

Отчёт по лабораторной работе №9

Управление SELinux

Яковлева Дарья Сергеевна

29 октября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Получить практические навыки работы с контекстами безопасности и политиками SELinux в Linux.

Выполнение лабораторной работы

Проверка состояния SELinux

```
root@dsyakovleva:~ -- -bash

dsyakovleva@dsyakovleva:~$ su -
Password:
Last login: Tue Oct 28 23:05:58 MSK 2025 on pts/0
root@dsyakovleva:~# 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

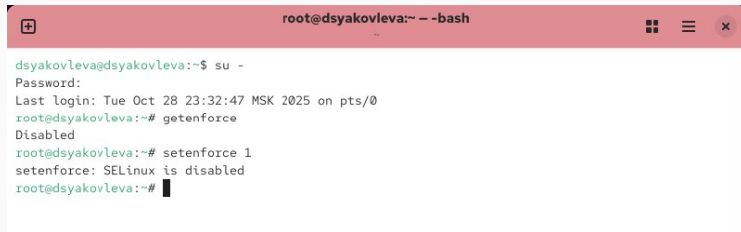
File contexts:
Controlling terminal:          unconfined_u:object_r:user_devpts_t:s0
/etc/passwd                   system_u:object_r:passwd_file_t:s0
/etc/shadow                   system_u:object_r:shadow_t:s0
/bin/bash                     system_u:object_r:shell_exec_t:s0
/bin/login                    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@dsyakovleva:~# getenforce
Enforcing
root@dsyakovleva:~# setenforce 0
root@dsyakovleva:~# getenforce
Permissive
root@dsyakovleva:~#
```

Изменение режима работы

```
selinux [-M--] 16 L:[ 1+21 22/ 29] *(927 /1185b) 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-wi
#
# 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
```

A terminal window with a pink title bar. The title bar contains a window control icon on the left, the text 'root@dsyakovleva:~ -- -bash' in the center, and window control icons on the right. The terminal content shows a user switching to root and checking the SELinux status.

```
root@dsyakovleva:~ -- -bash
dsyakovleva@dsyakovleva:~$ su -
Password:
Last login: Tue Oct 28 23:32:47 MSK 2025 on pts/0
root@dsyakovleva:~# getenforce
Disabled
root@dsyakovleva:~# setenforce 1
setenforce: SELinux is disabled
root@dsyakovleva:~#
```

Рис. 3: Проверка статуса SELinux после отключения

Восстановление режима Enforcing

```
selinux [----] 17 L:[ 1+21 22/ 29] *(928 /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-wi
#
# 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
```



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

Рис. 5: Восстановление контекста безопасности

```
Complete!  
root@dsyakovleva:~# mkdir /web  
root@dsyakovleva:~# cd /web  
root@dsyakovleva:/web# touch index.html  
root@dsyakovleva:/web# mcedit index.html  
  
root@dsyakovleva:/web# mcedit index.html  
  
root@dsyakovleva:/web# █
```

Рис. 6: Создание каталога и файла index.html

Редактирование index.html

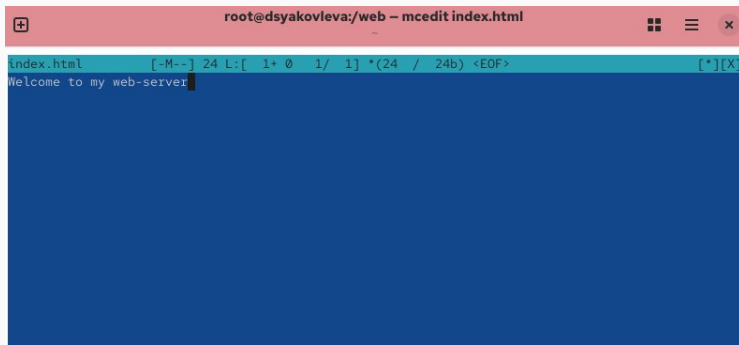


Рис. 7: Редактирование файла index.html

Проверка работы веб-сервера

```
root@dsyakovleva:/web# systemctl start httpd
root@dsyakovleva:/web# systemctl enable httpd
Created symlink '/etc/systemd/system/multi-user.target.wants/httpd.service' → '/usr/lib/systemd/system/httpd.service'.
root@dsyakovleva:/web# su dsyakovleva
dsyakovleva@dsyakovleva:/web$ lynx http://localhost
dsyakovleva@dsyakovleva:/web$ su -
Password:
Last login: Tue Oct 28 23:49:06 MSK 2025 on pts/0
root@dsyakovleva:~# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
root@dsyakovleva:~# 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@dsyakovleva:~# lynx http://localhost
root@dsyakovleva:~#
```

Рис. 8: Попытка доступа к веб-странице до смены контекста

Изменение контекста каталога /web

```
#DocumentRoot "/var/www/html"

DocumentRoot "/web"

#
# Relax access to content within /var/www.
#
#<Directory "/var/www">
#     AllowOverride None
#     # Allow open access:
#     Require all granted
#</Directory>

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

# Further relax access to the default document root:
<Directory "/var/www/html">
    #
```

1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 10Quit

Рис. 9: Изменение пути к DocumentRoot и настройка доступа

Успешный доступ к веб-странице

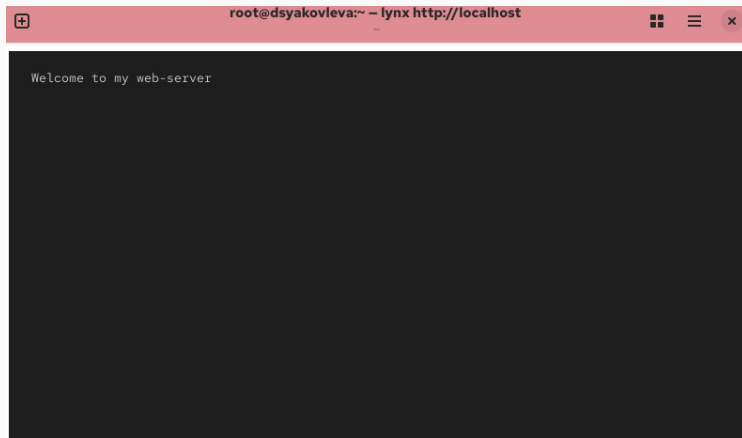


Рис. 10: Отображение пользовательской веб-страницы

Работа с переключателями SELinux

```
root@dsyakovleva:~# 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@dsyakovleva:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (off , off) Allow ftpd to anon write
root@dsyakovleva:~# setsebool ftpd_anon_write on

Usage: setsebool [ -NPV ] boolean value | bool1=val1 bool2=val2...

root@dsyakovleva:~# getsebool ftpd_anon_write
Error getting active value for ftpd
root@dsyakovleva:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (off , off) Allow ftpd to anon write
root@dsyakovleva:~#
root@dsyakovleva:~# setsebool -P ftpd_anon_write on

Usage: setsebool [ -NPV ] boolean value | bool1=val1 bool2=val2...

root@dsyakovleva:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (off , off) Allow ftpd to anon write
root@dsyakovleva:~#
```

Контрольные вопросы

- `getenforce` — проверка текущего режима
- `setenforce 0 / 1` — изменение режима
- `sestatus -v` — просмотр состояния SELinux
- `restorecon` — восстановление контекста безопасности
- `semanage fcontext` — настройка контекста файлов
- `getsebool / setsebool` — управление переключателями

Итоги работы

В ходе лабораторной работы были изучены принципы работы SELinux, способы изменения режимов безопасности, восстановления контекстов и настройки политик для сервисов. Получены практические навыки администрирования SELinux и повышения безопасности системы.