Отчёт по лабораторной работе №9

Управление SELinux

Амина Аджигалиева

Содержание

# 1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

# 2 Ход выполнения работы

## 2.1 Управление режимами SELinux

Сначала я получила административные права с помощью команды su.  
Затем выполнила команду sestatus -v, чтобы просмотреть текущее состояние системы безопасности SELinux.  
Из вывода видно, что SELinux включён (enabled), политика загружена (targeted), а текущий режим — enforcing.  
Это означает, что система применяет политики безопасности, ограничивая доступ процессов в соответствии с заданными контекстами.

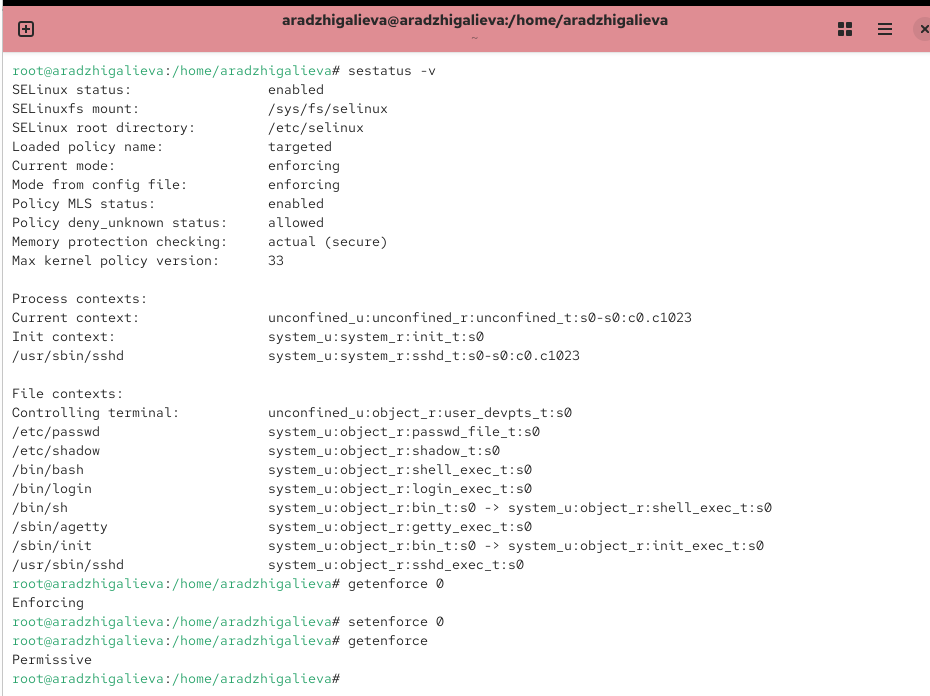


Рис. 1: Просмотр состояния SELinux с помощью sestatus

Чтобы уточнить режим работы SELinux, я ввела команду getenforce.  
Она подтвердила, что система находится в режиме Enforcing.  
Далее я временно перевела SELinux в разрешающий режим (Permissive) командой setenforce 0, после чего снова проверила состояние через getenforce.

Затем я открыла файл конфигурации /etc/sysconfig/selinux в текстовом редакторе nano и установила параметр SELINUX=disabled, чтобы полностью отключить SELinux после перезагрузки.  
На скриншоте видно, что значение параметра изменено.

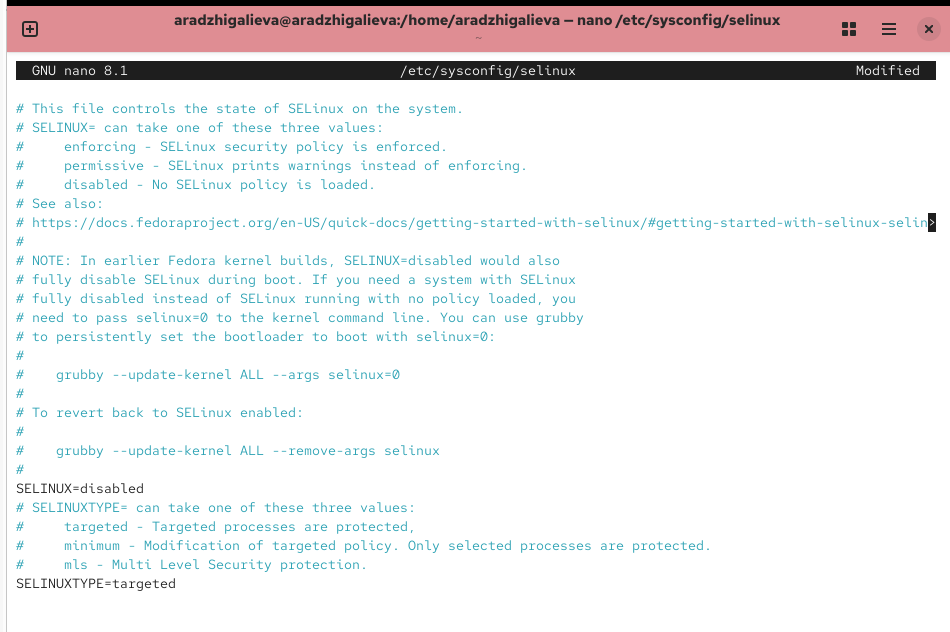


Рис. 2: Отключение SELinux через конфигурационный файл

После перезагрузки я снова вошла под пользователем root и проверила состояние SELinux командой getenforce.  
Вывод показал Disabled, что подтверждает успешное отключение системы безопасности.  
Попытка переключить режим с помощью setenforce 1 завершилась сообщением об ошибке, так как при полностью отключённом SELinux это невозможно.



Рис. 3: Проверка статуса SELinux после перезагрузки

Далее я повторно отредактировала файл /etc/sysconfig/selinux, установив параметр SELINUX=enforcing, чтобы вернуть SELinux в режим принудительного контроля.



Рис. 4: Включение SELinux (режим enforcing)

После перезагрузки системы появилось предупреждающее сообщение о необходимости восстановления меток безопасности SELinux.  
Процесс перемаркировки файловой системы может занять продолжительное время.

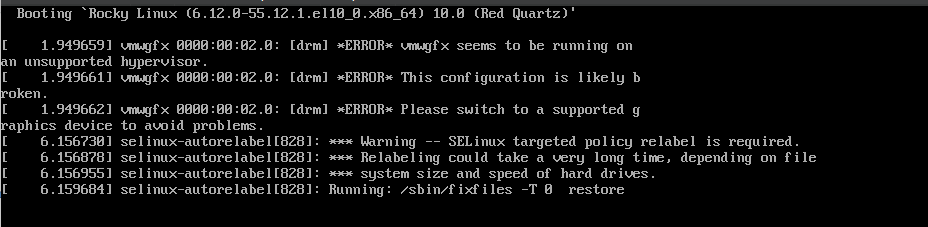


Рис. 5: Автоматическая перемаркировка файловой системы при загрузке

Когда система загрузилась, я снова проверила состояние SELinux командой sestatus -v.  
Результаты подтвердили, что SELinux снова работает в режиме enforcing, с политикой targeted.



Рис. 6: SELinux активен в режиме enforcing после перезагрузки

## 2.2 Использование restorecon для восстановления контекста безопасности

Для демонстрации восстановления контекста безопасности я выполнила команду ls -Z /etc/hosts, чтобы просмотреть текущие метки SELinux файла /etc/hosts.  
Далее я скопировала этот файл в домашний каталог и снова проверила контекст. Он изменился на admin\_home\_t, так как копирование считается созданием нового файла.

Затем я переместила файл обратно в каталог /etc и убедилась, что контекст остался неправильным.  
Для исправления я применила команду restorecon -v /etc/hosts, после чего контекст безопасности был восстановлен до исходного — net\_conf\_t.

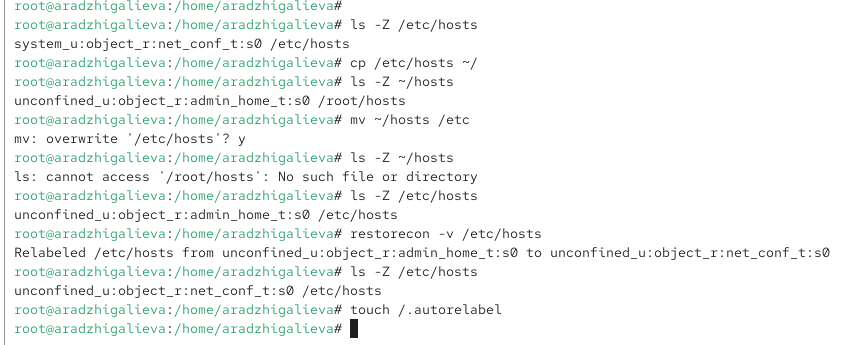


Рис. 7: Восстановление контекста безопасности файла /etc/hosts

Чтобы выполнить массовое исправление контекстов безопасности всей файловой системы, я создала пустой файл /.autorelabel и перезагрузила систему.  
При загрузке снова появилось сообщение о перемаркировке файлов, подтверждающее, что SELinux выполняет автоматическое восстановление меток.

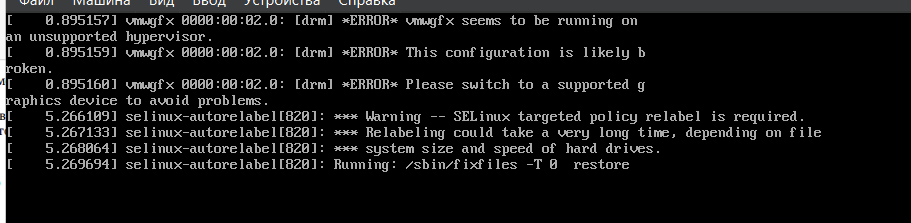


Рис. 8: Автоматическая перемаркировка при перезагрузке системы

# 3 Ход выполнения работы

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

Сначала я получила административные права и установила необходимые пакеты для работы веб-сервера: httpd и lynx.  
Затем создала новый каталог /web, который будет использоваться как корневая директория для веб-контента, и добавила в него файл index.html с текстом «Welcome to my web-server».

Далее я открыла файл конфигурации /etc/httpd/conf/httpd.conf и изменила параметры.  
Закомментировала строку DocumentRoot "/var/www/html" и добавила DocumentRoot "/web".  
Также заменила блок <Directory "/var/www"> на <Directory "/web">, разрешив доступ ко всем пользователям.  
Это позволило серверу Apache использовать новую директорию в качестве источника веб-страниц.

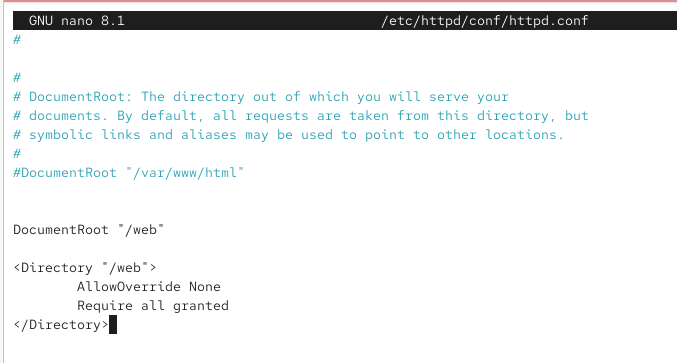


Рис. 9: Изменение параметров конфигурации Apache

После запуска службы httpd в браузере lynx при обращении к адресу http://localhost появилась стандартная тестовая страница Rocky Linux, что означает успешный запуск сервера, но указанный каталог ещё не был настроен для SELinux.

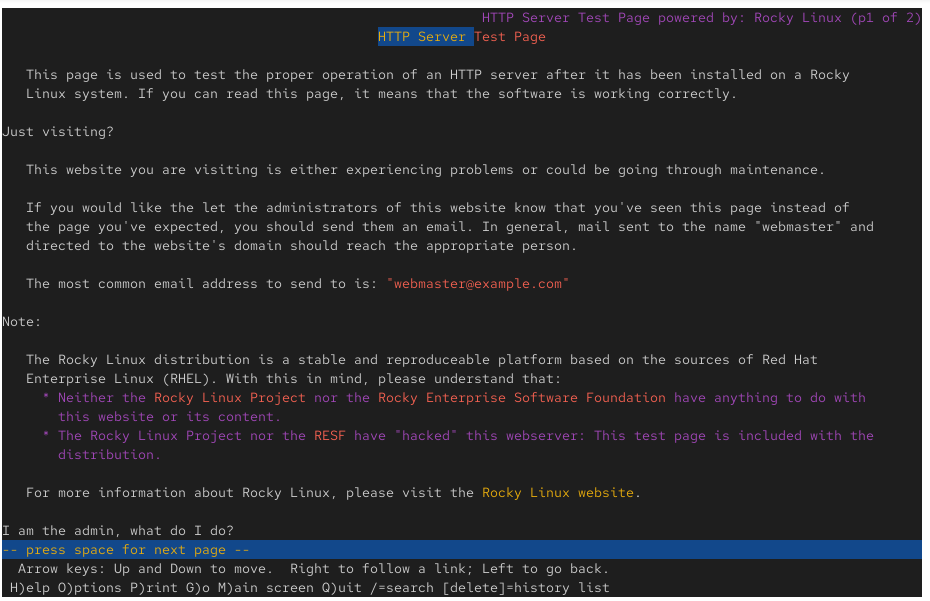


Рис. 10: Отображение стандартной страницы Rocky Linux

Чтобы разрешить доступ Apache к каталогу /web, я применила новую метку контекста безопасности SELinux для этого пути.  
Сначала добавила контекст с помощью команды semanage fcontext -a -t httpd\_sys\_content\_t "/web(/.\*)?", затем выполнила восстановление контекста командой restorecon -R -v /web.  
После этого файлы в каталоге получили правильную метку безопасности httpd\_sys\_content\_t.

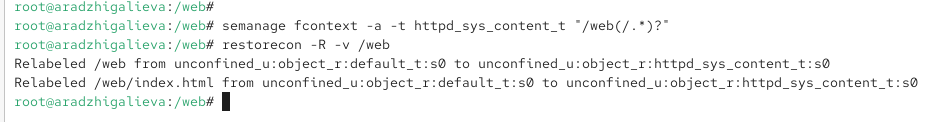


Рис. 11: Применение контекста безопасности к каталогу /web

После внесённых изменений я снова открыла веб-сайт через lynx и убедилась, что теперь отображается созданная мной страница с текстом «Welcome to my web-server».  
Это подтверждает, что контекст безопасности настроен корректно и сервер имеет доступ к каталогу /web.



Рис. 12: Отображение пользовательской страницы веб-сервера

## 3.2 Работа с переключателями SELinux

Затем я изучила работу переключателей (boolean) SELinux для службы FTP.  
Сначала с помощью команды getsebool -a | grep ftp я просмотрела все доступные параметры.  
Из вывода видно, что большинство из них имеют значение off, включая ftpd\_anon\_write, который отвечает за разрешение анонимной записи.

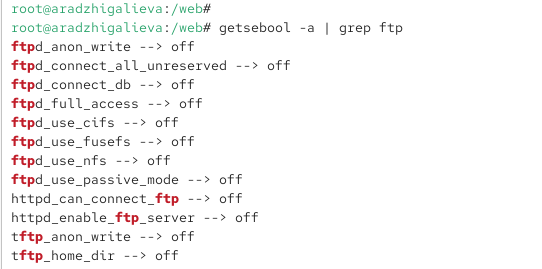


Рис. 13: Просмотр текущих значений переключателей FTP

Далее я уточнила назначение данного переключателя при помощи semanage boolean -l | grep ftpd\_anon, после чего изменила его значение командой setsebool ftpd\_anon\_write on.  
Команда getsebool ftpd\_anon\_write показала, что временная настройка переключателя включена (on), но постоянная — нет.

Чтобы сделать изменение постоянным, я использовала параметр -P:  
setsebool -P ftpd\_anon\_write on.  
После этого оба значения — временное и постоянное — стали равны on, что подтверждает успешное включение параметра.

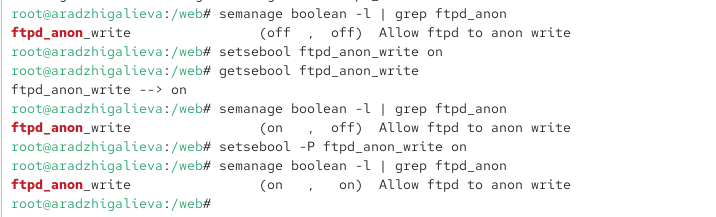


Рис. 14: Включение и проверка состояния переключателя ftpd\_anon\_write

# 4 Контрольные вопросы

1. **Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете?**  
   Для временного перевода SELinux в режим Permissive используется команда:  
   setenforce 0.
2. **Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете?**  
   Для вывода списка всех переключателей SELinux используется команда:  
   getsebool -a.
3. **Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита?**  
   Для удобного анализа сообщений SELinux необходимо установить пакет:  
   setroubleshoot.
4. **Какие команды вам нужно выполнить, чтобы применить тип контекста httpd\_sys\_content\_t к каталогу /web?**  
   Необходимо добавить и применить контекст безопасности следующими командами:  
   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?**  
   Для полного отключения SELinux нужно отредактировать файл:  
   /etc/sysconfig/selinux,  
   установив параметр SELINUX=disabled.
6. **Где SELinux регистрирует все свои сообщения?**  
   Сообщения SELinux записываются в системный журнал:  
   /var/log/audit/audit.log.
7. **Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию?**  
   Для просмотра доступных контекстов и параметров службы ftp используется команда:  
   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?**  
   Самый простой способ — временно перевести SELinux в разрешающий режим:  
   setenforce 0.  
   Если после этого сервис начнёт работать корректно, значит, проблема связана с политикой SELinux.

# 5 Заключение

В ходе выполнения лабораторной работы я изучила механизмы управления системой безопасности SELinux и её взаимодействие с сервисами Linux.  
Были рассмотрены режимы работы SELinux — enforcing, permissive и disabled, а также способы их изменения как временно, так и через конфигурационные файлы.  
На практике я выполнила настройку SELinux для нестандартного каталога веб-сервера, применила корректные контексты безопасности и убедилась в правильной работе сервиса Apache.  
Кроме того, я освоила использование переключателей (boolean) SELinux и научилась изменять их временно и постоянно.  
Полученные знания и навыки позволяют уверенно управлять политиками безопасности SELinux, обеспечивая защиту системных служб и корректное функционирование сервисов в среде Linux.