

Отчёт по лабораторной работе №9

Управление SELinux

Шаханеоядж Хаоладар

Содержание

1	Цель работы	5
2	Выполнение	6
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	12
2.4	Работа с переключателями SELinux	14
3	Контрольные вопросы	16
4	Заключение	18

Список иллюстраций

2.1	Вывод команды <code>sestatus -v</code>	7
2.2	Переключение режима SELinux в Permissive	8
2.3	Редактирование файла <code>/etc/sysconfig/selinux</code> — отключение SELinux	8
2.4	Проверка отключения SELinux	9
2.5	Сообщение о необходимости relabeling при загрузке	9
2.6	Повторная проверка SELinux после relabeling	10
2.7	Использование <code>restorecon</code> и подготовка к relabeling	11
2.8	Процесс relabeling SELinux при загрузке	11
2.9	Изменение DocumentRoot и настроек каталога в файле конфигурации Apache	12
2.10	Страница Apache по умолчанию при первом запуске	13
2.11	Применение нового контекста безопасности к каталогу <code>/web</code>	13
2.12	Отображение пользовательской страницы веб-сервера	14
2.13	Просмотр и изменение переключателей SELinux для службы FTP	15

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Выполнение

2.1 Управление режимами SELinux

1. Сначала был запущен терминал и получены полномочия администратора с помощью команды **su -**.

После этого проверен текущий статус SELinux командой **sestatus -v**.

На экране отображены подробные сведения о политике безопасности:

- **SELinux status: enabled** — система SELinux включена;
- **Loaded policy name: targeted** — используется целевая политика, при которой защита применяется только к определённым процессам;
- **Current mode: enforcing** — включён режим принудительного контроля доступа;
- **Policy MLS status: enabled** — активирована многоуровневая защита (MLS).

```

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

```

Рис. 2.1: Вывод команды sestatus -v

2. Для уточнения текущего режима работы SELinux введена команда **getenforce**.

Вывод **Enforcing** подтверждает, что система работает в режиме строгого применения политик.

3. Для переключения SELinux в разрешающий режим (Permissive) использовалась команда **setenforce 0**,

после чего повторная проверка (**getenforce**) показала состояние **Permissive**.

В этом режиме нарушения фиксируются, но не блокируются.

```
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
#
# 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: Переключение режима SELinux в Permissive

- Далее открыт файл конфигурации `/etc/sysconfig/selinux` и параметр **SELINUX** изменён на значение **disabled**, что полностью отключает SELinux после перезагрузки.

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

Рис. 2.3: Редактирование файла `/etc/sysconfig/selinux` — отключение SELinux

- После перезагрузки выполнена проверка состояния SELinux командой **getenforce** — система сообщила, что SELinux **Disabled**. Попытка включить SELinux через **setenforce 1** завершилась сообщением: «*SELinux is disabled*», что подтверждает невозможность динамического включения без перезагрузки.


```
selinux [~M--] 17 L:[ 4+18 22/ 30] *(928 /1187b) 0010 0x00A [*][X]
# 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=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: Проверка отключения SELinux

6. Затем в том же конфигурационном файле значение **SELINUX** было изменено обратно на **enforcing**.

После перезагрузки система выдала предупреждение о необходимости восстановления меток безопасности (relabeling).

```
[ 1.996862] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 1.996863] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 1.996864] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 6.479801] selinux-autorelabel[831]: *** Warning -- SELinux targeted policy relabel is required.
[ 6.479857] selinux-autorelabel[831]: *** Relabeling could take a very long time, depending on file
[ 6.479890] selinux-autorelabel[831]: *** system size and speed of hard drives.
[ 6.482279] selinux-autorelabel[831]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 2.5: Сообщение о необходимости relabeling при загрузке

7. После завершения relabeling и перезапуска команда **sestatus -v** вновь показала, что SELinux включён и работает в режиме **enforcing**.

```

root@haoladar:/home/haoladar# 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@haoladar:/home/haoladar#

```

Рис. 2.6: Повторная проверка SELinux после relabeling

2.2 Использование restorecon для восстановления контекста безопасности

1. Для начала был выполнен переход в режим суперпользователя.
Затем проверен контекст безопасности файла `/etc/hosts` командой **ls -Z /etc/hosts** —
он имел тип **net_conf_t**, соответствующий сетевым конфигурационным файлам.
2. Файл `/etc/hosts` был скопирован в домашний каталог (**cp /etc/hosts ~/**).
После проверки контекста нового файла (**ls -Z ~/hosts**)
видно, что тип контекста изменился на **admin_home_t**, так как копирование создало новый объект.
3. При перемещении файла обратно в `/etc` (**mv ~/hosts /etc**)
контекст остался прежним — **admin_home_t**, что не соответствует назначению файла.

4. Для восстановления корректного контекста была применена команда **restorecon -v /etc/hosts**, которая изменила тип обратно на **net_conf_t**.

5. Проверка (**ls -Z /etc/hosts**) подтвердила правильное восстановление контекста.

Затем была создана метка **.autorelabel** (**touch /.autorelabel**),

чтобы при следующей перезагрузке система выполнила массовое восстановление контекстов безопасности.

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

Рис. 2.7: Использование restorecon и подготовка к relabeling

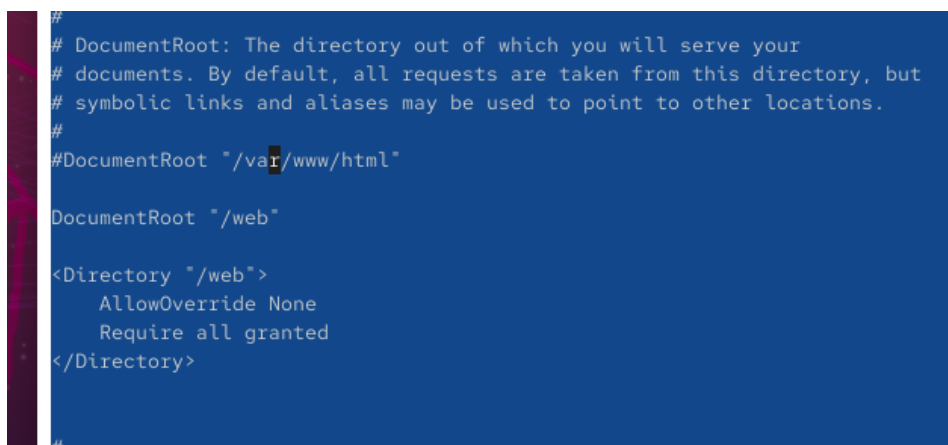
6. После перезагрузки отображено сообщение о запуске **SELinux autorelabel**, подтверждающее автоматическое восстановление всех контекстов файловой системы.

```
[ 0.730408] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 0.730410] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 0.730411] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 3.856812] selinux-autorelabel[8271]: *** Warning -- SELinux targeted policy relabel is required.
[ 3.856884] selinux-autorelabel[8271]: *** Relabeling could take a very long time, depending on file
[ 3.856905] selinux-autorelabel[8271]: *** system size and speed of hard drives.
[ 3.859106] selinux-autorelabel[8271]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 2.8: Процесс relabeling SELinux при загрузке

2.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

1. Был запущен терминал и получены полномочия администратора. Установлены необходимые пакеты `httpd` и `lynx`. Затем создан новый каталог `/web`, предназначенный для размещения файлов веб-сервера. Внутри каталога создан файл `index.html` с текстом «Welcome to my web-server».
2. В конфигурационном файле `/etc/httpd/conf/httpd.conf` закомментирована строка, указывающая стандартный корневой каталог `/var/www/html`, и добавлена новая строка `DocumentRoot "/web"`. Также был добавлен раздел, определяющий права доступа к новому каталогу.



```
#
# 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. 2.9: Изменение `DocumentRoot` и настроек каталога в файле конфигурации Apache

3. После запуска службы `httpd` и включения её автозагрузки при обращении к `http://localhost` через текстовый браузер `lynx` отобразилась стандартная тестовая страница Rocky Linux. Это означало, что доступ к каталогу `/web` блокируется политикой безопасности SELinux.

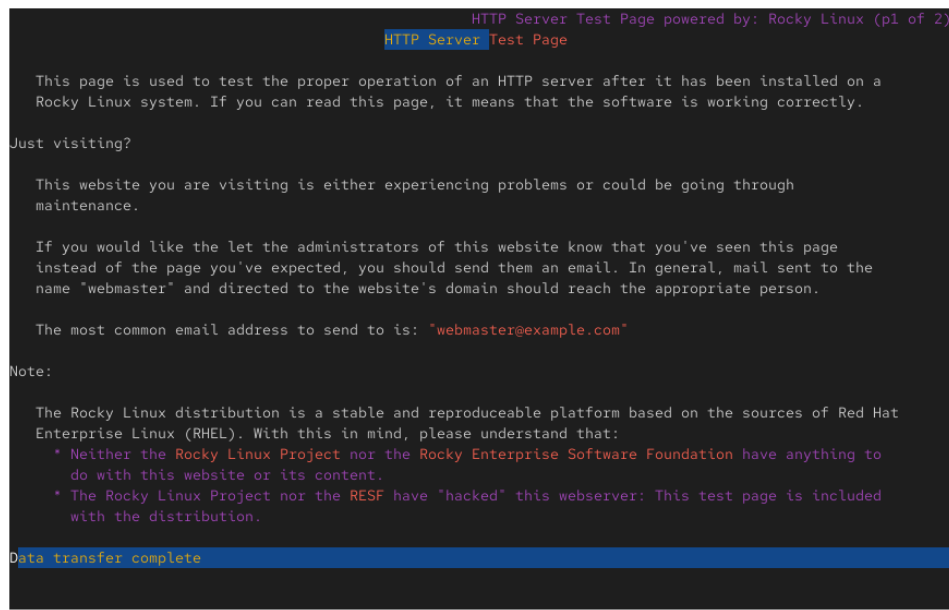


Рис. 2.10: Страница Apache по умолчанию при первом запуске

4. Для разрешения доступа веб-сервера к новому каталогу был добавлен контекст безопасности типа `httpd_sys_content_t` и выполнено восстановление контекста. В результате каталог `/web` и файл `index.html` получили корректные метки безопасности, позволяющие Apache считывать их содержимое.

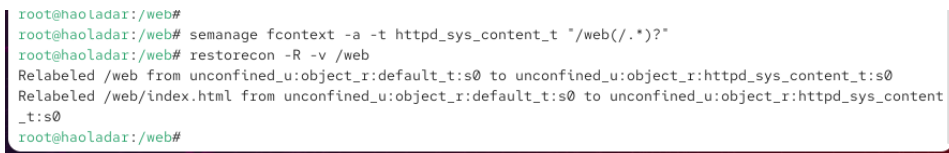


Рис. 2.11: Применение нового контекста безопасности к каталогу `/web`

5. После обновления контекста безопасности и повторного обращения к веб-серверу страница с сообщением «Welcome to my web server» отобразилась успешно, что подтверждает правильную настройку SELinux для нового расположения веб-контента.

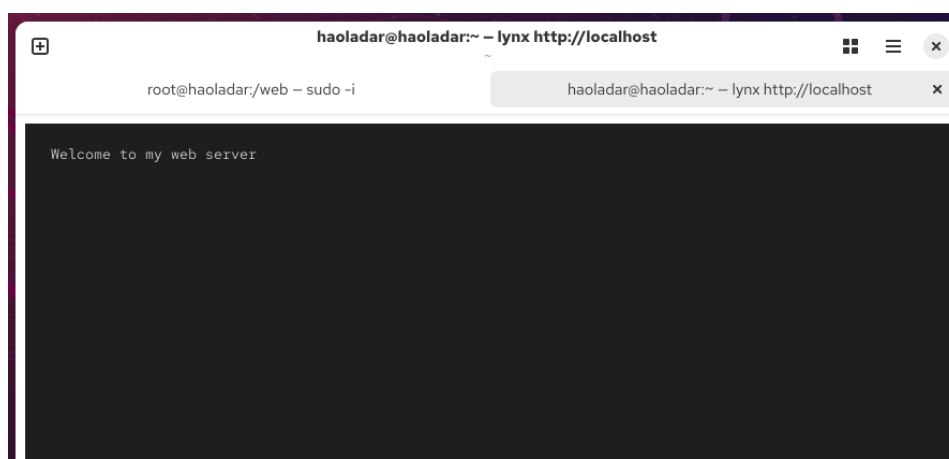


Рис. 2.12: Отображение пользовательской страницы веб-сервера

2.4 Работа с переключателями SELinux

1. После получения прав суперпользователя был просмотрен список переключателей SELinux, связанных со службой FTP. Среди них параметр `ftpd_anon_write` имел состояние `off`, то есть запись для анонимных пользователей была запрещена.
2. С помощью утилиты `semanage` было получено описание переключателя `ftpd_anon_write`, подтверждающее, что он отвечает за разрешение записи для анонимных FTP-пользователей.
3. Переключатель был активирован и временно изменён на состояние `on`, после чего проверка показала, что изменение вступило в силу.
4. Для сохранения этого состояния после перезагрузки переключатель был установлен с постоянным флагом. Теперь оба значения — временное и постоянное — находятся в положении `on`.

```

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

```

Рис. 2.13: Просмотр и изменение переключателей SELinux для службы FTP

3 Контрольные вопросы

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

setenforce 0 — переводит SELinux в разрешающий режим (Permissive) до следующей перезагрузки системы.

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

getsebool -a — выводит список всех переключателей (boolean) SELinux и их текущее состояние.

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

setroubleshoot — пакет, обеспечивающий удобное отображение сообщений SELinux и рекомендации по устранению ошибок.

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(/.*)?"**** — добавление нового типа контекста.
- **restorecon -R -v /web** — применение контекста к каталогу и его содержимому.

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

/etc/sysconfig/selinux — в этом файле необходимо установить параметр SELINUX=disabled.

6. Где SELinux регистрирует все свои сообщения?

/var/log/audit/audit.log — основной журнал, в котором фиксируются все события SELinux.

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

semanage boolean -l | grep ftp — выводит список переключателей и связанных контекстов для службы FTP с их описанием.

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?

setenforce 0 — временно перевести SELinux в разрешающий режим.

Если после этого служба начнёт работать корректно, проблема связана с политикой SELinux.

4 Заключение

В ходе работы изучены режимы SELinux, методы их переключения и настройка контекстов безопасности. Освоены команды управления политиками, восстановления контекста и работы с переключателями SELinux.