

# **Отчёт по лабораторной работе №9**

**Управление SELinux**

Руслан Алиев

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение</b>	<b>6</b>
2.1	Управление режимами SELinux . . . . .	6
2.2	Использование restorecon для восстановления контекста безопасности . . . . .	11
2.3	Настройка контекста безопасности для нестандартного расположения файлов веб-сервера . . . . .	12
2.4	Работа с переключателями SELinux . . . . .	15
<b>3</b>	<b>Контрольные вопросы</b>	<b>17</b>
<b>4</b>	<b>Заключение</b>	<b>19</b>

# Список иллюстраций

2.1	Вывод команды <code>sestatus -v</code> . . . . .	6
2.2	Изменение режима SELinux на Permissive . . . . .	8
2.3	Отключение SELinux в файле конфигурации . . . . .	8
2.4	Попытка изменить режим при отключённом SELinux . . . . .	9
2.5	Включение SELinux в конфигурации . . . . .	9
2.6	Автоматическое восстановление меток SELinux . . . . .	10
2.7	Проверка состояния SELinux после включения . . . . .	10
2.8	Автоматическое восстановление контекста безопасности при загрузке	11
2.9	Изменение файла конфигурации Apache . . . . .	13
2.10	Стандартная тестовая страница Apache . . . . .	14
2.11	Применение нового контекста безопасности к каталогу <code>/web</code> . . . .	14
2.12	Отображение пользовательской страницы веб-сервера . . . . .	15
2.13	Просмотр и изменение переключателя <code>ftpd_anon_write</code> . . . . .	16

## **Список таблиц**

# 1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

## 2 Выполнение

### 2.1 Управление режимами SELinux

1. Для начала был запущен терминал и получены права суперпользователя с помощью команды **su -**.

Затем выполнена команда **sestatus -v** для просмотра текущей информации о состоянии SELinux.

```
root@raliev:/home/raliev# 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@raliev:/home/raliev# getenforce
Enforcing
root@raliev:/home/raliev# setenforce 0
root@raliev:/home/raliev# getenforce
Permissive
root@raliev:/home/raliev# █
```

Рис. 2.1: Вывод команды sestatus -v

Из вывода команды видно:

- **SELinux status: enabled** — система SELinux включена.
  - **Current mode: enforcing** — включён принудительный режим, при котором политики безопасности строго соблюдаются.
  - **Mode from config file: enforcing** — данный режим также задан в конфигурационном файле.
  - **Policy MLS status: enabled** — используется многоуровневая модель безопасности (MLS).
  - **Loaded policy name: targeted** — применяется политика *targeted*, ограничивающая доступ для определённых служб.
  - В разделе *Process contexts* указаны контексты процессов, таких как `init` и `sshd`.
  - В разделе *File contexts* отображаются метки безопасности системных файлов (`/etc/passwd`, `/etc/shadow`, `/bin/bash` и др.).
2. Для проверки текущего режима SELinux введена команда **getenforce**.  
Результат показал, что режим — *Enforcing* (принудительный).
  3. С помощью команды **setenforce 0** режим SELinux был изменён на *Permissive* (разрешающий).  
После повторного выполнения команды **getenforce** система подтвердила, что теперь SELinux работает в разрешающем режиме.

```
GNU nano 8.1 /etc/sysconfig/selinux Modified
# 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-with-selinux
#
# 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
```

Рис. 2.2: Изменение режима SELinux на Permissive

4. Затем был открыт файл конфигурации `/etc/sysconfig/selinux` с помощью редактора **nano**.

Параметр **SELINUX** был изменён на `disabled`, что полностью отключает SELinux после перезагрузки системы.

```
root@raliev:/home/raliev# getenforce
Disabled
root@raliev:/home/raliev# setenforce 1
setenforce: SELinux is disabled
root@raliev:/home/raliev#
```

Рис. 2.3: Отключение SELinux в файле конфигурации

5. После перезагрузки системы команда **getenforce** показала, что SELinux отключён (*Disabled*).

Попытка включить режим принудительного исполнения (**setenforce 1**) за-



вершилась ошибкой, поскольку при полностью отключённом SELinux изменение режима невозможно без перезагрузки.

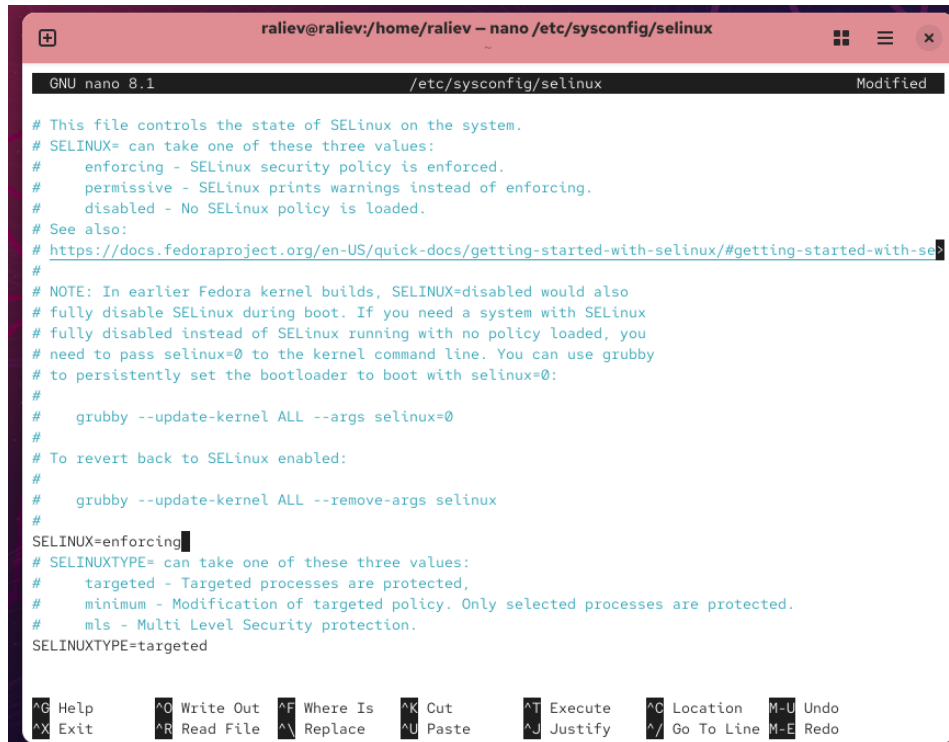


Рис. 2.4: Попытка изменить режим при отключённом SELinux

6. Для повторного включения SELinux значение параметра **SELINUX** в конфигурационном файле было изменено на **enforcing**.

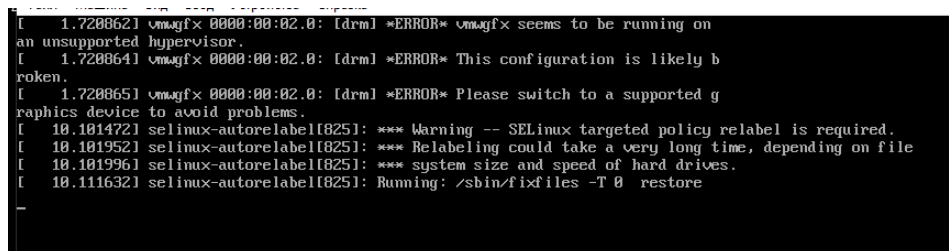


Рис. 2.5: Включение SELinux в конфигурации

7. После перезагрузки система выполнила процедуру **relabeling** — восстановление меток SELinux для всех файлов.

Процесс сопровождается предупреждением о необходимости переназначения контекстов и может занять некоторое время.

```
raliev@raliev:~$ su
Password:
root@raliev:/home/raliev# 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@raliev:/home/raliev#
```

Рис. 2.6: Автоматическое восстановление меток SELinux

8. После завершения восстановления и повторного запуска системы была снова выполнена команда **sestatus -v**.

Из вывода видно, что SELinux работает в режиме **Enforcing**.

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

Рис. 2.7: Проверка состояния SELinux после включения

## 2.2 Использование restorecon для восстановления контекста безопасности

1. Для начала были получены права суперпользователя.  
Затем с помощью команды **ls -Z /etc/hosts** был просмотрен контекст безопасности файла /etc/hosts.  
Метка контекста имела значение **net\_conf\_t**, что соответствует сетевым конфигурационным файлам.
2. Файл /etc/hosts был скопирован в домашний каталог (**cp /etc/hosts ~**), после чего его контекст изменился на **admin\_home\_t**, что характерно для файлов, созданных пользователем в домашней директории.
3. Затем файл был перемещён обратно в каталог /etc (**mv ~/hosts /etc**), и его контекст остался **admin\_home\_t**, что является некорректным для данного пути.
4. Для исправления контекста использована команда **restorecon -v /etc/hosts**.  
В результате контекст был возвращён к правильному значению **net\_conf\_t**, что подтверждает корректную работу утилиты restorecon.
5. Для массового исправления контекста безопасности на файловой системе была создана метка **/.autorelabel**, после чего выполнена перезагрузка.  
Во время загрузки система автоматически выполнила процедуру перемаркировки файловой системы.

```
[ 0.762788] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 0.762798] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 0.762793] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 7.432825] selinux-autorelabel(827): *** Warning -- SELinux targeted policy relabel is required.
[ 7.432138] selinux-autorelabel(827): *** Relabeling could take a very long time, depending on file
[ 7.432191] selinux-autorelabel(827): *** system size and speed of hard drives.
[ 7.449676] selinux-autorelabel(827): Running: zshin/files -T 0 - restore
[ 11.813732] selinux-autorelabel(834): Warning: Skipping the following R/O filesystems:
[ 11.815864] selinux-autorelabel(834): /run/credentials/systemd-journald.service
[ 11.815455] selinux-autorelabel(834): Relabeling / /boot /dev /dev/hugepages /dev/queue /dev/pts /dev/shm /run /sys /sys/fs/cgroup /sys/fs/pstore /sys/kernel
/debug /sys/kernel/tracing
```

Рис. 2.8: Автоматическое восстановление контекста безопасности при загрузке

## 2.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

1. В терминале были получены права суперпользователя и установлены необходимые пакеты **httpd** и **lynx** для развертывания и проверки работы веб-сервера.

После этого был создан каталог `/web` для размещения пользовательских веб-файлов.

2. В каталоге `/web` был создан файл **index.html** с содержимым:

*Welcome to my web-server.*

3. В конфигурационном файле Apache `/etc/httpd/conf/httpd.conf` были внесены изменения:

- строка `DocumentRoot "/var/www/html"` была закомментирована;
- добавлена новая строка `DocumentRoot "/web"`;
- добавлен блок конфигурации для каталога `/web`, разрешающий доступ к содержимому.



```
GNU nano 8.1 /etc/httpd/conf/httpd.conf
# you might expect, make sure that you have specifically enabled it
# below.
#
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
#DocumentRoot "/var/www/html"

DocumentRoot "/web"

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

#
# Relax access to content within /var/www.
#
#<Directory "/var/www">
#     AllowOverride None
```

Рис. 2.9: Изменение файла конфигурации Apache

4. После сохранения изменений служба Apache была запущена и добавлена в автозагрузку.

При первом обращении к веб-серверу через текстовый браузер **lynx** по адресу `http://localhost` отобразилась стандартная тестовая страница Apache — это указывает, что SELinux заблокировал доступ к новому каталогу `/web`.

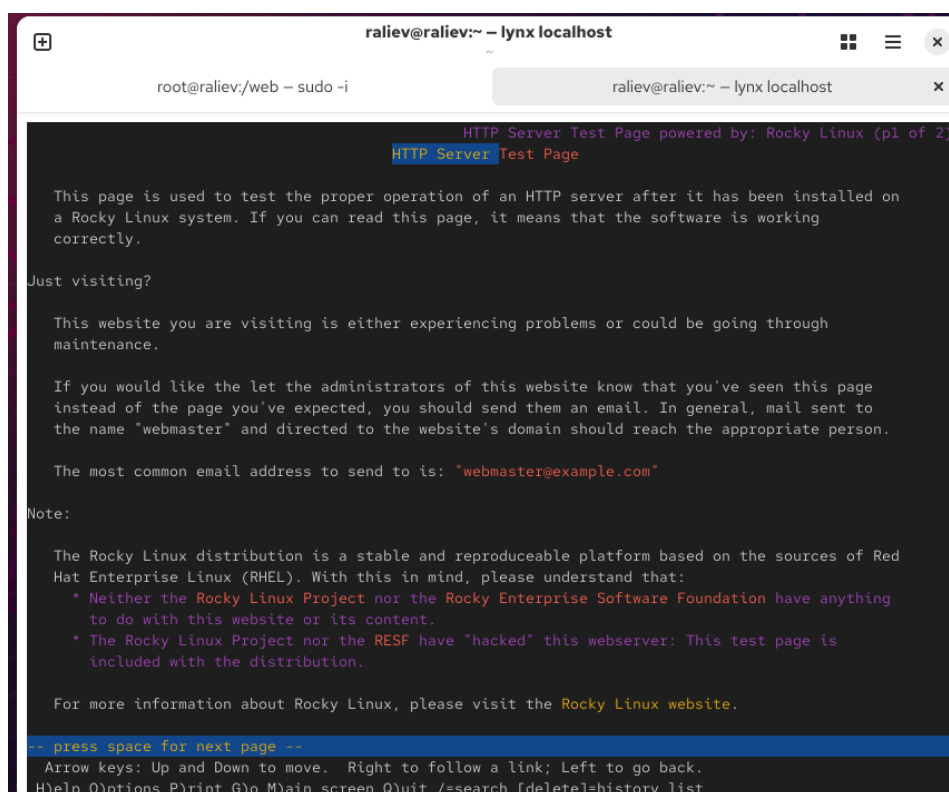


Рис. 2.10: Стандартная тестовая страница Apache

- Для корректной работы сервера в контексте безопасности SELinux был добавлен новый контекст для каталога /web:

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

Затем команда **restorecon -R -v /web** применила метки к каталогу и файлам.

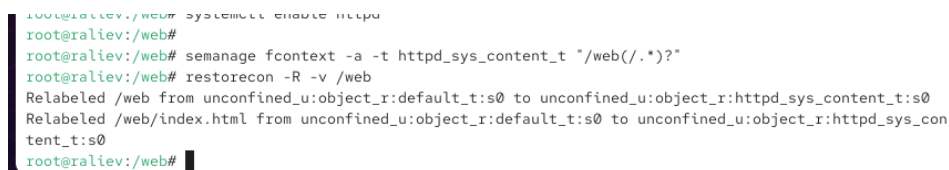


Рис. 2.11: Применение нового контекста безопасности к каталогу /web

- После обновления контекста и повторного обращения к веб-серверу через **lynx** по адресу `http://localhost` отобразилась пользовательская страница с надписью:

*Welcome to my web-server.*

Это подтвердило, что SELinux разрешает веб-серверу доступ к каталогу `/web` с правильной меткой безопасности.

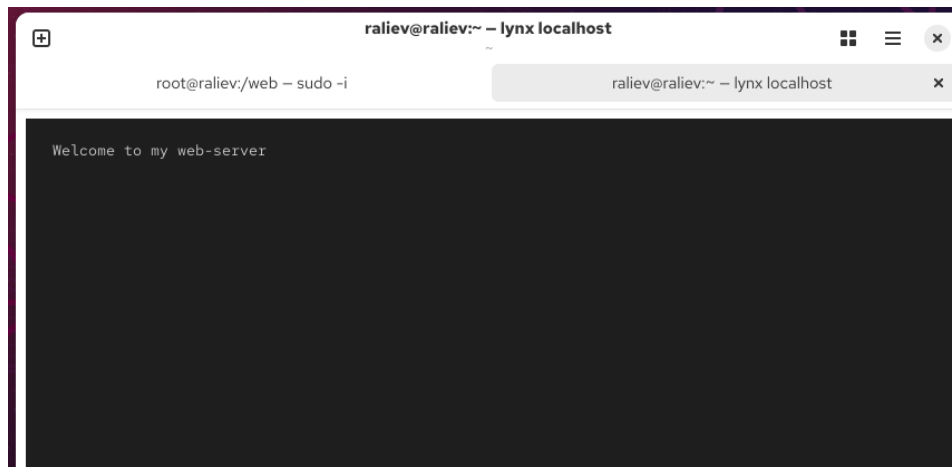


Рис. 2.12: Отображение пользовательской страницы веб-сервера

## 2.4 Работа с переключателями SELinux

1. В терминале с правами суперпользователя был просмотрен список переключателей SELinux, связанных с FTP-службой, с помощью команды:

**getsebool -a | grep ftp**

В результате обнаружен переключатель **ftpd\_anon\_write**, значение которого по умолчанию — *off*.

2. Для получения подробной информации о переключателях, связанных с анонимным доступом FTP, использована команда:

**semanage boolean -l | grep ftpd\_anon,**

которая показывает текущее состояние и назначение каждого параметра.

3. Для разрешения анонимной записи был включён переключатель **ftpd\_anon\_write**:

- временно, командой **setsebool ftpd\_anon\_write on;**

- затем — постоянно, с помощью **setsebool -P ftpd\_anon\_write on**.
4. После изменения параметров повторная проверка командой **getsebool ftpd\_anon\_write** и **semanage boolean -l | grep ftpd\_anon** показала, что оба состояния переключателя (*временное* и *постоянное*) установлены в значение **on**.

```
root@raliev:/web#
root@raliev:/web# 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@raliev:/web# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (off , off) Allow ftpd to anon write
root@raliev:/web# setsebool ftpd_anon_write on
root@raliev:/web# getsebool ftpd_anon_write
ftpd_anon_write --> on
root@raliev:/web# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (on , off) Allow ftpd to anon write
root@raliev:/web# setsebool -P ftpd_anon_write on
root@raliev:/web# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (on , on) Allow ftpd to anon write
root@raliev:/web#
```

Рис. 2.13: Просмотр и изменение переключателя ftpd\_anon\_write



## 3 Контрольные вопросы

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

`setenforce 0`

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

`getsebool -a`

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

`setroubleshoot`

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

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

`restorecon -R -v /web`

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

`/etc/sysconfig/selinux`

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

`/var/log/audit/audit.log`

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

```
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?**  
временно перевести SELinux в разрешающий режим командой **setenforce 0**  
и проверить работу сервиса

## 4 Заключение

В ходе лабораторной работы были изучены механизмы функционирования системы безопасности **SELinux** и её взаимодействие с сервисами операционной системы.

Были рассмотрены различные режимы работы SELinux — **Enforcing**, **Permissive** и **Disabled**, а также способы их переключения.

Изучены принципы настройки контекстов безопасности и восстановления меток при помощи утилит **restorecon** и **semanage**.