

Лабораторная работа №9

Управление SELinux

Наурузова Айшат Магомедовна

13 октября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux, научиться управлять режимами работы, контекстами безопасности и переключателями SELinux.

Ход выполнения работы

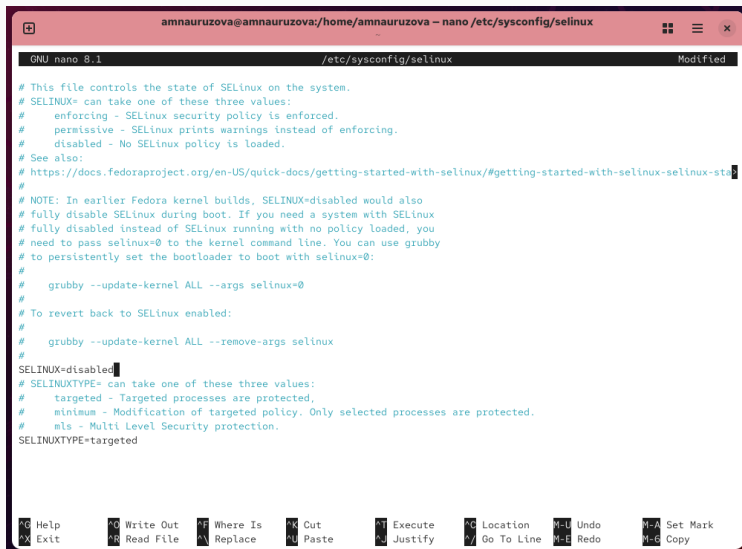
Проверка состояния SELinux

```
amnauruzova@amnauruzova:~$ su
Password:
root@amnauruzova:/home/amnauruzova# 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@amnauruzova:/home/amnauruzova# getenforce
Enforcing
root@amnauruzova:/home/amnauruzova# setenforce 0
root@amnauruzova:/home/amnauruzova# getenforce
Permissive
root@amnauruzova:/home/amnauruzova# █
```

Переключение режима работы



```
amnauruzova@amnauruzova:/home/amnauruzova - 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-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

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

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

Рис. 3: SELinux отключён, попытка включения невозможна

Включение SELinux и relabeling

```
[ OK ] Reached target sysinit.target - System Initialization.
[ OK ] Started alsa-state.service - Manage Sound Card State (restore and store).
[ OK ] Reached target sound.target - Sound Card.
       Starting dracut-shutdown.service - Restore /run/initramfs on shutdown...
       Starting selinux-autorelabel.service - Relabel all filesystems...
[ OK ] Finished dracut-shutdown.service - Restore /run/initramfs on shutdown.
[ 6.118278] selinux-autorelabel[827]: *** Warning -- SELinux targeted policy relabel is required.
[ 6.119051] selinux-autorelabel[827]: *** Relabeling could take a very long time, depending on file
[ 6.119248] selinux-autorelabel[827]: *** system size and speed of hard drives.
[ 6.121146] selinux-autorelabel[827]: Running: /sbin/fixfiles -T 0 restore
[ 9.273428] selinux-autorelabel[834]: Warning: Skipping the following R/O filesystems:
[ 9.274136] selinux-autorelabel[834]: /run/credentials/systemd-journald.service
[ 9.274928] selinux-autorelabel[834]: Relabeling / /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /run /sys /sys/fs/cgroup /s
l/debug /sys/kernel/tracing
```

Рис. 4: Автоматическое восстановление контекста SELinux при перезагрузке


```
[ OK ] Reached target sysinit.target - System Initialization.
[ OK ] Started alsa-state.service - Manage Sound Card State (restore and store).
[ OK ] Reached target sound.target - Sound Card.
       Starting dracut-shutdown.service - Restore /run/initramfs on shutdown...
       Starting selinux-autorelabel.service - Relabel all filesystems...
[ OK ] Finished dracut-shutdown.service - Restore /run/initramfs on shutdown.
[ 6.118278] selinux-autorelabel[827]: *** Warning -- SELinux targeted policy relabel is required.
[ 6.119851] selinux-autorelabel[827]: *** Relabeling could take a very long time, depending on file
[ 6.119248] selinux-autorelabel[827]: *** system size and speed of hard drives.
[ 6.121146] selinux-autorelabel[827]: Running: /sbin/fixfiles -T 0 restore
[ 9.273428] selinux-autorelabel[834]: Warning: Skipping the following R/O filesystems:
[ 9.274136] selinux-autorelabel[834]: /run/credentials/systemd-journald.service
[ 9.274928] selinux-autorelabel[834]: Relabeling / /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /run /sys /sys/fs/cgroup /s
l/debug /sys/kernel/tracing
```

Рис. 5: Проверка состояния SELinux после восстановления

Работа с контекстами безопасности

Восстановление контекста файла /etc/hosts

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

Рис. 6: Восстановление контекста файла /etc/hosts

```
Starting systemd-tmpfiles-setup.service - Create System Files and Directories...
[ OK ] Finished plymouth-read-write.service - Tell Plymouth To Write Out Runtime Data.
[ OK ] Finished systemd-tmpfiles-setup.service - Create System Files and Directories.
Starting systemd-update-utmp.service - Record System Boot/Shutdown in UTMP...
[ OK ] Finished systemd-update-utmp.service - Record System Boot/Shutdown in UTMP.
[ OK ] Reached target sysinit.target - System Initialization.
[ OK ] Started alsa-state.service - Manage Sound Card State (restore and store).
[ OK ] Reached target sound.target - Sound Card.
Starting dracut-shutdown.service - Restore /run/initramfs on shutdown...
Starting selinux-autorelabel.service - Relabel all filesystems...
[ OK ] Finished dracut-shutdown.service - Restore /run/initramfs on shutdown.
[ 5.569544] selinux-autorelabel[831]: *** Warning -- SELinux targeted policy relabel is required.
[ 5.571871] selinux-autorelabel[831]: *** Relabeling could take a very long time, depending on file
[ 5.571241] selinux-autorelabel[831]: *** system size and speed of hard drives.
[ 5.571858] selinux-autorelabel[831]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 7: Автоматическое перемаркирование файловой системы

Настройка SELinux для веб-сервера

Создание каталога и файла index.html

```
root@amnauruzova:~#  
root@amnauruzova:~# mkdir /web  
root@amnauruzova:~# cd /web  
root@amnauruzova:/web# touch index.html  
root@amnauruzova:/web# echo "Welcome to my web server" > index.html  
root@amnauruzova:/web# nano /etc/httpd/conf/httpd.conf  
root@amnauruzova:/web# systemctl start httpd  
root@amnauruzova:/web# systemctl enable httpd  
root@amnauruzova:/web#
```

Рис. 8: Создание каталога и файла index.html

Изменение конфигурации Apache

```
#  
# 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: Изменение конфигурации Apache

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

Рис. 10: Применение контекста безопасности SELinux

Проверка корректной работы веб-сервера

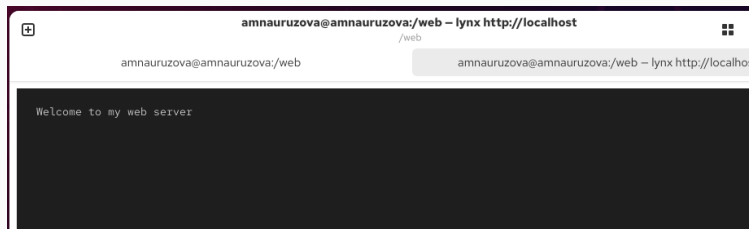


Рис. 11: Корректное отображение пользовательской страницы

Работа с переключателями SELinux

Настройка ftpd_anon_write

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

Рис. 12: Работа с переключателями SELinux для службы FTP

Итоги работы

В ходе лабораторной работы были изучены режимы работы SELinux, принципы восстановления и изменения контекстов безопасности, настройка SELinux для веб-сервера и FTP-службы.

Получены практические навыки администрирования и обеспечения безопасности системы Linux.