

Презентация по лабораторной работе №9

Управление SELinux

Амина Аджигалиева

15 октября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Получить навыки работы с контекстом безопасности и политиками SELinux, освоить настройку разрешений и контекстов безопасности для системных и пользовательских служб Linux.

Ход выполнения работы

Управление режимами SELinux

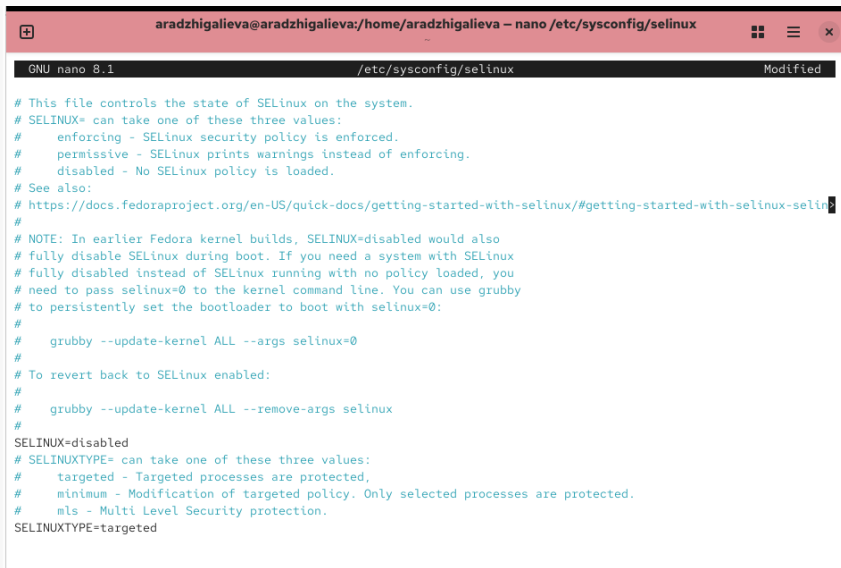
```
aradzhigalieva@aradzhigalieva:/home/aradzhigalieva

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

Управление режимами SELinux



```
aradzhigalieva@aradzhigalieva:/home/aradzhigalieva - 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-selin
#
# 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
```

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

Рис. 3: Проверка статуса SELinux после перезагрузки

Управление режимами SELinux

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


Использование restorecon

Восстановление контекста безопасности

```
root@aradzhigalieva:/home/aradzhigalieva#  
root@aradzhigalieva:/home/aradzhigalieva# ls -Z /etc/hosts  
system_u:object_r:net_conf_t:s0 /etc/hosts  
root@aradzhigalieva:/home/aradzhigalieva# cp /etc/hosts ~/  
root@aradzhigalieva:/home/aradzhigalieva# ls -Z ~/hosts  
unconfined_u:object_r:admin_home_t:s0 /root/hosts  
root@aradzhigalieva:/home/aradzhigalieva# mv ~/hosts /etc  
mv: overwrite '/etc/hosts'? y  
root@aradzhigalieva:/home/aradzhigalieva# ls -Z ~/hosts  
ls: cannot access '/root/hosts': No such file or directory  
root@aradzhigalieva:/home/aradzhigalieva# ls -Z /etc/hosts  
unconfined_u:object_r:admin_home_t:s0 /etc/hosts  
root@aradzhigalieva:/home/aradzhigalieva# 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@aradzhigalieva:/home/aradzhigalieva# ls -Z /etc/hosts  
unconfined_u:object_r:net_conf_t:s0 /etc/hosts  
root@aradzhigalieva:/home/aradzhigalieva# touch /.autorelabel  
root@aradzhigalieva:/home/aradzhigalieva# █
```

Рис. 5: Восстановление контекста безопасности файла /etc/hosts

```
Файл  машина  вид  ввод  устройство  справка
[ 0.895157] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 0.895159] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 0.895160] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 5.266109] selinux-autorelabel[820]: *** Warning -- SELinux targeted policy relabel is required.
[ 5.267133] selinux-autorelabel[820]: *** Relabeling could take a very long time, depending on file
[ 5.268064] selinux-autorelabel[820]: *** system size and speed of hard drives.
[ 5.269694] selinux-autorelabel[820]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 6: Автоматическая перемаркировка при перезагрузке системы

Настройка контекста безопасности веб-сервера

Изменение параметров Apache

```
GNU nano 8.1 /etc/httpd/conf/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. 7: Изменение параметров конфигурации Apache

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

Рис. 8: Применение контекста безопасности к каталогу /web

Проверка работы веб-сервера



Рис. 9: Отображение пользовательской страницы веб-сервера

Работа с переключателями SELinux

Просмотр и изменение параметров FTP

```
root@aradzhigalieva:/web#  
root@aradzhigalieva:/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
```

Рис. 10: Просмотр текущих значений переключателей FTP

Проверка состояния ftpd_anon_write

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

Рис. 11: Включение и проверка состояния переключателя ftpd_anon_write

Заключение

В ходе лабораторной работы я изучила систему безопасности SELinux, научилась изменять её режимы работы, восстанавливать контексты безопасности и настраивать взаимодействие с веб-сервером Apache.

Также были освоены методы управления переключателями SELinux, что позволяет эффективно администрировать безопасность в среде Linux.