

# **Лабораторная работа №9**

**Управление SELinux**

Хохлачёва Полина Дмитриевна

# 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>Ответы на вопросы</b>	<b>12</b>
<b>4</b>	<b>Выводы</b>	<b>13</b>

# Список иллюстраций

2.1	Просмотр,изменения . . . . .	6
2.2	Установка . . . . .	7
2.3	Посматриваем,исправляем, убеждаемся . . . . .	7
2.4	Устанавливаем . . . . .	8
2.5	Создаём . . . . .	8
2.6	Помещаем . . . . .	8
2.7	Запускаем . . . . .	9
2.8	Комментируем, добавляем . . . . .	10
2.9	Обращаемся . . . . .	10
2.10	Смотрим, изменяем . . . . .	11

## **Список таблиц**

# 1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

## 2 Выполнение лабораторной работы

Получаем полномочия администратора, смотрим текущую информацию о состоянии, изменение режим работы(рис. 2.1).

```
[khokhlacheva@khokhlacheva ~]$ su -
Пароль:
[root@khokhlacheva ~]# 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@khokhlacheva ~]# getenforce
Enforcing
[root@khokhlacheva ~]# setenforce 0
[root@khokhlacheva ~]# getenforce
Permissive
[root@khokhlacheva ~]# nano /etc/sysconfig/selinux
[root@khokhlacheva ~]#
```

Рис. 2.1: Просмотр,изменения

Установка с помощью редактора(рис. 2.2).

```
GNU nano 5.6.1 /etc/sysconfig/selinux
# 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://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html>
#
# NOTE: Up to RHEL 8 release included, 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 pr
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Рис. 2.2: Установка

Получаем полномочия администратора, просматриваем контекст безопасности файла, копируем файл в домашний каталог, переписываем существенный файл, исправляем контекст безопасности, убеждаемся в этом (рис. 2.3).

```
[khokhlacheva@khokhlacheva ~]$ su -
Пароль:
[root@khokhlacheva ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@khokhlacheva ~]# cp /etc/hosts ~/
[root@khokhlacheva ~]# ls -Z ~/hosts
? /root/hosts
[root@khokhlacheva ~]# mv ~/hosts /etc
mv: переписать '/etc/hosts'?
[root@khokhlacheva ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@khokhlacheva ~]# restorecon -v /etc/hosts
[root@khokhlacheva ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@khokhlacheva ~]# touch /.autorelabel
```

Рис. 2.3: Посматриваем, исправляем, убеждаемся

Устанавливаем необходимое программное обеспечение (рис. 2.4).

```
[khokhlacheva@khokhlacheva ~]$ su -
Пароль:
[root@khokhlacheva ~]# dnf -y install httpd
Rocky Linux 9 - BaseOS                8.8 kB/s | 4.1 kB    00:00
Rocky Linux 9 - BaseOS                999 kB/s | 2.5 MB    00:02
Rocky Linux 9 - AppStream             13 kB/s | 4.5 kB     00:00
Rocky Linux 9 - AppStream             2.2 MB/s | 9.5 MB    00:04
Rocky Linux 9 - Extras                8.7 kB/s | 2.9 kB     00:00
Пакет httpd-2.4.62-4.el9_6.4.x86_64 уже установлен.
Зависимости разрешены.
Отсутствуют действия для выполнения.
Выполнено!
[root@khokhlacheva ~]# dnf -y install lynx
Последняя проверка окончания срока действия метаданных: 0:00:17 назад, Пт 31 окт
2025 23:29:33.
Зависимости разрешены.
=====
Пакет      Архитектура  Версия      Репозиторий  Размер
=====
Установка:
lynx      x86_64      2.8.9-20.el9      appstream    1.5 M
=====
Результат транзакции
=====
Установка 1 Пакет

Объем загрузки: 1.5 M
Объем изменений: 6.1 M
Загрузка пакетов:
lynx-2.8.9-20.el9.x86_64.rpm                2.0 MB/s | 1.5 MB    00:00
-----
Общий размер                                1.3 MB/s | 1.5 MB    00:01
Проверка транзакции
Проверка транзакции успешно завершена.
Идет проверка транзакции
Тест транзакции проведен успешно.
Выполнение транзакции
Подготовка      : 1/1
Установка      : lynx-2.8.9-20.el9.x86_64 1/1
Запуск скрипта : lynx-2.8.9-20.el9.x86_64 1/1
Проверка       : lynx-2.8.9-20.el9.x86_64 1/1
```

Рис. 2.4: Устанавливаем

Создаём новое хранилище, создаём файл в каталоге с контентом веб-сервера(рис. 2.5).

```
oot@khokhlacheva ~]$ mkdir /web
oot@khokhlacheva ~]$ cd /web
oot@khokhlacheva web]$ touch index.html
```

Рис. 2.5: Создаём

Помещаем следующий текст(рис. 2.6).

```
oot@khokhlacheva web]$ systemctl start httpd
oot@khokhlacheva web]$ systemctl enable httpd
oot@khokhlacheva web]$ su khokhlacheva
khokhlacheva@khokhlacheva web]$ lynx http://localhost
```

Рис. 2.6: Помещаем



Запускаем веб-сервер(рис. 2.7).

```
#  
#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:
```

Рис. 2.7: Запускаем

Комментируем строки и добавляем следующие отделы(рис. 2.8).

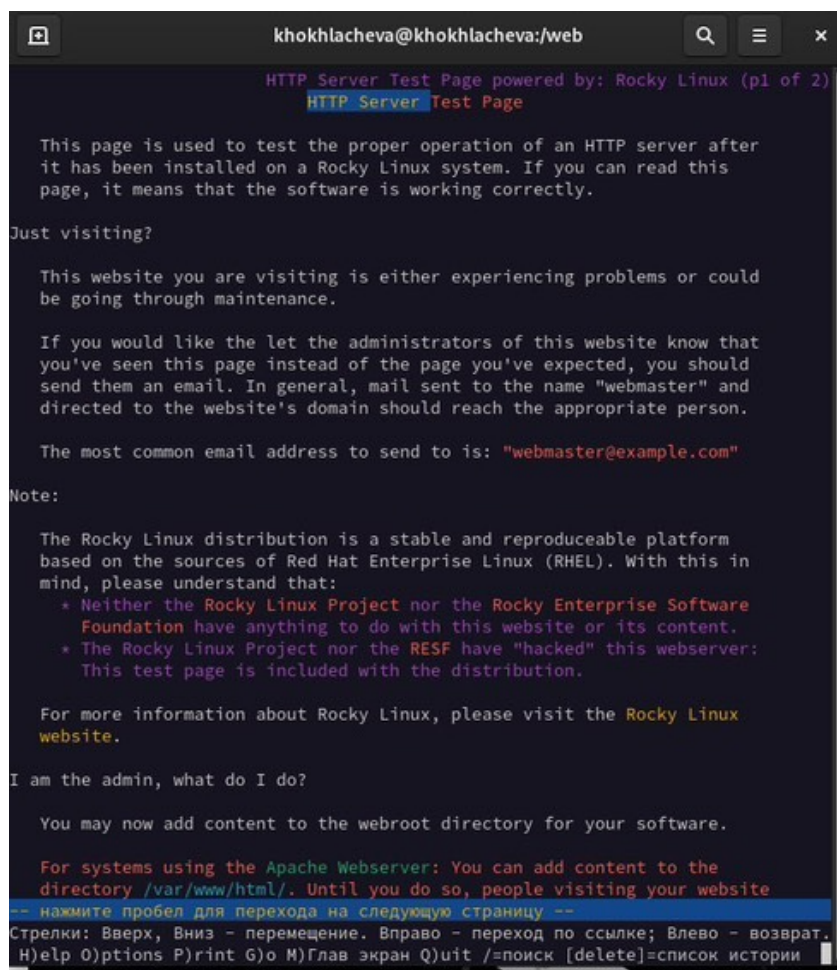


Рис. 2.8: Комментируем, добавляем

Снова обращаемся к веб-серверу(рис. 2.9).

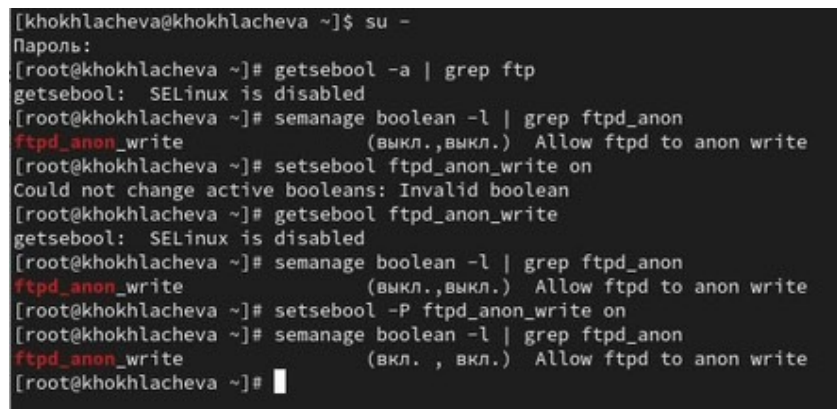


Рис. 2.9: Обращаемся

Получаем полномочия администратора, смотрим список переключателей, изменяем текущее значение переключателя для службы, повторно смотрим список, изменяем постоянное значение и снова смотрим список(рис. 2.10).

```
[khokhlacheva@khokhlacheva ~]$ su -
Пароль:
[root@khokhlacheva ~]# getsebool -a | grep ftp
getsebool: SELinux is disabled
[root@khokhlacheva ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (выкл.,выкл.) Allow ftpd to anon write
[root@khokhlacheva ~]# setsebool ftpd_anon_write on
Could not change active booleans: Invalid boolean
[root@khokhlacheva ~]# getsebool ftpd_anon_write
getsebool: SELinux is disabled
[root@khokhlacheva ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (выкл.,выкл.) Allow ftpd to anon write
[root@khokhlacheva ~]# setsebool -P ftpd_anon_write on
[root@khokhlacheva ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл. , вкл.) Allow ftpd to anon write
[root@khokhlacheva ~]#
```

Рис. 2.10: Смотрим, изменяем

## 3 Ответы на вопросы

1. `setenforce 0`
2. `getsebool -a`
3. `setroubleshoot-server` (или `setroubleshoot`)
4. `semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"` и затем `restorecon -Rv /web`
5. `/etc/selinux/config`
6. В файле `/var/log/audit/audit.log` (через службу `auditd`)
7. `semanage fcontext -l | grep ftp` (или `semanage fcontext -l -t ftp_t` для более точного поиска)
8. Временно переключить SELinux в разрешающий режим: `setenforce 0`

## 4 Выводы

Мы получили навыки работы с контекстом безопасности и политиками SELinux.