

Лабораторная работа №9

Управление SELinux

Максат Хемраев

15 октября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

Ход выполнения работы

- Активна политика **targeted**, режим **enforcing**

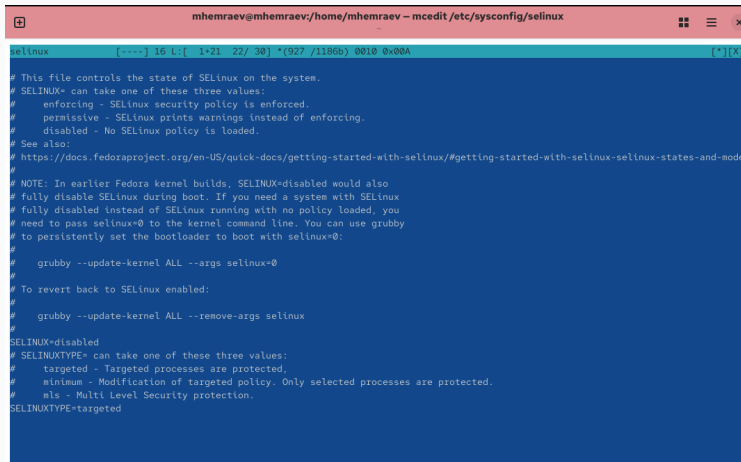
```
mhemraev@mhemraev:/home/mhemraev
+
mhemraev@mhemraev:~$ su
Password:
root@mhemraev:/home/mhemraev# sestatus -v
SELinux status:                enabled
SELinuxfs mount:               /sys/fs/selinux
SELinux root directory:        /etc/selinux
Loaded policy name:             targeted
Current mode:                   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@mhemraev:/home/mhemraev# getenforce
Enforcing
root@mhemraev:/home/mhemraev# setenforce 0
root@mhemraev:/home/mhemraev# getenforce
```

Переключение режимов SELinux

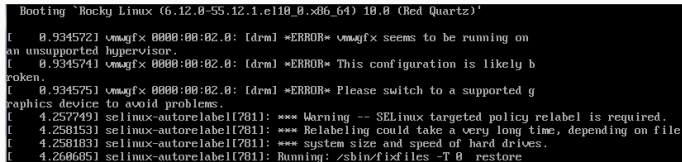
- Перевод в режим Permissive (setenforce 0)
- Редактирование /etc/sysconfig/selinux: параметр SELINUX=disabled



```
mhembraev@mhembraev:/home/mhembraev - mcedit /etc/sysconfig/selinux
selinux [----] 16 L:[ 1+21 22/ 30] *(927 /1186b) 0010 0x00A [*][X]

# 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-states-and-mode
#
# 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
```

- Установлено значение SELINUX=enforcing
- После перезагрузки запущен процесс релабелинга



```
Booting 'Rocky Linux (6.12.0-55.12.1.el10_0.x86_64) 10.0 (Red Quartz)'  
[ 0.934572] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on  
an unsupported hypervisor.  
[ 0.934574] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b  
roken.  
[ 0.934575] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g  
raphics device to avoid problems.  
[ 4.257749] selinux-autorelabel[781]: *** Warning -- SELinux targeted policy relabel is required.  
[ 4.258153] selinux-autorelabel[781]: *** Relabeling could take a very long time, depending on file  
[ 4.258183] selinux-autorelabel[781]: *** system size and speed of hard drives.  
[ 4.260685] selinux-autorelabel[781]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 3: Восстановление SELinux

Восстановление контекста безопасности

Проверка и исправление контекста /etc/hosts

- Проверен контекст безопасности файла /etc/hosts
- Восстановление выполнено командой `restorecon -v /etc/hosts`

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

Рис. 4: Восстановление контекста безопасности

Настройка контекста для веб-сервера

Создание и настройка каталога /web

- Применён контекст `httpd_sys_content_t`
- Восстановлены контексты через `restorecon -R -v /web`

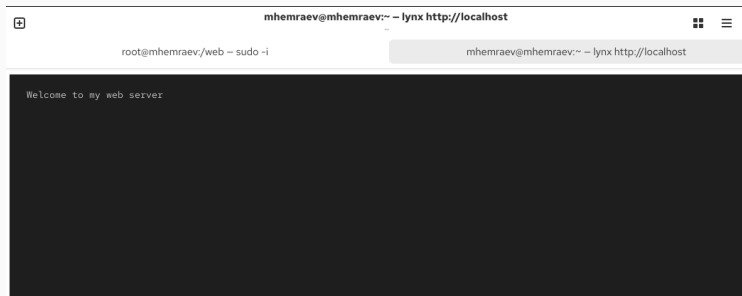


Рис. 5: Отображение страницы веб-сервера

Работа с переключателями SELinux

Изменение параметров для службы FTP

- Проверены текущие переключатели: `getsebool -a | grep ftp`
- Активирован `ftpd_anon_write` (временный и постоянный)

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

Заключение

В ходе работы изучены принципы функционирования и конфигурирования SELinux, выполнены практические действия по изменению режимов работы, восстановлению контекстов безопасности и настройке политик для различных сервисов.