Отчёт по лабораторной работе №9

Управление SELinux

Турсунов Мухамметназар

Содержание

# 1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

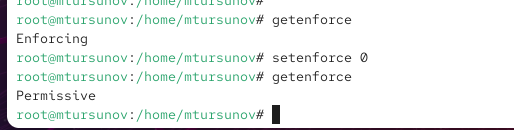
# 2 Выполнение

## 2.1 Управление режимами SELinux

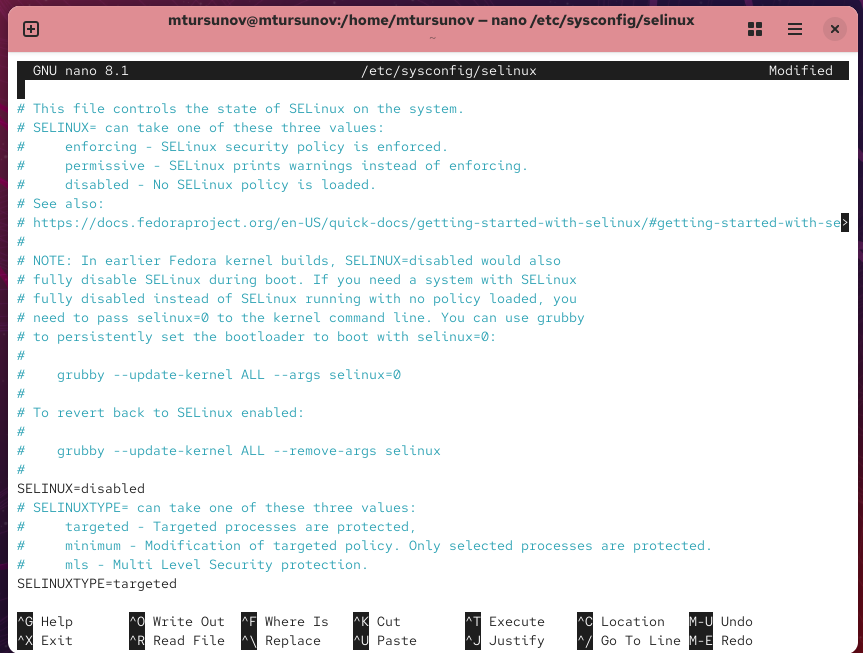
1. Сначала был выполнен переход в режим суперпользователя с помощью команды **su -**.  
   Далее просмотрено текущее состояние SELinux командой **sestatus -v**, которая показывает параметры политики и контексты безопасности.

* 
* Рис. 1: Вывод команды sestatus -v
* В результате видно:
  + **SELinux status: enabled** — механизм безопасности включён;
  + **Current mode: enforcing** — активен режим принудительного контроля;
  + **Loaded policy name: targeted** — применяется политика *targeted*, защищающая основные службы;
  + **Policy MLS status: enabled** — многоуровневая защита включена;
  + ниже отображаются контексты процессов и файлов, например, *system\_u:object\_r:passwd\_file\_t:s0* для */etc/passwd*.

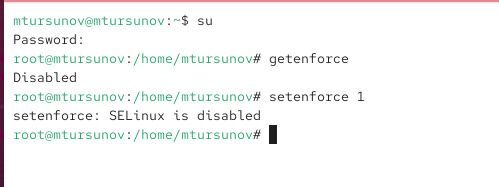
1. Для определения текущего режима SELinux использовалась команда **getenforce**.  
   По умолчанию система находилась в состоянии **Enforcing** — политика безопасности применялась ко всем процессам.  
   Затем командой **setenforce 0** режим был временно изменён на **Permissive**, при котором нарушения фиксируются, но не блокируются.  
   Повторная проверка через **getenforce** подтвердила изменение.

* 
* Рис. 2: Переключение режима SELinux на Permissive

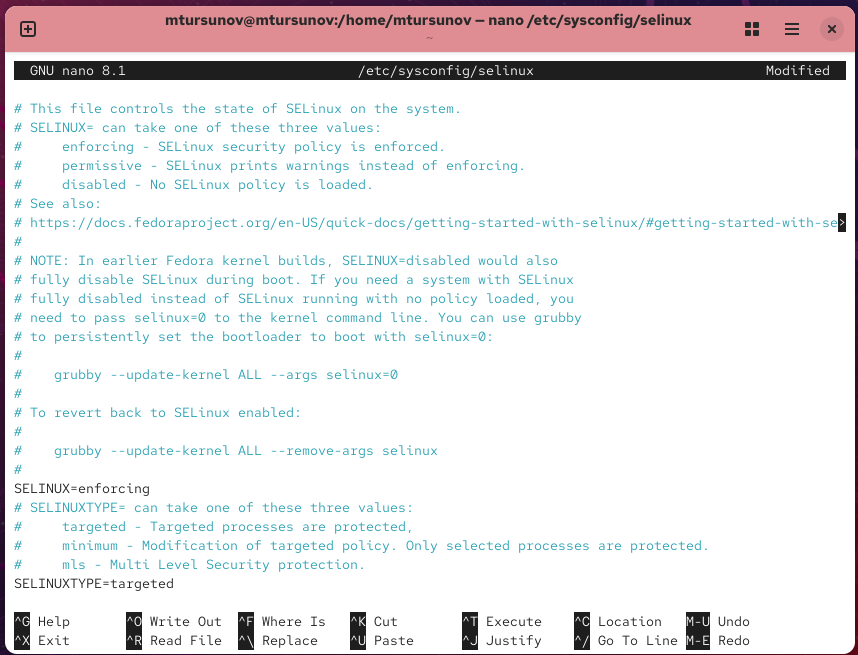
1. Далее был открыт файл */etc/sysconfig/selinux* с помощью текстового редактора **nano**.  
   В параметре **SELINUX** установлено значение *disabled*, что полностью отключает механизм SELinux после перезагрузки.

* 
* Рис. 3: Изменение параметра SELINUX=disabled

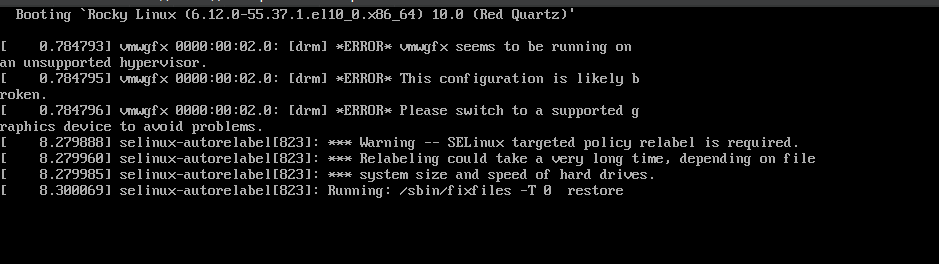
1. После перезагрузки выполнена проверка текущего состояния.  
   **getenforce** показал значение **Disabled**, что подтверждает отключение SELinux.  
   Попытка активировать его командой **setenforce 1** завершилась сообщением *SELinux is disabled*, так как смена режима невозможна без перезапуска системы.

* 
* Рис. 4: SELinux отключён — попытка включения невозможна

1. Для повторного включения защиты в том же конфигурационном файле установлено значение *SELINUX=enforcing*.  
   Поле **SELINUXTYPE** оставлено как *targeted*.

* 
* Рис. 5: Включение режима enforcing в конфигурационном файле

1. При следующей загрузке системы появилось предупреждение о необходимости восстановления меток SELinux (relabeling).  
   Процесс выполнялся автоматически и мог занять продолжительное время в зависимости от объёма файловой системы.

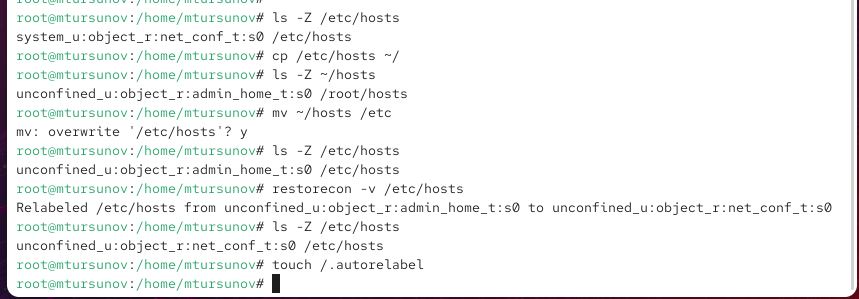
* 
* Рис. 6: Автоматическое восстановление меток SELinux при загрузке

1. После загрузки команда **sestatus -v** вновь показала, что SELinux включён и работает в режиме **enforcing**, а политика — *targeted*.

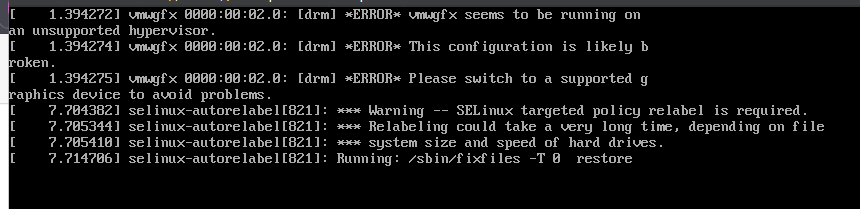
* 
* Рис. 7: SELinux снова включён, активен режим enforcing

## 2.2 Использование restorecon для восстановления контекста безопасности

1. Проверен текущий контекст безопасности файла */etc/hosts* командой **ls -Z /etc/hosts**.  
   Тип контекста — *net\_conf\_t*.
2. Файл был скопирован в домашний каталог с помощью команды **cp /etc/hosts ~/**.  
   После этого контекст нового файла *~/hosts* изменился на *admin\_home\_t*, что характерно для пользовательских файлов.
3. Файл из домашнего каталога был перемещён обратно в */etc*, после чего контекст остался *admin\_home\_t*, что не соответствует системным требованиям.
4. Для восстановления корректного контекста безопасности использовалась команда **restorecon -v /etc/hosts**.  
   Утилита изменила метку на *net\_conf\_t*, что подтверждено повторной проверкой **ls -Z /etc/hosts**.

* 
* Рис. 8: Использование restorecon для восстановления контекста файла hosts

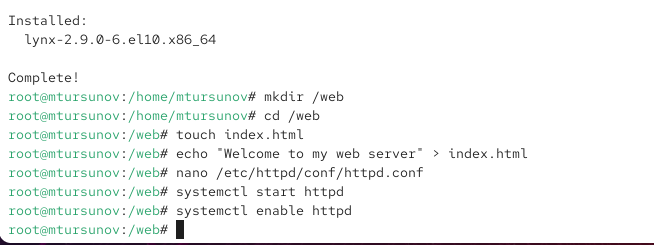
1. Для массового восстановления контекстов на всей файловой системе создан файл */.autorelabel* с помощью команды **touch /.autorelabel**.  
   После перезагрузки система автоматически перемаркировала все файлы, что сопровождалось сообщениями о выполнении relabel.

* 
* Рис. 9: Автоматическое восстановление контекстов SELinux после создания /.autorelabel

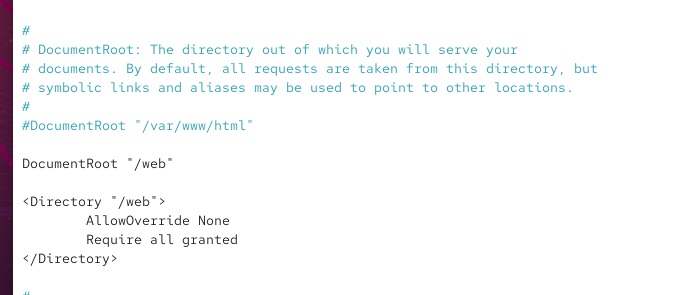
# 3 Выполнение

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

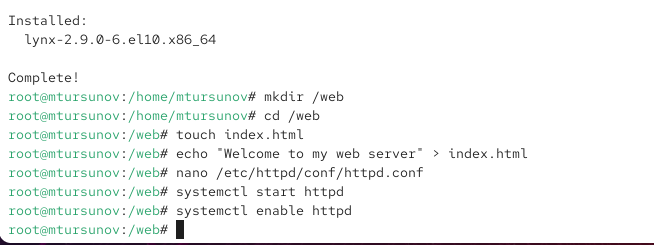
1. После получения полномочий администратора было установлено необходимое программное обеспечение для веб-сервера и текстового браузера: **httpd** и **lynx**.  
   Затем создан новый каталог для хранения веб-контента — */web*, в котором размещён файл *index.html* с тестовой строкой *Welcome to my web server*.

* 
* Рис. 10: Создание каталога /web и файла index.html

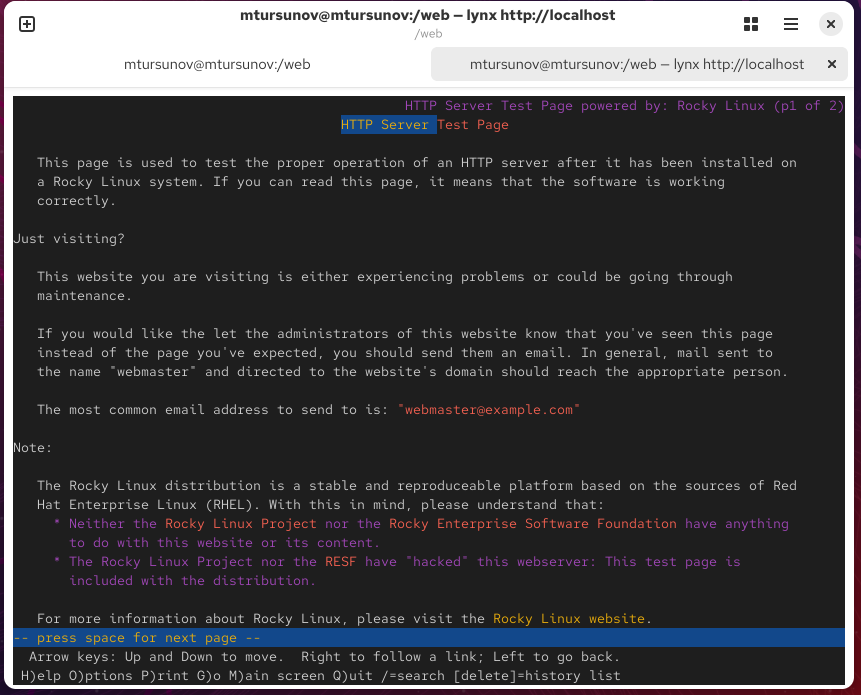
1. В конфигурационном файле */etc/httpd/conf/httpd.conf* была закомментирована стандартная строка  
   *DocumentRoot “/var/www/html”* и добавлена новая — *DocumentRoot “/web”*.  
   Также внесён соответствующий раздел **Directory** для нового каталога, разрешающий доступ к файлам.

* 
* Рис. 11: Изменение параметров DocumentRoot и Directory в httpd.conf

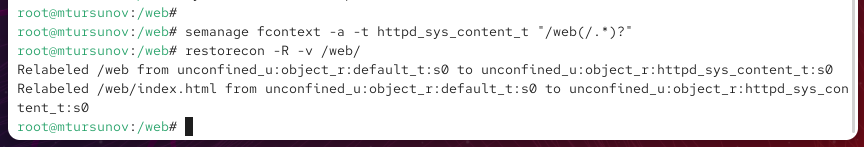
1. После внесения изменений запущена служба **httpd** и настроен её автоматический запуск при старте системы.

* 
* Рис. 12: Запуск службы httpd и её автозагрузка

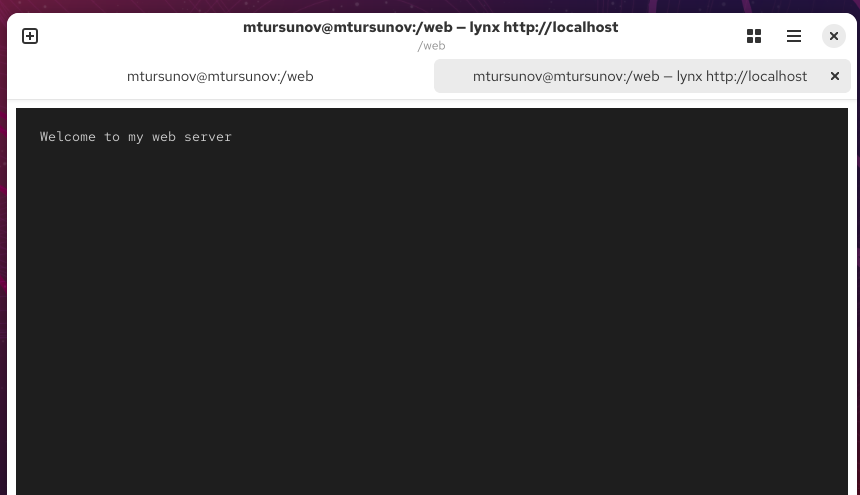
1. При обращении к локальному веб-серверу через текстовый браузер **lynx** отобразилась стандартная страница Rocky Linux, что говорит о том, что SELinux не разрешил использовать новый каталог */web*.

* 
* Рис. 13: Отображение стандартной страницы Rocky Linux

1. Для решения проблемы был назначен корректный контекст безопасности для каталога */web* с помощью команды  
   \*\*semanage fcontext -a -t httpd\_sys\_content\_t “/web(/.\*)?“**, а затем выполнено восстановление контекста** restorecon -R -v /web**.**  
   **В результате файлам и каталогу были присвоены метки безопасности, разрешающие доступ службе** httpd\*\*.

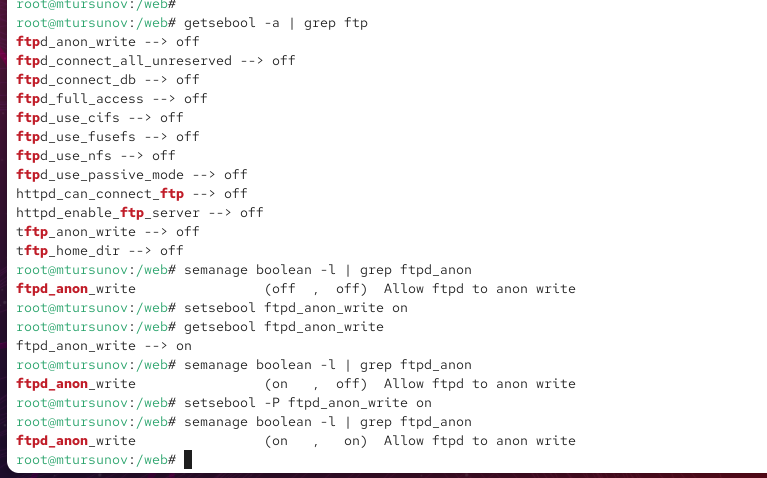
* 
* Рис. 14: Присвоение контекста httpd\_sys\_content\_t каталогу /web

1. Повторное обращение к серверу через **lynx http://localhost** показало корректную загрузку пользовательской страницы с текстом *Welcome to my web server*.  
   Это подтверждает, что настройка контекста SELinux для каталога /web выполнена успешно.

* 
* Рис. 15: Отображение пользовательской страницы веб-сервера

## 3.2 Работа с переключателями SELinux

1. Был выполнен просмотр всех переключателей SELinux, связанных с FTP-сервисом, командой **getsebool -a | grep ftp**.  
   Из вывода видно, что параметр **ftpd\_anon\_write** по умолчанию имеет состояние *off*.
2. Далее получен список переключателей для службы **ftpd\_anon** с пояснениями с помощью команды **semanage boolean -l | grep ftpd\_anon**.  
   Параметр **ftpd\_anon\_write** отвечает за разрешение анонимной записи в FTP.
3. Переключатель **ftpd\_anon\_write** был временно активирован командой **setsebool ftpd\_anon\_write on**, после чего проверено его состояние — значение изменилось на *on*.
4. Для сохранения параметра между перезагрузками он был включён постоянно с помощью команды **setsebool -P ftpd\_anon\_write on**.  
   Повторная проверка через **semanage boolean -l | grep ftpd\_anon** показала, что оба состояния (*runtime* и *persistent*) установлены в *on*.

* 
* Рис. 16: Просмотр и изменение состояния переключателя ftpd\_anon\_write

# 4 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?**  
   setenforce 0  
   (Временное переключение в разрешающий режим для проверки влияния SELinux)

# 5 Заключение

В ходе работы были изучены принципы управления системой безопасности **SELinux** в операционной системе Linux.  
Были рассмотрены режимы работы SELinux — **enforcing**, **permissive** и **disabled**, а также способы их временного и постоянного изменения.  
Проведена настройка контекста безопасности для нестандартного каталога веб-сервера */web*, что обеспечило корректный доступ службы **httpd** к его содержимому.  
С помощью инструментов **semanage** и **restorecon** освоены методы управления и восстановления меток безопасности.  
Также изучена работа с переключателями SELinux (**booleans**) на примере параметра **ftpd\_anon\_write**, который был изменён и закреплён на постоянной основе.