# Лабораторная работа №9

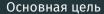
Управление SELinux

Лабси Мохаммед

17 октября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы



Получить навыки работы с контекстом безопасности и политиками SELinux, включая изменение режимов работы, настройку контекстов и управление переключателями.

Ход выполнения работы

## Просмотр состояния SELinux

```
mlahsi@mlahsi:~$ su
Password:
root@mlabsi:/home/mlabsi# sestatus -v
SELinux status:
                                enabled
SELinuxfs mount:
                               /svs/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
                                system_u:object_r:getty_exec_t:s0
/sbin/agetty
/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@mlabsi:/home/mlabsi#
```

## Проверка и изменение режима SELinux

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

Рис. 2: Изменение режима работы SELinux

#### Отключение SELinux

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

Рис. 3: SELinux отключён

Рис. 4: Переразметка меток безопасности

```
root@mlabsi:/home/mlabsi#
root@mlabsi:/home/mlabsi# ls -Z /etc/hosts
system u:object r:net conf t:s0 /etc/hosts
root@mlabsi:/home/mlabsi# cp /etc/hosts ~/
root@mlabsi:/home/mlabsi# ls -Z ~/hosts
unconfined u:object r:admin home t:s0 /root/hosts
root@mlabsi:/home/mlabsi# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
root@mlabsi:/home/mlabsi# ls -Z /etc/hosts
unconfined u:object r:admin home t:s0 /etc/hosts
root@mlabsi:/home/mlabsi# 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@mlabsi:/home/mlabsi# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
root@mlabsi:/home/mlabsi# touch /.autorelabel
root@mlabsi:/home/mlabsi#
```

Рис. 5: Восстановление контекста файла /etc/hosts

## Настройка контекста веб-сервера

```
root@mlabsi:/web# semanage fcontext -a -t httpd_sys_content_t */web(/.*)?*
root@mlabsi:/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_sy
s_content_t:s0
root@mlabsi:/web#
```

**Рис. 6:** Назначение контекста каталогу /web

## Работа с переключателями SELinux

```
root@mlabsi:/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@mlabsi:/web# semanage boolean -l | grep ftpd anon
                              (off . off) Allow ftpd to anon write
ftpd anon write
root@mlabsi:/web# setsebool ftpd anon write on
root@mlabsi:/web# getsebool ftpd anon write
ftpd anon write --> on
root@mlabsi:/web# semanage boolean -l | grep fpts anon
root@mlabsi:/web# semanage boolean -l | grep fptd anon
root@mlabsi:/web# semanage boolean -l | grep ftpd anon
ftpd anon write
                              (on . off) Allow ftpd to anon write
root@mlabsi:/web# setsebool -P ftpd anon write on
root@mlabsi:/web# semanage boolean -l | grep fptd anon
root@mlabsi:/web# semanage boolean -l | grep ftpd_anon
ftpd anon write
                         (on . on) Allow ftpd to anon write
root@mlabsi:/web#
```

Рис. 7: Переключатель ftpd\_anon\_write

Заключение

#### Заключение

В ходе лабораторной работы были изучены принципы работы SELinux, изменение его режимов, настройка контекстов безопасности и управление политиками доступа.