

# **Отчёт по лабораторной работе №9**

**Управление SELinux**

Анастасия Мазуркевич

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Ход выполнения</b>	<b>6</b>
2.1	Управление режимами SELinux . . . . .	6
2.2	Использование restorecon для восстановления контекста безопасности . . . . .	10
2.3	Настройка контекста безопасности для нестандартного расположения файлов веб-сервера . . . . .	11
2.4	Работа с переключателями SELinux . . . . .	14
<b>3</b>	<b>Контрольные вопросы</b>	<b>16</b>
<b>4</b>	<b>Заключение</b>	<b>18</b>

# Список иллюстраций

2.1	Проверка состояния SELinux . . . . .	7
2.2	Изменение конфигурации SELinux на disabled . . . . .	8
2.3	SELinux отключён . . . . .	8
2.4	Включение enforcing-режима SELinux . . . . .	9
2.5	Процесс восстановления меток SELinux при загрузке . . . . .	9
2.6	Повторная проверка статуса SELinux после включения . . . . .	10
2.7	Восстановление контекста безопасности с помощью restorecon . .	11
2.8	Автоматическое восстановление контекстов SELinux при загрузке	11
2.9	Создание каталога и файла index.html . . . . .	12
2.10	Изменение DocumentRoot и правил доступа . . . . .	12
2.11	Тестовая страница Apache по умолчанию . . . . .	13
2.12	Назначение и восстановление контекста безопасности для /web . .	13
2.13	Проверка веб-страницы после настройки контекста SELinux . . . .	14
2.14	Настройка переключателя ftpd_anon_write . . . . .	15

## **Список таблиц**

# 1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

## 2 Ход выполнения

### 2.1 Управление режимами SELinux

После входа в систему были получены права администратора с помощью команды `su -`.

Для проверки состояния SELinux использована команда `sestatus -v`.

Вывод показал, что SELinux **включён (enabled)**, политика — **targeted**, режим работы — **enforcing**.

Это означает, что система применяет политику безопасности к большинству процессов.

В отчёте также отображены контексты безопасности для процессов (Init, sshd) и системных файлов, включая `/etc/passwd`, `/etc/shadow`, `/bin/bash` и другие.

```

root@admazurkevich:/home/admazurkevich#
root@admazurkevich:/home/admazurkevich# 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@admazurkevich:/home/admazurkevich# getenforce
Enforcing
root@admazurkevich:/home/admazurkevich# setenforce 0
root@admazurkevich:/home/admazurkevich# getenforce
Permissive
root@admazurkevich:/home/admazurkevich#
root@admazurkevich:/home/admazurkevich# mcedit /etc/sysconfig/selinux
root@admazurkevich:/home/admazurkevich# █

```

Рис. 2.1: Проверка состояния SELinux

Команда `getenforce` подтвердила режим **Enforcing** — принудительное применение правил безопасности.

Далее режим SELinux был временно изменён на **Permissive** командой `setenforce 0`, что позволило регистрировать нарушения без их блокировки.

Повторная проверка через `getenforce` показала, что изменения вступили в силу.

В файле `/etc/sysconfig/selinux` значение параметра `SELINUX` было изменено на `disabled`, что полностью отключает SELinux после перезагрузки.

```
selinux [~M--] 16 L:[ 1+21 22/ 30] *(927 /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-with-selinux-selinux-states-and-
#
# 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
# SELINUX* 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.
SELINUX=disabled
```

Рис. 2.2: Изменение конфигурации SELinux на disabled

После перезагрузки команда `getenforce` показала, что SELinux теперь **отключён**.

Попытка вернуть режим с помощью `setenforce 1` завершилась сообщением о невозможности включения SELinux без перезагрузки, так как он был отключён на уровне конфигурации.

```
admazurkevich@admazurkevich:~$ su
Password:
root@admazurkevich:/home/admazurkevich# getenforce
Disabled
root@admazurkevich:/home/admazurkevich# setenforce 1
setenforce: SELinux is disabled
root@admazurkevich:/home/admazurkevich#
```

Рис. 2.3: SELinux отключён

Для повторного включения SELinux параметр SELINUX был изменён на `enforcing`.



```
selinux [~M~] 17 L:[ 1+21 22/ 30] *(928 /1187b) 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-with-selinux-selinux-states-and-
#
# 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
```

Рис. 2.4: Включение enforcing-режима SELinux

Во время загрузки система выдала предупреждение о необходимости восстановления меток безопасности, после чего начался процесс **relabeling** — переназначения контекстов безопасности.

```
Booting 'Rocky Linux (6.12.0-55.12.1.el10_0.x86_64) 10.0 (Red Quartz)'
```

```
[ 0.761348] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 0.761350] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 0.761359] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 4.099756] selinux-autorelabel[826]: *** Warning -- SELinux targeted policy relabel is required.
[ 4.099858] selinux-autorelabel[826]: *** Relabeling could take a very long time, depending on file
[ 4.099880] selinux-autorelabel[826]: *** system size and speed of hard drives.
[ 4.102420] selinux-autorelabel[826]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 2.5: Процесс восстановления меток SELinux при загрузке

После завершения загрузки повторная проверка командой `sestatus -v` показала, что SELinux снова работает в режиме **enforcing**, а политика безопасности успешно загружена.

```

admazurkevich@admazurkevich:~$ su
Password:
root@admazurkevich:/home/admazurkevich# 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@admazurkevich:/home/admazurkevich#

```

Рис. 2.6: Повторная проверка статуса SELinux после включения

## 2.2 Использование restorecon для восстановления контекста безопасности

Была проверена метка безопасности файла `/etc/hosts` с помощью `ls -Z /etc/hosts`.

Тип контекста имел значение **net\_conf\_t**, что соответствует системным сетевым конфигурационным файлам.

Далее файл `/etc/hosts` был скопирован в домашний каталог.

При проверке команды `ls -Z ~/hosts` стало видно, что копия получила контекст **admin\_home\_t**, так как была создана в пользовательской директории.

Затем файл из домашнего каталога был перемещён обратно в `/etc` с перезаписью оригинала.

После этого контекст остался прежним — **admin\_home\_t**, что не соответствует политике SELinux.

Для восстановления корректного контекста использовалась команда `restorecon -v /etc/hosts`.

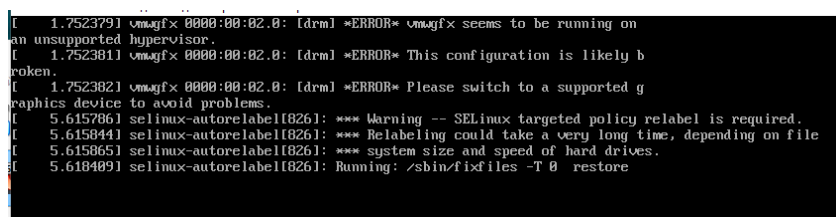
SELinux автоматически изменил метку безопасности на **net\_conf\_t**, соответствующую системному каталогу **/etc**.

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

Рис. 2.7: Восстановление контекста безопасности с помощью **restorecon**

Для массового восстановления всех контекстов безопасности в системе был создан файл **.autorelabel** командой **touch /.autorelabel**.

После перезагрузки система провела автоматическую процедуру **перемаркировки** всех файлов.



```
[ 1.752379] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 1.752381] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 1.752382] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 5.615786] selinux-autorelabel(826): *** Warning -- SELinux targeted policy relabel is required.
[ 5.615844] selinux-autorelabel(826): *** Relabeling could take a very long time, depending on file
[ 5.615865] selinux-autorelabel(826): *** system size and speed of hard drives.
[ 5.618499] selinux-autorelabel(826): Running: /sbin/fixfiles -T 0 restore
```

Рис. 2.8: Автоматическое восстановление контекстов SELinux при загрузке

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

После входа в систему были получены права администратора. Для установки необходимого ПО выполнена установка пакетов **httpd** и **lynx**, необходимых для запуска веб-сервера Apache и проверки его работы через текстовый браузер.

Создан новый каталог для веб-контента `/web`, в который был добавлен файл `index.html` с текстом «Welcome to my web-server».

```
Installed:
  lynx-2.9.0-6.el10.x86_64

Complete!
root@admazurkevich:/home/admazurkevich#
root@admazurkevich:/home/admazurkevich# mkdir /web
root@admazurkevich:/home/admazurkevich# cd /web
root@admazurkevich:/web# touch index.html
root@admazurkevich:/web# echo "Welcome to my web-server" > index.html
root@admazurkevich:/web#
```

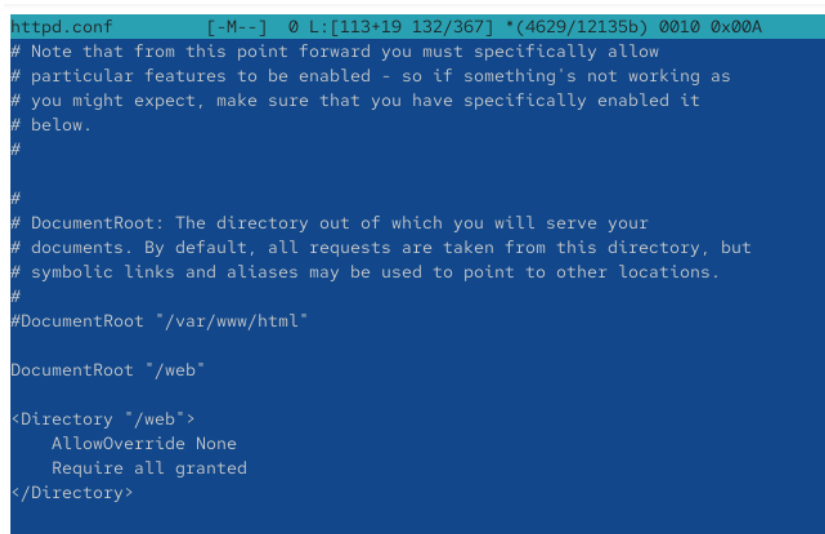
Рис. 2.9: Создание каталога и файла `index.html`

В конфигурационном файле `/etc/httpd/conf/httpd.conf` закомментирована стандартная строка

`DocumentRoot "/var/www/html"` и добавлена новая — `DocumentRoot "/web"`.

Также был изменён раздел доступа.

Эти изменения позволяют серверу Apache использовать новый каталог как корневой для веб-документов.



```
httpd.conf [-M--] 0 L:[113+19 132/367] *(4629/12135b) 0010 0x00A
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# 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>
```

Рис. 2.10: Изменение `DocumentRoot` и правил доступа

После запуска службы `httpd` командами `systemctl start httpd` и `systemctl enable httpd`, при обращении к веб-серверу через `lynx http://localhost` отобразилась стандартная страница Rocky Linux, что свидетельствует о некорректных

правах SELinux для нового каталога.

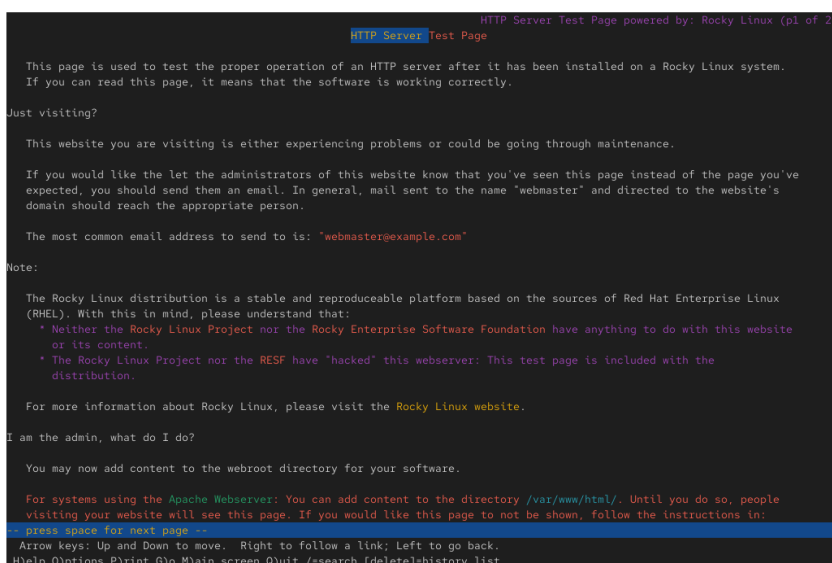


Рис. 2.11: Тестовая страница Apache по умолчанию

Для разрешения доступа Apache к каталогу `/web` была создана новая метка контекста безопасности.

Команда `semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"` назначила каталогу и его содержимому тип `httpd_sys_content_t`.

Далее команда `restorecon -R -v /web` применила эту метку на практике.

```
root@admazurkevich:/web#
root@admazurkevich:/web# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
root@admazurkevich:/web# 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@admazurkevich:/web#
```

Рис. 2.12: Назначение и восстановление контекста безопасности для `/web`

После этого при повторном обращении к `http://localhost` в браузере **lynx** отобразилась пользовательская страница с текстом «**Welcome to my web-server**», что подтверждает корректную настройку SELinux и Apache.

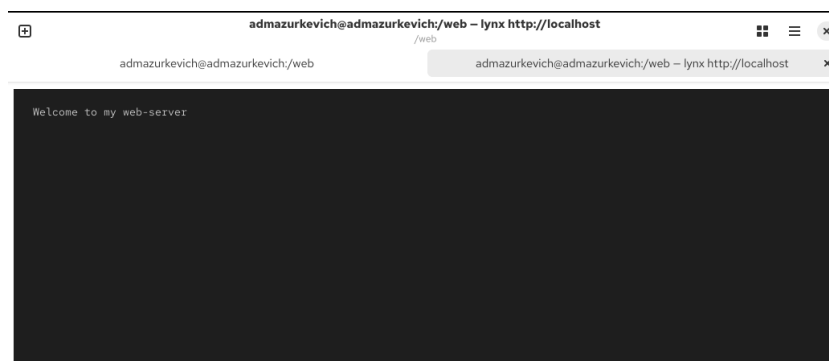


Рис. 2.13: Проверка веб-страницы после настройки контекста SELinux

## 2.4 Работа с переключателями SELinux

Для управления поведением SELinux относительно служб FTP была проведена настройка переключателей (boolean-параметров).

Команда `getsebool -a | grep ftp` показала список параметров, связанных с FTP, включая `ftpd_anon_write`, значение которого по умолчанию — **off**.

Далее с помощью `semanage boolean -l | grep ftpd_anon` были получены пояснения по назначению этих параметров.

Затем параметр `ftpd_anon_write` был активирован командой `setsebool ftpd_anon_write on`, что изменило состояние на уровне выполнения.

Команда `getsebool ftpd_anon_write` подтвердила его включение.

Однако при повторной проверке через `semanage boolean -l` было видно, что настройка активна только временно.

Для постоянного включения параметра применена команда `setsebool -P ftpd_anon_write on`.

Повторная проверка показала, что теперь `ftpd_anon_write` включён как во времени выполнения, так и в постоянной конфигурации.

```

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

```

Рис. 2.14: Настройка переключателя ftpd\_anon\_write

Параметр ftpd\_anon\_write имеет значение **on (on, on)**, что означает — разрешена анонимная запись для службы FTP как временно, так и на постоянной основе.

## 3 Контрольные вопросы

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

Для временного перевода SELinux в режим **Permissive** применяется команда:

```
setenforce 0
```

Чтобы вернуть принудительный режим (**Enforcing**), используется команда:

```
setenforce 1.
```

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

Для просмотра всех доступных переключателей (boolean-параметров) SELinux используется команда:

```
getsebool -a.
```

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

Для анализа сообщений SELinux в удобочитаемом виде необходимо установить пакет:

```
setroubleshoot.
```

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

Применяются две команды:

1. Назначение нового типа контекста:

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

2. Применение изменений:



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

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

Для полного отключения SELinux редактируется файл конфигурации:

```
/etc/sysconfig/selinux,
```

в котором параметр SELINUX устанавливается в значение disabled.

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

Журнал SELinux хранится в файле:

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

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

Чтобы узнать доступные типы контекстов и настройки для службы FTP, используется команда:

```
semanage fcontext -l | grep ftp
```

или для переключателей:

```
semanage boolean -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.
```

Если после этого служба начинает работать корректно, значит, проблема была вызвана политиками SELinux.

## 4 Заключение

В ходе лабораторной работы были изучены и practically применены основные механизмы управления системой безопасности SELinux в Linux.

Выполнены операции по изменению режимов работы SELinux (Enforcing, Permissive, Disabled), редактированию конфигурационного файла `/etc/sysconfig/selinux`, а также проверке состояния системы с помощью команд `sestatus` и `getenforce`. Освоены методы восстановления контекстов безопасности командой `restorecon` и массовой перемаркировки файлов через `.autorelabel`.

Проведена настройка контекста безопасности для нестандартного каталога веб-сервера и работа с переключателями SELinux, управляющими поведением служб (например, `ftpd_anon_write`).