

Отчёт по лабораторной работе №9

Управление SELinux

Яковлева Дарья Сергеевна

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
2.1	Управление режимами SELinux	6
2.2	Использование restorecon для восстановления контекста безопасности	9
2.3	Настройка контекста безопасности для нестандартного расположения файлов веб-сервера	10
2.4	Работа с переключателями SELinux	13
3	Контрольные вопросы	14
4	Заключение	16

Список иллюстраций

2.1	Просмотр состояния SELinux	7
2.2	Отключение SELinux в конфигурационном файле	8
2.3	Проверка статуса SELinux после отключения	8
2.4	Включение принудительного режима SELinux	9
2.5	Восстановление контекста безопасности и создание .autorelabel . .	10
2.6	Создание каталога и файла index.html	10
2.7	Редактирование файла index.html	11
2.8	Изменение пути к DocumentRoot и настройка доступа	11
2.9	Попытка доступа к веб-странице до смены контекста	12
2.10	Отображение пользовательской веб-страницы	12
2.11	Проверка и изменение состояния переключателя ftpd_anon_write	13

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Выполнение лабораторной работы

2.1 Управление режимами SELinux

Получаю административные права с помощью команды `su -` (см. рис. [fig. 2.1]).

Проверяю текущие параметры SELinux с помощью команды `sestatus -v`.

Из вывода видно, что SELinux включён (*enabled*), используется политика *targeted*, текущий режим — *enforcing*, то есть политика безопасности принудительно применяется.

Отображаются также параметры: - **SELinuxfs mount** — точка монтирования системных файлов SELinux;

- **SELinux root directory** — путь к конфигурационным файлам SELinux;
- **Loaded policy name** — активная политика безопасности;
- **Current mode / Mode from config file** — текущий и заданный в конфигурации режим работы;
- **Policy MLS status** — включённый многоуровневый контроль безопасности;
- **Policy deny_unknown status** — реакция системы на неизвестные объекты (разрешено);
- **Memory protection checking** — защита памяти в активном состоянии;
- **Max kernel policy version** — версия политики ядра.

Также показаны контексты процессов (`unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023`) и файлов (`system_u:object_r:passwd_file_t:s0` и др.) (см. рис. [fig. 2.1]).

```
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:~#
```

Рис. 2.1: Просмотр состояния SELinux

Проверяю текущий режим работы SELinux с помощью `getenforce` — получаю значение *Enforcing*.

Переключаю SELinux в разрешающий режим (*Permissive*) командой `setenforce 0` и повторно выполняю `getenforce` — теперь режим изменён (см. рис. [fig. 2.1]).

Открываю файл `/etc/sysconfig/selinux` через текстовый редактор и изменяю строку `SELINUX=disabled`, чтобы полностью отключить SELinux (см. рис. [fig. 2.2]).

```
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

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

Рис. 2.2: Отключение SELinux в конфигурационном файле

После перезагрузки системы снова проверяю состояние SELinux с помощью `getenforce`.

Система сообщает, что SELinux отключён (*Disabled*).

Попытка выполнить `setenforce 1` не приводит к изменению состояния, так как при отключённом SELinux переключение режима невозможно (см. рис. [fig. 2.3]).

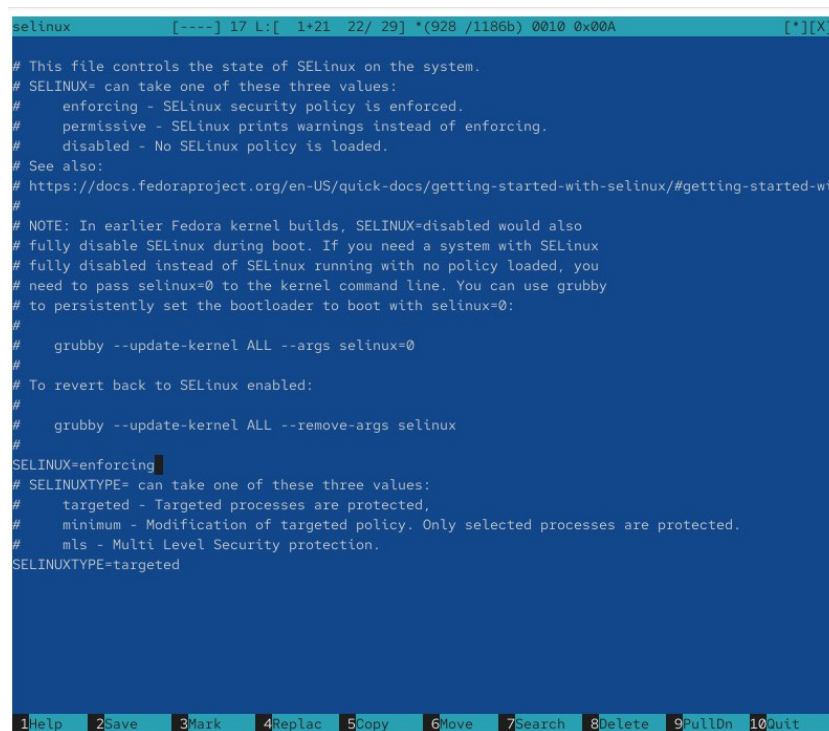
```
root@dsyakovleva:~ -- -bash

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. 2.3: Проверка статуса SELinux после отключения

Повторно открываю файл `/etc/sysconfig/selinux` и изменяю параметр обратно на `SELINUX=enforcing`, чтобы вернуть принудительный режим (см. рис. [fig. 2.4]).

После этого система требует восстановления контекстов безопасности и перезагрузки.



```
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

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

Рис. 2.4: Включение принудительного режима SELinux

После перезагрузки система сообщает о восстановлении меток SELinux.

2.2 Использование restorecon для восстановления контекста безопасности

Проверяю контекст безопасности файла /etc/hosts с помощью `ls -Z`.
Вижу, что у файла установлен тип `net_conf_t`.
Копирую файл /etc/hosts в домашний каталог и снова проверяю метку — теперь она имеет тип `admin_home_t`, поскольку копирование создаёт новый файл с контекстом домашнего каталога (см. рис. [fig. 2.5]).

Перемещаю файл обратно в /etc и проверяю контекст — тип остаётся `admin_home_t`.

Выполняю команду `restorecon -v /etc/hosts`, чтобы восстановить правильный контекст.

Тип контекста меняется обратно на `net_conf_t`, что подтверждает корректное восстановление.

Для массового исправления контекстов безопасности создаю файл `.autorelabel` и перезагружаю систему (см. рис. [fig. 2.5]).

```
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. 2.5: Восстановление контекста безопасности и создание `.autorelabel`

2.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Получаю административные права и создаю новый каталог `/web` для размещения веб-контента (см. рис. [fig. 2.6]).

Перехожу в каталог и создаю пустой файл `index.html`, который затем открываю в редакторе `mcedit` для редактирования.

```
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. 2.6: Создание каталога и файла `index.html`

В файл `index.html` добавляю строку **Welcome to my web-server** — содержимое, которое будет отображаться при обращении к локальному веб-серверу (см. рис. [fig. 2.7]).

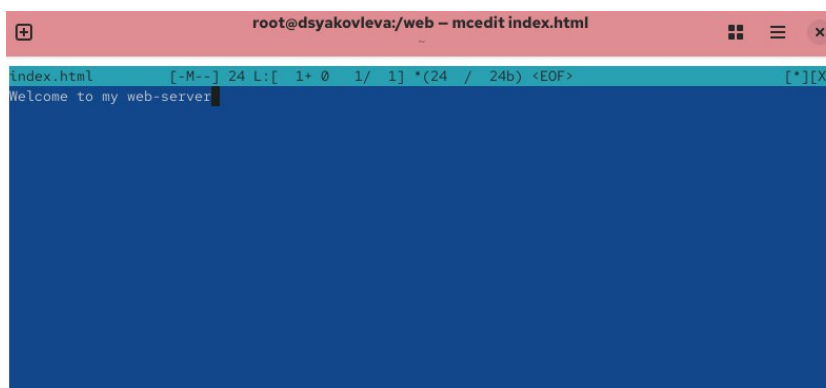


Рис. 2.7: Редактирование файла `index.html`

Редактирую конфигурационный файл `/etc/httpd/conf/httpd.conf`: (см. рис. [fig. 2.8]).

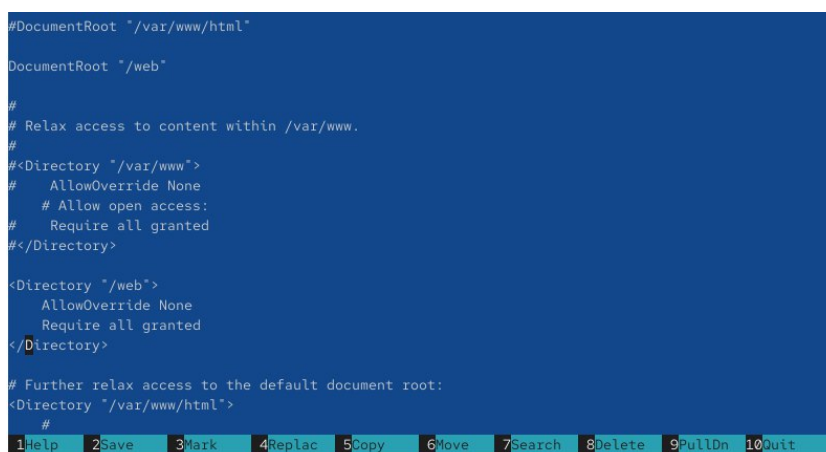


Рис. 2.8: Изменение пути к `DocumentRoot` и настройка доступа

Запускаю и активирую службу Apache с помощью команд `systemctl start httpd` и `systemctl enable httpd`.

При попытке открыть `http://localhost` через текстовый браузер lynx поначалу отображается стандартная страница Red Hat, так как у каталога `/web` отсутствует корректный контекст безопасности (см. рис. [fig. 2.9]).

```

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. 2.9: Попытка доступа к веб-странице до смены контекста

Для устранения проблемы назначаю каталогу /web контекст `httpd_sys_content_t` с помощью команды

```
semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?",
```

затем восстанавливаю контексты:

```
restorecon -R -v /web.
```

После этого повторно открываю `http://localhost` в `lynx` и вижу корректное отображение содержимого файла `index.html` с сообщением **Welcome to my web-server** (см. рис. [fig. 2.10]).

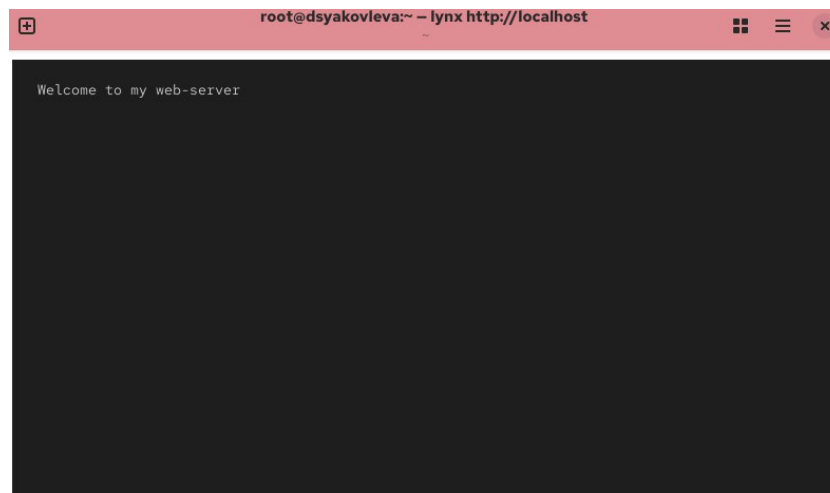


Рис. 2.10: Отображение пользовательской веб-страницы

2.4 Работа с переключателями SELinux

Получаю список переключателей SELinux, связанных с FTP-службой, с помощью `getsebool -a | grep ftp`.

Из вывода видно, что параметр `ftpd_anon_write` имеет значение *off*, то есть анонимная запись через FTP запрещена.

Просматриваю подробное описание переключателя через `semanage boolean -l | grep ftpd_anon` — он отвечает за разрешение анонимной записи на FTP-сервере (см. рис. [fig. 2.11]).

Изменяю временное значение переключателя командой `setsebool ftpd_anon_write on`,

а затем делаю изменение постоянным с помощью

`setsebool -P ftpd_anon_write on`.

После проверки видно, что настройка всё ещё имеет значение (*off, off*), что означает, что разрешение анонимной записи остаётся отключённым (см. рис. [fig. 2.11]).

```
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:~#
```

Рис. 2.11: Проверка и изменение состояния переключателя `ftpd_anon_write`

3 Контрольные вопросы

1. **Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете?**

Используется команда `setenforce 0`.

2. **Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете?**

Используется команда `getsebool -a`.

3. **Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита?**

Необходимо установить пакет `setroubleshoot`.

4. **Какие команды вам нужно выполнить, чтобы применить тип контекста `httpd_sys_content_t` к каталогу `/web`?**

Используются команды:

```
semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
```

и

```
restorecon -R -v /web.
```

5. **Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux?**

Нужно изменить файл `/etc/sysconfig/selinux`.

6. **Где SELinux регистрирует все свои сообщения?**

Сообщения SELinux записываются в журнал `/var/log/audit/audit.log`.

7. **Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию?**

Используется команда `semanage fcontext -l | grep ftp`.

8. **Ваш сервис работает не так, как ожидалось, и вы хотите узнать, связано ли это с SELinux или чем-то ещё. Какой самый простой способ узнать?**

Самый простой способ — временно перевести SELinux в разрешающий режим командой `setenforce 0` и проверить работу сервиса.

4 Заключение

В ходе лабораторной работы были изучены механизмы управления политиками безопасности SELinux.

Также изучена работа с переключателями SELinux, обеспечивающими гибкую настройку политик безопасности для различных служб.

В результате работы сформировано понимание принципов функционирования SELinux и его роли в обеспечении безопасности системы.