Лабораторная работа №9

Управление SELinux

Комягин Андрей Николаевич

Содержание

# 1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

# 2 Выполнение лабораторной работы

## 2.1 Управление режимами SELinux

Просмотрим текущую информацию о состоянии SELinux. Посмотрим, в каком режиме работает SELinux, изменим режим работы SELinux на разрешающий. (рис. 1).

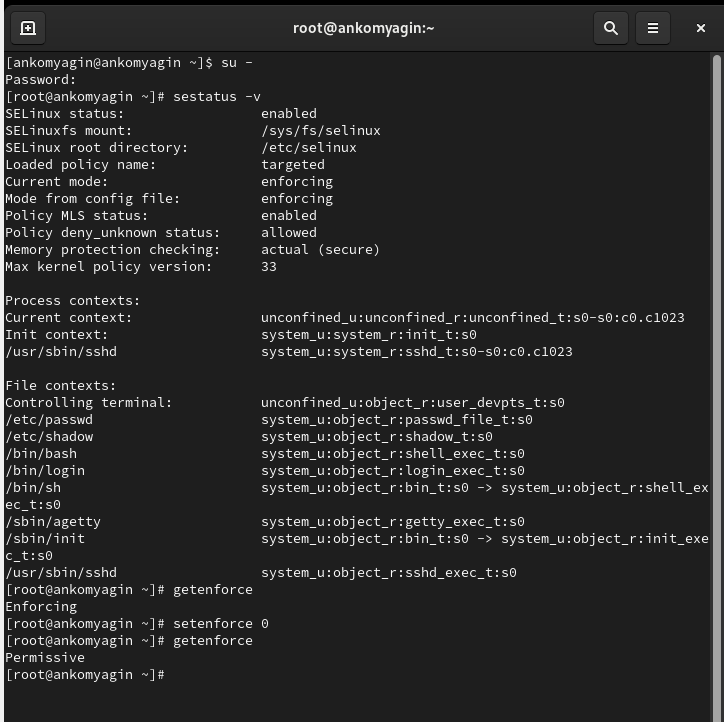


Рис. 1: Состояние и режим работы SELinux

1. **SELinux status**:
   * enabled: SELinux включен и работает.
2. **SELinuxfs mount**:
   * Указывает, где в файловой системе смонтирована файловая система SELinux (/sys/fs/selinux).
3. **SELinux root directory**:
   * Путь к директории, где хранятся конфигурационные файлы SELinux (/etc/selinux).
4. **Loaded policy name**:
   * targeted: Загружена политика “targeted”, которая фокусируется на защите определённых процессов.
5. **Current mode**:
   * enforcing: SELinux работает в режиме принудительного контроля, что означает, что он будет блокировать действия, которые нарушают политику безопасности.
6. **Mode from config file**:
   * Показывает, что режим, указанный в конфигурационном файле, также “enforcing”.
7. **Policy MLS status**:
   * enabled: Указывает на то, что поддержка многоуровневой безопасности (MLS) включена.
8. **Policy deny\_unknown status**:
   * Указывает, разрешено ли блокирование неизвестных объектов.
9. **Memory protection checking**:
   * Указывает на проверку защиты памяти.
10. **Max kernel policy version**:

* Указывает максимальную версию политики ядра.

1. **Process contexts**:

* Отображает контексты процессов, показывая текущие контексты безопасности для различных процессов.

1. **File contexts**:

* Показаны контексты безопасности для различных файлов.

В файле /etc/sysconfig/selinux с помощью редактора установим **SELINUX=disabled** (рис. 2).

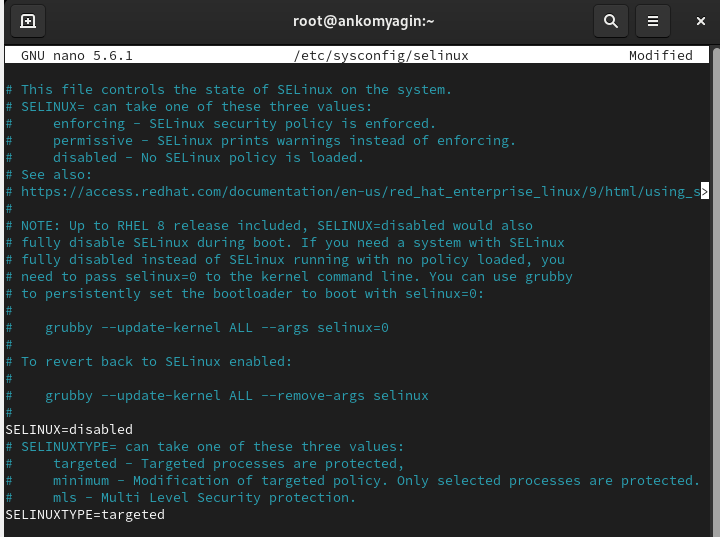


Рис. 2: SELINUX=disabled

Посмотрим статус SELinux. Попробуем переключить режим работы SELinux. Мы не можем переключаться между отключённым и принудительным режимом без перезагрузки системы. (рис. 3).

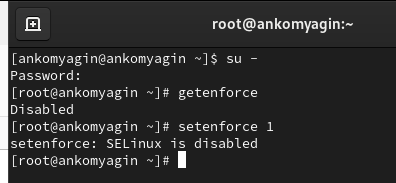


Рис. 3: Переключение режимов

Откроем файл /etc/sysconfig/selinux с помощью редактора и установим: **SELINUX=enforcing** (рис. 4).

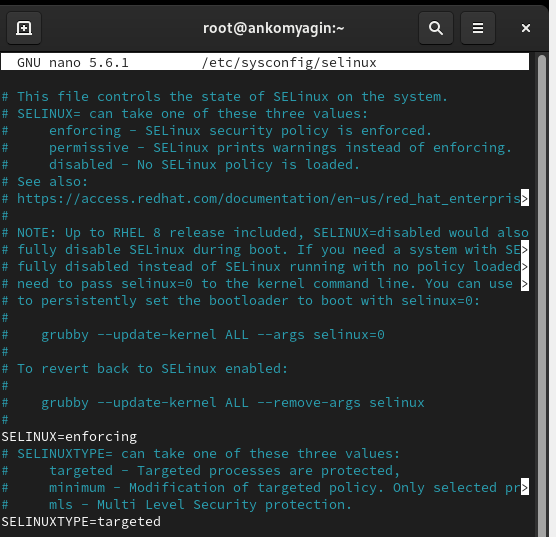


Рис. 4: SELINUX=enforcing

После перезагрузки просмотрим текущую информацию о состоянии SELinux (рис. 5).

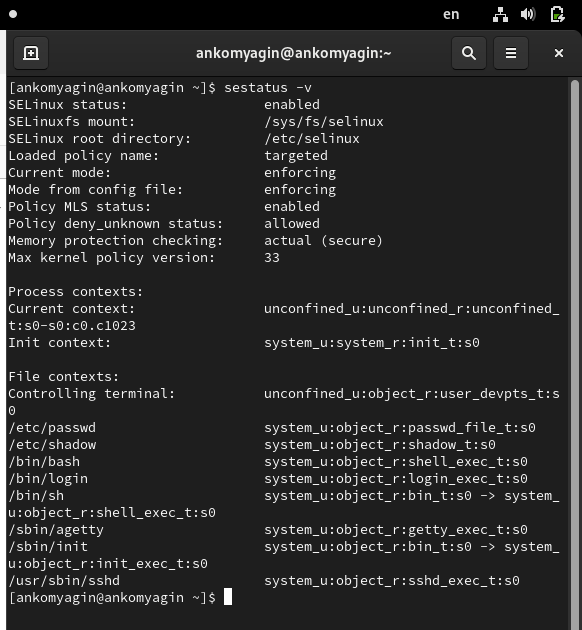


Рис. 5: информация о состоянии

## 2.2 Использование restorecon для восстановления контекста безопасности

Посмотрим контекст безопасности файла /etc/hosts. Мы увидим, что у файла есть метка контекста net\_conf\_t.

Скопируем файл /etc/hosts в домашний каталог. Проверим контекст файла ~/hosts: Поскольку копирование считается созданием нового файла, то параметр контекста в файле ~/hosts, расположенном в домашнем каталоге, станет admin\_home\_t.

Попытаемся перезаписать существующий файл hosts из домашнего каталога в каталог /etc: mv ~/hosts /etc

Убедиимя, что тип контекста по-прежнему установлен на admin\_home\_t:

Исправим контекст безопасности и убедимся, что тип контекста изменился:

Для массового исправления контекста безопасности на файловой системе введём **touch /.autorelabel**(рис. 6)

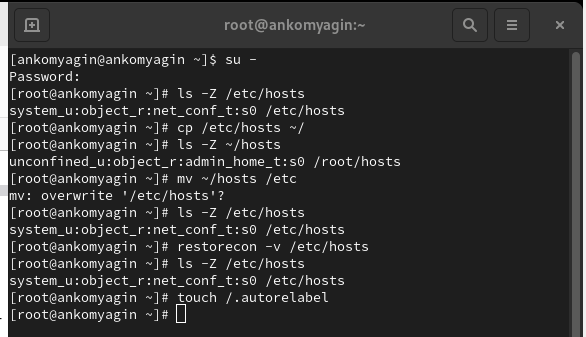


Рис. 6: контекст безопасности

Перезагрузим систему. Файловая система автоматически перемаркирована(рис. 7)



Рис. 7: перемаркировка

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

Установим необходимое программное обеспечение (рис. 8).

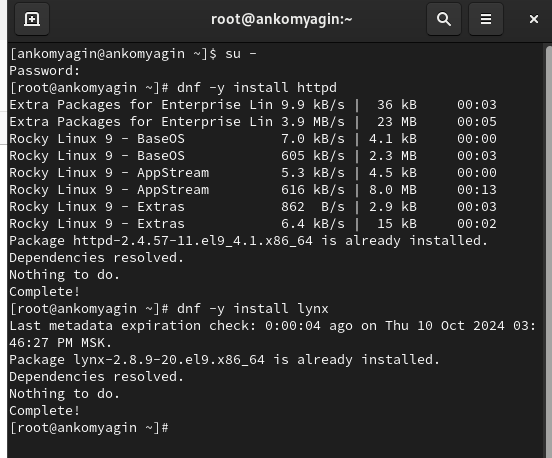


Рис. 8: установка по

Создадим новое хранилище для файлов web-сервера. Создадим файл index.html в каталоге с контентом веб-сервера и поместим в файл **Welcome to my web-server**(рис. 9)

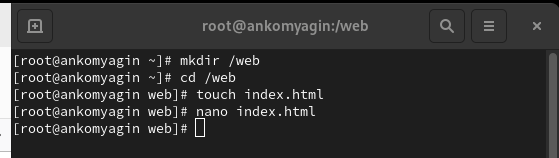


Рис. 9: web-сервер

Отредактируем файл **/etc/httpd/conf/httpd.conf**(рис. 10)

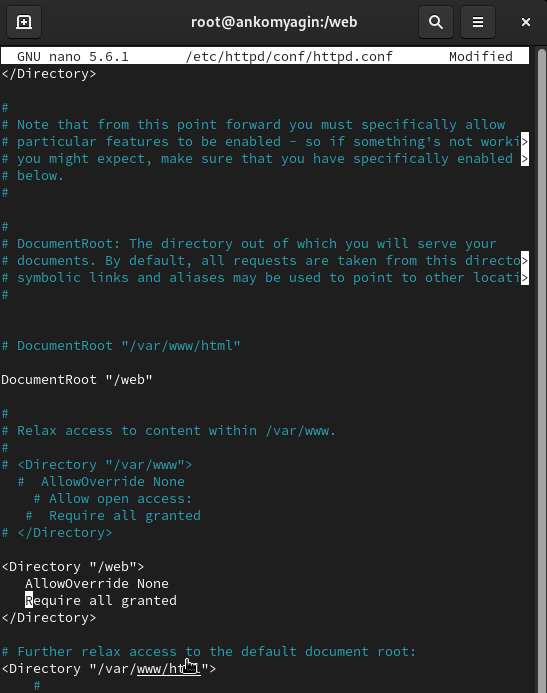


Рис. 10: редактирование /etc/httpd/conf/httpd.conf

Запустим веб-сервер и службу httpd(рис. 11)

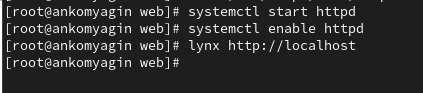


Рис. 11: запуск сервера и службы

Применим новую метку контекста к /web. Восстановим контекст безопасности. (рис. 12)

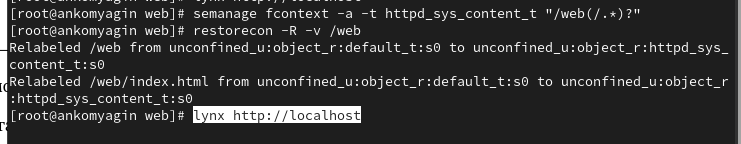


Рис. 12: новая метка контекста к веб

Обратимся к веб-серверу(рис. 13)

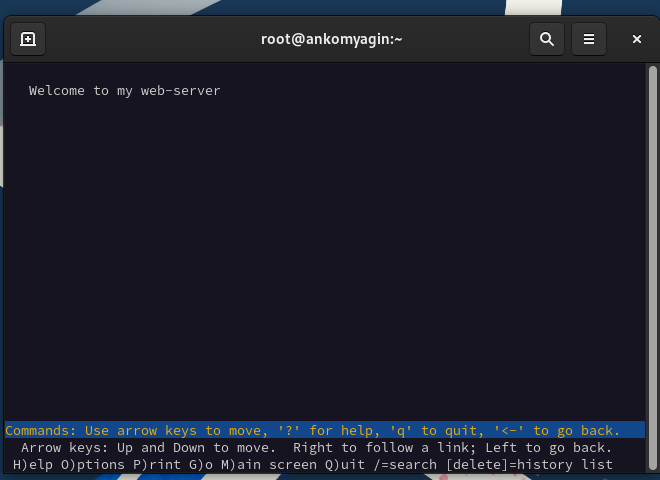


Рис. 13: веб-сервер

## 2.4 Работа с переключателями SELinux

Перегрузим систему командой reboot. Вновь перегрузим систему командой reboot. Убедимся, что система загрузилась в графическом режиме(рис. 14)

|  |
| --- |
| режимы системы |

Рис. 14: режимы системы

# 3 Контрольные вопросы

# 4 Вывод

В ходе выполнения лабораторной работы я получил навыки управления системными службами операционной системы посредством systemd.

# Список литературы

[Туис, курс Администрирование операционных систем](https://esystem.rudn.ru/course/view.php?id=5946)