

Лабораторная работа №9

Управление SELinux

Сидорова А.В.

Российский университет дружбы народов, Москва, Россия

Информация

- Сидорова Арина Валерьевна
- студентка НПИбд-02-24
- ст.б. 1132242912
- Российский университет дружбы народов

Вводная часть

SELinux является критически важным компонентом безопасности современных Linux-систем, обеспечивающим мандатный контроль доступа для защиты от несанкционированных действий и ограничения последствий потенциальных уязвимостей.

Объект исследования

- Система принудительного контроля доступа SELinux в операционной системе Linux.

Предмет исследования

- Механизмы управления контекстами безопасности, режимами работы и политиками доступа SELinux.

Цель: Получить практические навыки работы с системой безопасности SELinux, включая управление режимами работы, контекстами безопасности и политиками доступа.

Задачи:

1. Освоить управление режимами работы SELinux (Enforcing, Permissive, Disabled).
2. Научиться восстанавливать контексты безопасности файлов и каталогов.
3. Получить навыки настройки контекстов безопасности для нестандартных расположений служб.
4. Изучить работу с переключателями (boolean) SELinux.

Выполнение лабораторной работы

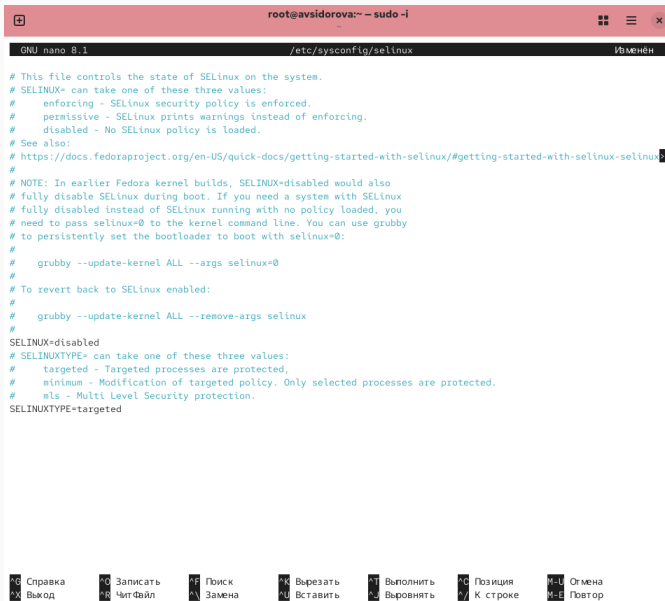
Посмотрим текущую информацию о состоянии SELinux: `sestatus -v` Посмотрим, в каком режиме работает SELinux: `getenforce` Изменим режим работы SELinux на разрешающий `setenforce 0` и снова введем `getenforce`

```
avsidorova@avsidorova:~$ sudo -i
[sudo] пароль для avsidorova:
root@avsidorova:~# 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
```

В файле /etc/sysconfig/selinux с помощью редактора установим SELINUX=disabled



```
root@avsidorova:~ -- sudo -i
GNU nano 8.1 /etc/sysconfig/selinux ИВМЕНЕВ

# 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://docs.fedoraproject.org/en-US/quick-docs/getting-started-with-selinux/#getting-started-with-selinux-selinux>
#
# NOTE: In earlier Fedora kernel builds, 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
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted

^G Справка      ^O Записать    ^F Поиск      ^K Вырезать   ^T Выполнить  ^C Позиция    ^M Отмена
^X Выход        ^R ЧитФайл    ^\ Замена     ^U Вставить   ^J Вывернуть  ^_ К строке   ^M Повтор
```

Посмотрим статус SELinux: getenforce SELinux теперь отключён.

Попробуем переключить режим работы SELinux: setenforce 1 Мы не можем переключаться между отключённым и принудительным режимом без перезагрузки системы.

A terminal window with a red title bar. The terminal shows a user named avsidorova at a shell prompt. They run 'sudo -i' and enter a password. The prompt changes to root. Then they run 'getenforce' which outputs 'Disabled'. Next, they run 'setenforce 1' which outputs 'setenforce: SELinux is disabled'. The terminal ends with the root prompt and a cursor.

```
avsidorova@avsidorova:~$ sudo -i
[sudo] пароль для avsidorova:
root@avsidorova:~# getenforce
Disabled
root@avsidorova:~# setenforce 1
setenforce: SELinux is disabled
root@avsidorova:~#
```

Рис. 3: SELinux теперь отключён

Откроем файл `/etc/sysconfig/selinux` с помощью редактора и установим:

SELINUX=enforcing Перезагрузим систему.



```
root@avsidorova:~ - sudo -i
GNU nano 8.1 /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://docs.fedoraproject.org/en-US/quick-docs/getting-started-with-selinux/#getting-started-with-selinux-selinux
#
# NOTE: In earlier Fedora kernel builds, 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 protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

После перезагрузки в терминале с полномочиями администратора посмотрим текущую информацию о состоянии SELinux:

sestatus -v

```
avsidorova@avsidorova:~$ sudo -i
[sudo] пароль для avsidorova:
root@avsidorova:~# 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

root@avsidorova:~#
```

Посмотрим контекст безопасности файла `/etc/hosts`. У файла есть метка контекста `net_conf_t`.

Скопируем файл `/etc/hosts` в домашний каталог. Проверим контекст файла `~/hosts`.

Поскольку копирование считается созданием нового файла, то параметр контекста в файле `~/hosts`, расположенном в домашнем каталоге, станет `admin_home_t`.

Попытаемся перезаписать существующий файл `hosts` из домашнего каталога в каталог `/etc`:
`mv ~/hosts /etc` Убедимся, что тип контекста по-прежнему установлен на `admin_home_t`.

Исправим контекст безопасности.

Убедимся, что тип контекста изменился: `ls -Z /etc/hosts`

Для массового исправления контекста безопасности на файловой системе введем

`touch /.autorelabel`

```
root@avsidorova:~# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@avsidorova:~# cp /etc/hosts ~/
root@avsidorova:~# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 ~/hosts
root@avsidorova:~# mv ~/hosts /etc
mv: переписать '/etc/hosts'? да
root@avsidorova:~# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
root@avsidorova:~# 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@avsidorova:~# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
root@avsidorova:~# touch /.autorelabel
root@avsidorova:~#
```

Рис. 6: Использование `restorecon` для восстановления контекста безопасности

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Установим необходимое программное обеспечение

```
avsidorova@avsidorova:~$ sudo -i
[sudo] пароль для avsidorova:
root@avsidorova:~# dnf -y install httpd
Rocky Linux 10 - BaseOS                    5.3 kB/s | 4.3 kB    00:00
Rocky Linux 10 - BaseOS                    1.6 MB/s | 22 MB     00:14
Rocky Linux 10 - AppStream                 11 kB/s | 4.3 kB     00:00
Rocky Linux 10 - AppStream                 1.7 MB/s | 2.2 MB     00:01
Rocky Linux 10 - Extras                    6.0 kB/s | 3.1 kB     00:00
Rocky Linux 10 - Extras                    6.5 kB/s | 5.5 kB     00:00
Пакет httpd-2.4.63-1.el10_0.2.x86_64 уже установлен.
Зависимости разрешены.
Нет действий для выполнения.
Выполнено!
root@avsidorova:~# dnf -y install lynx
Последняя проверка окончания срока действия метаданных: 0:00:30 назад, Вт 28 окт 2025 16:15:00.
Зависимости разрешены.
=====
Пакет            Архитектура      Версия            Репозиторий      Размер
=====
Установка:
  lynx            x86_64           2.9.0-6.el10     appstream         1.6 M
=====
Результат транзакции
=====
Установка 1 Пакет

Объем загрузки: 1.6 M
Объем изменений: 6.0 M
Загрузка пакетов:
lynx-2.9.0-6.el10.x86_64.rpm                    1.4 MB/s | 1.6 MB    00:01
=====
Общий размер                                1.1 MB/s | 1.6 MB    00:01
Проверка транзакции
Проверка транзакции успешно завершена.
Идет проверка транзакции
Тест транзакции проведен успешно.
Выполнение транзакции
```


Создадим новое хранилище для файлов web-сервера

Создадим файл index.html в каталоге с контентом веб-сервера и поместим в файл следующий текст: Welcome to my web-server

выполнено:

```
root@avsidorova:~# mkdir /web
root@avsidorova:~# cd /web
root@avsidorova:/web# touch index.html
root@avsidorova:/web# nano index.html
root@avsidorova:/web# nano /etc/httpd/conf/httpd.conf
root@avsidorova:/web#
```

Рис. 8: mkdir /web; touch index.html

В файле /etc/httpd/conf/httpd.conf закомментируем строку

Затем в этом же файле ниже закомментируем раздел

```
GNU nano 8.1 /etc/httpd/conf/httpd.conf ИВМЕНЕВ
# below.
#
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# 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>
# Further relax access to the default document root:
<Directory "/var/www/html">
#
# Possible values for the Options directive are "None", "All",
# or any combination of:
#   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
#
# Note that "MultiViews" must be named *explicitly* --- "Options All"
# doesn't give it to you.
#
# The Options directive is both complicated and important. Please see
# http://httpd.apache.org/docs/2.4/mod/core.html#options
# for more information.
#
```

Запустим веб-сервер и службу httpd:

systemctl start httpd systemctl enable httpd

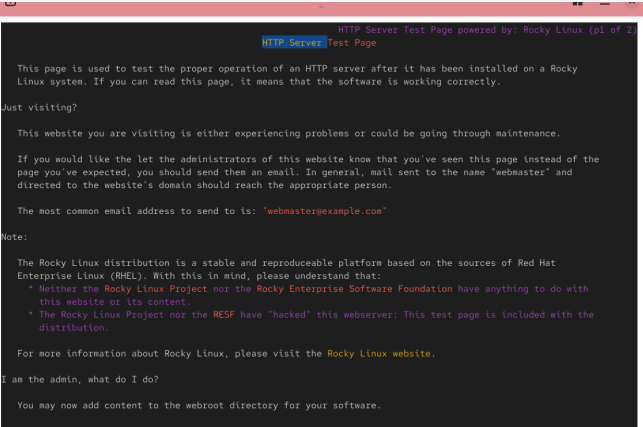
```
root@avsidorova:/web# systemctl start httpd  
root@avsidorova:/web# systemctl enable httpd  
root@avsidorova:/web# lynx http://localhost
```

Рис. 10: start; enable

В терминале под учётной записью своего пользователя при обращении к веб-серверу

в текстовом браузере lynx: `lynx http://localhost`

Мы увидим веб-страницу Red Hat по умолчанию, а не содержимое только что созданного файла `index.html`.



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

This page is used to test the proper operation of an HTTP server after it has been installed on a Rocky
Linux system. If you can read this page, it means that the software is working correctly.

Just visiting?

This website you are visiting is either experiencing problems or could be going through maintenance.

If you would like the let the administrators of this website know that you've seen this page instead of the
page you've expected, you should send them an email. In general, mail sent to the name 'webmaster' and
directed to the website's domain should reach the appropriate person.

The most common email address to send to is: "webmaster@example.com"

Note:

The Rocky Linux distribution is a stable and reproduceable platform based on the sources of Red Hat
Enterprise Linux (RHEL). With this in mind, please understand that:
* Neither the Rocky Linux Project nor the Rocky Enterprise Software Foundation have anything to do with
this website or its content.
* The Rocky Linux Project nor the RESF have "hacked" this webserver: This test page is included with the
distribution.

For more information about Rocky Linux, please visit the Rocky Linux website.

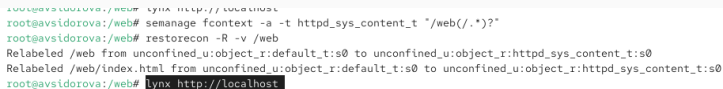
I am the admin, what do I do?

You may now add content to the webroot directory for your software.
```

В терминале с полномочиями администратора применим новую метку контекста

к /web: semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"

Восстановим контекст безопасности: restorecon -R -v /web

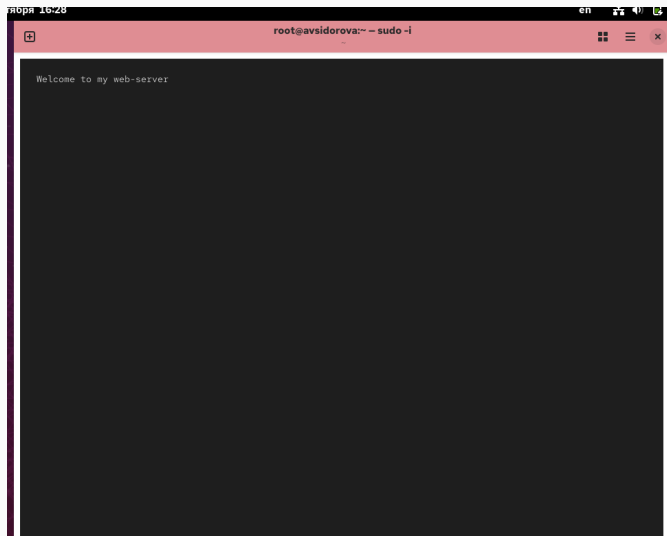


```
root@avsidorova:/web# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
root@avsidorova:/web# restorecon -R -v /web
Relabeled /web from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:httpd_sys_content_t:s0
Relabeled /web/index.html from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:httpd_sys_content_t:s0
root@avsidorova:/web# lynx http://localhost
```

Рис. 12: Применим новую метку и восстановим контекст безопасности

В терминале под учётной записью своего пользователя снова обратимся к веб-серверу:

`lynx http://localhost` На экране отображена запись «Welcome to my web-server».



Посмотрим список переключателей SELinux для службы ftp.

Для службы ftpd_anon посмотрим список переключателей: `semanage boolean -l | grep ftpd_anon`

Изменим текущее значение переключателя для службы ftpd_anon_write с off на on: `setsebool ftpd_anon_write on`

Повторно посмотрим список переключателей SELinux для службы ftpd_anon_write:

```
getsebool ftpd_anon_write
```

Посмотрим список переключателей: `semanage boolean -l | grep ftpd_anon` Обратим внимание, что настройка времени выполнения включена, но постоянная настройка по-прежнему отключена.

Изменим постоянное значение переключателя для службы ftpd_anon_write с off на on:

setsebool -P ftpd_anon_write on

Посмотрим список переключателей: semanage boolean -l | grep ftpd_anon

```
root@avsidorova: ~  
root@avsidorova:~# 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@avsidorova:~# semanage boolean -l | grep ftpd_anon  
bash: semanage: команда не найдена...  
root@avsidorova:~# semanage boolean -l | grep ftpd_anon  
ftpd_anon_write (выкл.,выкл.) Allow ftpd to anon write  
root@avsidorova:~# setsebool ftpd_anon_write on  
root@avsidorova:~# getsebool ftpd_anon_write  
ftpd_anon_write --> on  
root@avsidorova:~# semanage boolean -l | grep ftpd_anon  
ftpd_anon_write (вкл.,выкл.) Allow ftpd to anon write  
root@avsidorova:~# setsebool -P ftpd_anon_write on
```

Результаты

- Освоено переключение между режимами SELinux с помощью `setenforce` и редактирования конфигурационных файлов.
- Применена команда `restorecon` для восстановления корректных контекстов безопасности.
- Настроен контекст `httpd_sys_content_t` для нестандартного каталога веб-сервера `/web`.
- Освоено управление переключателями SELinux через `setsebool` и `semanage boolean`.
- Получены навыки диагностики проблем с помощью утилит `sestatus`, `getenforce`, `ls -Z`.

...