

# **Лабораторная работа № 9**

**Отчёт**

Ермишина Мария Кирилловна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>3</b>	<b>Контрольные вопросы</b>	<b>13</b>
<b>4</b>	<b>Выводы</b>	<b>14</b>

# Список иллюстраций

2.1	Разрешающий режим SELinux . . . . .	6
2.2	disabled в файле SELinux . . . . .	7
2.3	Проверка изменений . . . . .	7
2.4	enforcing в файле SELinux . . . . .	7
2.5	Принудительный режим активен . . . . .	7
2.6	Использование restorecon . . . . .	8
2.7	Установка прог. обеспеч. . . . .	9
2.8	Редакция текстового файла . . . . .	10
2.9	Первый запуск сайта . . . . .	10
2.10	Восстановка контекста безопасности . . . . .	11
2.11	Второй запуск . . . . .	11
2.12	Работа с переключателями SELinux . . . . .	12

## **Список таблиц**

# 1 Цель работы

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

## 2 Выполнение лабораторной работы

1. Управление режимами SELinux Запустите терминал и получите полномочия администратора. Просмотрите текущую информацию о состоянии SELinux: (рис. 2.1)

- sestatus -v Посмотрите, в каком режиме работает SELinux: (рис. 2.1)
- getenforce Измените режим работы SELinux на разрешающий (Permissive): (рис. 2.1)
- setenforce 0 и снова введите (рис. 2.1)
- getenforce

```
[terminash@terminash ~]$ su -
Password:
[root@terminash ~]# 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@terminash ~]# getenforce
Enforcing
[root@terminash ~]# setenforce 0
[root@terminash ~]# getenforce
Permissive
[root@terminash ~]#
```

Рис. 2.1: Разрешающий режим SELinux

В файле /etc/sysconfig/selinux с помощью редактора установите: (рис. 2.2) - SELINUX=disabled

```
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
```

Рис. 2.2: disabled в файле SELinux

Перезагрузите систему. После перезагрузки запустите терминал и получите полномочия администратора. Посмотрите статус SELinux: - `getenforce` Вы увидите, что SELinux теперь отключён. Попробуйте переключить режим работы SELinux: - `setenforce 1`

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

Рис. 2.3: Проверка изменений

Откройте файл `/etc/sysconfig/selinux` с помощью редактора и установите: (рис. 2.4) - `SELINUX=enforcing` Перезагрузите систему.

```
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
```

Рис. 2.4: enforcing в файле SELinux

После перезагрузки в терминале с полномочиями администратора просмотрите текущую информацию о состоянии SELinux: (рис. 2.5) - `sestatus -v`

```
[ermimash@ermimash ~]$ 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-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/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
[ermimash@ermimash ~]$
```

Рис. 2.5: Принудительный режим активен

2. Использование restorecon для восстановления контекста безопасности (рис. 2.6) Запустите терминал и получите полномочия администратора. Посмотрите контекст безопасности файла /etc/hosts:

- `ls -Z /etc/hosts` Скопируйте файл /etc/hosts в домашний каталог:
- `cp /etc/hosts ~/` Проверьте контекст файла ~/hosts:
- `ls -Z ~/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:
- `mv ~/hosts /etc` Убедитесь, что тип контекста по-прежнему установлен на admin\_home\_t:
- `ls -Z /etc/hosts` Исправьте контекст безопасности:
- `restorecon -v /etc/hosts` Убедитесь, что тип контекста изменился:
- `ls -Z /etc/hosts` Для массового исправления контекста безопасности на файловой системе введите
- `touch /.autorelabel`

```
fermimash@fermimash ~]$ su -
Password:
su: Authentication failure
fermimash@fermimash ~]$ su -
Password:
[root@fermimash ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@fermimash ~]# cp /etc/hosts ~/
[root@fermimash ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@fermimash ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
[root@fermimash ~]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@fermimash ~]# 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@fermimash ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@fermimash ~]# touch /.autorelabel
[root@fermimash ~]#
```

Рис. 2.6: Использование restorecon

3. Настройка контекста безопасности для нестандартного расположения файлов веб-сервера Запустите терминал и получите полномочия администратора. Установите необходимое программное обеспечение: (рис. 2.7)

- `dnf -y install httpd`



- `dnf -y install lynx` Создайте новое хранилище для файлов web-сервера: (рис. 2.7)
- `mkdir /web` Создайте файл `index.html` в каталоге с контентом веб-сервера: (рис. 2.7)
- `cd /web`
- `touch index.html` и поместите в файл следующий текст “Welcome to my web-server”

```
[ermimash@ermimash ~]$ su -
Password:
[root@ermimash ~]# dnf -y install httpd
Rocky Linux 9 - BaseOS                               5.2 kB/s | 4.1 kB  00:00
Rocky Linux 9 - BaseOS                               2.4 MB/s | 2.5 MB  00:01
Rocky Linux 9 - AppStream                             3.0 kB/s | 4.5 kB  00:01
Rocky Linux 9 - AppStream                             6.1 MB/s | 9.5 MB  00:01
Rocky Linux 9 - Extras                                6.9 kB/s | 2.9 kB  00:00
Package httpd-2.4.62-4.el9_6.4.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@ermimash ~]# dnf -y install lynx
Last metadata expiration check: 0:00:18 ago on Fri 31 Oct 2025 11:11:58 AM MSK.
Dependencies resolved.
=====
Package                Architecture      Version           Repository        Size
=====
Installing:
lynx                   x86_64            2.8.9-20.el9     appstream         1.5 M
=====
Transaction Summary
=====
Install 1 Package

Total download size: 1.5 M
Installed size: 6.1 M
Downloading Packages:
lynx-2.8.9-20.el9.x86_64.rpm                                3.1 MB/s | 1.5 MB  00:00
-----
Total                                                                1.9 MB/s | 1.5 MB  00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      : 1/1
  Installing     : lynx-2.8.9-20.el9.x86_64 1/1
  Running scriptlet: lynx-2.8.9-20.el9.x86_64 1/1
  Verifying      : lynx-2.8.9-20.el9.x86_64 1/1
Installed:
  lynx-2.8.9-20.el9.x86_64
Complete!
[root@ermimash ~]# mkdir /web
[root@ermimash ~]# cd /web
[root@ermimash web]# touch index.html
```

Рис. 2.7: Установка прог. обеспеч.

В файле `/etc/httpd/conf/httpd.conf` закомментируйте строку `DocumentRoot "/var/www/html"` и ниже добавьте строку `"DocumentRoot"/web"` (рис. 2.8) Затем в этом же файле ниже закомментируйте раздел: (рис. 2.8) `<Directory "/var/www"> AllowOverride None Require all granted` и добавьте следующий раздел, определяющий правила доступа: (рис. 2.8) `<Directory "/web"> AllowOverride None Require all granted`

```
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>
```

Рис. 2.8: Редакция текстового файла

Запустите веб-сервер и службу httpd: (рис. 2.10) - `systemctl start httpd - systemctl enable httpd` В терминале под учётной записью своего пользователя при обращении к веб-серверу в текстовом браузере lynx: (рис. 2.9) - `lynx http://localhost`

```
HTTP Server Test Page HTTP Server Test Page powered by: Rocky Linux

This page is used to test the proper operation of an HTTP server after it has been installed on a Rocky Linux
system. If you can read this page, it means that the software is working correctly.

Just visiting?

This website you are visiting is either experiencing problems or could be going through maintenance.

If you would like the let the administrators of this website know that you've seen this page instead of the
page you've expected, you should send them an email. In general, mail sent to the name "webmaster" and
directed to the website's domain should reach the appropriate person.

The most common email address to send to is: "webmaster@example.com"

Note:

The Rocky Linux distribution is a stable and reproducible platform based on the sources of Red Hat
Enterprise Linux (RHEL). With this in mind, please understand that:
  * Neither the Rocky Linux Project nor the Rocky Enterprise Software Foundation have anything to do with
    this website or its content.
  * The Rocky Linux Project nor the RESF have "hacked" this webserver: This test page is included with the
    distribution.

For more information about Rocky Linux, please visit the Rocky Linux website.

I am the admin, what do I do?

You may now add content to the webroot directory for your software.

For systems using the Apache Webserver: You can add content to the directory /var/www/html/. Until you do so,
people visiting your website will see this page. If you would like this page to not be shown, follow the
instructions in: /etc/httpd/conf.d/welcome.conf.

For systems using Nginx: You can add your content in a location of your choice and edit the root
configuration directive in /etc/nginx/nginx.conf.

[ Powered by Rocky Linux ] [ poweredby.png ]

Apache® is a registered trademark of the Apache Software Foundation in the United States and/or other
countries.
NGINX™ is a registered trademark of F5 Networks, Inc..
```

Рис. 2.9: Первый запуск сайта

В терминале с полномочиями администратора примените новую метку контекста к /web: (рис. 2.10) - `semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"` Восстановите контекст безопасности: (рис. 2.10) - `restorecon -R -v /web`

```
[root@ermimash web]# nano index.html
[root@ermimash web]# nano /etc/httpd/conf/httpd.conf
[root@ermimash web]# systemctl start httpd
[root@ermimash web]# systemctl enable httpd
[root@ermimash web]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
[root@ermimash web]# restorecon -R -v /web\
> ^C
[root@ermimash web]# restorecon -R -v /web
```

Рис. 2.10: Восстановка контекста безопасности

В терминале под учётной записью своего пользователя снова обратитесь к веб-серверу: (рис. 2.11) - lynx <http://localhost>

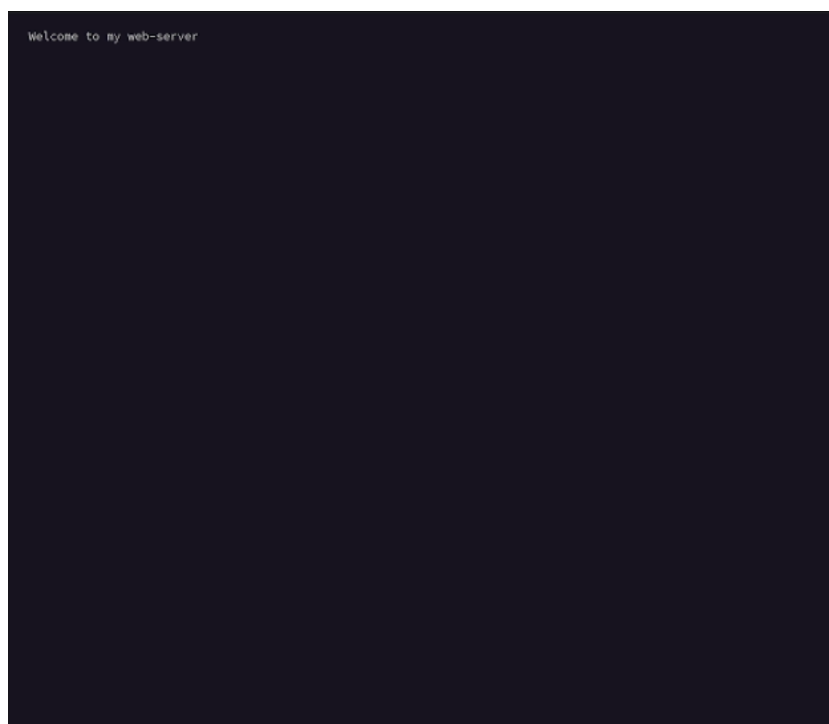


Рис. 2.11: Второй запуск

4. Работа с переключателями SELinux Запустите терминал и получите полномочия администратора. Посмотрите список переключателей SELinux для службы ftp:
  - `getsebool -a | grep ftp` Для службы `ftpd_anon` посмотрите список переключателей с пояснением, за что отвечает каждый переключатель, включён он или выключен:
  - `semanage boolean -l | grep ftpd_anon` Измените текущее значение переключателя для службы `ftpd_anon_write` с `off` на `on`:

- `setsebool ftpd_anon_write on` Повторно посмотрите список переключателей SELinux для службы `ftpd_anon_write`:
- `getsebool ftpd_anon_write` Посмотрите список переключателей с пояснением:
- `semanage boolean -l | grep ftpd_anon` Измените постоянное значение переключателя для службы `ftpd_anon_write` с `off` на `on`:
- `setsebool -P ftpd_anon_write on` Посмотрите список переключателей:
- `semanage boolean -l | grep ftpd_anon`

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

Рис. 2.12: Работа с переключателями SELinux

### 3 Контрольные вопросы

1. `setenforce 0`
2. `getsebool -a`
3. `audit2allow`
4. `semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?" restorecon -R -v /web`
5. `/etc/sysconfig/selinux`
6. По умолчанию в `/var/log/audit/audit.log`
7. `getsebool -a | grep ftp`
8. Просмотреть контекст безопасности процессора `ps -eZ` или `id -Z`

## 4 Выводы

Получены навыки работы с контекстом безопасности и политиками SELinux.