

# Лабораторная работа №9

Управление SELinux

---

Турсунов Мухамметназар

17 октября 2025

Российский университет дружбы народов, Москва, Россия

## Цель работы

---

Изучение принципов работы системы безопасности **SELinux**, освоение режимов работы, восстановления контекстов и настройки политик безопасности для служб Linux.

## Управление режимами SELinux

---

# Проверка состояния SELinux

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

Рис. 1: Вывод команды sestatus -v

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

Рис. 2: Изменение режима на Permissive

# Отключение SELinux

```
mtursunov@mtursunov:/home/mtursunov - nano /etc/sysconfig/selinux
GNU nano 8.1 /etc/sysconfig/selinux Modified
# 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-se
#
# 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

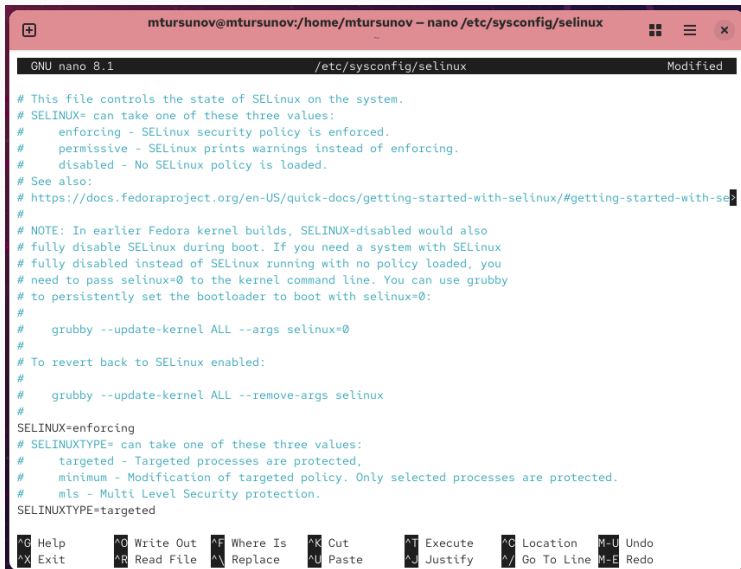
^G Help      ^O Write Out ^F Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line M-E Redo
```

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

Рис. 4: Попытка включения SELinux при disabled



# Повторное включение enforcing



The screenshot shows a terminal window with the title bar "mtursunov@mtursunov:/home/mtursunov - nano /etc/sysconfig/selinux". The window contains the contents of the `/etc/sysconfig/selinux` file, which is being edited with the nano text editor. The file's status bar at the top indicates "GNU nano 8.1" and "Modified". The file content includes comments about SELinux states (enforcing, permissive, disabled) and a section for SELinux types (targeted, minimum, mls). The current configuration is `SELINUX=enforcing` and `SELINUXTYPE=targeted`. The bottom of the window shows the nano editor's command palette with various shortcuts like `^G Help`, `^O Write Out`, `^F Where Is`, `^K Cut`, `^T Execute`, `^C Location`, `M-U Undo`, `^X Exit`, `^R Read File`, `^N Replace`, `^U Paste`, `^J Justify`, `^_ Go To Line`, and `M-E Redo`.

```
mtursunov@mtursunov:/home/mtursunov - nano /etc/sysconfig/selinux
GNU nano 8.1 /etc/sysconfig/selinux Modified

# 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-se
#
# 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

^G Help      ^O Write Out ^F Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File ^N Replace   ^U Paste     ^J Justify   ^_ Go To Line M-E Redo
```

## Восстановление меток при загрузке

```
Booting `Rocky Linux (6.12.0-55.37.1.el10_0.x86_64) 10.0 (Red Quartz)`  
[ 0.784793] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on  
an unsupported hypervisor.  
[ 0.784795] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b  
roken.  
[ 0.784796] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g  
raphics device to avoid problems.  
[ 0.279888] selinux-autorelabel[823]: *** Warning -- SELinux targeted policy relabel is required.  
[ 0.279960] selinux-autorelabel[823]: *** Relabeling could take a very long time, depending on file  
[ 0.279985] selinux-autorelabel[823]: *** system size and speed of hard drives.  
[ 0.300069] selinux-autorelabel[823]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 6: Автоматическое восстановление меток SELinux

## Проверка статуса после восстановления

```
password:
root@mtursunov:/home/mtursunov# 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@mtursunov:/home/mtursunov#
```

Рис. 7: SELinux снова включён, режим enforcing

## Восстановление контекста безопасности

---

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

Рис. 8: Восстановление контекста файла hosts

```
[ 1.394272] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 1.394274] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 1.394275] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 7.704382] selinux-autorelabel[821]: *** Warning -- SELinux targeted policy relabel is required.
[ 7.705344] selinux-autorelabel[821]: *** Relabeling could take a very long time, depending on file
[ 7.705410] selinux-autorelabel[821]: *** system size and speed of hard drives.
[ 7.714706] selinux-autorelabel[821]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 9: Автоматическое перемаркирование файловой системы

## Настройка контекста для веб-сервера

---

```
Installed:
  lynx-2.9.0-6.el10.x86_64

Complete!
root@mtursunov:/home/mtursunov# mkdir /web
root@mtursunov:/home/mtursunov# cd /web
root@mtursunov:/web# touch index.html
root@mtursunov:/web# echo "Welcome to my web server" > index.html
root@mtursunov:/web# nano /etc/httpd/conf/httpd.conf
root@mtursunov:/web# systemctl start httpd
root@mtursunov:/web# systemctl enable httpd
root@mtursunov:/web# █
```

Рис. 10: Создание каталога /web и файла index.html



## Изменение DocumentRoot в 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>
```

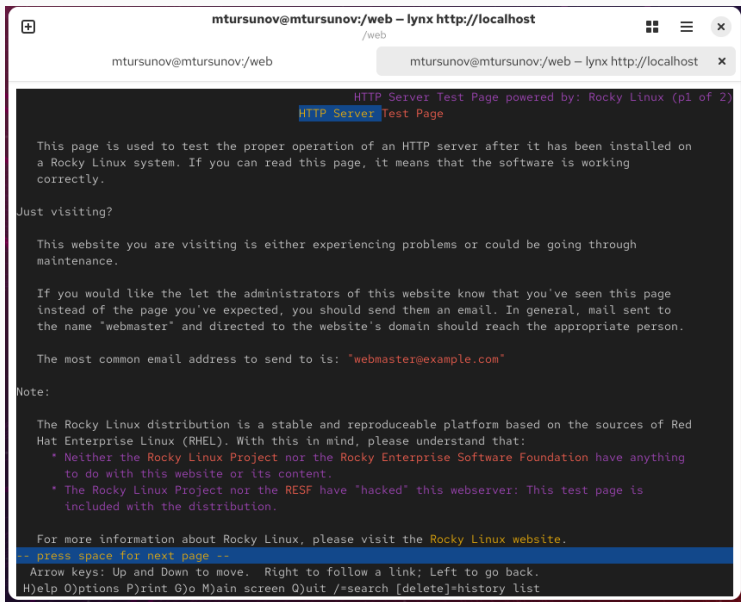
Рис. 11: Редактирование конфигурации Apache

```
Installed:
  lynx-2.9.0-6.el10.x86_64

Complete!
root@mtursunov:/home/mtursunov# mkdir /web
root@mtursunov:/home/mtursunov# cd /web
root@mtursunov:/web# touch index.html
root@mtursunov:/web# echo "Welcome to my web server" > index.html
root@mtursunov:/web# nano /etc/httpd/conf/httpd.conf
root@mtursunov:/web# systemctl start httpd
root@mtursunov:/web# systemctl enable httpd
root@mtursunov:/web# █
```

Рис. 12: Запуск службы httpd

# Проверка результата в браузере lynx



The screenshot shows the Lynx web browser interface. The title bar at the top reads "mtursunov@mtursunov:/web - lynx http://localhost". Below the title bar, there are two tabs: "mtursunov@mtursunov:/web" and "mtursunov@mtursunov:/web - lynx http://localhost". The main content area displays the "HTTP Server Test Page" powered by Rocky Linux (p1 of 2). The page text includes a welcome message, instructions on how to report issues, and information about the Rocky Linux distribution. At the bottom, there are navigation instructions for the Lynx browser.

```
mtursunov@mtursunov:/web - lynx http://localhost
/web
mtursunov@mtursunov:/web      mtursunov@mtursunov:/web - lynx http://localhost x

HTTP Server Test Page powered by: Rocky Linux (p1 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.
-- 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
```

## Присвоение контекста httpd\_sys\_content\_t

```
root@mtursunov:/web#  
root@mtursunov:/web# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"  
root@mtursunov:/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@mtursunov:/web#
```

Рис. 14: Настройка контекста каталога /web

## Корректное отображение веб-страницы

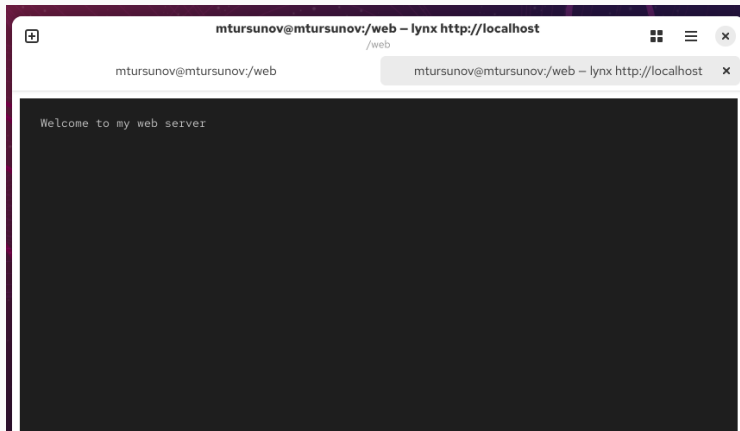


Рис. 15: Отображение пользовательской страницы веб-сервера

## Работа с переключателями SELinux

---

## Проверка состояния переключателей

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

Рис. 16: Просмотр и изменение переключателя ftpd\_anon\_write

## Итоги работы

---



В ходе работы были изучены режимы функционирования SELinux: **Enforcing**, **Permissive** и **Disabled**.

Отработаны навыки восстановления контекстов безопасности, применения политик доступа и настройки правил для служб Linux.

Освоено использование инструментов **semanage**, **restorecon** и **setsebool**.

SELinux был успешно возвращён в активный режим **enforcing** с корректной политикой безопасности.