Презентация по лабораторной работе №9

Управление SELinux

Агджабекова Эся Рустамовна

13 октября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Цель

Получить навыки работы с контекстом безопасности и политиками SELinux, освоить управление режимами работы, восстановление контекстов безопасности и настройку SELinux для различных служб.

Ход выполнения работы

Проверка состояния SELinux

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

Переключение режима SELinux

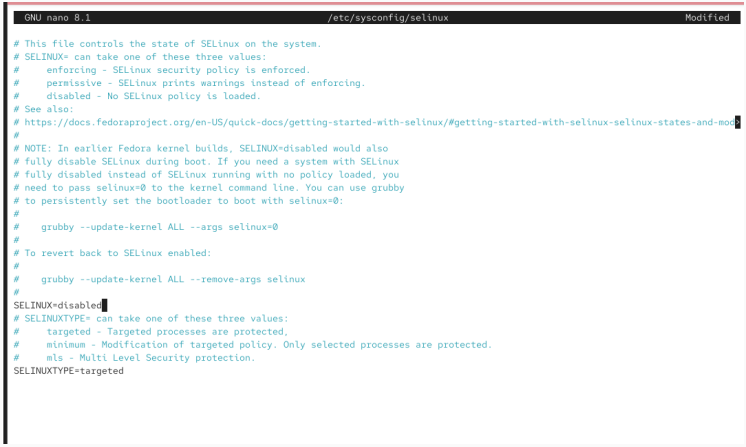

Рис. 2: Переключение режима SELinux в Permissive

Отключение SELinux

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

Рис. 3: Отключение SELinux в конфигурационном файле

Проверка отключённого режима

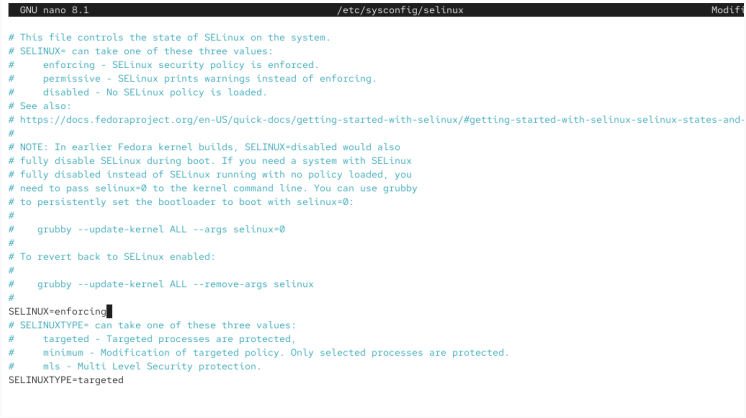

Рис. 4: Попытка включить SELinux после отключения

Восстановление enforcing-режима

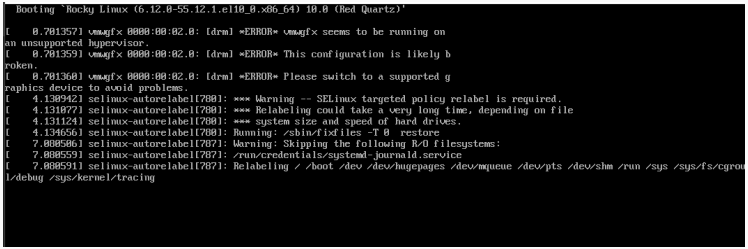

Рис. 5: Процесс relabeling при включении SELinux

Проверка состояния после relabeling

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

Рис. 6: Проверка состояния SELinux после восстановления

Использование restorecon

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

Рис. 7: Восстановление контекста безопасности с помощью restorecon

Настройка контекста для веб-сервера

```
  GNU nano 8.1                                    /etc/httpd/conf/httpd.conf
</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#

#
# 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. 8: Изменение конфигурационного файла httpd.conf для новой директории

Проверка работы веб-сервера

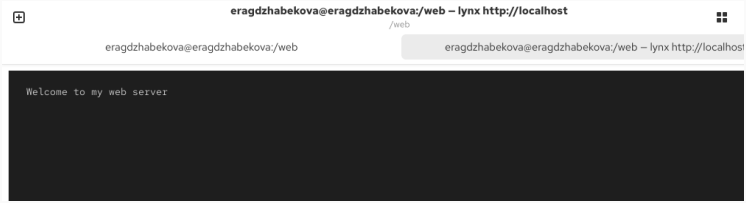

Рис. 9: Отображение пользовательской страницы веб-сервера

Настройка boolean-переменных

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

Рис. 10: Настройка переключателя SELinux для службы FTP

Итоги работы

Вывод

В ходе лабораторной работы были изучены режимы работы SELinux, механизмы управления контекстами безопасности и настройка политик для различных служб.

Получены практические навыки администрирования, необходимые для обеспечения безопасности и стабильности системы Linux.