

Презентация по лабораторной работе №9

Управление SELinux

Анна Саенко

15 октября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

1. Ознакомиться с режимами работы SELinux
2. Научиться изменять и отключать SELinux
3. Освоить восстановление контекстов безопасности
4. Настроить контексты безопасности для веб-сервера
5. Изучить работу переключателей SELinux

Ход выполнения работы

Проверка состояния SELinux

```
aasaenko@aasaenko:~$ su
Password:
root@aasaenko:/home/aasaenko#
root@aasaenko:/home/aasaenko# 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@aasaenko:/home/aasaenko# getenforce
Enforcing
root@aasaenko:/home/aasaenko# setenforce 0
root@aasaenko:/home/aasaenko#
```

Переключение режимов 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-sta
#
# 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: Отключение SELinux и переход в Permissive режим

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

Рис. 3: Редактирование файла `/etc/sysconfig/selinux`


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

Рис. 4: Использование restorecon для восстановления контекста /etc/hosts

```
[ 1.524052] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 1.524054] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 1.524055] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 4.326063] selinux-autorelabel[825]: *** Warning -- SELinux targeted policy relabel is required.
[ 4.327192] selinux-autorelabel[825]: *** Relabeling could take a very long time, depending on file
[ 4.328224] selinux-autorelabel[825]: *** system size and speed of hard drives.
[ 4.329238] selinux-autorelabel[825]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 5: Автоматическое восстановление контекстов при загрузке

Изменение каталога DocumentRoot

```
#  
# 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. 6: Настройка нового каталога /web в конфигурации Apache

```
root@aasaenko:/web#
root@aasaenko:/web# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
root@aasaenko:/web# restorecon -v -R /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@aasaenko:/web#
```

Рис. 7: Присвоение типа httpd_sys_content_t каталогу /web

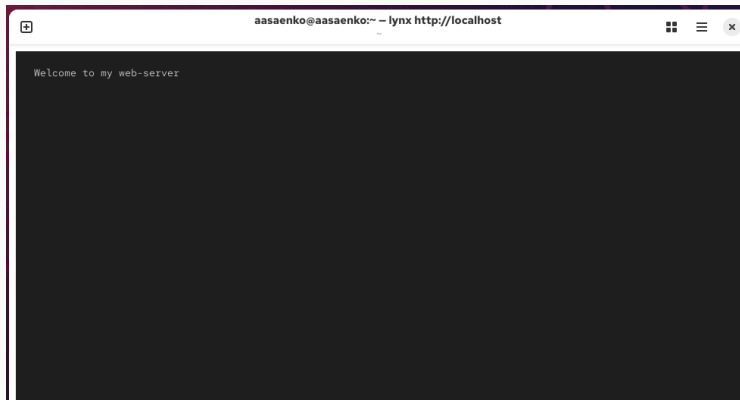


Рис. 8: Отображение пользовательской страницы “Welcome to my web-server”

Проверка состояния переключателя FTP

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

Рис. 9: Просмотр и изменение переключателей ftpd anon write

Выводы по проделанной работе

В ходе лабораторной работы были освоены:

- управление режимами SELinux (Enforcing, Permissive, Disabled);
- восстановление и настройка контекстов безопасности;
- применение SELinux для защиты веб-сервера;
- использование переключателей безопасности и их постоянная активация.

Полученные знания позволили понять, как SELinux контролирует доступ и повышает безопасность системы.