Лабораторная работа №9

Управление SELinux

Сулейм Гамбердов

16 октября 2025

Российский университет дружбы народов, Москва, Россия

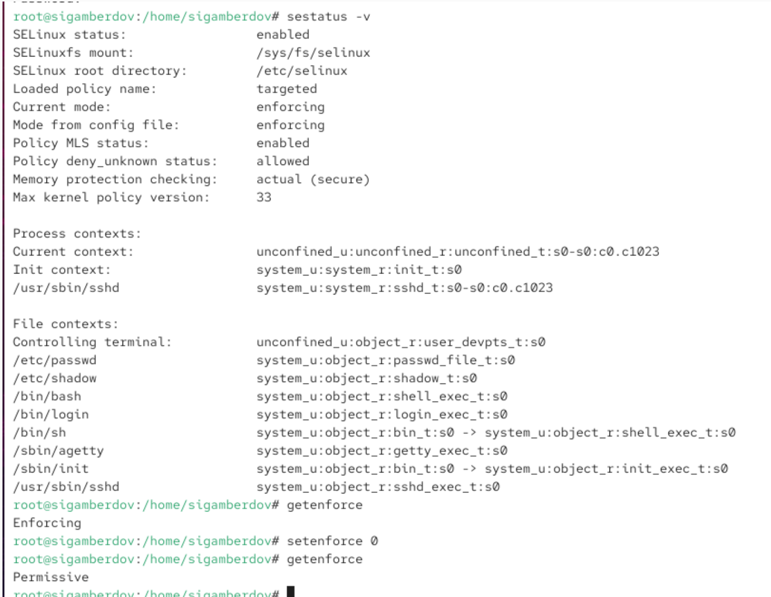
Цель работы

Основная цель

Получить навыки работы с контекстом безопасности и политиками SELinux, научиться изменять режимы работы, восстанавливать контексты и применять политики к нестандартным каталогам.

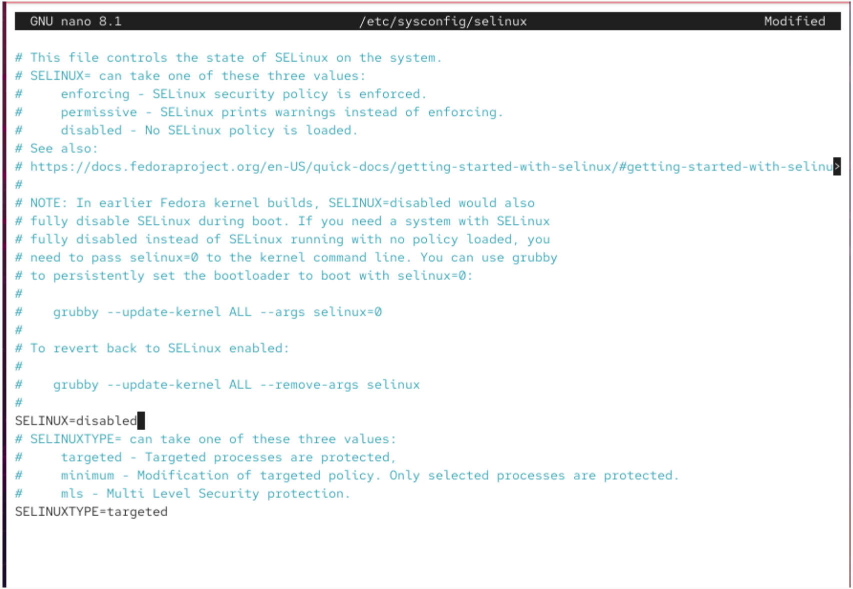
Ход выполнения работы

Проверка состояния SELinux



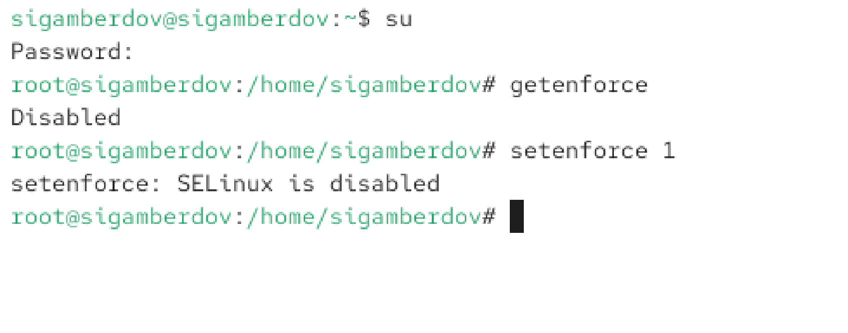
```
root@sigamberdov:/home/sigamberdov# sestatus -v
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
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@sigamberdov:/home/sigamberdov# getenforce
Enforcing
root@sigamberdov:/home/sigamberdov# setenforce 0
root@sigamberdov:/home/sigamberdov# getenforce
Permissive
root@sigamberdov:/home/sigamberdov#
```

Изменение режима работы SELinux



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

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these 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-selinu>
#
# 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
```

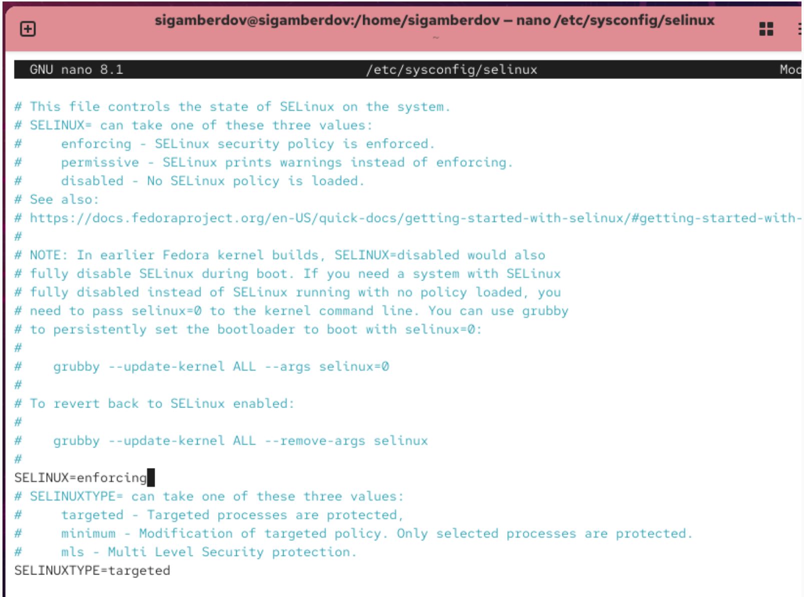
Отключение и повторное включение SELinux



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

Рис. 3: Отключение SELinux в конфигурационном файле

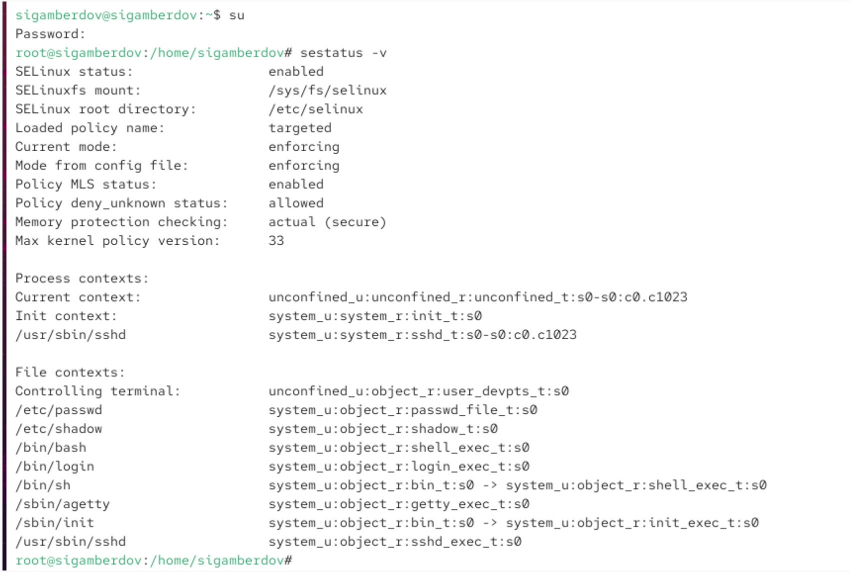
Отключение и повторное включение SELinux



sigamberdov@sigamberdov:/home/sigamberdov – nano /etc/sysconfig/selinux

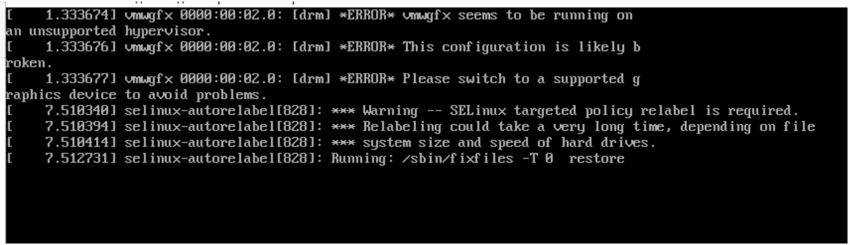
```
 GNU nano 8.1                       /etc/sysconfig/selinux                       Mod

# 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-
#
# 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=enforcing
# 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
```

Отключение и повторное включение SELinux



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

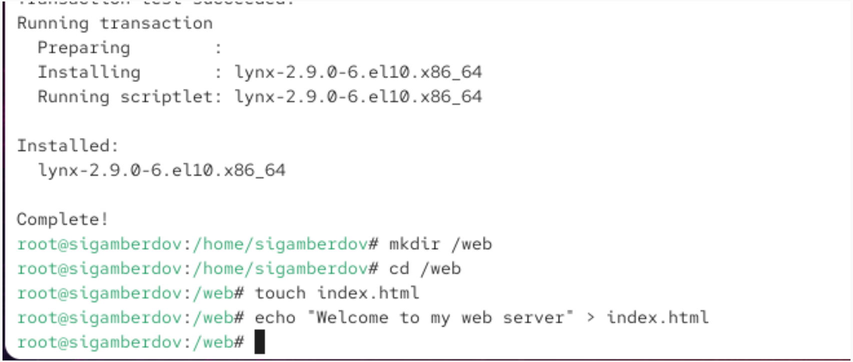
Восстановление контекста безопасности



```
[    1.333674] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[    1.333676] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[    1.333677] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[    7.510340] selinux-autorelabel[828]: *** Warning -- SELinux targeted policy relabel is required.
[    7.510394] selinux-autorelabel[828]: *** Relabeling could take a very long time, depending on file
[    7.510414] selinux-autorelabel[828]: *** system size and speed of hard drives.
[    7.512731] selinux-autorelabel[828]: Running: /sbin/fixfiles -T 0  restore
```

Рис. 6: Использование restorecon и autorelabel для восстановления контекста

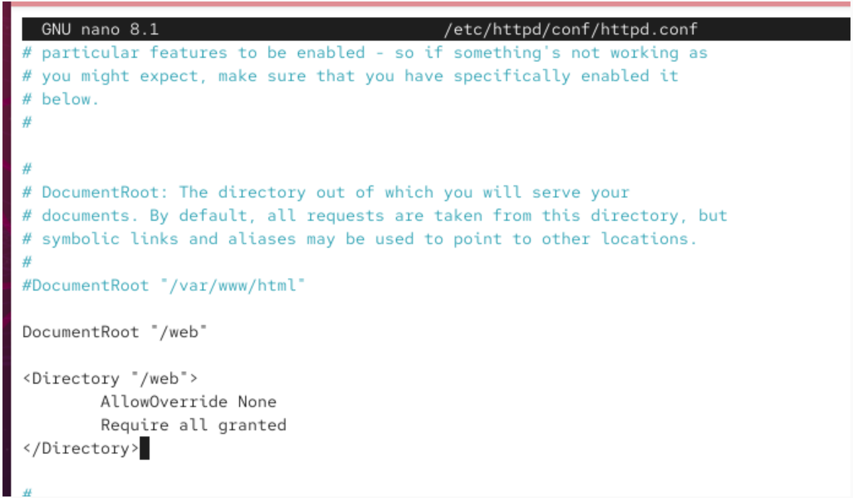
Настройка контекста для каталога веб-сервера



```
Transaction test succeeded.
Running transaction
  Preparing        :
  Installing       : lynx-2.9.0-6.el10.x86_64
  Running scriptlet: lynx-2.9.0-6.el10.x86_64

Installed:
  lynx-2.9.0-6.el10.x86_64

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

Рис. 7: Установка lynx и подготовка каталога /web

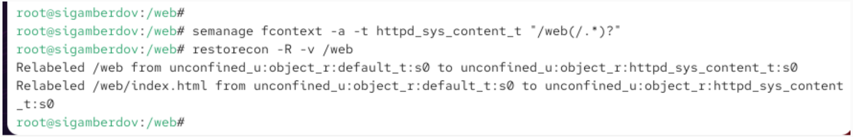
Настройка контекста для каталога веб-сервера



```
  GNU nano 8.1                              /etc/httpd/conf/httpd.conf
# 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. 8: Изменение конфигурации DocumentRoot

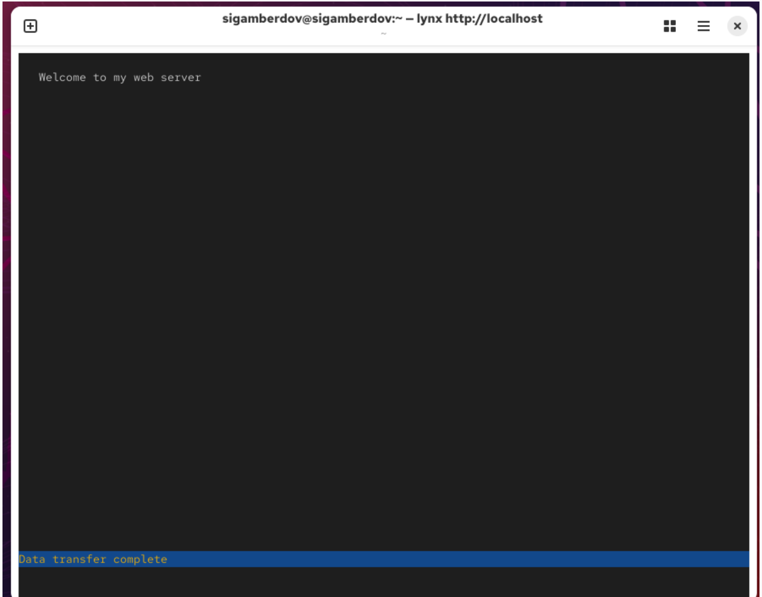
Настройка контекста для каталога веб-сервера



```
root@sigamberdov:/web#
root@sigamberdov:/web# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
root@sigamberdov:/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@sigamberdov:/web#
```

Рис. 9: Назначение контекста безопасности для каталога /web

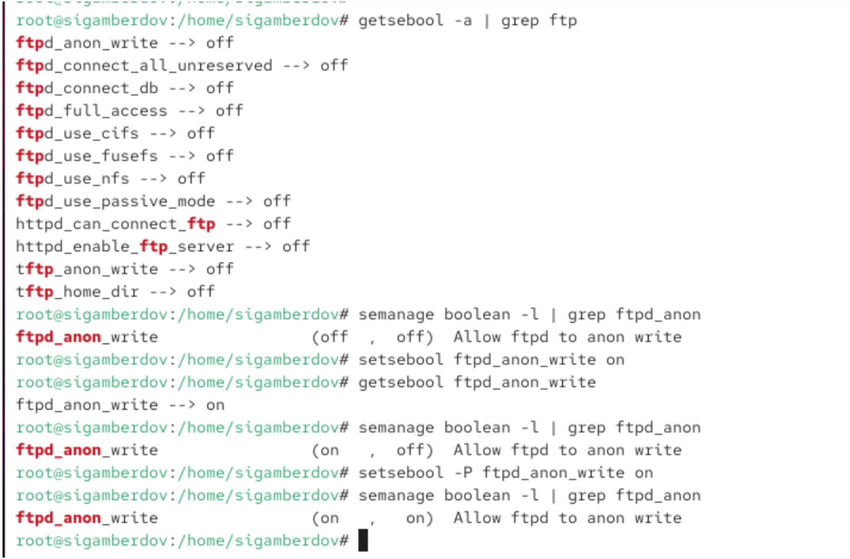
Настройка контекста для каталога веб-сервера



```
Welcome to my web server
```

```
Data transfer complete
```

Настройка параметров SELinux для FTP



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

Итоги работы

Вывод

В ходе лабораторной работы были освоены приёмы администрирования SELinux:

- изменение режимов работы системы безопасности;
- назначение и восстановление контекстов безопасности;
- настройка SELinux для нестандартных каталогов веб-сервера и FTP-сервиса.

Работа позволила понять принципы функционирования механизма SELinux и его роль в обеспечении безопасности Linux-систем.