

Лабораторная работа №9

Управление SELinux

Юсупова К. Р.

Российский университет дружбы народов, Москва, Россия

Информация

- Юсупова Ксения Равиловна
- Российский университет дружбы народов
- Номер студенческого билета- 1132247531
- [1132247531@pfur.ru]

Вводная часть

Получить навыки работы с контекстом безопасности и политиками SELinux.

Выполнение лабораторной работы

Выполнение лабораторной работы

Получили права администратора. Проверили состояние SELinux - система активна в режиме enforcing с политикой targeted. Конфигурационные файлы расположены в /etc/selinux. Проверили контексты безопасности процессов и файлов

```
[ksyusha@yu ~]$ su -
Пароль:
[root@yu ~]# 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-s0:c0
                               .c1023
Init context:                  system_u:system_r:init_t:s0
/usr/sbin/sshd                 system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:         unconfined_u:object_r:user_devpts_t:s0
/etc/passwd                   system_u:object_r:passwd_file_t:s0
/etc/shadow                   system_u:object_r:shadow_t:s0
/bin/bash                     system_u:object_r:shell_exec_t:s0
/bin/login                    system_u:object_r:login_exec_t:s0
/bin/sh                       system_u:object_r:bin_t:s0 -> system_u:object_r
                               :shell_exec_t:s0
/sbin/agetty                  system_u:object_r:getty_exec_t:s0
/sbin/init                    system_u:object_r:bin_t:s0 -> system_u:object_r
                               :init_exec_t:s0
:                             system_u:object_r:bin_t:s0 -> system_u:object_r
                               :init_exec_t:s0
/usr/sbin/sshd                 system_u:object_r:sshd_exec_t:s0
```

Рис. 1: Выполнили пункты 1 и 2 из раздела 9.4.1. (Управление режимами SELinux)

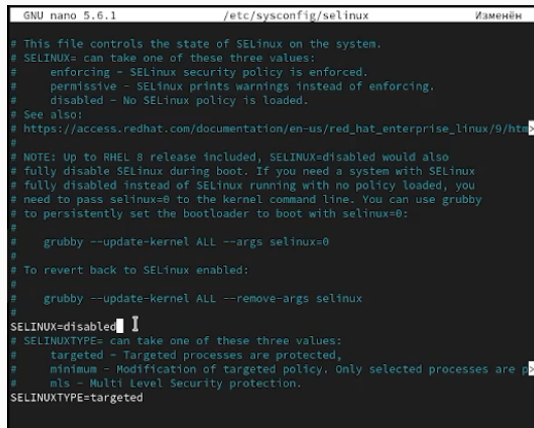
Посмотрели, в каком режиме работает SELinux. По умолчанию SELinux находится в режиме принудительного исполнения (Enforcing). Изменили режим работы SELinux на разрешающий (Permissive) и снова ввели `getenforce`

```
[root@yu ~]# getenforce
Enforcing
[root@yu ~]# setenforce 0
[root@yu ~]# getenforce
Permissive
[root@yu ~]# cd ~/etc/sysconfig/selinux
-bash: cd: /root/etc/sysconfig/selinux: Нет такого файла или каталога
```

Рис. 2: Выполнили пункты 3 и 4 из раздела 9.4.1. (Управление режимами SELinux)

Выполнение лабораторной работы

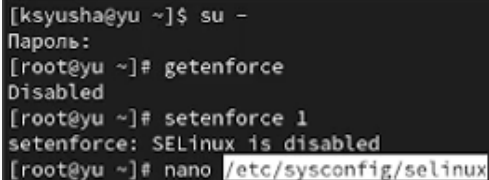
В файле `/etc/sysconfig/selinux` с помощью редактора установили `SELINUX=disabled` и перезагрузили систему



```
GNU nano 5.6.1 /etc/sysconfig/selinux Изменён
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
# See also:
# https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html
#
# NOTE: Up to RHEL 8 release included, SELINUX=disabled would also
# 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=disabled I
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are p
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Рис. 3: Выполнили пункт 5 из раздела 9.4.1. (Управление режимами SELinux)

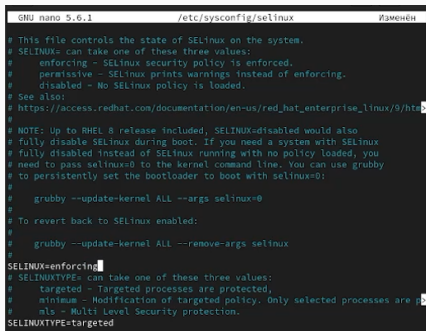
После перезагрузки запустили терминал и получили полномочия администратора. Посмотрели статус SELinux и увидели, что SELinux теперь отключён. Попробовали переключить режим работы SELinux, мы не можем переключаться между отключённым и принудительным режимом без перезагрузки системы

A terminal window with a black background and white text. The user 'ksyusha@yu' is in their home directory '~'. They enter 'su -' to become root. The prompt changes to '[root@yu ~]#'. They enter 'getenforce' and see 'Disabled'. Then they enter 'setenforce 1' and see 'setenforce: SELinux is disabled'. Finally, they enter 'nano /etc/sysconfig/selinux', where the file path is highlighted in white on a black background.

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

Рис. 4: Выполнили пункты 6, 7 и 8 из раздела 9.4.1. (Управление режимами SELinux)

Открыли файл `/etc/sysconfig/selinux` с помощью редактора и установили `SELINUX=enforcing` и перезагрузили систему. Во время загрузки системы получили предупреждающее сообщение о необходимости восстановления меток SELinux, что может занять некоторое время, а также потребовало дополнительной перезагрузки системы



```
GNU nano 5.6.1 /etc/sysconfig/selinux  Изменен
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
# See also:
# https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html
#
# NOTE: Up to RHEL 8 release included, SELINUX=disabled would also
# 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 p
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

После перезагрузки в терминале с полномочиями администратора просмотрели текущую информацию о состоянии SELinux, и убедились, что система работает в принудительном режиме (enforcing) использования SELinux.

```
(ksyusha@yu ~)$ su -
Пароль:
[root@yu ~]# 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-s0:c0.
c1023
Init context:                   system_u:system_r:init_t:s0
/usr/sbin/sshd                  system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:          unconfined_u:object_r:user_devpts_t:s0
/etc/passwd                    system_u:object_r:passwd_file_t:s0
/etc/shadow                    system_u:object_r:shadow_t:s0
/bin/bash                      system_u:object_r:shell_exec_t:s0
/bin/login                     system_u:object_r:login_exec_t:s0
/bin/sh                         system_u:object_r:bin_t:s0 -> system_u:object_r:
shell_exec_t:s0
/sbin/agetty                   system_u:object_r:getty_exec_t:s0
/sbin/init                     system_u:object_r:bin_t:s0 -> system_u:object_r:
init_exec_t:s0
/usr/sbin/sshd                 system_u:object_r:sshd_exec_t:s0
```

Рис. 6: Выполнили пункт 11 из раздела 9.4.1. (Управление режимами SELinux)

Проверили контекст файла /etc/hosts. Скопировали его в домашний каталог - контекст изменился. Исправили контекст безопасности и выполнили массовое восстановление меток

```
[root@yu ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@yu ~]# cp /etc/hosts ~/
[root@yu ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@yu ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@yu ~]# mv ~/hosts /etc
mv: переписать '/etc/hosts'? y
[root@yu ~]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@yu ~]# 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@yu ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@yu ~]# touch /.autorelabel
[root@yu ~]# reboot
```

Рис. 7: Выполнили пункт 1-8 из раздела 9.4.2. (Использование restorecon для восстановления контекста безопасности)

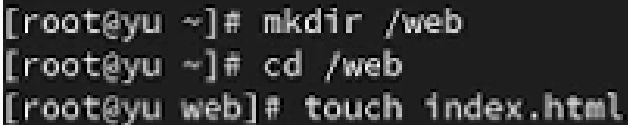
Запустили терминал и получили полномочия администратора. Установили необходимое программное обеспечение.

```
[ksyusha@yu ~]$ su -
Пароль:
[root@yu ~]# dnf -y install httpd
Последняя проверка окончания срока действия метаданных: 0:53:42 назад, Ср 29 о
кт 2025 16:56:02.
Пакет httpd-2.4.62-4.el9_6.4.x86_64 уже установлен.
Зависимости разрешены.
Отсутствуют действия для выполнения.
Выполнено!
[root@yu ~]# dnf -y install lynx
Последняя проверка окончания срока действия метаданных: 0:53:51 назад, Ср 29 о
кт 2025 16:56:02.
Зависимости разрешены.
=====
Пакет      Архитектура  Версия      Репозиторий  Размер
=====
Установка:
  lynx      x86_64       2.8.9-20.el9  appstream    1.5 М
Результат транзакции
=====
Установка 1 Пакет

Объем загрузки: 1.5 М
Объем изменений: 6.1 М
Загрузка пакетов:
[===                ] --- B/s |  0 B    --:-- ETA
```

Рис. 8: Выполнили пункты 1 и 2 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)

Создали новое хранилище для файлов web-сервера и файл index.html в каталоге с контентом веб-сервера

A terminal window with a black background and white text. It shows three commands being executed in sequence: 'mkdir /web', 'cd /web', and 'touch index.html'. The prompt changes from '[root@yu ~]' to '[root@yu web]' after the second command.

```
[root@yu ~]# mkdir /web
[root@yu ~]# cd /web
[root@yu web]# touch index.html
```

Рис. 9: Выполнили пункты 3 и 4 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)

Поместили в файл данный нам текст

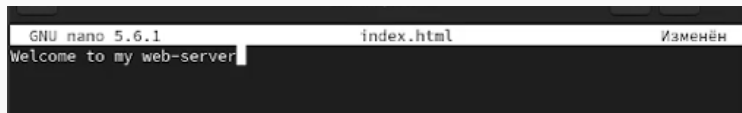
A screenshot of the GNU nano 5.6.1 text editor. The editor's title bar shows 'GNU nano 5.6.1' on the left, 'index.html' in the center, and 'Изменён' (Changed) on the right. The main editing area has a dark background with light-colored text. The first line of the file contains the text 'Welcome to my web-server' followed by a cursor. The rest of the file is empty.

Рис. 10: Выполнили пункт 4 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)

Выполнение лабораторной работы

В файле `/etc/httpd/conf/httpd.conf` закомментировали строку `DocumentRoot "/var/www/html"` и ниже добавили строку `DocumentRoot "/web"`. Затем в этом же файле ниже закомментируйте необходимый раздел и добавили следующий раздел, определяющий правила доступа

```
# 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. 11: Выполнили пункт 5 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)

Запустили веб-сервер и службу httpd

```
[root@yu web]# systemctl start httpd  
[root@yu web]# systemctl enable httpd
```

Рис. 12: Выполнили пункт 6 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)

Выполнение лабораторной работы

В терминале под учётной записью своего пользователя при обращении к веб-серверу в текстовом браузере lynx увидели веб-страницу Red Hat по умолчанию, а не содержимое только что созданного файла index.html

```
HTTP Server Test Page powered by: Rocky Linux (p2 of 2)

For systems using the Apache Webserver: You can add content to the
directory /var/www/html/. Until you do so, people visiting your
website will see this page. If you would like this page to not be
shown, follow the instructions in: /etc/httpd/conf.d/welcome.conf.

For systems using Nginx: You can add your content in a location of
your choice and edit the root configuration directive in
/etc/nginx/nginx.conf.
[ Powered by Rocky Linux ] [poweredby.png]

Apache™ is a registered trademark of the Apache Software Foundation
in the United States and/or other countries.
NGINX™ is a registered trademark of F5 Networks, Inc..

I
```

В терминале с полномочиями администратора применили новую метку контекста и восстановили контекст безопасности

```
[root@yu web]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"  
[root@yu web]# restorecon -R -v /web  
Relabeled /web from unconfined_u:object_r:default_t:s0 to unconfined_u:object_  
r:httpd_sys_content_t:s0  
Relabeled /web/index.html from unconfined_u:object_r:default_t:s0 to unconfine  
d_u:object_r:httpd_sys_content_t:s0  
[root@yu web]#
```

Рис. 14: Выполнили пункт 8 и 9 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)

В терминале под учётной записью своего пользователя снова обратились к веб-серверу. Теперь мы получили доступ к своей пользовательской веб-странице. На экране отобразилась запись «Welcome to my web-server»

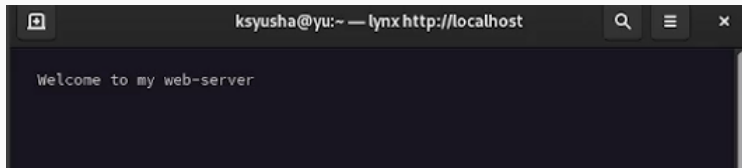


Рис. 15: Выполнили пункт 10 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)

Выполнение лабораторной работы

Просмотрели список переключателей SELinux для службы FTP. Обнаружили переключатель `ftpd_anon_write` в состоянии «off». Используя команды `setsebool` и `setsebool -P`, изменили значение переключателя сначала для текущей сессии, а затем на постоянной основе. После применения настроек убедились, что переключатель `ftpd_anon_write` переведен в состояние «on», что разрешает анонимным пользователям FTP-сервера выполнять операции записи. Данная настройка сохранится после перезагрузки системы.

```
[ksyusha@yu ~]$ su -
Пароль:
[root@yu ~]# 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@yu ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (выкл.,выкл.) Allow ftpd to anon write
[root@yu ~]# setsebool ftpd_anon_write on
[root@yu ~]# getsebool ftpd_anon_write
ftpd_anon_write --> on
[root@yu ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл.,выкл.) Allow ftpd to anon write
[root@yu ~]# setsebool -P ftpd_anon_write on
[root@yu ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл., вкл.) Allow ftpd to anon write
[root@yu ~]#
```

Выводы

В ходе лабораторной работы мы получили навыки работы с контекстом безопасности и политиками SELinux.