Отчёт по лабораторной работе №9

Управление SELinux

Шаханеоядж Хаоладар

Содержание

Список иллюстраций

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.

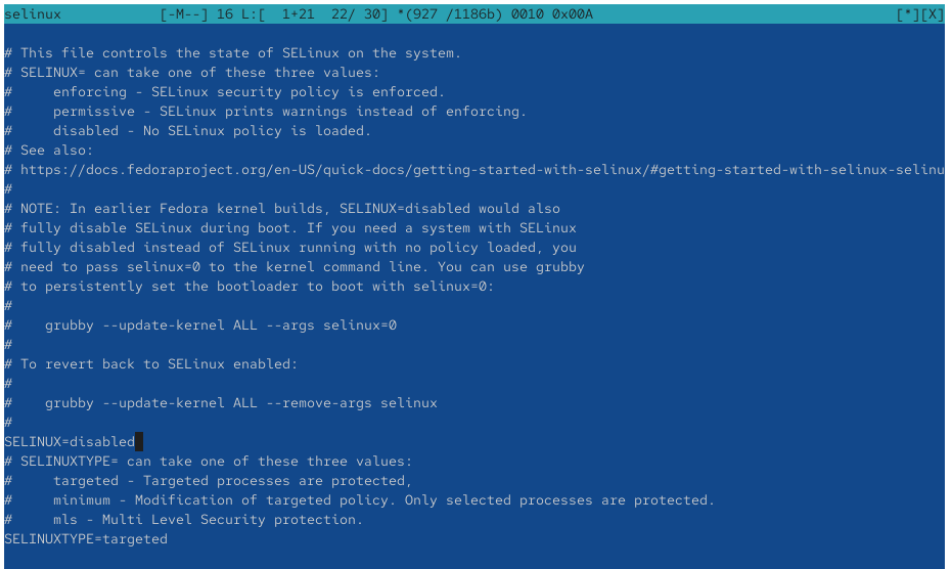

Рис. 2.2: Переключение режима SELinux в Permissive

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

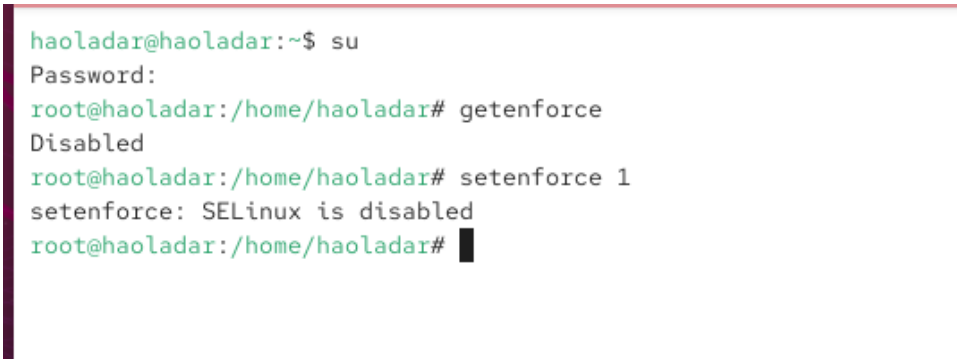

Рис. 2.3: Редактирование файла /etc/sysconfig/selinux — отключение SELinux

5. 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.

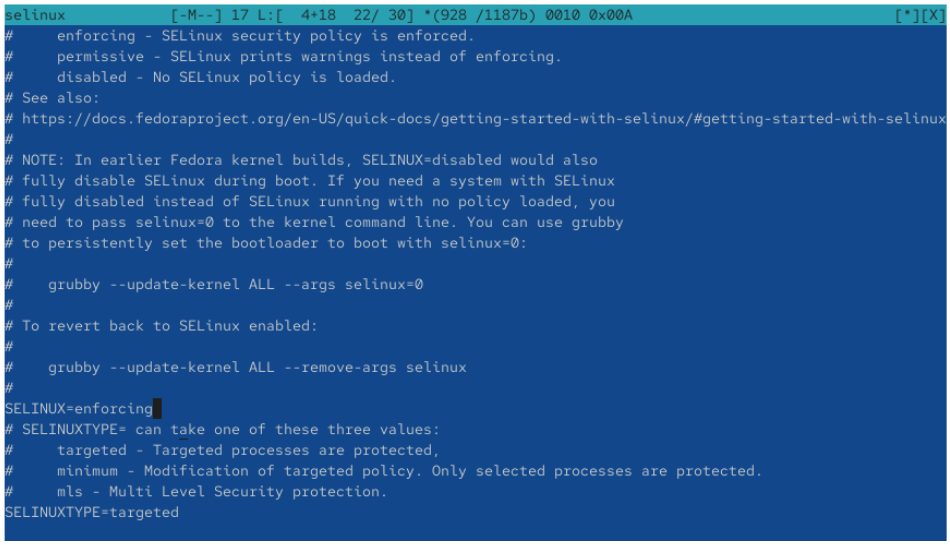

Рис. 2.4: Проверка отключения SELinux

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).

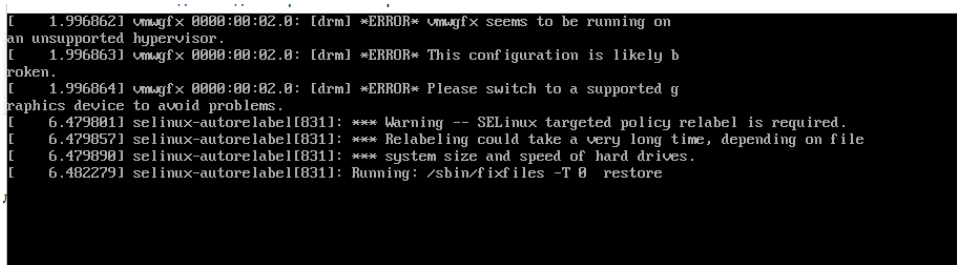

Рис. 2.5: Сообщение о необходимости relabeling при загрузке

7. После завершения relabeling и перезапуска команда **sestatus -v** вновь показала,

   что SELinux включён и работает в режиме **enforcing**.

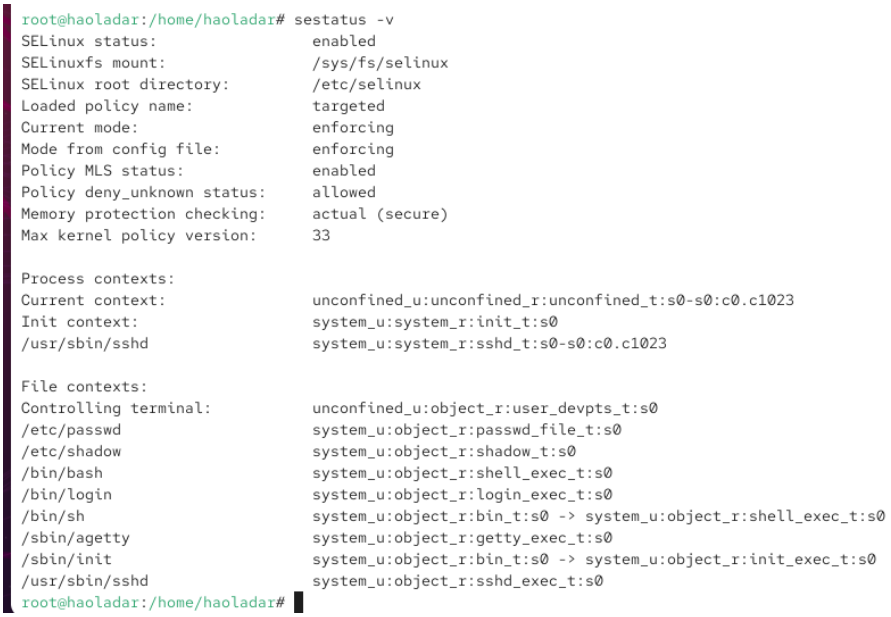

Рис. 2.6: Повторная проверка SELinux после relabeling

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.

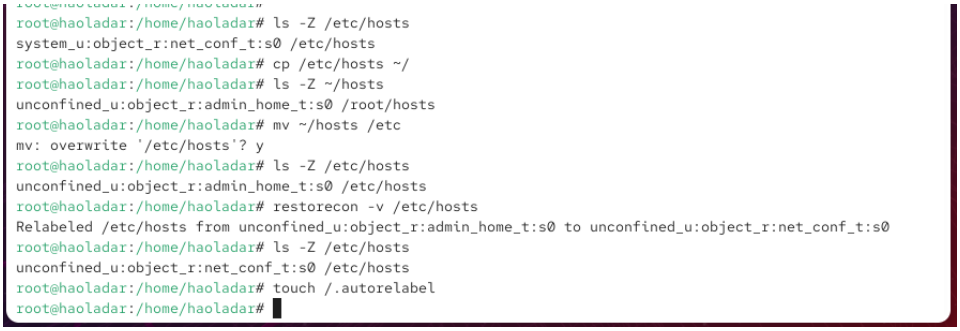

Рис. 2.7: Использование restorecon и подготовка к relabeling

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

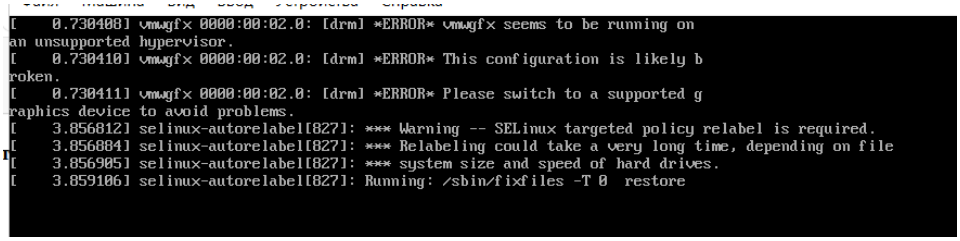

Рис. 2.8: Процесс relabeling SELinux при загрузке

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.

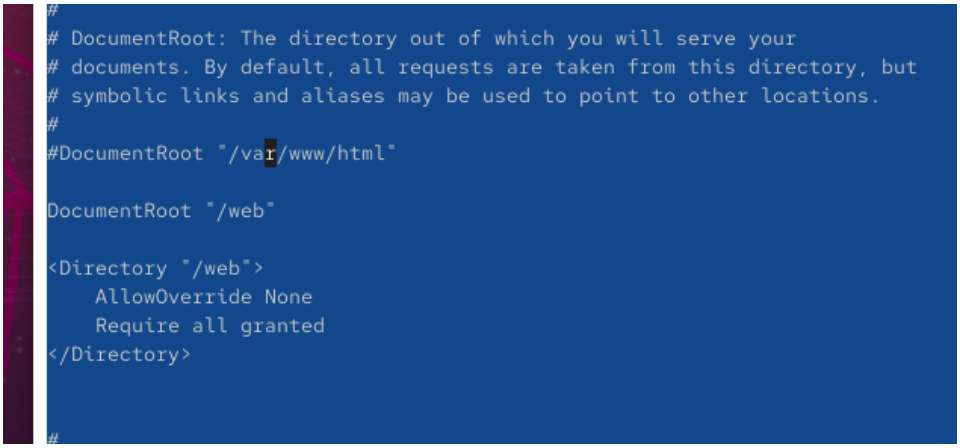

Рис. 2.9: Изменение DocumentRoot и настроек каталога в файле конфигурации Apache

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.

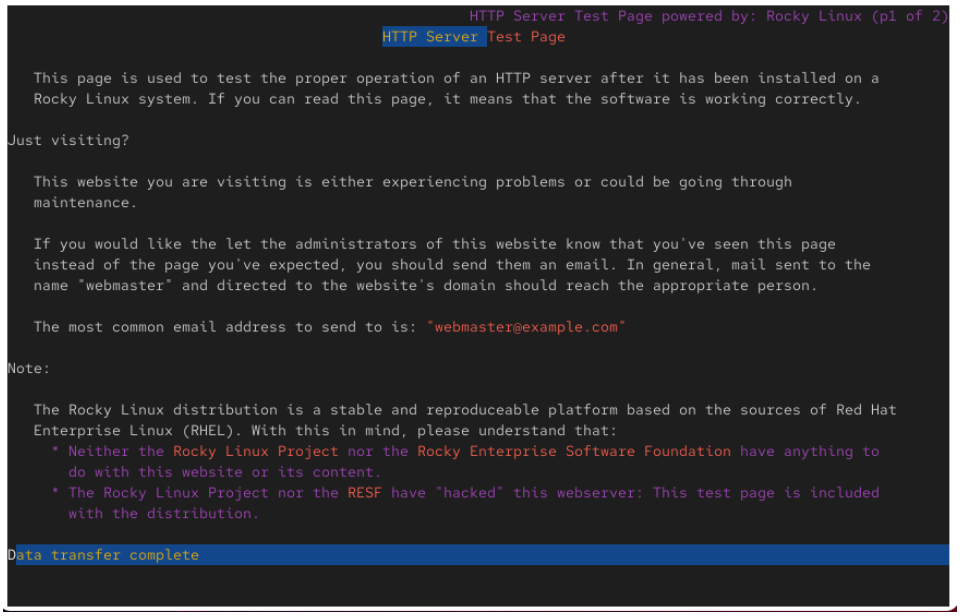

Рис. 2.10: Страница Apache по умолчанию при первом запуске

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.

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

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.

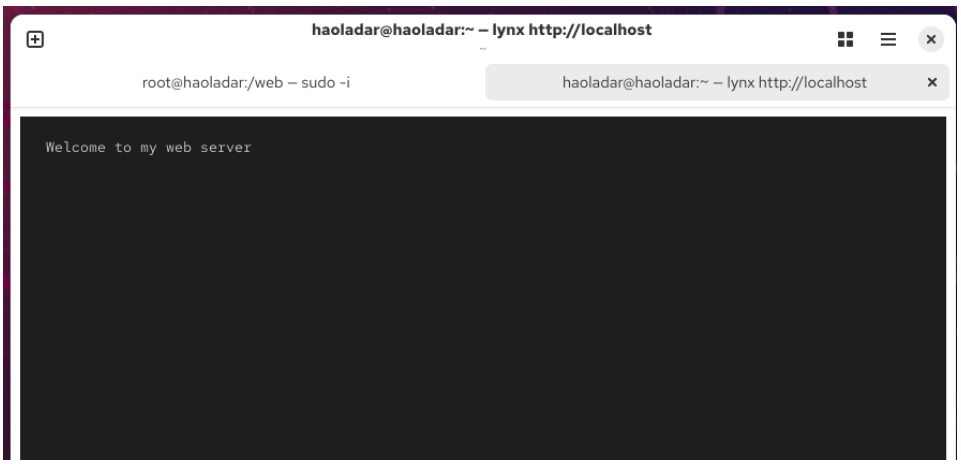

Рис. 2.12: Отображение пользовательской страницы веб-сервера

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`.

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.