Отчёт по лабораторной работе №9

Управление SELinux

Яковлева Дарья Сергеевна

Содержание

# 1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

# 2 Выполнение лабораторной работы

## 2.1 Управление режимами SELinux

Получаю административные права с помощью команды su - (см. рис. [fig. 1]).

Проверяю текущие параметры SELinux с помощью команды sestatus -v.  
Из вывода видно, что SELinux включён (*enabled*), используется политика *targeted*, текущий режим — *enforcing*, то есть политика безопасности принудительно применяется.  
Отображаются также параметры: - **SELinuxfs mount** — точка монтирования системных файлов SELinux;  
- **SELinux root directory** — путь к конфигурационным файлам SELinux;  
- **Loaded policy name** — активная политика безопасности;  
- **Current mode / Mode from config file** — текущий и заданный в конфигурации режим работы;  
- **Policy MLS status** — включённый многоуровневый контроль безопасности;  
- **Policy deny\_unknown status** — реакция системы на неизвестные объекты (разрешено);  
- **Memory protection checking** — защита памяти в активном состоянии;  
- **Max kernel policy version** — версия политики ядра.  
Также показаны контексты процессов (unconfined\_u:unconfined\_r:unconfined\_t:s0-s0:c0.c1023) и файлов (system\_u:object\_r:passwd\_file\_t:s0 и др.) (см. рис. [fig. 1]).

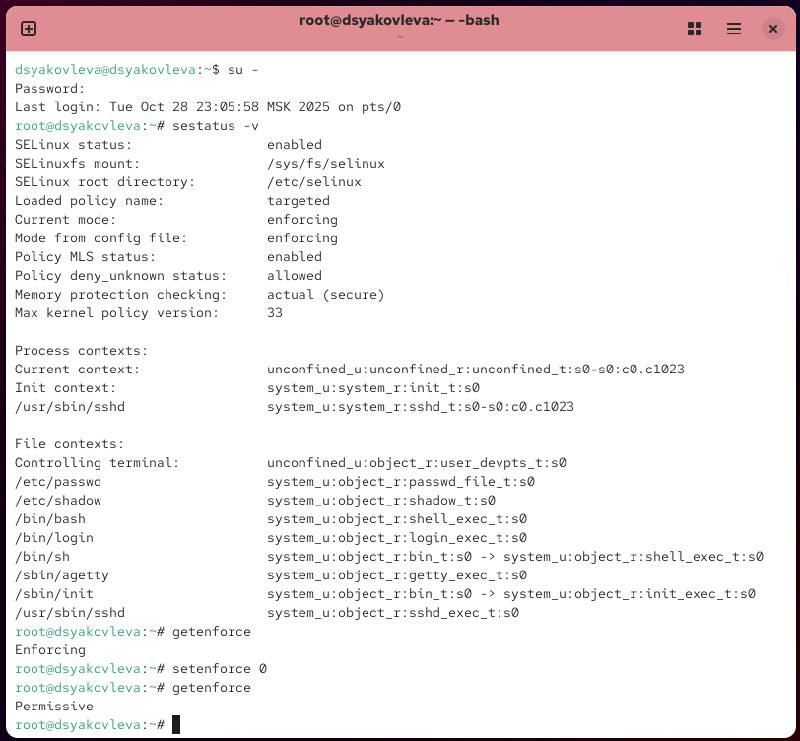


Рис. 1: Просмотр состояния SELinux

Проверяю текущий режим работы SELinux с помощью getenforce — получаю значение *Enforcing*.  
Переключаю SELinux в разрешающий режим (*Permissive*) командой setenforce 0 и повторно выполняю getenforce — теперь режим изменён (см. рис. [fig. 1]).

Открываю файл /etc/sysconfig/selinux через текстовый редактор и изменяю строку  
SELINUX=disabled, чтобы полностью отключить SELinux (см. рис. [fig. 2]).

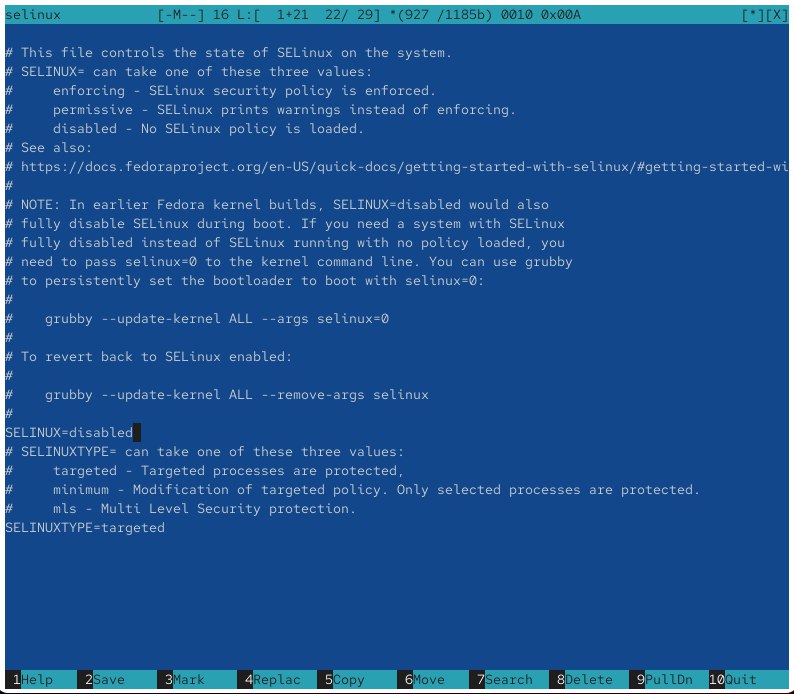


Рис. 2: Отключение SELinux в конфигурационном файле

После перезагрузки системы снова проверяю состояние SELinux с помощью getenforce.  
Система сообщает, что SELinux отключён (*Disabled*).  
Попытка выполнить setenforce 1 не приводит к изменению состояния, так как при отключённом SELinux переключение режима невозможно (см. рис. [fig. 3]).

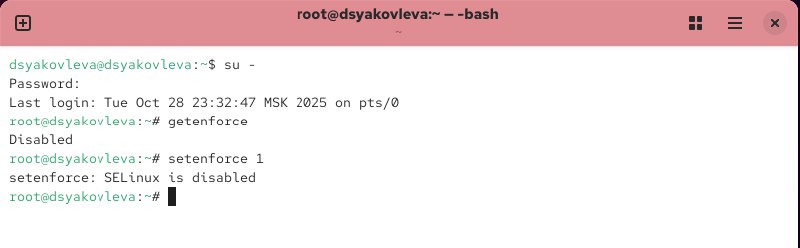


Рис. 3: Проверка статуса SELinux после отключения

Повторно открываю файл /etc/sysconfig/selinux и изменяю параметр обратно на  
SELINUX=enforcing, чтобы вернуть принудительный режим (см. рис. [fig. 4]).  
После этого система требует восстановления контекстов безопасности и перезагрузки.

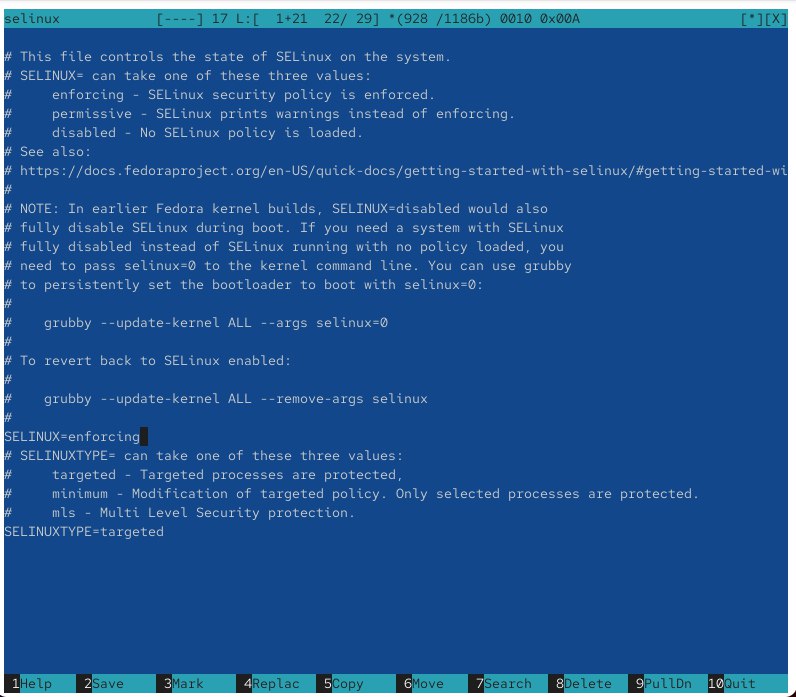


Рис. 4: Включение принудительного режима SELinux

После перезагрузки система сообщает о восстановлении меток SELinux.

## 2.2 Использование restorecon для восстановления контекста безопасности

Проверяю контекст безопасности файла /etc/hosts с помощью ls -Z.  
Вижу, что у файла установлен тип net\_conf\_t.  
Копирую файл /etc/hosts в домашний каталог и снова проверяю метку — теперь она имеет тип admin\_home\_t, поскольку копирование создаёт новый файл с контекстом домашнего каталога (см. рис. [fig. 5]).

Перемещаю файл обратно в /etc и проверяю контекст — тип остаётся admin\_home\_t.  
Выполняю команду restorecon -v /etc/hosts, чтобы восстановить правильный контекст.  
Тип контекста меняется обратно на net\_conf\_t, что подтверждает корректное восстановление.  
Для массового исправления контекстов безопасности создаю файл .autorelabel и перезагружаю систему (см. рис. [fig. 5]).

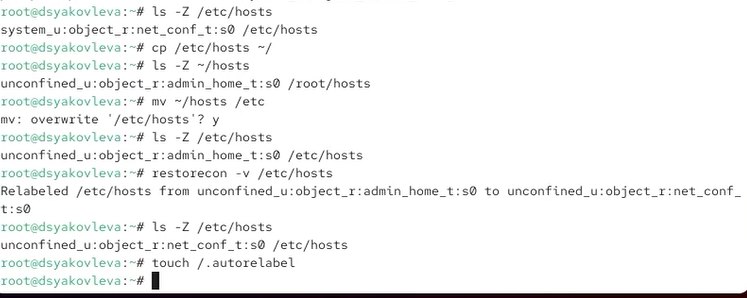


Рис. 5: Восстановление контекста безопасности и создание .autorelabel

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

Получаю административные права и создаю новый каталог /web для размещения веб-контента (см. рис. [fig. 6]).  
Перехожу в каталог и создаю пустой файл index.html, который затем открываю в редакторе mcedit для редактирования.

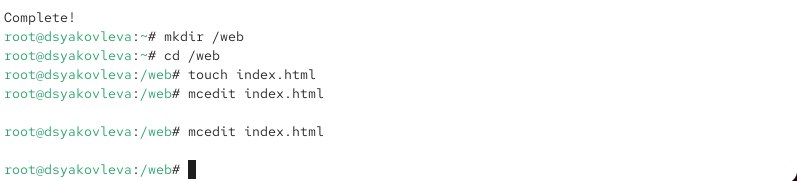


Рис. 6: Создание каталога и файла index.html

В файл index.html добавляю строку **Welcome to my web-server** — содержимое, которое будет отображаться при обращении к локальному веб-серверу (см. рис. [fig. 7]).

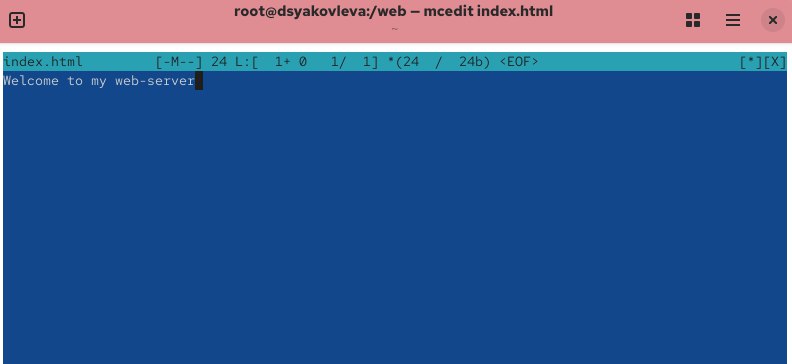


Рис. 7: Редактирование файла index.html

Редактирую конфигурационный файл /etc/httpd/conf/httpd.conf: (см. рис. [fig. 8]).

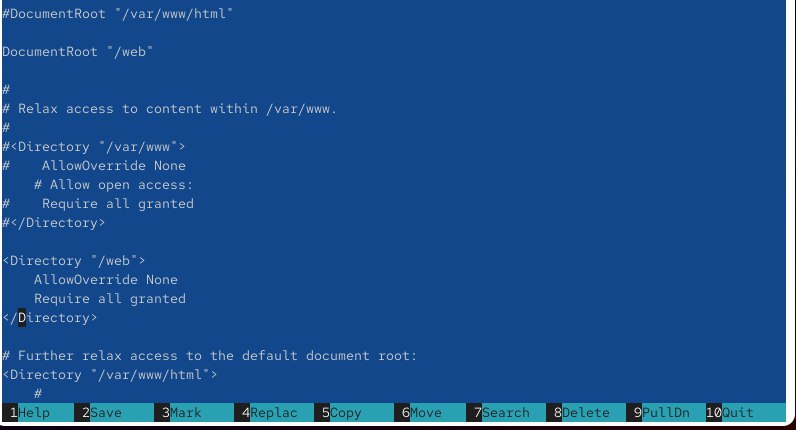


Рис. 8: Изменение пути к DocumentRoot и настройка доступа

Запускаю и активирую службу Apache с помощью команд systemctl start httpd и systemctl enable httpd.  
При попытке открыть http://localhost через текстовый браузер lynx поначалу отображается стандартная страница Red Hat, так как у каталога /web отсутствует корректный контекст безопасности (см. рис. [fig. 9]).

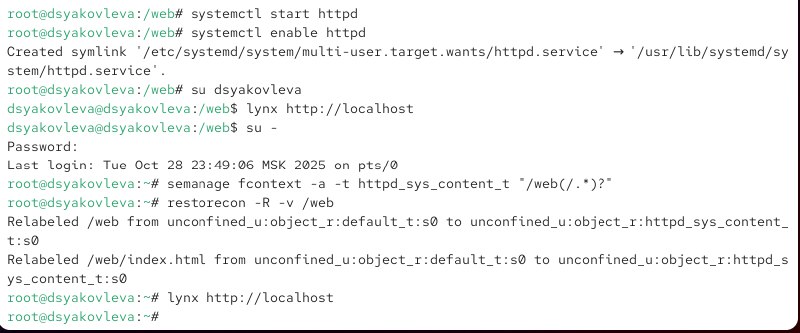


Рис. 9: Попытка доступа к веб-странице до смены контекста

Для устранения проблемы назначаю каталогу /web контекст httpd\_sys\_content\_t с помощью команды  
semanage fcontext -a -t httpd\_sys\_content\_t "/web(/.\*)?",  
затем восстанавливаю контексты:  
restorecon -R -v /web.  
После этого повторно открываю http://localhost в lynx и вижу корректное отображение содержимого файла index.html с сообщением **Welcome to my web-server** (см. рис. [fig. 10]).

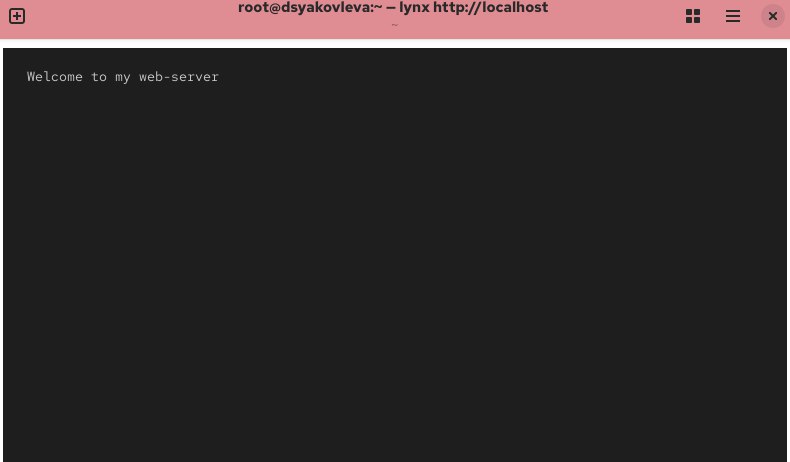


Рис. 10: Отображение пользовательской веб-страницы

## 2.4 Работа с переключателями SELinux

Получаю список переключателей SELinux, связанных с FTP-службой, с помощью getsebool -a | grep ftp.  
Из вывода видно, что параметр ftpd\_anon\_write имеет значение *off*, то есть анонимная запись через FTP запрещена.  
Просматриваю подробное описание переключателя через semanage boolean -l | grep ftpd\_anon — он отвечает за разрешение анонимной записи на FTP-сервере (см. рис. [fig. 11]).

Изменяю временное значение переключателя командой  
setsebool ftpd\_anon\_write on,  
а затем делаю изменение постоянным с помощью  
setsebool -P ftpd\_anon\_write on.  
После проверки видно, что настройка всё ещё имеет значение *(off, off)*, что означает, что разрешение анонимной записи остаётся отключённым (см. рис. [fig. 11]).

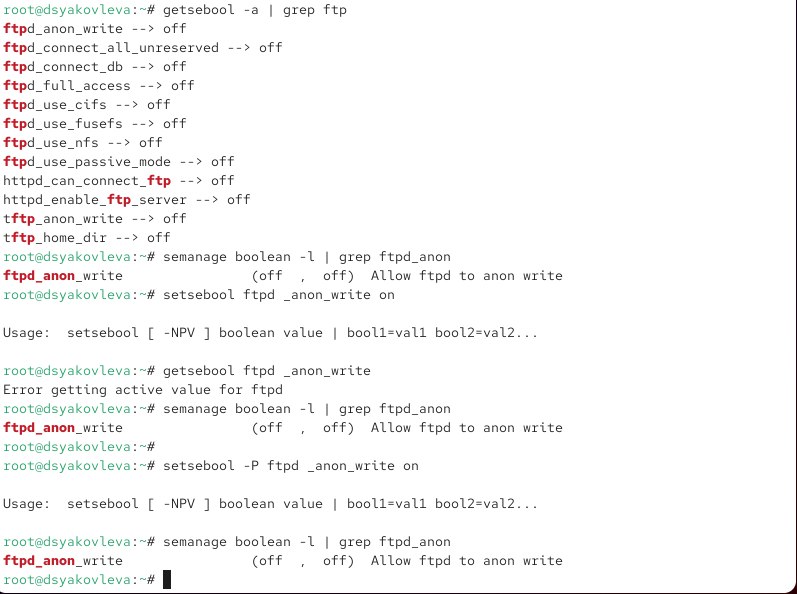


Рис. 11: Проверка и изменение состояния переключателя ftpd\_anon\_write

# 3 Контрольные вопросы

1. **Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете?**  
   Используется команда setenforce 0.
2. **Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете?**  
   Используется команда getsebool -a.
3. **Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита?**  
   Необходимо установить пакет setroubleshoot.
4. **Какие команды вам нужно выполнить, чтобы применить тип контекста httpd\_sys\_content\_t к каталогу /web?**  
   Используются команды:  
   semanage fcontext -a -t httpd\_sys\_content\_t "/web(/.\*)?"  
   и  
   restorecon -R -v /web.
5. **Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux?**  
   Нужно изменить файл /etc/sysconfig/selinux.
6. **Где SELinux регистрирует все свои сообщения?**  
   Сообщения SELinux записываются в журнал /var/log/audit/audit.log.
7. **Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию?**  
   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 командой setenforce 0 и проверить работу сервиса.

# 4 Заключение

В ходе лабораторной работы были изучены механизмы управления политиками безопасности SELinux.  
Также изучена работа с переключателями SELinux, обеспечивающими гибкую настройку политик безопасности для различных служб.  
В результате работы сформировано понимание принципов функционирования SELinux и его роли в обеспечении безопасности системы.