

# Лабораторная работа №9

Управление SELinux

---

Анастасия Мазуркевич

16 октября 2025

Российский университет дружбы народов, Москва, Россия

## Цель работы

---

Получить практические навыки работы с механизмом безопасности **SELinux**, изучить режимы работы, контексты безопасности и управление политиками доступа.

## Ход выполнения

---

# Управление режимами SELinux

```
root@admazurkevich:/home/admazurkevich#
root@admazurkevich:/home/admazurkevich# 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@admazurkevich:/home/admazurkevich# getenforce
Enforcing
root@admazurkevich:/home/admazurkevich# setenforce 0
root@admazurkevich:/home/admazurkevich# getenforce
Permissive
root@admazurkevich:/home/admazurkevich#
root@admazurkevich:/home/admazurkevich# mcedit /etc/sysconfig/selinux
root@admazurkevich:/home/admazurkevich#
```

```
selinux [-M--] 16 L:[ 1+21 22/ 30] *(927 /1186b) 0010 0x00A [*][X]

# 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-states-and-
#
# 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
```

Рис. 2: Изменение конфигурации SELinux

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

Рис. 3: SELinux отключён

```
selinux      [-M--] 17 L:[ 1+21 22/ 30] *(928 /1187b) 0010 0x00A      [*][X]

# 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-states-and-
#
# 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
```

Рис. 4: Включение enforcing-режима SELinux



```
Booting 'Rocky Linux (6.12.0-55.12.1.el10_0.x86_64) 10.0 (Red Quartz)'  
[ 0.761348] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on  
an unsupported hypervisor.  
[ 0.761350] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b  
roken.  
[ 0.761350] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g  
raphics device to avoid problems.  
[ 4.099756] selinux-autorelabel[826]: *** Warning -- SELinux targeted policy relabel is required.  
[ 4.099858] selinux-autorelabel[826]: *** Relabeling could take a very long time, depending on file  
[ 4.099880] selinux-autorelabel[826]: *** system size and speed of hard drives.  
[ 4.102420] selinux-autorelabel[826]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 5: Процесс восстановления меток при загрузке

```
admazurkevich@admazurkevich:~$ su
Password:
root@admazurkevich:/home/admazurkevich# 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@admazurkevich:/home/admazurkevich#
```

Рис. 6: Повторная проверка статуса SELinux

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

Рис. 7: Контекст безопасности файла hosts

```
[ 1.752379] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 1.752381] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 1.752382] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 5.615786] selinux-autorelabel[826]: *** Warning -- SELinux targeted policy relabel is required.
[ 5.615844] selinux-autorelabel[826]: *** Relabeling could take a very long time, depending on file
[ 5.615865] selinux-autorelabel[826]: *** system size and speed of hard drives.
[ 5.618489] selinux-autorelabel[826]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 8: Автоматическое восстановление контекстов SELinux

Installed:

lynx-2.9.0-6.el10.x86\_64

Complete!

```
root@admazurkevich:/home/admazurkevich#
```

```
root@admazurkevich:/home/admazurkevich# mkdir /web
```

```
root@admazurkevich:/home/admazurkevich# cd /web
```

```
root@admazurkevich:/web# touch index.html
```

```
root@admazurkevich:/web# echo "Welcome to my web-server" > index.html
```

```
root@admazurkevich:/web# █
```

Рис. 9: Создание каталога и файла index.html

## Изменение конфигурации Apache

```
httpd.conf      [-M--]  0 L:[113+19 132/367] *(4629/12135b) 0010 0x00A
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# 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"

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

Рис. 10: Изменение настроек httpd.conf

```
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 to 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 reproducible 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.

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:
-- press space for next page --
Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
H)elp O)ptions P)rint G)o M)ain screen Q)uit /s=search [delete]=history list
```

Рис. 11: Страница Apache по умолчанию

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

Рис. 12: Назначение и восстановление контекста безопасности для /web



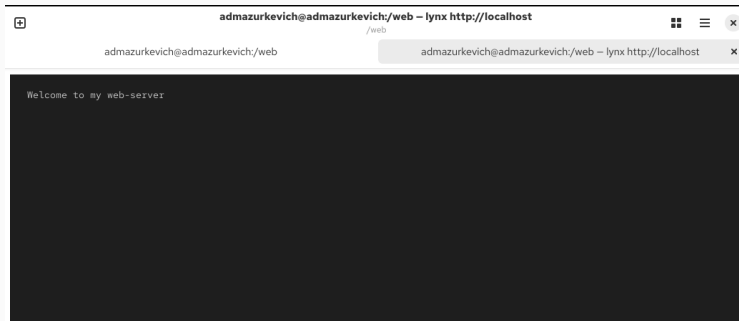


Рис. 13: Отображение пользовательской страницы

## Настройка переключателя ftpd\_anon\_write

```
admazurkevich@admazurkevich:/web$ su
Password:
root@admazurkevich:/web#
root@admazurkevich:/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@admazurkevich:/web#
root@admazurkevich:/web# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (off , off) Allow ftpd to anon write
root@admazurkevich:/web# setsebool ftpd_anon_write on
root@admazurkevich:/web# getsebool ftpd_anon_write
ftpd_anon_write --> on
root@admazurkevich:/web# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (on , off) Allow ftpd to anon write
root@admazurkevich:/web# setsebool -P ftpd_anon_write on
root@admazurkevich:/web# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (on , on) Allow ftpd to anon write
root@admazurkevich:/web#
```

## Заключение

---

В ходе работы были изучены:

- режимы SELinux и их назначение;
- методы изменения и проверки состояния системы;
- восстановление контекстов безопасности с помощью **restorecon**;
- применение политик для нестандартных каталогов веб-сервера;
- управление переключателями SELinux.

Освоены практические приёмы настройки и диагностики SELinux, что повышает уровень защиты и управляемости Linux-систем.