

# Лабораторная работа №9

Презентация

---

Ермишина М. К.

31 октября 2025

Российский университет дружбы народов, Москва, Россия

# Информация

---

- Ермишина Мария Кирилловна
- студент группы НПИбд-01-24
- Российский университет дружбы народов
- 1132230166@pfur.ru
- <https://github.com/ErmiMash>

# Элементы презентации

---

Целью данной лабораторной работы является получение навыков работы с контекстом безопасности и политиками SELinux.

# Выполнение лабораторной работы

---

# Управление режимами SELinux

Запустите терминал и получите полномочия администратора. Просмотрите текущую информацию о состоянии SELinux: Посмотрите, в каком режиме работает SELinux: - getenforce Измените режим работы SELinux на разрешающий (Permissive): - setenforce 0 Еще раз проверяем режим работы.

```
[root@localhost ~]# su -
Password:
[root@localhost ~]# 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:     31

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:rlogin_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:agetty_exec_t:s0
/sbin/init                   system_u:object_r:bin_t:s0 -> system_u:object_r:rinit_exec_t:s0
/usr/sbin/sshd               system_u:object_r:sshd_exec_t:s0

[root@localhost ~]# getenforce
enforcing
[root@localhost ~]# setenforce 0
[root@localhost ~]# getenforce
Permissive
[root@localhost ~]#
```

# Первое редактирование файла

В файле `/etc/sysconfig/selinux` с помощью редактора установите `SELINUX=disabled` и перезапустите систему. Посмотрите статус SELinux: - `getenforce` Попробуйте переключить режим работы SELinux: - `setenforce 1`

```
[root@localhost ~]# su -  
Password:  
[root@localhost ~]# getenforce  
disabled  
[root@localhost ~]# setenforce 1  
setenforce: SELinux is disabled  
[root@localhost ~]# nano /etc/sysconfig/selinux  
[root@localhost ~]# reboot
```



## Второе редактирование - принужительный режим

Откройте файл /etc/sysconfig/selinux с помощью редактора и установите: - SELINUX=enforcing Перезагрузите систему. После перезагрузки в терминале с полномочиями администратора просмотрите текущую информацию о

```
termash@termash ~]$ 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

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/rsync                   system_u:object_r:rsync_t:s0 -> system_u:object_r:shell_exec_t:s0
/sbin/agetty                 system_u:object_r:agetty_exec_t:s0
/sbin/init                   system_u:object_r:rsync_t:s0 -> system_u:object_r:init_exec_t:s0
/usr/sbin/rsysd               system_u:object_r:rsysd_exec_t:s0
termash@termash ~]$
```

состоянии SELinux: - sestatus -v

# Использование restorecon для восстановления контекста безопасности

Запустите терминал и получите полномочия администратора. Посмотрите контекст безопасности файла /etc/hosts. Скопируйте файл /etc/hosts в домашний каталог. Проверьте контекст файла ~/hosts. Поскольку копирование считается созданием нового файла, то параметр контекста в файле ~/hosts, расположенном в домашнем каталоге, станет admin\_home\_t. Попробуйте перезаписать существующий файл hosts из домашнего каталога в каталог /etc. Убедитесь, что тип контекста по-прежнему установлен на admin\_home\_t. Исправьте контекст безопасности. Убедитесь, что тип контекста изменился. Для массового исправления контекста безопасности на файловой

```
[root@localhost ~]# su -
Password:
su: Authentication failure
[root@localhost ~]# su -
Password:
[root@localhost ~]# ls -l /etc/hosts
system_u:object_r:inet_conf_t:0 /etc/hosts
[root@localhost ~]# cp /etc/hosts ~/
[root@localhost ~]# ls -l ~/hosts
unconfined_u:object_r:admin_home_t:s0 ~/hosts
[root@localhost ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
[root@localhost ~]# ls -l /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@localhost ~]# restorecon -v /etc/hosts
Relabeled /etc/hosts from unconfined_u:object_r:admin_home_t:s0 to unconfined_u:object_r:inet_conf_t:0
[root@localhost ~]# ls -l /etc/hosts
unconfined_u:object_r:inet_conf_t:s0 /etc/hosts
[root@localhost ~]# touch ./autorelabel
[root@localhost ~]#
```

системе введите

# Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Запустите терминал и получите полномочия администратора. Установите необходимое программное обеспечение: `- dnf -y install httpd - dnf -y install lynx`  
Создайте новое хранилище для файлов веб-сервера и создайте файл `index.html` в каталоге с контентом веб-сервера и поместите в файл следующий текст “Welcome to my web-server” В файле `/etc/httpd/conf/httpd.conf`

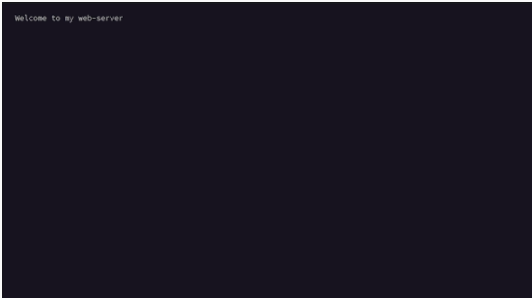
отредактируйте строки.

```
DocumentRoot "/web"
#
# Relax access to content within /var/www.
#
<Directory "/var/www">
    AllowOverride None
    # Allow .com access
    Require all granted
</Directory>

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

## Запуск веб-сервер и службу

- `systemctl start httpd` - `systemctl enable httpd` В терминале под учётной записью своего пользователя при обращении к веб-серверу в текстовом браузере `lynx`:
- `lynx http://localhost` Первый запуск имеет неправильный вывод, в терминале с полномочиями администратора примените новую метку контекста к `/web` - `semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"`. Восстановите контекст безопасности: - `restorecon -R -v /web`

A dark terminal window with the text "Welcome to my web-server" in the top left corner.

Welcome to my web-server

# Работа с переключателями SELinux

Запустите терминал и получите полномочия администратора. Посмотрите список переключателей SELinux для службы ftp. Для службы “ftpd\_anon” посмотрите список переключателей с пояснением, за что отвечает каждый переключатель, включён он или выключен. Измените текущее значение переключателя для службы ftpd anon write с off на on. Посмотрите список

переключателей с пояснением.

```
[root@shellperimash ~]# su -
Password:
[root@shellperimash ~]# 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
ftp_anon_write --> off
tftp_home_dir --> off
[root@shellperimash ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (off, off) Allow ftpd to anon write
[root@shellperimash ~]# setsebool ftpd_anon_write on
[root@shellperimash ~]# getsebool ftpd_anon_write
ftpd_anon_write --> on
[root@shellperimash ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (on, off) Allow ftpd to anon write
[root@shellperimash ~]# setsebool -P ftpd_anon_write on
[root@shellperimash ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (on, on) Allow ftpd to anon write
[root@shellperimash ~]#
```

Получены навыки работы с контекстом безопасности и политиками SELinux.