Отчёт по лабораторной работе №9

Управление SELinux

Лабси Мохаммед

Содержание

# 1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

# 2 Выполнение работы

## 2.1 Просмотр состояния SELinux

Для начала были получены права администратора с помощью команды su.  
После ввода пароля выполнена команда sestatus -v.

Вывод команды показывает подробную информацию о состоянии SELinux:  
- SELinux status: enabled — система безопасности SELinux включена;  
- SELinuxfs mount: /sys/fs/selinux — точка монтирования файловой системы SELinux;  
- SELinux root directory: /etc/selinux — корневой каталог конфигурации SELinux;  
- Loaded policy name: targeted — используется политика, защищающая только определённые процессы;  
- Current mode: enforcing — политика SELinux активно применяется;  
- Mode from config file: enforcing — тот же режим задан в конфигурации;  
- Policy MLS status: enabled — поддержка многоуровневой безопасности включена;  
- Policy deny\_unknown status: allowed — неизвестные объекты разрешены;  
- Memory protection checking: actual (secure) — контроль памяти активен;  
- Process contexts и File contexts — показывают контексты безопасности активных процессов и файлов.

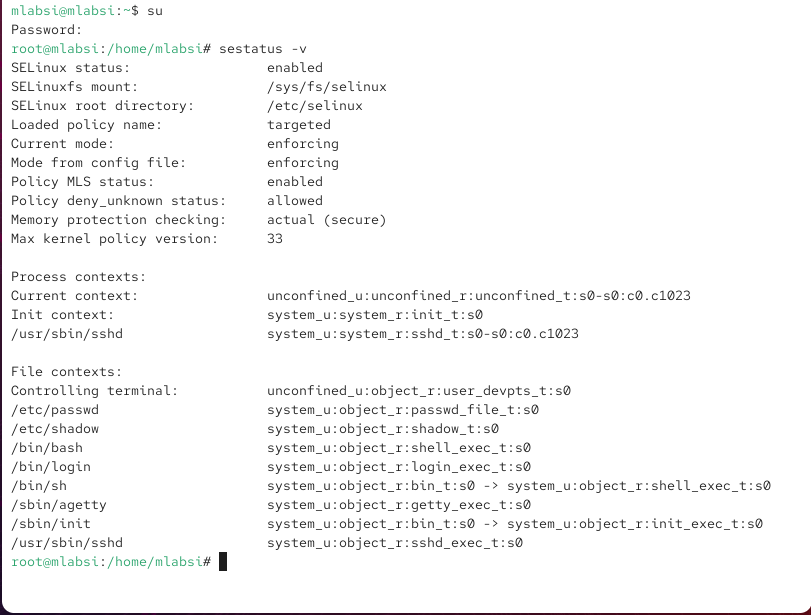


Рис. 1: Проверка состояния SELinux

## 2.2 Проверка и изменение режима SELinux

Режим SELinux был проверен с помощью команды getenforce.  
По умолчанию система находилась в состоянии Enforcing (принудительное исполнение политики).  
Затем режим был изменён на разрешающий Permissive.  
Повторная проверка показала, что SELinux работает в режиме Permissive.

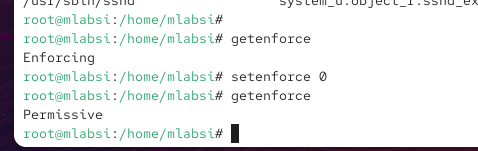


Рис. 2: Изменение режима работы SELinux

## 2.3 Отключение SELinux через конфигурационный файл

Для полного отключения SELinux был отредактирован файл конфигурации /etc/sysconfig/selinux.  
В нём параметр SELINUX был изменён на disabled и сохранены изменения.

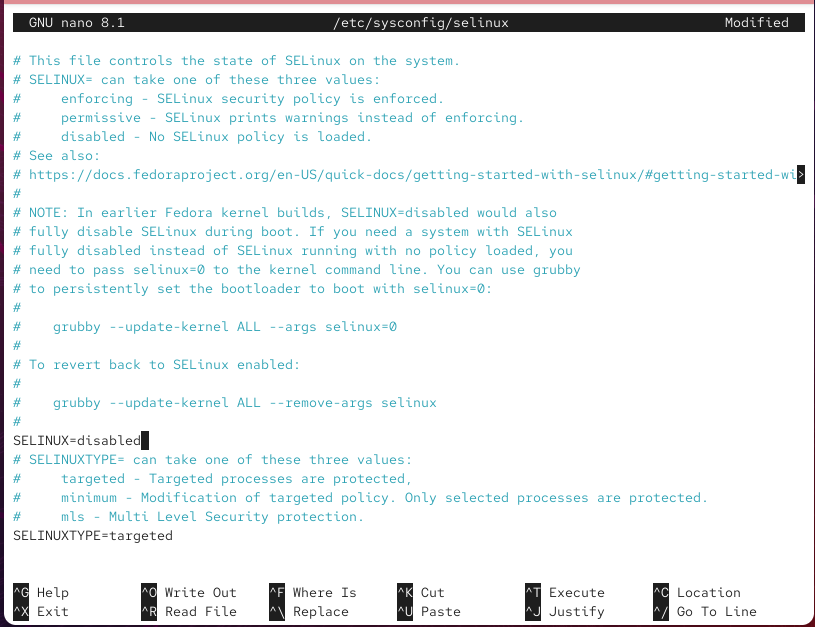


Рис. 3: Редактирование конфигурации SELinux (отключение)

После перезагрузки проверка состояния показала, что SELinux отключён.  
Попытка включить SELinux без перезагрузки завершилась сообщением, что SELinux is disabled.

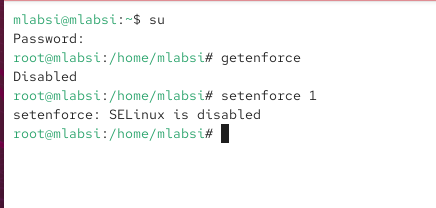


Рис. 4: SELinux отключён

## 2.4 Включение SELinux и возврат в режим Enforcing

Для повторного включения SELinux параметр SELINUX в файле /etc/sysconfig/selinux был изменён на enforcing.

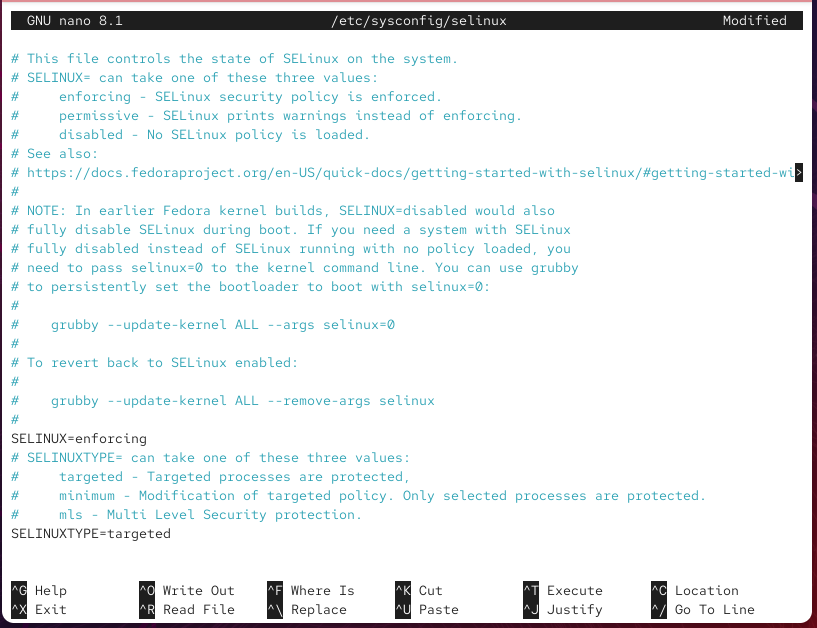


Рис. 5: Редактирование конфигурации SELinux (включение)

После перезагрузки система вывела предупреждение о необходимости переразметки меток безопасности (relabeling), что может занять некоторое время.

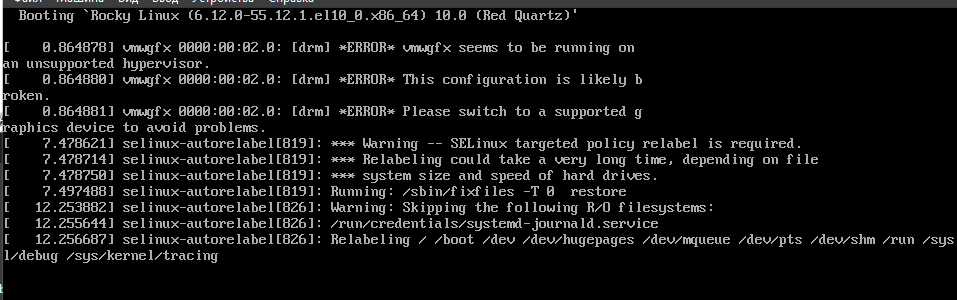


Рис. 6: Переразметка меток безопасности при загрузке

После завершения перезагрузки команда sestatus -v показала, что SELinux снова работает в режиме enforcing.

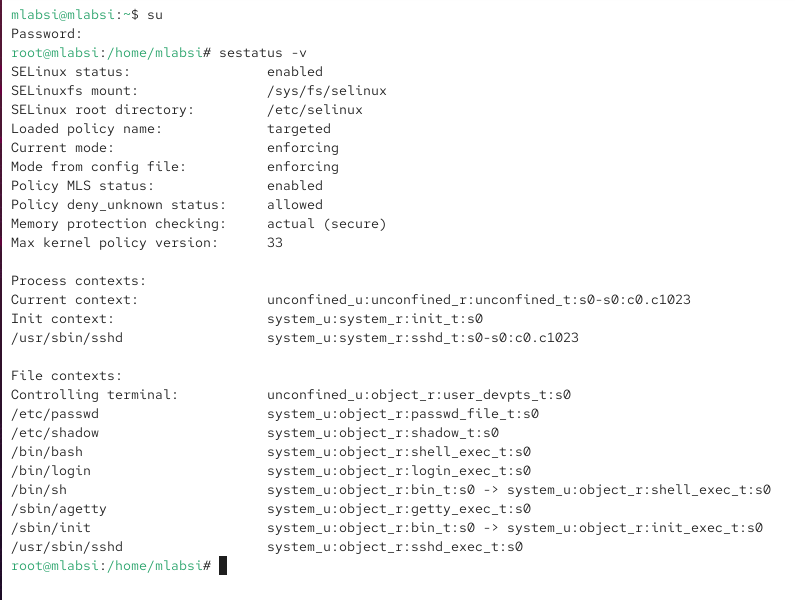


Рис. 7: Проверка состояния SELinux после включения

## 2.5 Восстановление контекста безопасности файлов

Для примера использовался системный файл /etc/hosts.  
При проверке его контекста была получена метка system\_u:object\_r:net\_conf\_t:s0.  
После копирования файла в домашний каталог его контекст изменился на admin\_home\_t, поскольку копирование создает новый объект.  
При перемещении файла обратно в /etc контекст остался прежним — admin\_home\_t.  
Для восстановления корректного контекста была использована команда restorecon -v /etc/hosts, после чего контекст вернулся к исходному — net\_conf\_t.

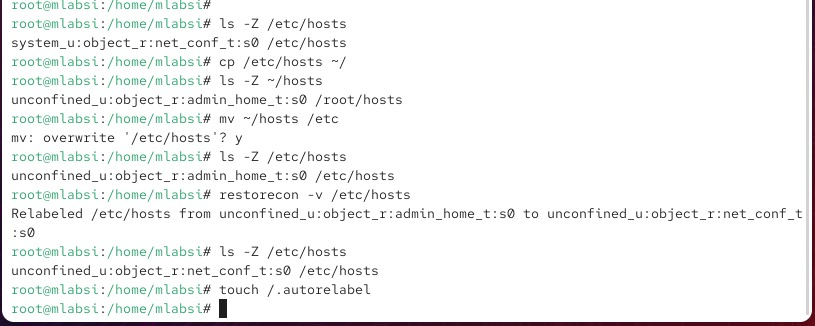


Рис. 8: Восстановление контекста безопасности файла /etc/hosts

Для массового восстановления контекста безопасности на всей файловой системе была создана команда touch /.autorelabel.  
После перезагрузки система автоматически провела процесс перемаркировки (relabeling).

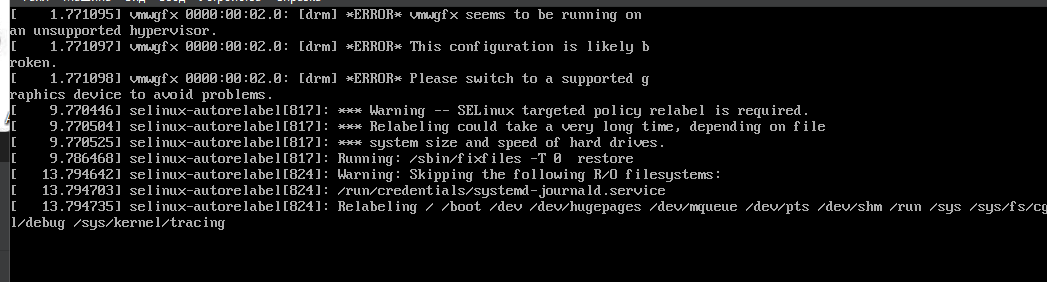


Рис. 9: Автоматическая перемаркировка файловой системы при загрузке

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

Для начала были установлены необходимые пакеты httpd и lynx.  
Создан новый каталог для веб-контента /web и файл index.html с текстом «Welcome to my web-server».

В конфигурационном файле /etc/httpd/conf/httpd.conf были внесены изменения:  
строка DocumentRoot “/var/www/html” закомментирована и заменена на DocumentRoot “/web”.  
Также добавлен новый раздел с правами доступа:

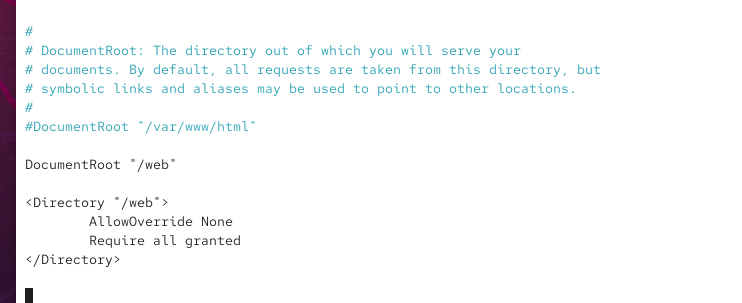


Рис. 10: Изменение конфигурации веб-сервера

После запуска веб-сервера и обращения к адресу http://localhost отображалась стандартная тестовая страница Rocky Linux, что указывает на отсутствие доступа к пользовательскому каталогу.

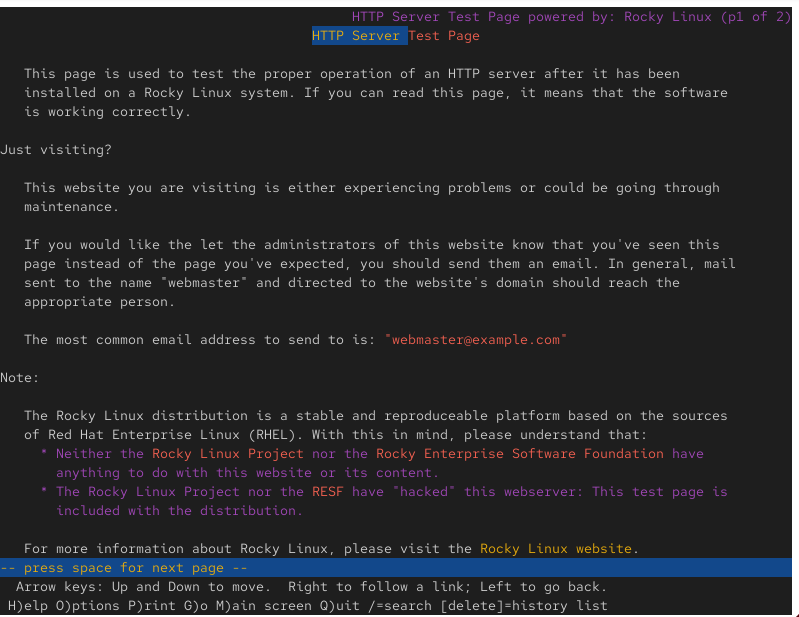


Рис. 11: Тестовая страница Rocky Linux

Для решения этой проблемы был задан новый контекст безопасности каталогу /web.  
Выполнена команда semanage fcontext для назначения типа httpd\_sys\_content\_t и восстановлен контекст при помощи restorecon.  
В результате каталог /web и файл index.html получили корректные метки безопасности.

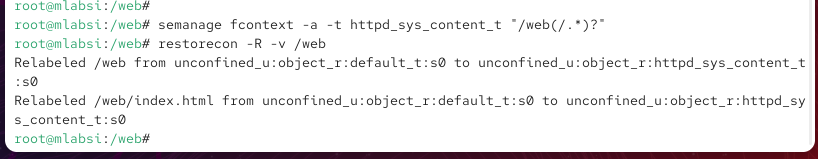


Рис. 12: Назначение контекста безопасности каталогу /web

После этого при повторном обращении к серверу в браузере lynx отображается страница с пользовательским сообщением «Welcome to my web server».

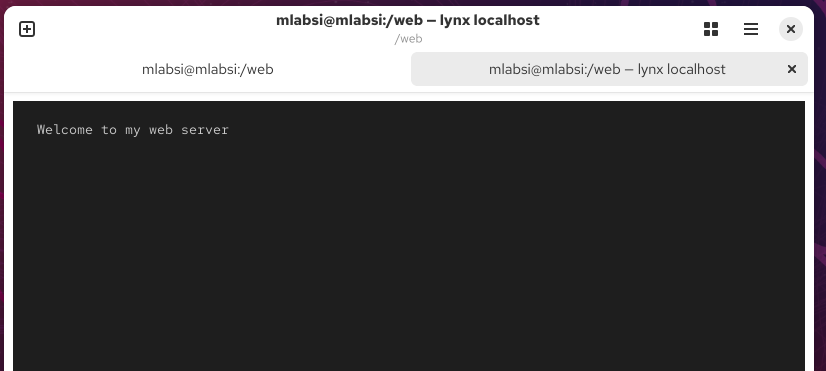


Рис. 13: Доступ к пользовательской веб-странице

## 2.7 Работа с переключателями SELinux

Для анализа переключателей SELinux, связанных с FTP-службой, была выполнена команда getsebool -a | grep ftp.  
В списке найден параметр ftpd\_anon\_write, отвечающий за возможность анонимной записи через FTP, который по умолчанию имел состояние off.

Затем была выполнена команда semanage boolean -l | grep ftpd\_anon для отображения описания параметра и его текущего состояния.  
Параметр ftpd\_anon\_write был временно включён при помощи setsebool ftpd\_anon\_write on.  
Проверка показала, что состояние изменилось на on, однако настройка постоянной (persistent) конфигурации осталась выключенной.

Для включения постоянной настройки был применён ключ -P

Повторная проверка с помощью semanage boolean -l | grep ftpd\_anon показала, что переключатель ftpd\_anon\_write теперь включён как временно, так и постоянно (on , on).

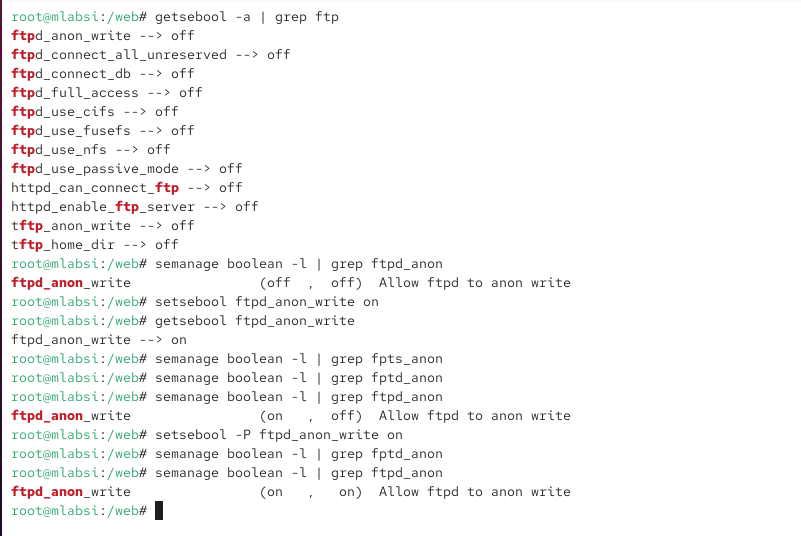


Рис. 14: Работа с переключателями SELinux для FTP

# 3 Контрольные вопросы

1. **Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете?**  
   Для временного перевода SELinux в разрешающий режим используется команда  
   **setenforce 0**.  
   После этого можно проверить состояние командой **getenforce**.
2. **Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете?**  
   Для вывода полного списка переключателей SELinux используется команда  
   **getsebool -a**.  
   Она отображает все логические параметры (boolean) и их текущее состояние.
3. **Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита?**  
   Для интерпретации сообщений SELinux используется пакет **setroubleshoot**.  
   Он позволяет получать понятные уведомления о причинах блокировок и рекомендациях по их устранению.
4. **Какие команды вам нужно выполнить, чтобы применить тип контекста httpd\_sys\_content\_t к каталогу /web?**  
   Необходимо выполнить следующие команды:
   * \*\*semanage fcontext -a -t httpd\_sys\_content\_t “/web(/.\*)?“\*\* — добавляет правило для назначения типа контекста.
   * **restorecon -R -v /web** — применяет изменения и обновляет контекст безопасности каталога.
5. **Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux?**  
   Для полного отключения SELinux необходимо отредактировать файл **/etc/sysconfig/selinux**,  
   изменив строку **SELINUX=enforcing** на **SELINUX=disabled**.
6. **Где SELinux регистрирует все свои сообщения?**  
   Журнал событий SELinux записывается в файл **/var/log/audit/audit.log**.  
   Если служба аудита недоступна, сообщения также могут появляться в **/var/log/messages**.
7. **Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию?**  
   Для просмотра контекстов и разрешённых типов, связанных с FTP, используется команда  
   **semanage fcontext -l | grep ftp**.  
   Она показывает все файлы и каталоги, имеющие контексты, применяемые к FTP-службе.
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 с помощью  
   **setenforce 0** и проверить, изменилось ли поведение сервиса.  
   Если после этого сервис начал работать корректно, значит, причина связана с политикой SELinux.

# 4 Заключение

В ходе работы были изучены принципы управления безопасностью с помощью SELinux, включая изменение режимов работы, настройку контекстов безопасности и использование переключателей политик.