinova ~]# ls -Z /etc/hosts  
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
```

Рис. 8: Подтверждаем перезаписывание файла и тип контекста все еще admin_home_t

Исправьте контекст безопасности, убедитесь, что тип контекста изменился, для массового исправления контекста безопасности на файловой системе введите

```
[root@vvustinova ~]# restorecon -v /etc/hosts
Relabeled /etc/hosts from unconfined_u:object_r:admin_home_t:s0 to unconfined_u:object_r:net_conf_t:s0
[root@vvustinova ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@vvustinova ~]# touch /.autorelabel
[root@vvustinova ~]#
```

Рис. 9: Опция -v показывает процесс изменения, тип контекста изменился на net_conf_t, вводим команду и перезапускаем машину

Использование restorecon для восстановления контекста безопасности

Во время перезапуска не забудьте нажать клавишу Esc на клавиатуре, чтобы вы видели загрузочные сообщения

```
[ OK ] Finished Automatic Boot Loader Update.
[ OK ] Finished Create Volatile Files and Directories.
      Starting Record System Boot/Shutdown in UTMP...
[ OK ] Finished Record System Boot/Shutdown in UTMP.
[ OK ] Reached target System Initialization.
[ OK ] Started Manage Sound Card State (restore and store).
[ OK ] Reached target Sound Card.
      Starting Restore /run/initramfs on shutdown...
      Starting Relabel all filesystems...
[ OK ] Finished Restore /run/initramfs on shutdown.
[ 46.679290] selinux-autorelabel[781]: *** Warning -- SELinux targeted policy relabel is required.
[ 46.683976] selinux-autorelabel[781]: *** Relabeling could take a very long time, depending on file
[ 46.685853] selinux-autorelabel[781]: *** system size and speed of hard drives.
[ 46.728486] selinux-autorelabel[781]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 10: нажимаем esc во время перезапуска и видим, что система перемаркирована автоматически

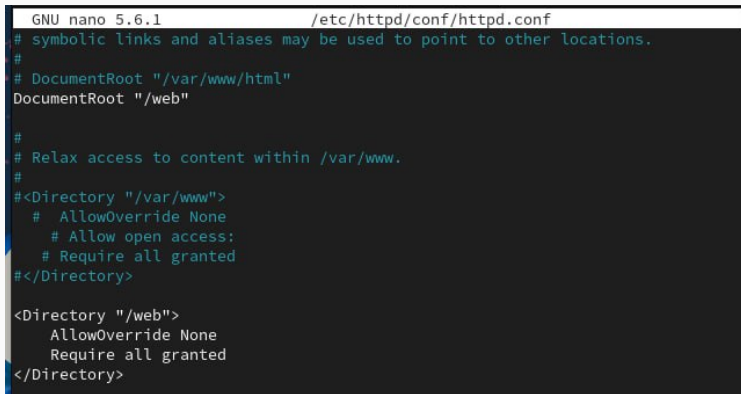
Создайте новое хранилище для файлов web-сервера, создайте файл index.html в каталоге с контентом веб-сервера, и поместите туда: Welcome to my web-server

```
Выполнено:  
[root@vvustinova ~]# mkdir /web  
[root@vvustinova ~]# cd /web  
[root@vvustinova web]# touch index.html  
[root@vvustinova web]# nano index.html
```

Рис. 11: создаем новое хранилище, переходим туда и создаем файл, через редактор nano добавляем туда строчку

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

В файле `/etc/httpd/conf/httpd.conf` закомментируйте строку `DocumentRoot "/var/www/html"` и ниже добавьте строку

A screenshot of a terminal window showing the configuration of the httpd.conf file using the nano text editor. The title bar of the window reads "GNU nano 5.6.1 /etc/httpd/conf/httpd.conf". The visible text in the editor is as follows:

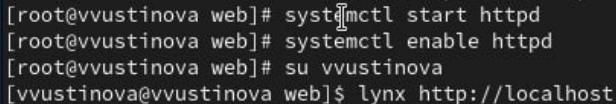
```
# symbolic links and aliases may be used to point to other locations.
#
# DocumentRoot "/var/www/html"
DocumentRoot "/web"

#
# Relax access to content within /var/www.
#
#<Directory "/var/www">
#   AllowOverride None
#   Allow open access:
#   Require all granted
#</Directory>

<Directory "/web">
    AllowOverride None
    Require all granted
</Directory>
```

Рис. 12: Комментируем строчку и добавляем ниже: `DocumentRoot "/web"`, также ниже комментируем целый раздел и вместо него пишем другое

Запустите веб-сервер и службу httpd, в терминале под учётной записью своего пользователя при обращении к веб-серверу в текстовом браузере lynx, вы увидите веб-страницу Red Hat по умолчанию, а не содержимое только что созданного файла index.html



```
[root@vvustinova web]# systemctl start httpd
[root@vvustinova web]# systemctl enable httpd
[root@vvustinova web]# su vvustinova
[vvustinova@vvustinova web]$ lynx http://localhost
```

Рис. 13: Мы открыли файл и вышли из него

В терминале с полномочиями администратора примените новую метку контекста к /web, восстановите контекст безопасности

```
[root@vvustinova ~]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"  
[root@vvustinova ~]# restorecon -R -v /web  
Relabeled /web from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:  
d_sys_content_t:s0  
Relabeled /web/index.html from unconfined_u:object_r:default_t:s0 to unconfined  
ject_r:httpd_sys_content_t:s0  
[root@vvustinova ~]# su vvustinova
```

Рис. 14: Прodelали все действия, и презагружаем машину

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Теперь вы получите доступ к своей пользовательской веб-странице. В случае успеха на экране должна быть отображена запись «Welcome to my web-server»

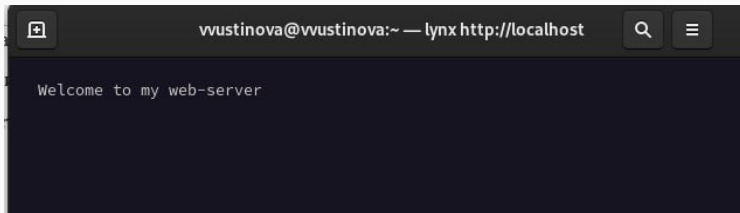


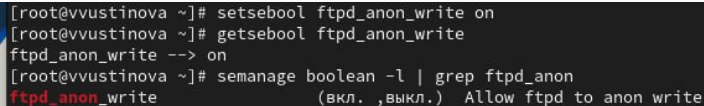
Рис. 15: Открываем и смотрим, у нас все получилось!

Посмотрите список переключателей SELinux для службы ftp, Вы увидите переключатель `ftpd_anon_write` с текущим значением `off`, для службы `ftpd_anon` посмотрите список переключателей

```
[root@vvustinova ~]# getsebool -a | grep ftp
ftpd_anon_write --> off
ftpd_connect_all_unreserved --> off
ftpd_connect_db --> off
ftpd_full_access --> off
ftpd_use_cifs --> off
ftpd_use_fusefs --> off
ftpd_use_nfs --> off
ftpd_use_passive_mode --> off
httpd_can_connect_ftp --> off
httpd_enable_ftp_server --> off
tftp_anon_write --> off
tftp_home_dir --> off
[root@vvustinova ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (выкл.,выкл.) Allow ftpd to anon write
```

Рис. 16: Видим что все переключатели выключены

Измените текущее значение переключателя для службы `ftpd_anon_write` с `off` на `on`, повторно посмотрите список переключателей SELinux для службы `ftpd_anon_write`, посмотрите список переключателей с пояснением

A terminal window with a dark background and light-colored text. The text shows a series of commands and their outputs in a root shell. The first command sets the 'ftpd_anon_write' boolean to 'on'. The second command confirms this setting. The third command lists all SELinux booleans, filtered for those containing 'ftpd_anon'. The output shows 'ftpd_anon_write' is currently 'off', with a note that it can be turned on or off to allow ftpd to write anonymously.

```
[root@vvustinova ~]# setsebool ftpd_anon_write on
[root@vvustinova ~]# getsebool ftpd_anon_write
ftpd_anon_write --> on
[root@vvustinova ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write              (вкл. ,выкл.) Allow ftpd to anon write
```

Рис. 17: Настройка времени выполнения включена, но постоянная настройка по-прежнему отключена.

Измените постоянное значение переключателя для службы ftpd_anon_write с off на on, посмотрите список переключателей

```
[root@vvustinova ~]# setsebool -P ftpd_anon_write on
[root@vvustinova ~]#
[root@vvustinova ~]#
[root@vvustinova ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write          (вкл. , вкл.) Allow ftpd to anon write
[root@vvustinova ~]#
```

Рис. 18: Теперь все включено, переключатели разрешают анонимную запись на FTP сервер через селинукс

Мы успешно получили навыки работы с контекстом безопасности и политиками SELinux.