

# Лабораторная работа №9

## Управление SELinux

---

Шаханеоядж Хаоладар

16 октября 2025

Российский университет дружбы народов, Москва, Россия

## Цель работы

---

## Основная цель

---

Получить навыки работы с контекстом безопасности и политиками SELinux.

## Ход выполнения работы

---

# Управление режимами SELinux

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

# Управление режимами SELinux

```
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
#
# 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: Переключение режима SELinux в Permissive

## Управление режимами SELinux

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

Рис. 3: Редактирование конфигурационного файла SELinux

# Управление режимами SELinux

```
selinux      [-M--] 17 L:[ 4+18 22/ 30 ] *(928 /1187b) 0010 0x00A      [*][X]
#      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
#
# 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: Проверка отключения SELinux

# Управление режимами SELinux

```
[ 1.996862] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on  
an unsupported hypervisor.  
[ 1.996863] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b  
roken.  
[ 1.996864] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g  
raphics device to avoid problems.  
[ 6.479801] selinux-autorelabel[831]: *** Warning -- SELinux targeted policy relabel is required.  
[ 6.479857] selinux-autorelabel[831]: *** Relabeling could take a very long time, depending on file  
[ 6.479890] selinux-autorelabel[831]: *** system size and speed of hard drives.  
[ 6.482279] selinux-autorelabel[831]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 5: Сообщение о необходимости relabeling

# Управление режимами SELinux

```
root@haoladar:/home/haoladar# 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@haoladar:/home/haoladar#
```

Рис. 6: Повторная проверка SELinux после relabeling

## Восстановление контекста безопасности

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

Рис. 7: Проверка и исправление контекста файла hosts

## Восстановление контекста безопасности

```
[ 0.730400] vmmqfx 0000:00:02.0: [drm] *ERROR* vmmqfx seems to be running on  
an unsupported hypervisor.  
[ 0.730410] vmmqfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b  
roken.  
[ 0.730411] vmmqfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g  
raphics device to avoid problems.  
[ 3.056812] selinux-autorelabel[827]: *** Warning -- SELinux targeted policy relabel is required.  
[ 3.856884] selinux-autorelabel[827]: *** Relabeling could take a very long time, depending on file  
[ 3.856985] selinux-autorelabel[827]: *** system size and speed of hard drives.  
[ 3.859186] selinux-autorelabel[827]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 8: Процесс relabeling SELinux при загрузке

## Изменение DocumentRoot и прав доступа

```
#  
# 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. 9: Настройка Apache: изменение каталога веб-сервера

# Настройка контекста безопасности веб-сервера

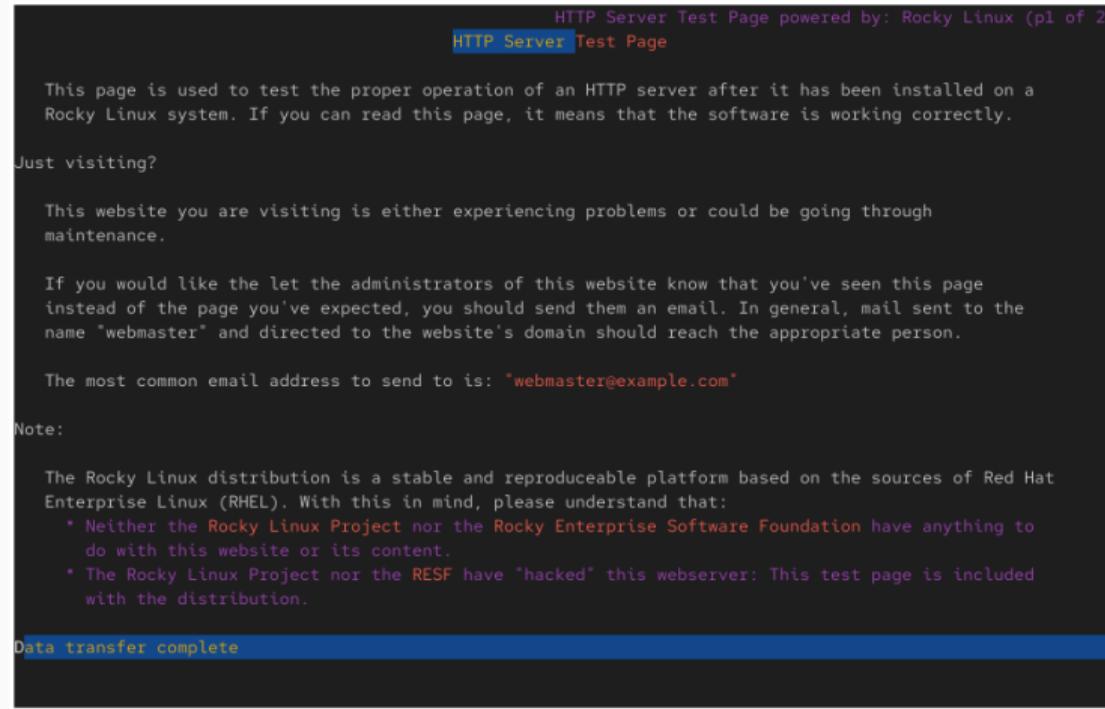


Рис. 10: Стандартная страница Apache при первом запуске

# Настройка контекста безопасности веб-сервера

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

Рис. 11: Применение контекста httpd\_sys\_content\_t

## Настройка контекста безопасности веб-сервера

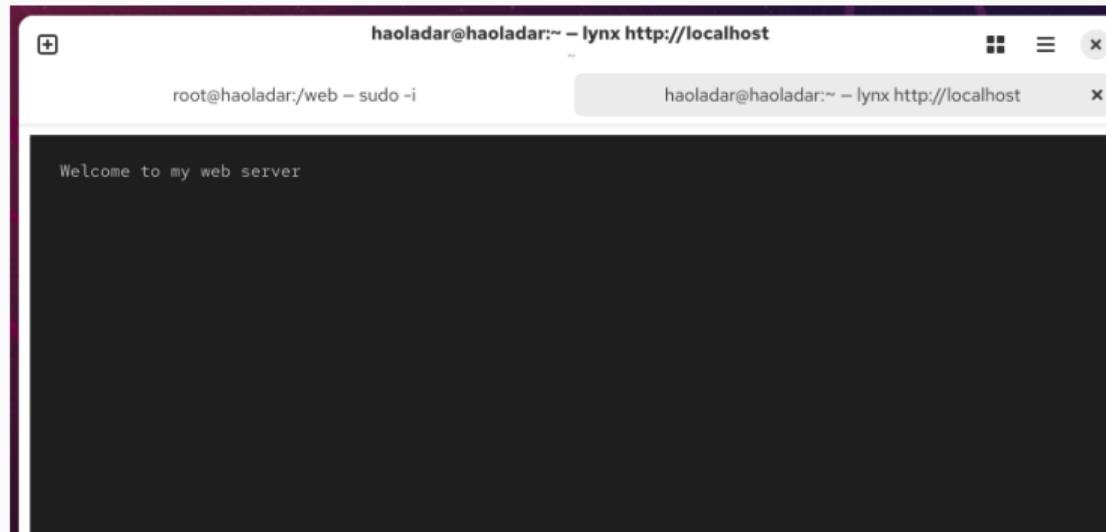


Рис. 12: Отображение пользовательской страницы веб-сервера

## Переключатели службы FTP

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

Рис. 13: Просмотр и изменение переключателей SELinux

## Итоги работы

---

Изучены режимы работы SELinux, способы их переключения и восстановление контекстов безопасности.

Освоены приёмы настройки политик, работы с веб-каталогами и управления переключателями SELinux.