Лабораторная работа №9

Управление SELinux

Анастасия Мазуркевич

16 октября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Цель лабораторной работы

Получить практические навыки работы с механизмом безопасности SELinux, изучить режимы работы, контексты безопасности и управление политиками доступа.

Ход выполнения

Управление режимами SELinux

```
root@admazurkevich:/home/admazurkevich#
root@admazurkevich:/home/admazurkevich# 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@admazurkevich:/home/admazurkevich# getenforce
Enforcing
root@admazurkevich:/home/admazurkevich# setenforce 0
root@admazurkevich:/home/admazurkevich# getenforce
Permissive
root@admazurkevich:/home/admazurkevich#
root@admazurkevich:/home/admazurkevich# mcedit /etc/sysconfig/selinux

root@admazurkevich:/home/admazurkevich#
```

Управление режимами SELinux

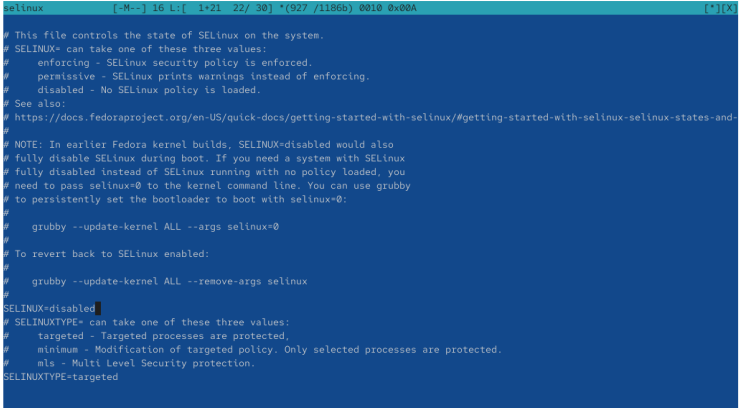

Рис. 2: Изменение конфигурации SELinux

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

Рис. 3: SELinux отключён

Управление режимами SELinux

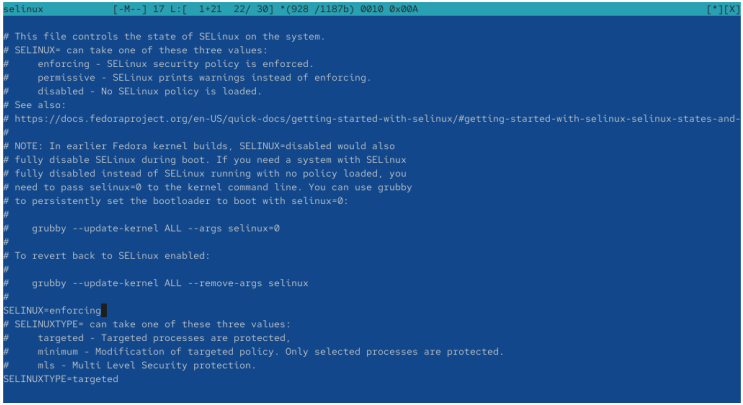

Рис. 4: Включение enforcing-режима SELinux

Управление режимами SELinux

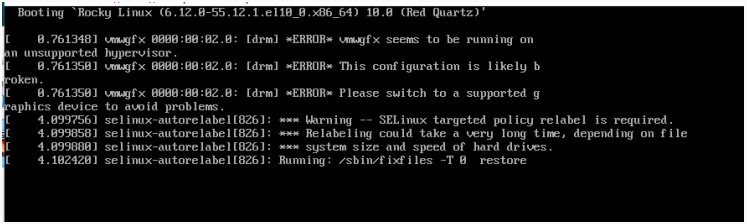

Рис. 5: Процесс восстановления меток при загрузке

Управление режимами SELinux

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

Рис. 6: Повторная проверка статуса SELinux

Использование restorecon

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

Рис. 7: Контекст безопасности файла hosts

Использование restorecon

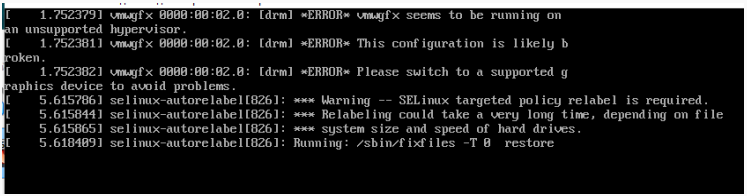

Рис. 8: Автоматическое восстановление контекстов SELinux

Изменение каталога DocumentRoot

```
Installed:
  lynx-2.9.0-6.el10.x86_64

Complete!
root@admazurkevich:/home/admazurkevich#
root@admazurkevich:/home/admazurkevich# mkdir /web
root@admazurkevich:/home/admazurkevich# cd /web
root@admazurkevich:/web# touch index.html
root@admazurkevich:/web# echo "Welcome to my web-server" > index.html
root@admazurkevich:/web#
```

Рис. 9: Создание каталога и файла index.html

Изменение конфигурации Apache

```
httpd.conf          [-M--]  0 L:[113+19 132/367] *(4629/12135b) 0010 0x00A
# 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. 10: Изменение настроек httpd.conf

Проверка доступа

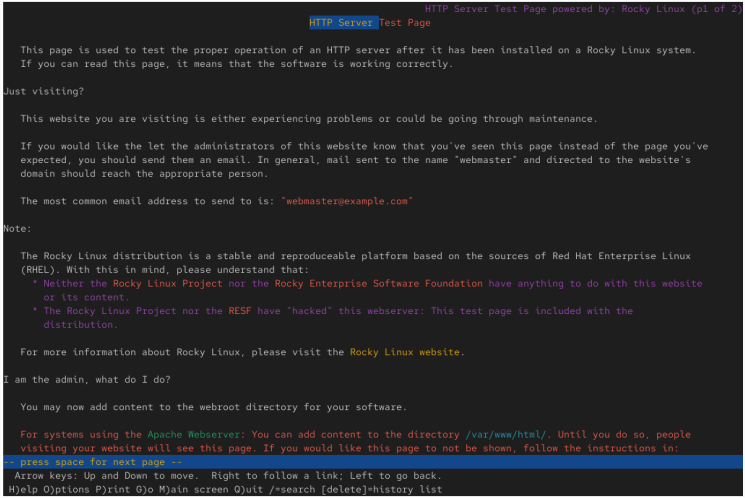

Рис. 11: Страница Apache по умолчанию

Настройка контекста безопасности

```
root@admazurkevich:/web# systemctl enable httpd
root@admazurkevich:/web#
root@admazurkevich:/web# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
root@admazurkevich:/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@admazurkevich:/web#
```

Рис. 12: Назначение и восстановление контекста безопасности для /web

Проверка результата

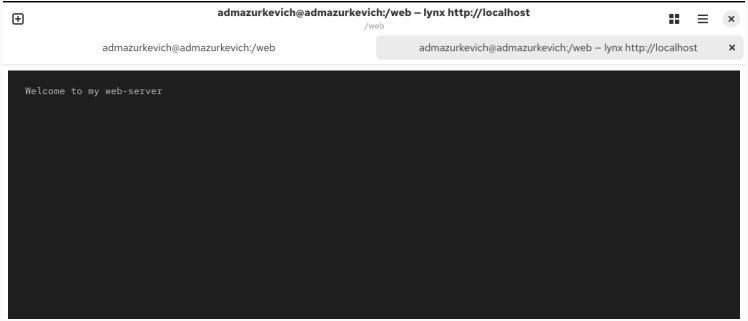

Рис. 13: Отображение пользовательской страницы

Настройка переключателя ftpd_anon_write

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

Заключение

Вывод

В ходе работы были изучены:

- режимы SELinux и их назначение;
- методы изменения и проверки состояния системы;
- восстановление контекстов безопасности с помощью `restorecon`;
- применение политик для нестандартных каталогов веб-сервера;
- управление переключателями SELinux.

Освоены практические приёмы настройки и диагностики SELinux, что повышает уровень защиты и управляемости Linux-систем.