

Лабораторная работа №9

Управление SELinux

Ришард Когенгар

20 января 2026

Российский университет дружбы народов, Москва, Россия

Цель работы

Получить практические навыки администрирования SELinux:

- управление режимами работы; - настройка контекстов безопасности; - использование boolean-переключателей; - диагностика проблем доступа.

Ход выполнения работы

Переключение режимов SELinux

- Проверка режима работы
- Перевод SELinux в разрешающий режим
- Анализ поведения системы
- Возврат в принудительный режим

Режим **permissive** используется для диагностики и отладки.

```
-----  
root@rishardkogengar:~# 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
```

Полное отключение SELinux

- Изменение конфигурационного файла
- Установка режима disabled
- Перезагрузка системы
- Проверка состояния после загрузки

Переключение режимов невозможно при отключённом SELinux.

```
rishard@rishardkogengar:~$ su
Password:
root@rishardkogengar:/home/rishard# getenforce
Disabled
root@rishardkogengar:/home/rishard# setenforce 1
setenforce: SELinux is disabled
root@rishardkogengar:/home/rishard#
```

Возврат SELinux в enforcing

- Изменение параметра SELINUX
- Перезагрузка системы
- Автоматическая перемаркировка файлов
- Проверка статуса после загрузки

Система вернулась в безопасный режим enforcing.

```
[ OK ] Reached target sysinit.target - System Initialization.
[ OK ] Started alsa-state.service - Manage Sound Card State (restore and store).
[ OK ] Reached target sound.target - Sound Card.
Starting dracut-shutdown.service - Restore /run/initramfs on shutdown...
Starting selinux-autorelabel.service - Relabel all filesystems...
[ OK ] Finished dracut-shutdown.service - Restore /run/initramfs on shutdown.
[ 8.151261] selinux-autorelabel[1046]: *** Warning -- SELinux targeted policy relabel is required.
[ 8.152701] selinux-autorelabel[1046]: *** Relabeling could take a very long time, depending on file
[ 8.154300] selinux-autorelabel[1046]: *** system size and speed of hard drives.
[ 8.159105] selinux-autorelabel[1046]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 3: Автоперемаркировка SELinux

Проверка контекста файлов

- Анализ контекста файла `/etc/hosts`
- Копирование файла в домашний каталог
- Изменение контекста при копировании

Контекст изменяется, так как файл считается новым объектом.

```
root@rishardkogengar:/home/rishard#  
root@rishardkogengar:/home/rishard# ls -Z /etc/hosts  
system_u:object_r:net_conf_t:s0 /etc/hosts  
root@rishardkogengar:/home/rishard# cp /etc/hosts ~/  
root@rishardkogengar:/home/rishard# ls -Z ~/hosts  
unconfined_u:object_r:admin_home_t:s0 /root/hosts  
root@rishardkogengar:/home/rishard# mv ~/hosts /etc  
mv: overwrite '/etc/hosts'? y  
root@rishardkogengar:/home/rishard# ls -Z /etc/hosts  
unconfined_u:object_r:admin_home_t:s0 /etc/hosts  
root@rishardkogengar:/home/rishard# 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@rishardkogengar:/home/rishard# ls -Z /etc/hosts  
unconfined_u:object_r:net_conf_t:s0 /etc/hosts  
root@rishardkogengar:/home/rishard# touch /.autorelabel  
root@rishardkogengar:/home/rishard#
```

Рис. 4: Контекст `/etc/hosts`

- Перезапись файла с неверным контекстом
- Восстановление контекста безопасности
- Проверка результата

Контекст успешно возвращён к `net_conf_t`.

```
[ OK ] Started alsa-state.service - Manage Sound Card State (restore and store).
[ OK ] Reached target sound.target - Sound Card.
       Starting dracut-shutdown.service - Restore /run/initramfs on shutdown...
       Starting selinux-autorelabel.service - Relabel all filesystems...
[ OK ] Finished dracut-shutdown.service - Restore /run/initramfs on shutdown.
[ 5.361606] selinux-autorelabel[1030]: *** Warning -- SELinux targeted policy relabel is required.
[ 5.362240] selinux-autorelabel[1030]: *** Relabeling could take a very long time, depending on file
[ 5.362386] selinux-autorelabel[1030]: *** system size and speed of hard drives.
[ 5.364888] selinux-autorelabel[1030]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 5: restorecon

- Установка Apache и lynx
- Создание каталога `/web`
- Создание пользовательской страницы
- Изменение DocumentRoot

Используется нестандартный каталог для контента.

```
GNU nano 8.1 /etc/httpd/conf/httpd.conf
# 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"

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

Проблема доступа SELinux

- Запуск веб-сервера
- Проверка доступа через lynx
- Отображение стандартной страницы Apache

SELinux блокирует доступ к /web.

```
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.
```

Настройка контекста для /web

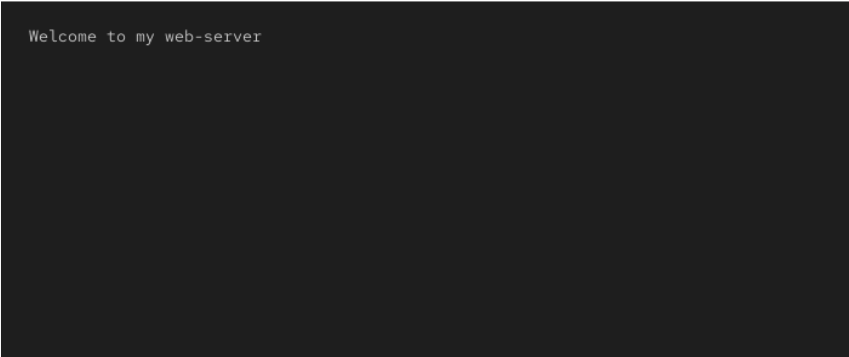
- Назначение контекста `httpd_sys_content_t`
- Восстановление контекстов
- Повторная проверка доступа

Апаче получил доступ к пользовательскому контенту.

```
root@rishardkogengar:/web#  
root@rishardkogengar:/web# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"  
root@rishardkogengar:/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@rishardkogengar:/web# systemctl restart httpd  
root@rishardkogengar:/web# █
```

Рис. 8: Контекст для /web

- Проверка через lynx
- Отображение пользовательской страницы
- Подтверждение корректной работы

A screenshot of a terminal window with a dark background. The text "Welcome to my web-server" is displayed in a light-colored, monospaced font at the top left of the window.

```
Welcome to my web-server
```

Рис. 9: Пользовательская страница

Постоянная настройка переключателя

- Включение boolean-переключателя постоянно
- Проверка временного и постоянного состояния
- Анализ результата

Переключатель включён полностью.

```
root@rishardkogengar:/web#  
root@rishardkogengar:/web# 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@rishardkogengar:/web# semanage boolean -l | grep ftpd_anon  
ftpd_anon_write (off , off) Allow ftpd to anon write  
root@rishardkogengar:/web# setsebool ftpd_anon write on
```

Итоги работы

- Изучены режимы работы SELinux
- Освоена работа с контекстами безопасности
- Настроен доступ Apache к нестандартному каталогу
- Рассмотрены boolean-переключатели SELinux