Отчёт по лабораторной работе №9

Управление SELinux

Эзиз Хатамов

Содержание

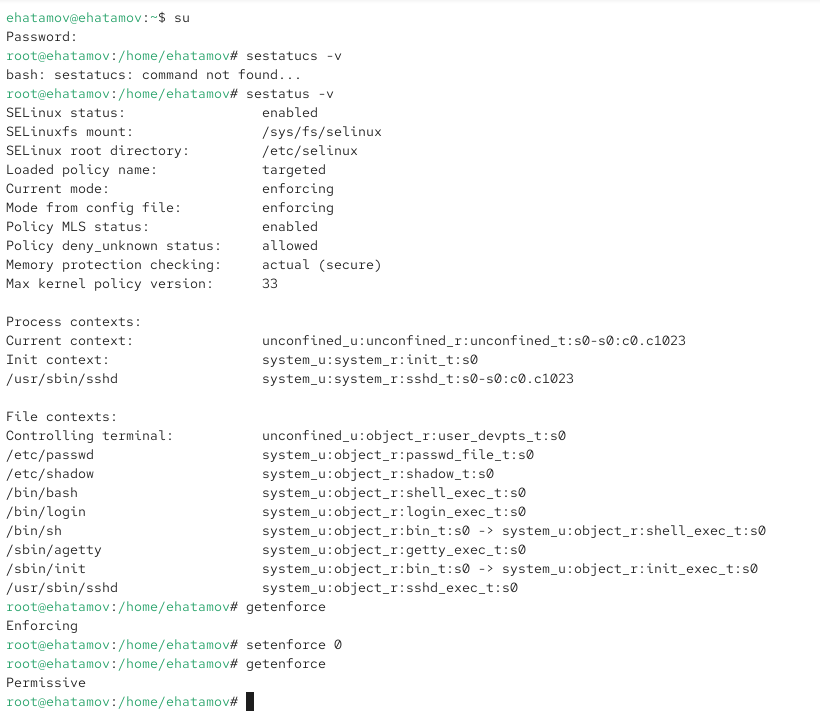
# 1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

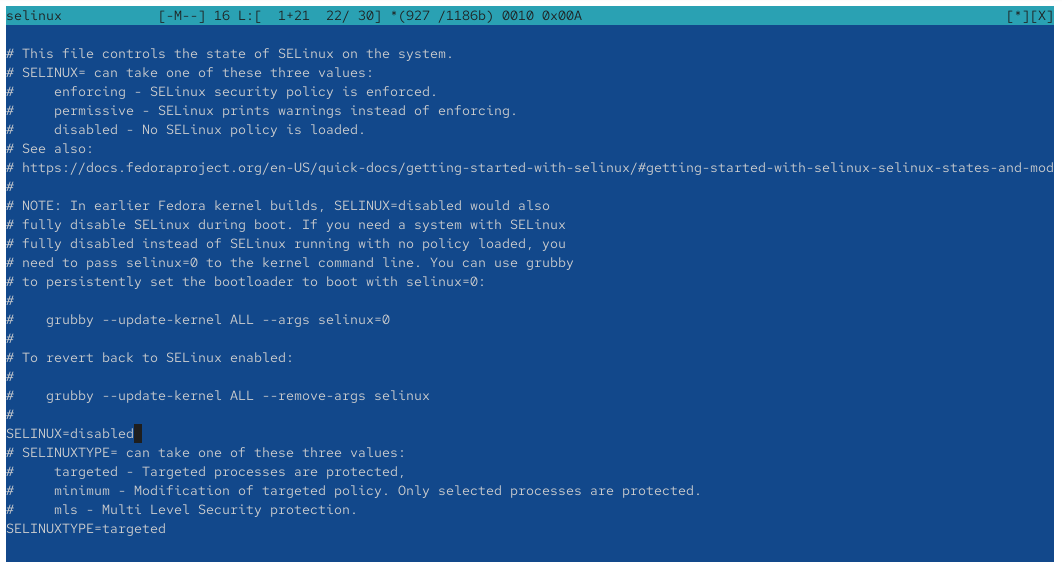
# 2 Отчёт по выполнению работы

## 2.1 Управление режимами SELinux

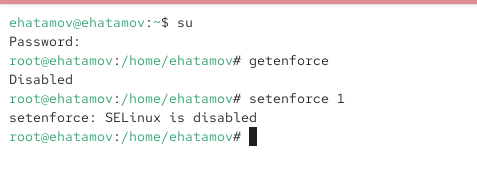
1. В терминале были получены полномочия администратора с помощью команды **su -**.
2. Для просмотра текущего состояния SELinux выполнена команда **sestatus -v**.  
   Вывод показал:
   * **SELinux status: enabled** — SELinux включён.
   * **SELinuxfs mount:** /sys/fs/selinux — точка монтирования файловой системы SELinux.
   * **SELinux root directory:** /etc/selinux — каталог, где хранятся политики SELinux.
   * **Loaded policy name:** targeted — используется целевая политика (защищаются только отдельные процессы).
   * **Current mode:** enforcing — принудительный режим, в котором политика SELinux активно применяется.
   * **Mode from config file:** enforcing — значение по умолчанию установлено в конфигурации.
   * **Policy MLS status:** enabled — многоуровневая система безопасности (MLS) включена.
   * **Policy deny\_unknown status:** allowed — неизвестные объекты разрешены.
   * **Memory protection checking:** actual (secure) — защита памяти активна.
   * **Max kernel policy version:** 33 — версия политики ядра.

* 
* Рис. 1: Вывод команды sestatus -v

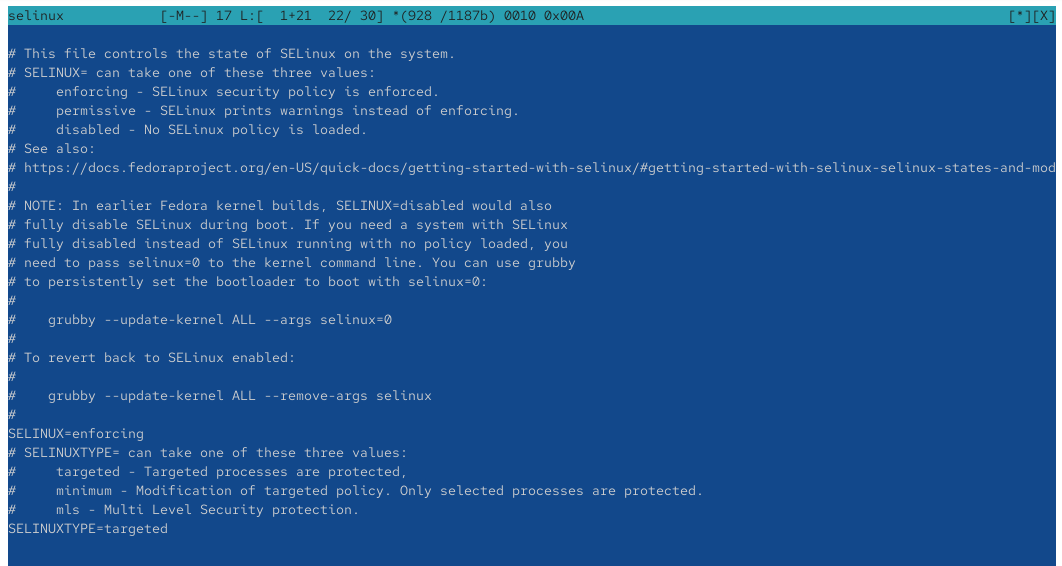
1. С помощью команды **getenforce** определён текущий режим SELinux — **Enforcing**.
2. Командой **setenforce 0** режим был изменён на **Permissive**, что подтверждено повторным вызовом **getenforce**.  
   В этом режиме SELinux не блокирует действия, а только регистрирует возможные нарушения.

* 
* Рис. 2: Переключение режима SELinux в Permissive

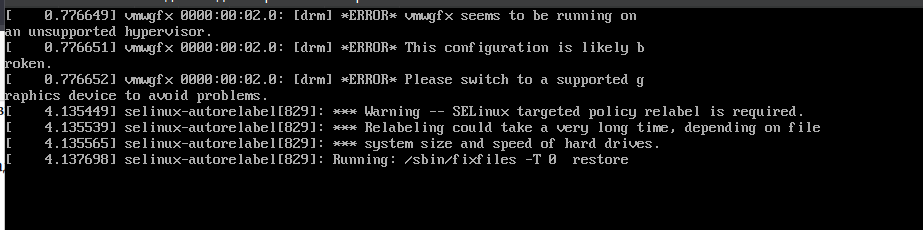
1. В конфигурационном файле **/etc/sysconfig/selinux** параметр **SELINUX** изменён на значение **disabled**, что полностью отключает SELinux после перезагрузки системы.

* 
* Рис. 3: Изменение файла /etc/sysconfig/selinux — отключение SELinux

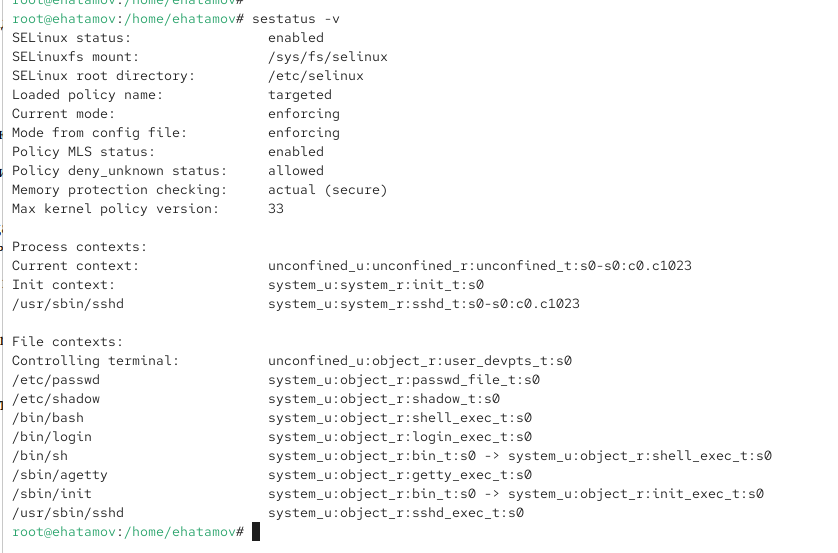
1. После перезагрузки системы выполнена команда **getenforce**, показавшая результат **Disabled**, что подтверждает успешное отключение SELinux.

* 
* Рис. 4: SELinux отключён

1. Попытка включить SELinux командой **setenforce 1** завершилась сообщением **“SELinux is disabled”**, что подтверждает невозможность переключения между режимами без перезагрузки.
2. В файле **/etc/sysconfig/selinux** параметр был снова изменён на **SELINUX=enforcing**, после чего система перезагружена.

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

1. При загрузке системы появилось предупреждение **“SELinux targeted policy relabel is required”** — система автоматически перемаркировала файлы для восстановления корректных контекстов безопасности.

* 
* Рис. 6: Автоматическое перемаркирование при загрузке системы

1. После завершения загрузки команда **sestatus -v** подтвердила, что SELinux снова работает в режиме **Enforcing**.

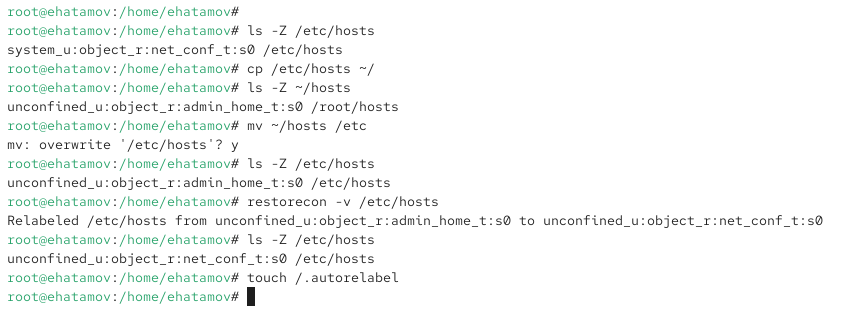
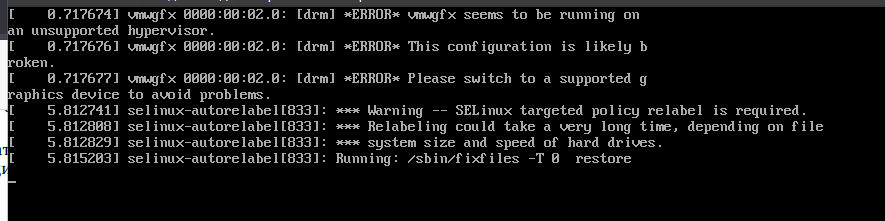


Рис. 7: SELinux включён и работает в режиме Enforcing

## 2.2 Восстановление контекста безопасности с помощью restorecon

1. В терминале с полномочиями администратора просмотрен контекст безопасности файла **/etc/hosts** с помощью команды **ls -Z /etc/hosts**.  
   Тип контекста — **net\_conf\_t**.
2. Файл **/etc/hosts** был скопирован в домашний каталог, где его контекст изменился на **admin\_home\_t**, так как копирование создаёт новый файл.
3. После возврата файла в каталог **/etc** командой **mv ~/hosts /etc**, его контекст остался **admin\_home\_t**, что неверно.
4. Для восстановления корректного контекста применена команда **restorecon -v /etc/hosts**, после чего контекст был успешно изменён обратно на **net\_conf\_t**.
5. Для массового восстановления контекстов была создана специальная метка командой **touch /.autorelabel**.  
   После перезагрузки система автоматически перемаркировала файлы, что отразилось в загрузочных сообщениях.

* 
* Рис. 8: Использование restorecon и автоматического перемаркирования

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

1. В терминале были получены полномочия администратора и установлены необходимые пакеты httpd и lynx. Это обеспечило возможность запуска веб-сервера Apache и проверки его работы через текстовый браузер.
2. Создан каталог /web, предназначенный для хранения файлов веб-сервера, и в нём создан файл index.html со строкой: Welcome to my web-server.
3. В конфигурационном файле /etc/httpd/conf/httpd.conf была закомментирована стандартная строка DocumentRoot “/var/www/html” и добавлена новая строка DocumentRoot “/web”. Также был изменён раздел Directory, определяющий политику доступа:

AllowOverride None  
Require all granted

Это разрешает доступ ко всем ресурсам каталога /web без ограничений.

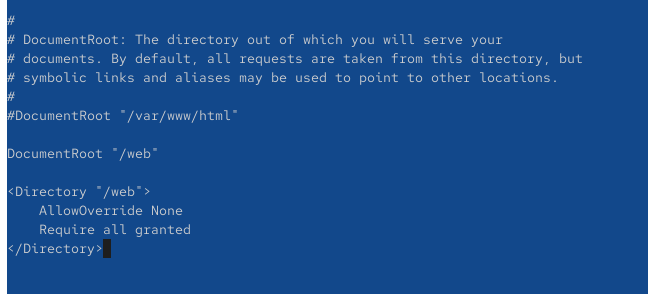


Рис. 9: Изменение конфигурации DocumentRoot и Directory

1. После перезапуска службы httpd при обращении к веб-серверу через lynx http://localhost отобразилась стандартная страница теста Rocky Linux. Это свидетельствует о том, что SELinux заблокировал доступ к новому каталогу /web.

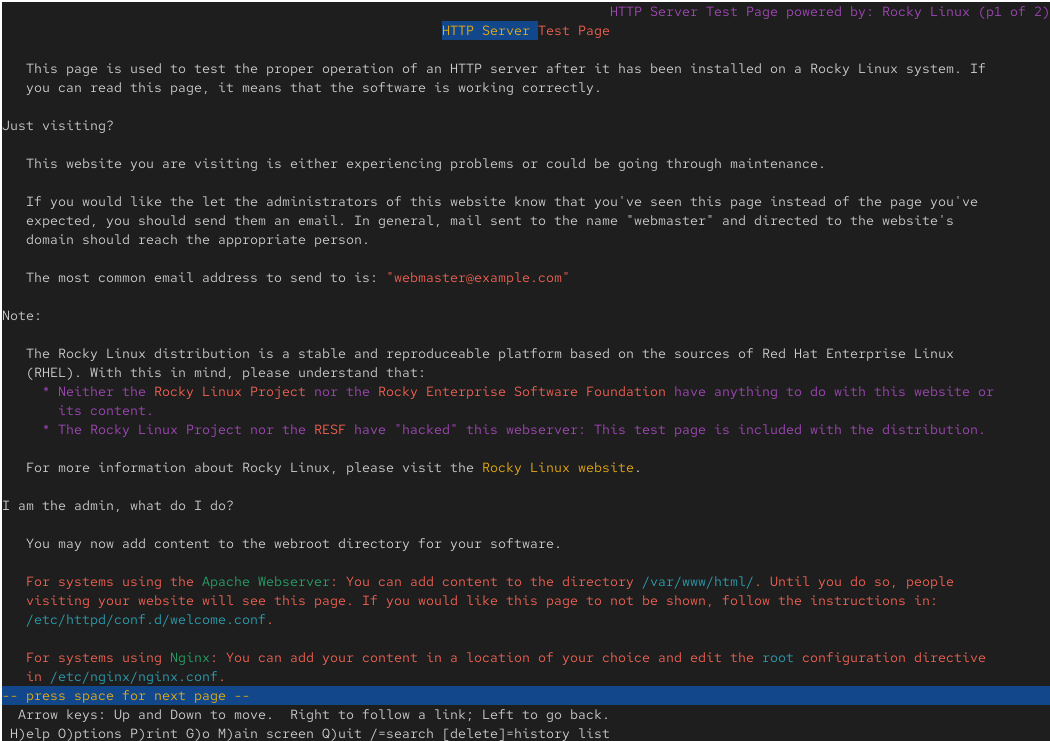


Рис. 10: Стандартная тестовая страница Rocky Linux

1. Для устранения этой проблемы новому каталогу был присвоен корректный контекст безопасности. Сначала добавлено новое правило контекста для каталога /web с типом httpd\_sys\_content\_t, затем выполнено восстановление контекста. В результате каталогу /web и файлу index.html был назначен правильный тип безопасности, что позволило веб-серверу обращаться к содержимому.

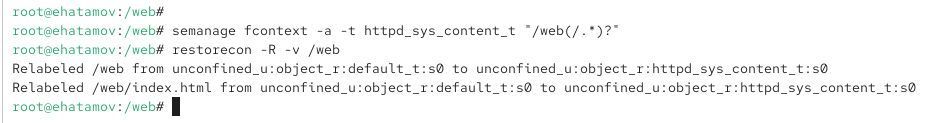


Рис. 11: Применение контекста безопасности для каталога /web

1. После повторного обращения к серверу через браузер lynx страница успешно отобразила текст: Welcome to my web-server. Это подтверждает правильную настройку контекста безопасности.

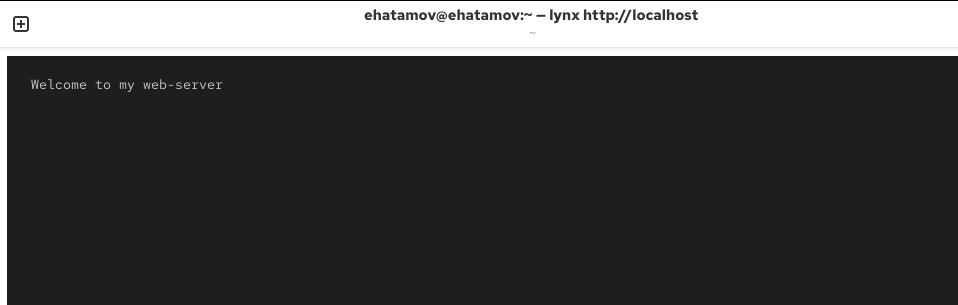


Рис. 12: Отображение пользовательской страницы веб-сервера

## 2.4 Работа с переключателями SELinux

1. После получения прав администратора был выполнен просмотр всех переключателей SELinux, связанных со службой ftp. Из вывода видно, что параметр ftpd\_anon\_write имеет значение off, что означает запрет на анонимную запись.
2. Для получения более подробной информации использовалась команда для вывода всех доступных переключателей ftpd\_anon, что показало их текущее состояние и назначение — Allow ftpd to anon write.
3. Значение переключателя ftpd\_anon\_write было изменено на on. После проверки состояние изменилось на активное, что означает включение временной настройки.
4. Для сохранения изменения между перезагрузками параметр был установлен с постоянным флагом. Повторная проверка подтвердила, что ftpd\_anon\_write теперь активен как во временной, так и в постоянной конфигурации.



Рис. 13: Проверка и изменение переключателей SELinux для ftpd\_anon\_write

# 3 Контрольные вопросы

1. **Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете?**
   * setenforce 0 — временно переводит SELinux в разрешающий режим (**Permissive**) без перезагрузки системы.
2. **Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете?**
   * getsebool -a — отображает список всех доступных переключателей SELinux и их текущие состояния.
3. **Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита?**
   * Пакет **setroubleshoot** — обеспечивает расшифровку и понятное представление сообщений SELinux в системных журналах.
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(/.\*)?" — добавляет правило для каталога /web.
   * restorecon -R -v /web — применяет новое правило и изменяет контекст безопасности каталога и его содержимого.
5. **Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux?**
   * /etc/sysconfig/selinux — конфигурационный файл, где параметр **SELINUX** устанавливается в значение **disabled**.
6. **Где SELinux регистрирует все свои сообщения?**
   * Все сообщения SELinux записываются в файл **/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 — показывает все доступные типы контекстов, связанные со службой 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 — временно перевести SELinux в разрешающий режим (**Permissive**) и проверить, устранится ли проблема. Если сервис заработал, причина связана с политикой SELinux.

# 4 Заключение

В ходе лабораторной работы были изучены принципы работы механизма SELinux, его режимы функционирования (**Enforcing**, **Permissive**, **Disabled**) и способы их изменения. На практике была выполнена настройка контекста безопасности для нестандартного каталога веб-сервера, что позволило обеспечить корректное взаимодействие Apache с системой безопасности.