Лабораторная работа №9

Управление SELinux

Турсунов Мухамметназар

17 октября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Основная цель

Изучение принципов работы системы безопасности **SELinux**, освоение режимов работы, восстановления контекстов и настройки политик безопасности для служб Linux.

Управление режимами SELinux

Проверка состояния SELinux

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

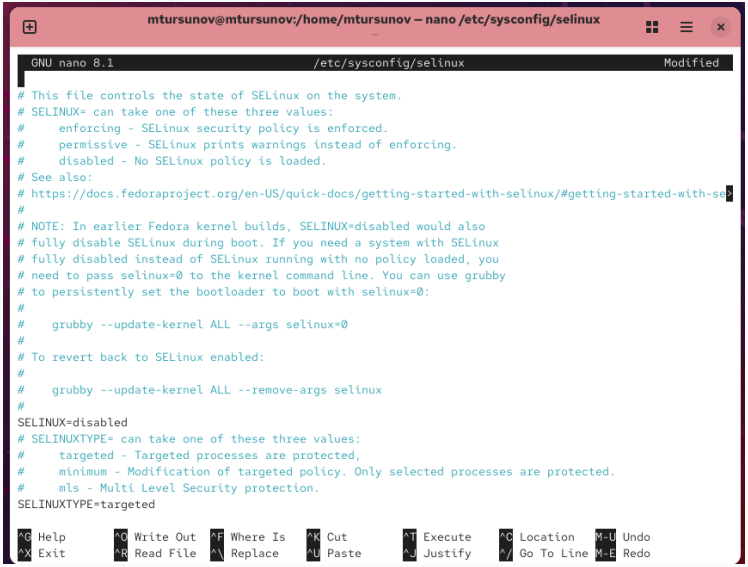
Рис. 1: Вывод команды sestatus -v

Переключение режима работы

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

Рис. 2: Изменение режима на Permissive

Отключение SELinux



Проверка отключённого состояния

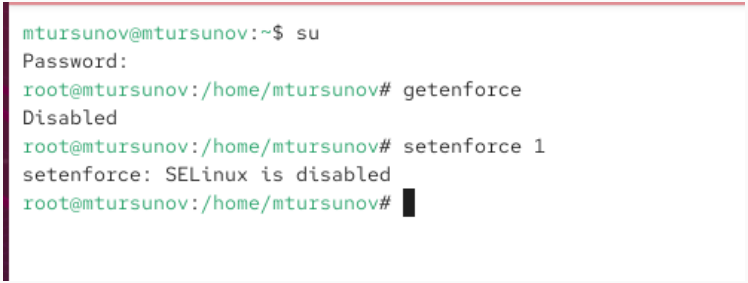
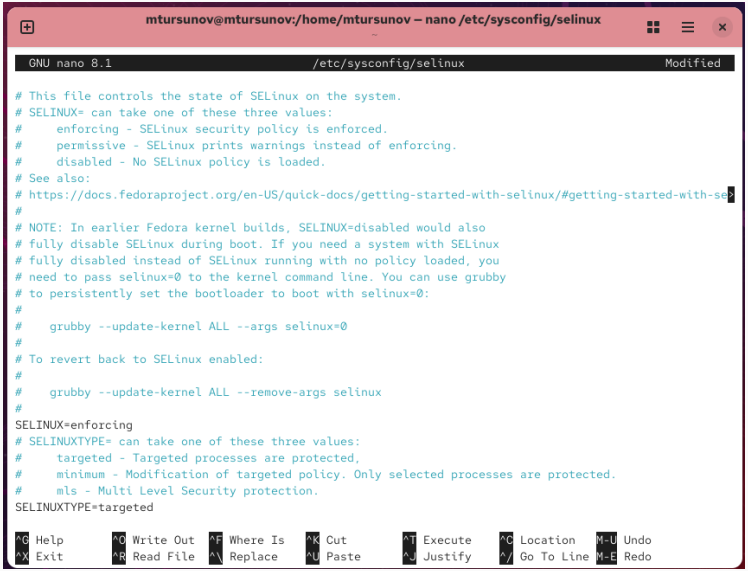


Рис. 4: Попытка включения SELinux при disabled

Повторное включение enforcing



Восстановление меток при загрузке

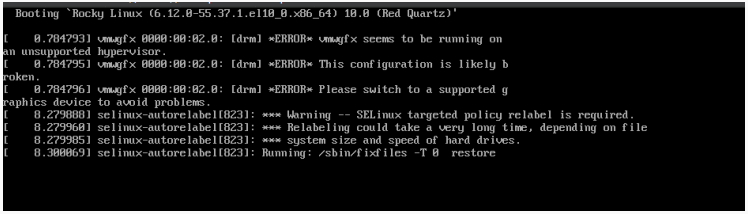


Рис. 6: Автоматическое восстановление меток SELinux

Проверка статуса после восстановления

```
Password:
root@mtursunov:/home/mtursunov# 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@mtursunov:/home/mtursunov#
```

Рис. 7: SELinux снова включён, режим enforcing

Восстановление контекста безопасности

Использование restorecon

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

Рис. 8: Восстановление контекста файла hosts

Массовое восстановление контекстов

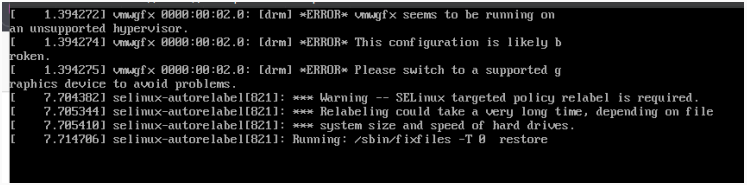


Рис. 9: Автоматическое перемаркирование файловой системы

Настройка контекста для веб-сервера

Новый каталог и файл index.html

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

Complete!
root@mtursunov:/home/mtursunov# mkdir /web
root@mtursunov:/home/mtursunov# cd /web
root@mtursunov:/web# touch index.html
root@mtursunov:/web# echo "Welcome to my web server" > index.html
root@mtursunov:/web# nano /etc/httpd/conf/httpd.conf
root@mtursunov:/web# systemctl start httpd
root@mtursunov:/web# systemctl enable httpd
root@mtursunov:/web#
```

Рис. 10: Создание каталога /web и файла index.html

Изменение DocumentRoot в httpd.conf

```
#
# 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. 11: Редактирование конфигурации Apache

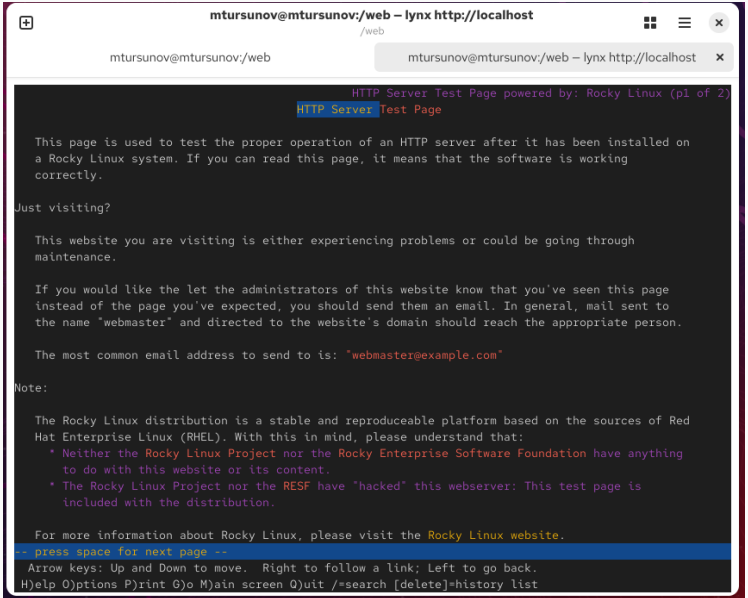
Старт службы httpd

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

Complete!
root@mtursunov:/home/mtursunov# mkdir /web
root@mtursunov:/home/mtursunov# cd /web
root@mtursunov:/web# touch index.html
root@mtursunov:/web# echo "Welcome to my web server" > index.html
root@mtursunov:/web# nano /etc/httpd/conf/httpd.conf
root@mtursunov:/web# systemctl start httpd
root@mtursunov:/web# systemctl enable httpd
root@mtursunov:/web#
```

Рис. 12: Запуск службы httpd

Проверка результата в браузере lynx



Присвоение контекста httpd_sys_content_t

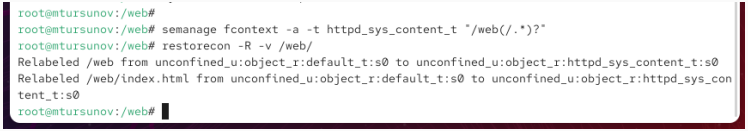


Рис. 14: Настройка контекста каталога /web

Корректное отображение веб-страницы

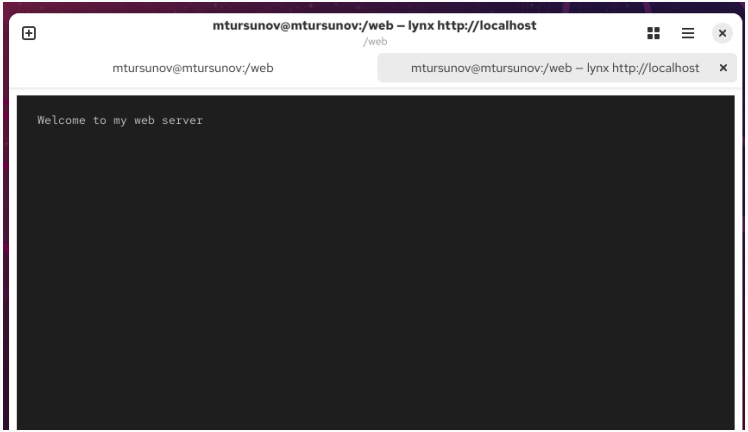


Рис. 15: Отображение пользовательской страницы веб-сервера

Работа с переключателями SELinux

Проверка состояния переключателей

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

Рис. 16: Просмотр и изменение переключателя ftpd_anon_write

Итоги работы

Вывод

В ходе работы были изучены режимы функционирования **SELinux**:
Enforcing, **Permissive** и **Disabled**.
Отработаны навыки восстановления контекстов безопасности, применения политик доступа и настройки правил для служб Linux.
Освоено использование инструментов **semanage**, **restorecon** и **setsebool**.
SELinux был успешно возвращён в активный режим **enforcing** с корректной политикой безопасности.