

# Лабораторная работа №9

## Управление SELinux

---

Тукаев Тимур

16 октября 2025

Российский университет дружбы народов, Москва, Россия

## Цель работы

---

## Основная цель

---

Получить навыки работы с контекстом безопасности и политиками SELinux.

Освоить принципы конфигурирования, изменения режима работы и восстановления контекстов безопасности.

## Ход выполнения работы

---

# Проверка состояния SELinux

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

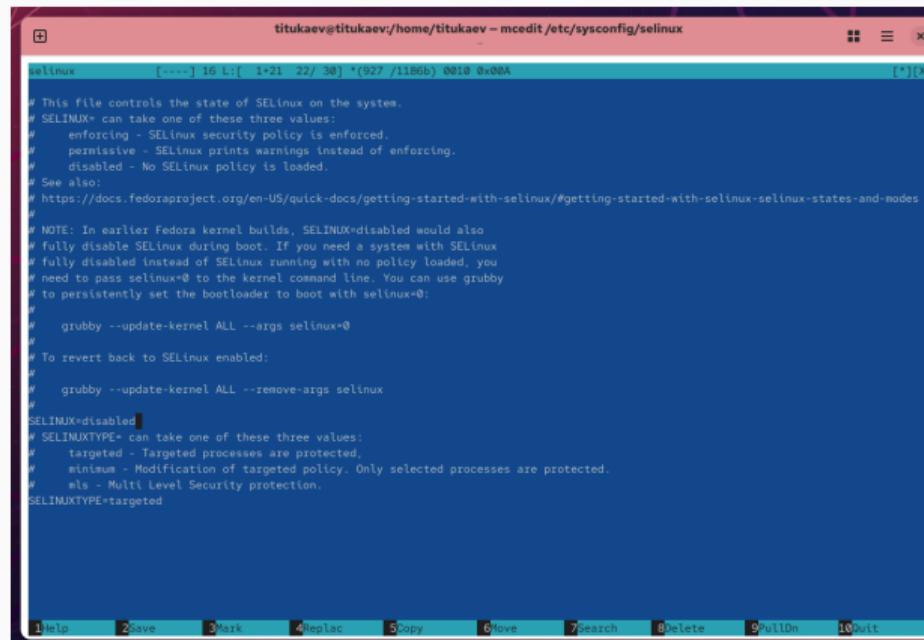
Process contexts:
Current context:                 unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
Init context:                     system_u:system_r:init_t:s0
/usr/sbin/sshd                      system_u:system_r:sshd_t:s0-s0:c0.c1023

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@titukaev:/home/titukaev# getenforce
Enforcing
root@titukaev:/home/titukaev# setenforce 0
root@titukaev:/home/titukaev# getenforce
Permissive
root@titukaev:/home/titukaev#
```

Рис. 1: Проверка состояния SELinux

Команда `sestatus -v` показала, что система работает в режиме Enforcing.

# Изменение режима работы SELinux



```
titukaev@titukaev:~$ mcedit /etc/sysconfig/selinux

selinux
# 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-modes
#
# 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 grubpy
# to persistently set the bootloader to boot with selinux=0:
#
#     grubpy --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#     grubpy --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

titukaev@titukaev:~$
```

Рис. 2: Изменение режима работы SELinux

Режим переведён в Permissive с помощью `setenforce 0`, затем в Disabled через изменение 4/13

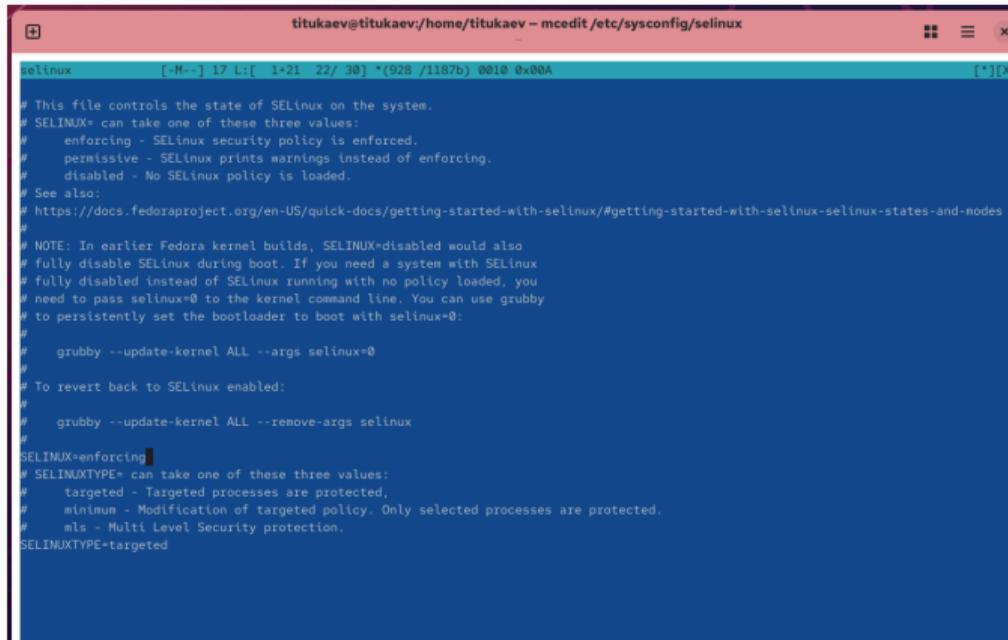
## Проверка после перезагрузки

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

Рис. 3: Проверка отключённого состояния SELinux

SELinux отключён. Попытка включить без перезагрузки невозможна.

## Повторное включение SELinux



```
titukaev@titukaev:~/home/titukaev - mcedit /etc/sysconfig/selinux

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-selinux-states-and-modes
#
# 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 grubpy
# to persistently set the bootloader to boot with selinux=0:
#
#   grubpy --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubpy --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: Повторное включение SELinux

Файл `/etc/sysconfig/selinux` изменён на `SELINUX=enforcing`.

## Завершение relabeling

```
Booting `Rocky Linux (6.12.0-55.12.1.el10_0.x86_64) 10.0 (Red Quartz)'

[    1.785036] vmmqfx 0000:00:02.0: [drm] *ERROR* vmmqfx seems to be running on
an unsupported hypervisor.
[    1.785038] vmmqfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[    1.785039] vmmqfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[   10.881428] selinux-autorelabel[858]: *** Warning -- SELinux targeted policy relabel is required.
[   10.881513] selinux-autorelabel[858]: *** Relabeling could take a very long time, depending on file
[   10.881664] selinux-autorelabel[858]: *** system size and speed of hard drives.
[   10.892671] selinux-autorelabel[858]: Running: /sbin/fixfiles -T 0  restore
```

Рис. 5: Сообщение о восстановлении меток безопасности

Система автоматически пересоздала метки контекста безопасности.

SELinux работает в режиме Enforcing.

# Восстановление контекста безопасности

```
root@titukaev:/home/titukaev#  
root@titukaev:/home/titukaev# 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_t: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@titukaev:/home/titukaev#
```

Рис. 6: Использование restorecon для восстановления контекста

Использованы команды `restorecon` и `./autorelabel` для восстановления контекстов

## Настройка контекста для веб-сервера

```
#  
# 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. 7: Редактирование httpd.conf и настройка каталога /web

Создан каталог **/web**, добавлен файл **index.html**.

В конфигурации Apache изменён путь **DocumentRoot**.

# Применение нового контекста SELinux

```
Installed:  
lynx-2.9.0-6.el10.x86_64  
  
Complete!  
root@titukaev:/home/titukaev# mkdir /web  
root@titukaev:/home/titukaev# cd /web  
root@titukaev:/web# touch index.html  
root@titukaev:/web# echo "Welcome yo my web-server" > index.html  
root@titukaev:/web# mcedit /etc/httpd/conf/httpd.conf  
  
root@titukaev:/web# systemctl start httpd  
root@titukaev:/web# systemctl enable httpd  
root@titukaev:/web# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"  
root@titukaev:/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@titukaev:/web#
```

Рис. 8: Применение контекста безопасности к /web

К каталогу `/web` применён контекст `httpd_sys_content_t` и выполнено `restorecon -R -v /web`.

## Проверка доступа к веб-странице



Рис. 9: Проверка работы веб-сервера

После применения контекста страница доступна по адресу <http://localhost>.

# Работа с переключателями SELinux

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

Рис. 10: Настройка переключателя `ftpd_anon_write`

Просмотр, временное и постоянное включение переключателя `ftpd_anon_write` для

## Итоги работы

---

## Вывод

---

Изучены режимы работы SELinux и практические методы их изменения.

Освоены приёмы назначения и восстановления контекстов безопасности, настройки веб-сервера и управления переключателями SELinux.

Полученные навыки обеспечивают эффективную настройку и защиту системы Linux.