Отчёт по лабораторной работе №9

Управление SELinux

Руслан Алиев

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. 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.

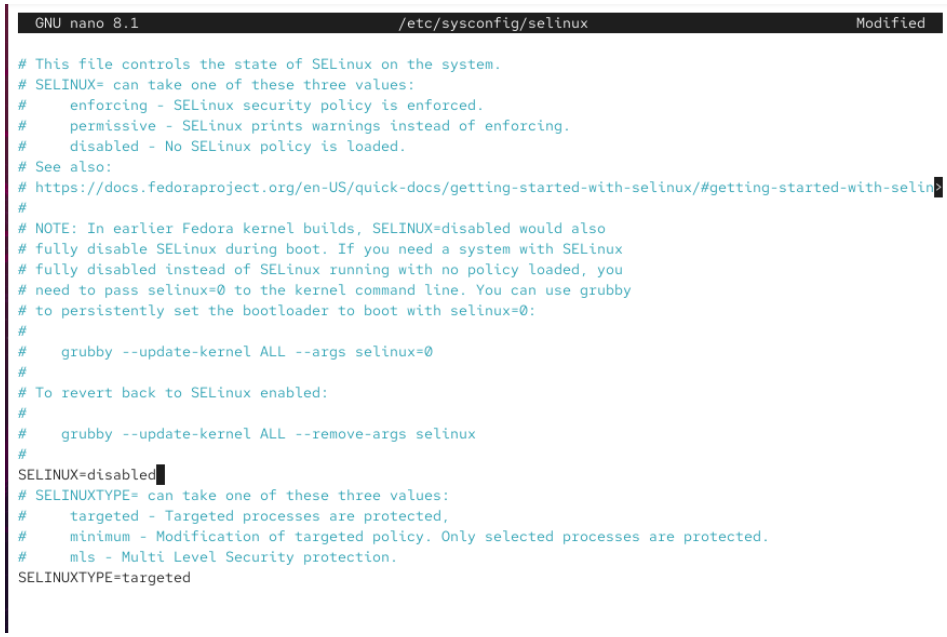

Рис. 2.2: Изменение режима SELinux на Permissive

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.

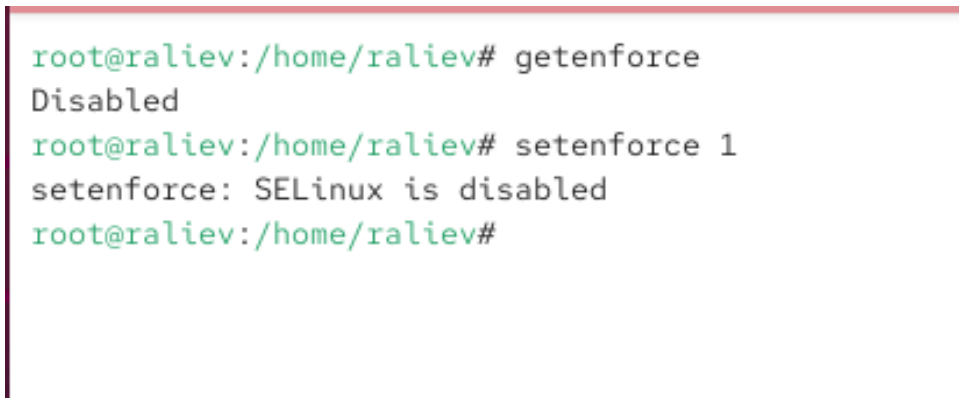

Рис. 2.3: Отключение SELinux в файле конфигурации

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.

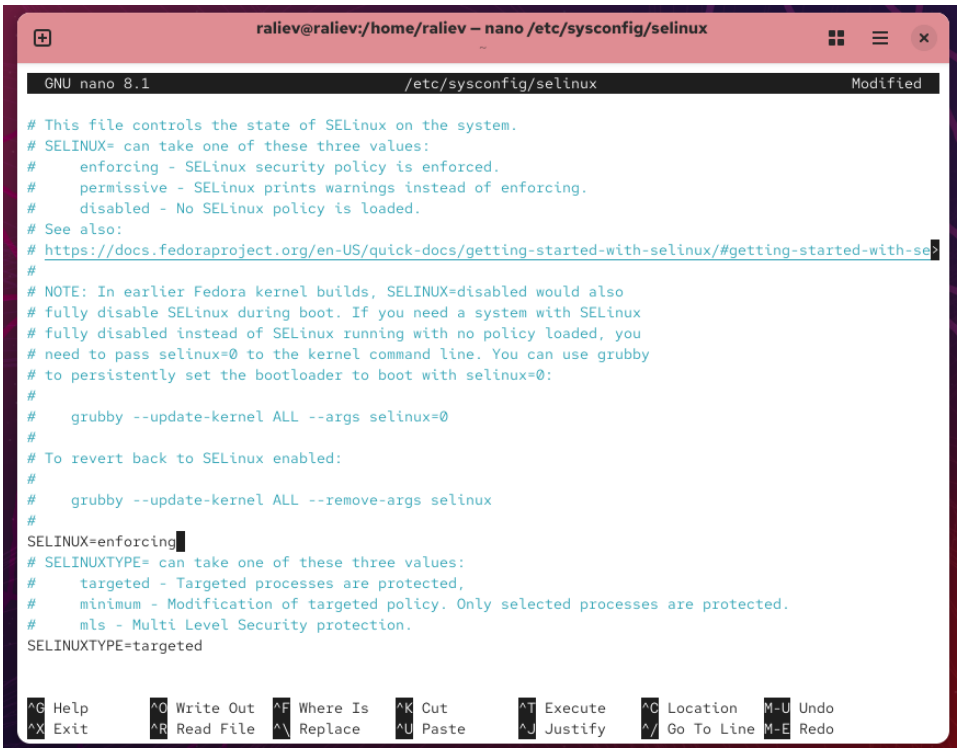

Рис. 2.4: Попытка изменить режим при отключённом SELinux

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

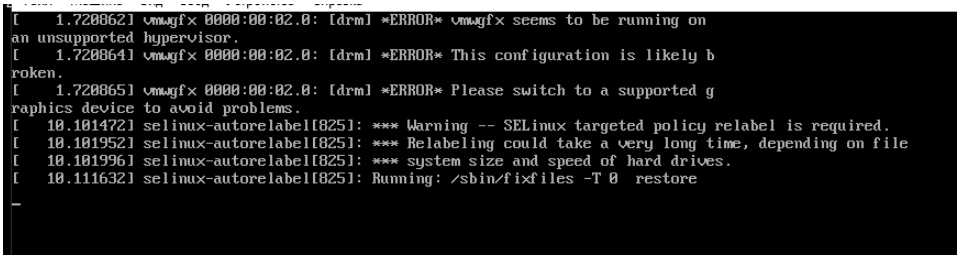

Рис. 2.5: Включение SELinux в конфигурации

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.

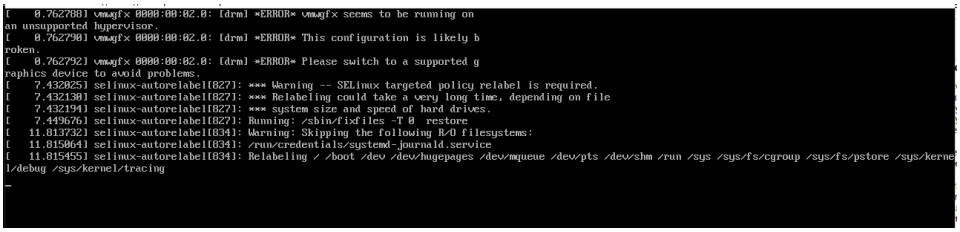

Рис. 2.8: Автоматическое восстановление контекста безопасности при загрузке

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.

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`.

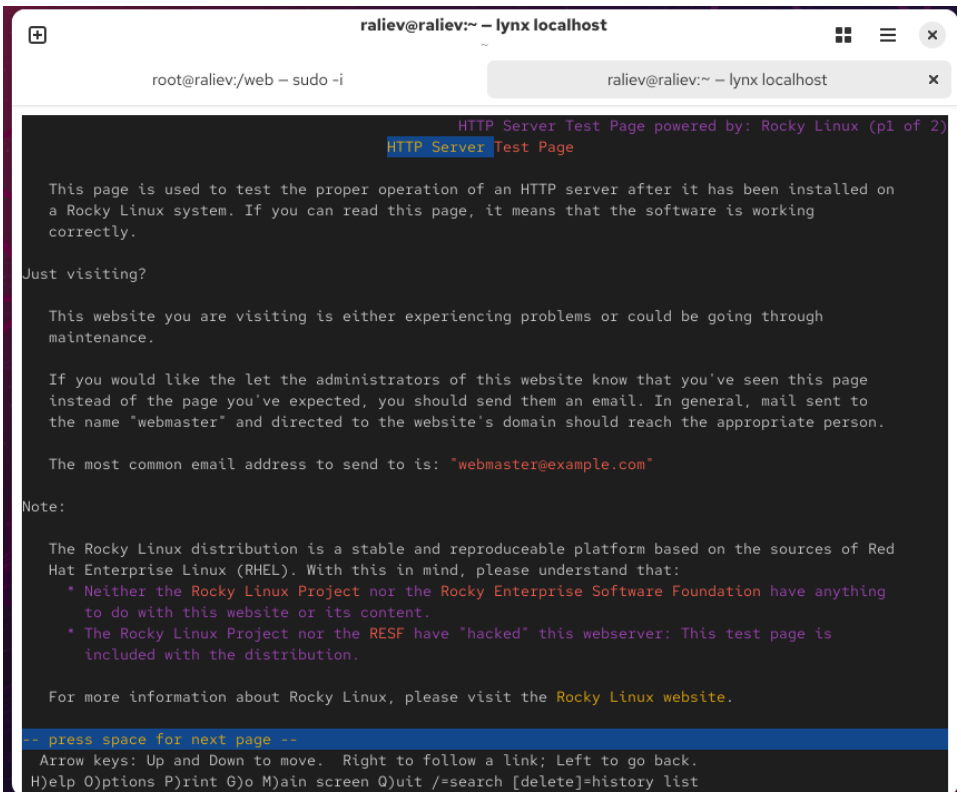

Рис. 2.10: Стандартная тестовая страница Apache

5. 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.

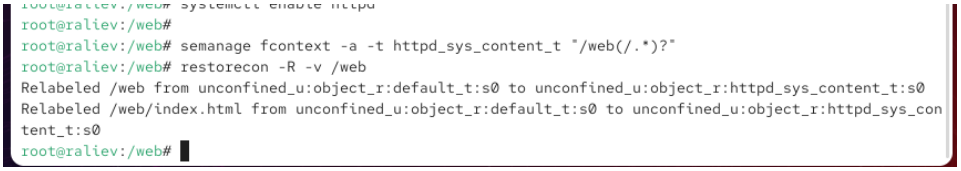

Рис. 2.11: Применение нового контекста безопасности к каталогу /web

6. 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.

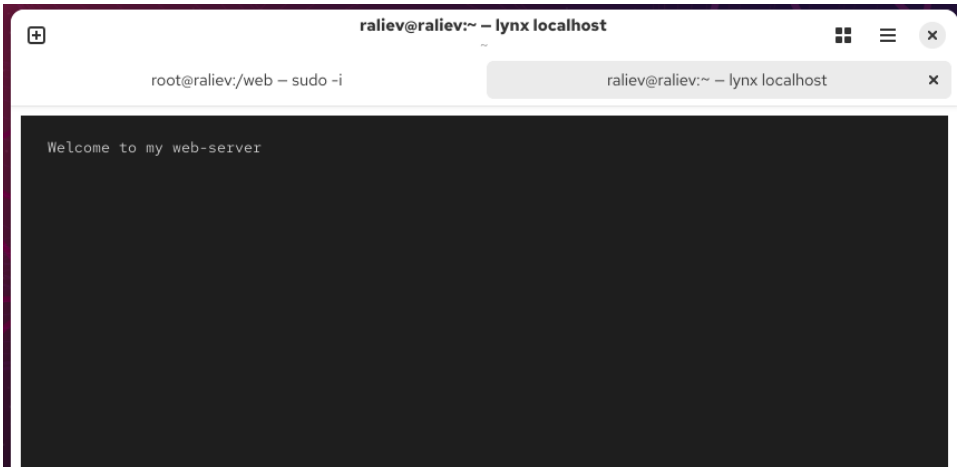

Рис. 2.12: Отображение пользовательской страницы веб-сервера

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**.

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**.