

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

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

```
/usr/sbin/sshd                                system_u:object_r:sshd_ex
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

```
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

Включение и перерозметка меток

```
Booting 'Rocky Linux (6.12.0-55.12.1.el10_0.x86_64) 10.0 (Red Quartz)'
```

[0.864878] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[0.864880] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[0.864881] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[7.470621] selinux-autorelabel[819]: *** Warning -- SELinux targeted policy relabel is required.
[7.478714] selinux-autorelabel[819]: *** Relabeling could take a very long time, depending on file
[7.478750] selinux-autorelabel[819]: *** system size and speed of hard drives.
[7.497488] selinux-autorelabel[819]: Running: /sbin/fixfiles -T 0 restore
[12.253802] selinux-autorelabel[826]: Warning: Skipping the following R/O filesystems:
[12.255644] selinux-autorelabel[826]: /run/credentials/systemd-journald.service
[12.256607] selinux-autorelabel[826]: Relabeling / /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /run /sys
/l/debug /sys/kernel/tracing

Рис. 4: Перерозметка 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

```
root@mlabsi:/web#  
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_sys_content_t:s0  
root@mlabsi:/web#
```

Рис. 6: Назначение контекста каталогу /web

```
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
ftpd_anon_write (off , off) Allow ftpd to 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

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