Лабораторная работа №9

Управление SELinux

Щемелев Илья Владимирович

Российский университет дружбы народов, Москва, Россия

Цель работы

Формулировка цели

Получить навыки работы с контекстом безопасности и политиками SELinux.

Ход выполнения работы

Перевод в Permissive (setenforce 0)

```
root@ivschemelev:~# 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@ivschemelev:~# getenforce
Enforcing
root@ivschemelev:~# setenforce 0
root@ivschemelev:~# getenforce
Permissive
root@ivschemelev:~#
```

Отключение SELinux в конфигурации

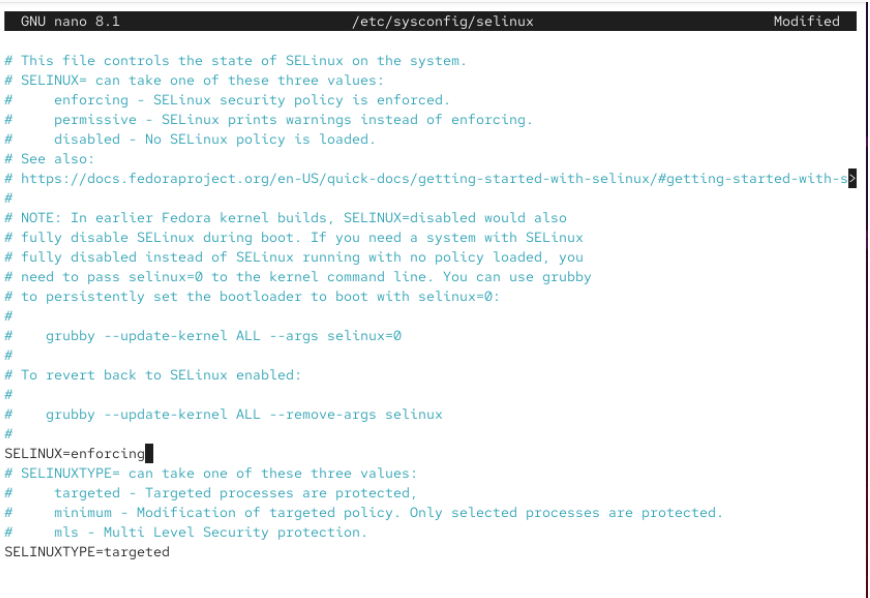
```
  GNU nano 8.1                        /etc/sysconfig/selinux                        Modified

# 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-s
#
# 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
```

Проверка Disabled и реакция на setenforce

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

Рис. 3: SELinux отключён и не переключается без перезагрузки

Возврат SELINUX=enforcing



Проверка enforcing после перезагрузки

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

Контекст /etc/hosts и восстановление меток

```
root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@ivschemelev:/home/ivschemelev# cp /etc/hosts ~/
root@ivschemelev:/home/ivschemelev# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
root@ivschemelev:/home/ivschemelev# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
root@ivschemelev:/home/ivschemelev# ls -Z ~/hosts
ls: cannot access '/root/hosts': No such file or directory
root@ivschemelev:/home/ivschemelev# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
root@ivschemelev:/home/ivschemelev# 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@ivschemelev:/home/ivschemelev# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
root@ivschemelev:/home/ivschemelev# touch /.autorelabel
root@ivschemelev:/home/ivschemelev#
```

Рис. 6: Восстановление контекста /etc/hosts (restorecon)

Сообщения перемаркировки при загрузке

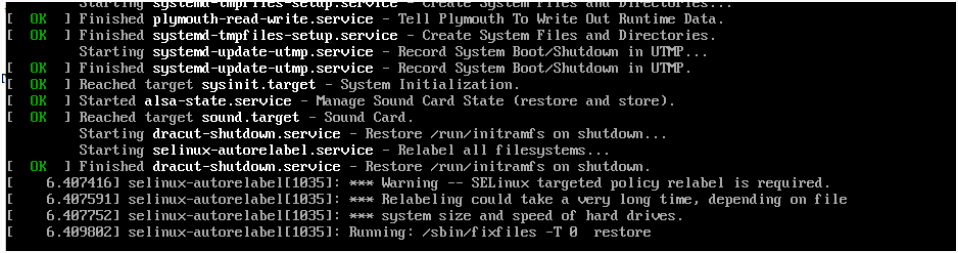
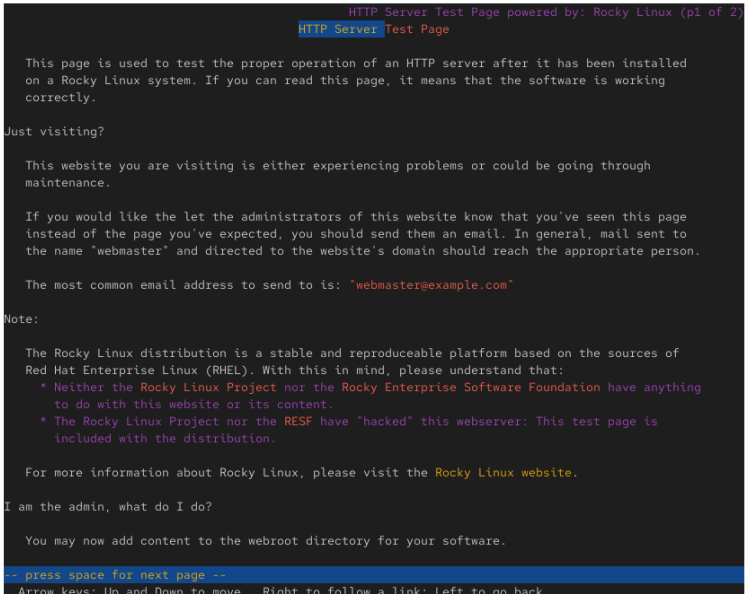


Рис. 7: Автоматическая перемаркировка файловой системы (autorelabel)

Изменение DocumentRoot и правил доступа

```
  GNU nano 8.1                          /etc/httpd/conf/httpd.conf
#
# 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/"

DocumentRoot "/web"

<Directory "/web">
 AllowOverride None
 Require all granted
</Directory>
```

Страница по умолчанию до настройки SELinux



Назначение контекста httpd_sys_content_t и restorecon

```
root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# mkdir /web
root@ivschemelev:/home/ivschemelev# cd /web
root@ivschemelev:/web# touch index.html
root@ivschemelev:/web# echo "Welcome to my web-server" > index.html
root@ivschemelev:/web# nano /etc/httpd/conf/httpd.conf
root@ivschemelev:/web#
root@ivschemelev:/web# systemctl start httpd
root@ivschemelev:/web# systemctl enable htppd
Failed to enable unit: Unit htppd.service does not exist
root@ivschemelev:/web# systemctl enable httpd
root@ivschemelev:/web# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
root@ivschemelev:/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_co
ntent_t:s0
root@ivschemelev:/web# systemctl restart httpd
root@ivschemelev:/web#
```

Рис. 10: semanage fcontext и restorecon для /web

Проверка через lynx: пользовательская страница

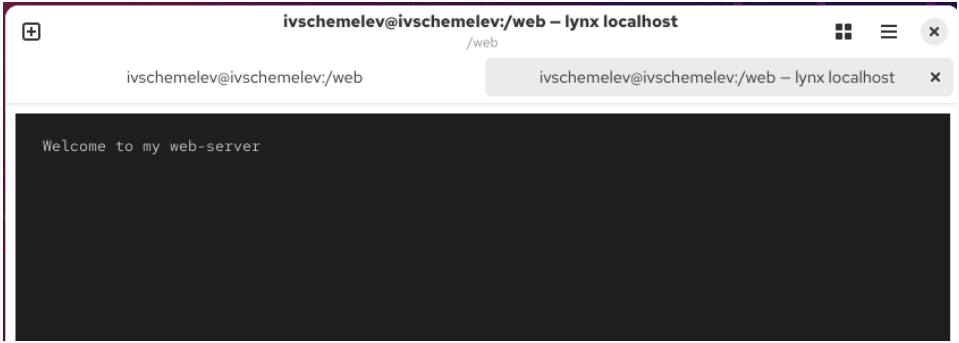


Рис. 11: Welcome to my web-server

Проверка и включение ftpd_anon_write

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

Итоги работы

Заключение

Выполнено управление режимами SELinux (Enforcing/Permissive/Disabled), подтверждена невозможность переключения из Disabled без перезагрузки. Отработано восстановление контекстов безопасности с помощью restorecon и массовая перемаркировка через `/.autorelabel`. Настроен доступ httpd к нестандартному каталогу `/web` путём назначения корректного типа контекста `httpd_sys_content_t`. Изучены и изменены boolean-переключатели SELinux на примере `ftpd_anon_write` (временное и постоянное включение).