Отчёт о лабораторной работе

Лабораторная работа 9. Управление SELinux

Баранов Никита Дмитриевич

Содержание

# 1. Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

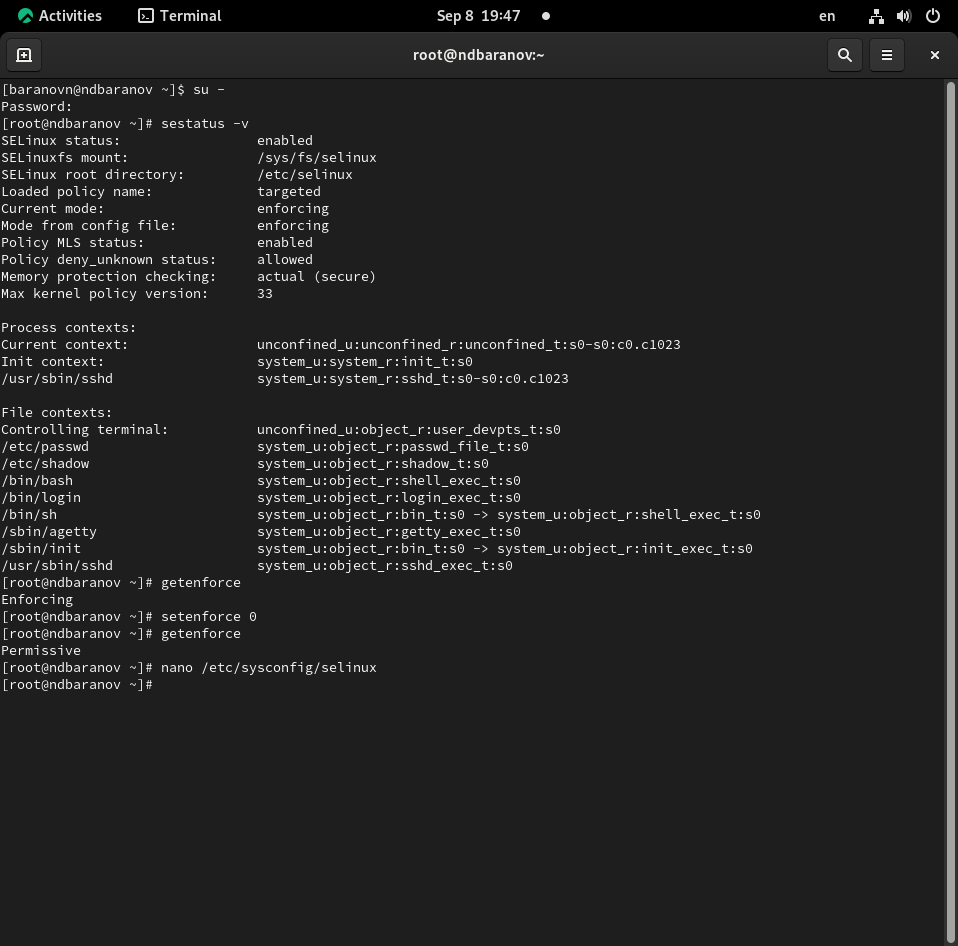
# 2. Задание

1. Продемонстрируйте навыки по управлению режимами SELinux (см. раздел 9.4.1).
2. Продемонстрируйте навыки по восстановлению контекста безопасности SELinux (см. раздел 9.4.2).
3. Настройте контекст безопасности для нестандартного расположения файлов вебслужбы (см. раздел 9.4.3).
4. Продемонстрируйте навыки работы с переключателями SELinux (см. раздел 9.4.4).

# 3. Выполнение лабораторной работы

## 3.1 Работа с режимами SELinux

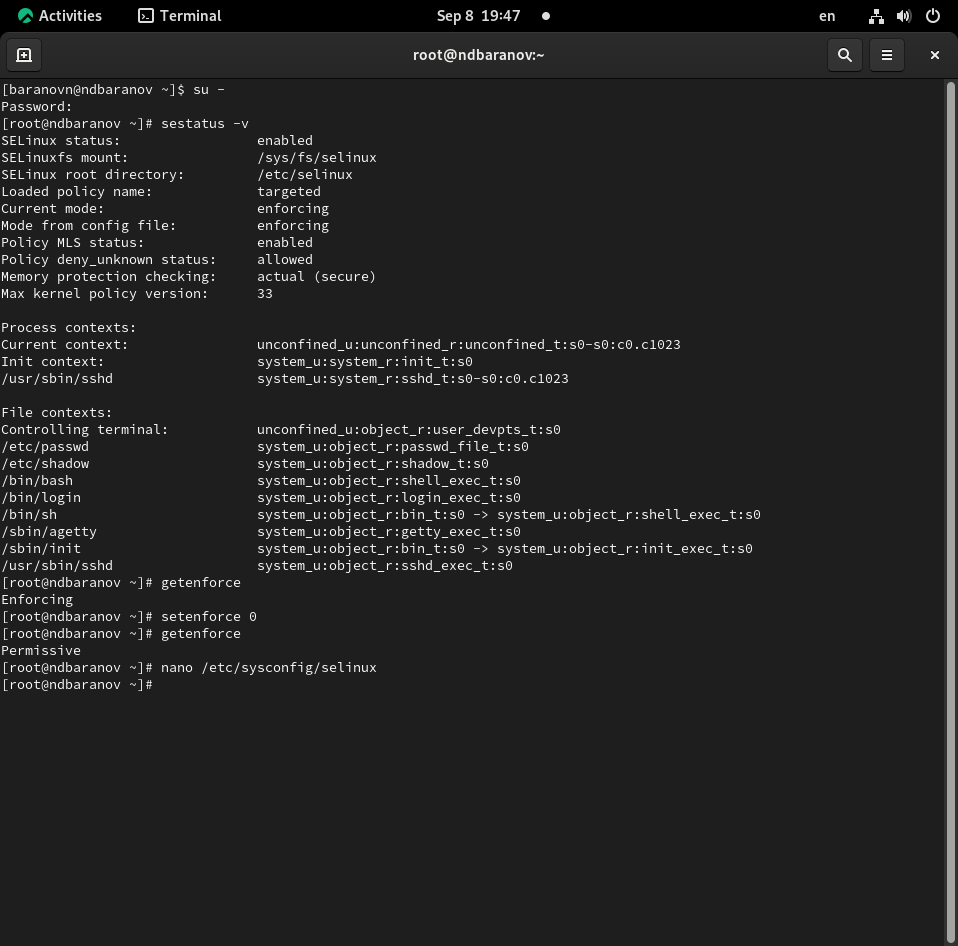
Получаем полномочия администратора и просматриваем текущую информацию о состоянии SELinux (рис. [**fig:001?**]).



Просмотр статуса SELinux

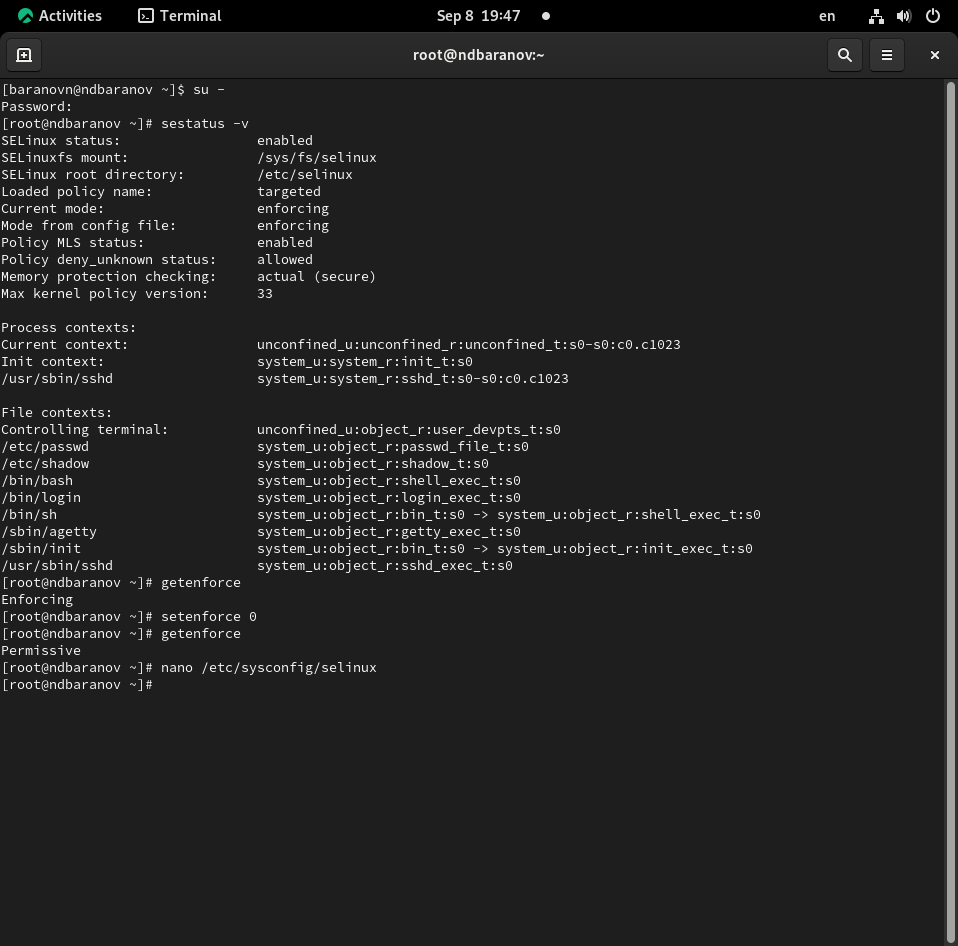
**Информация о состоянии SELinux:** - SELinux status: enabled - SELinux включен - SELinuxfs mount: /sys/fs/selinux - точка монтирования файловой системы SELinux - SELinux root directory: /etc/selinux - корневой каталог конфигурации SELinux - Loaded policy name: targeted - загружена политика targeted - Current mode: enforcing - текущий режим: принудительный - Mode from config file: enforcing - режим из конфигурационного файла: принудительный - Policy MLS status: enabled - поддержка многоуровневой безопасности включена - Policy deny\_unknown status: allowed - политика разрешает неизвестные статусы - Memory protection checking: actual (secure) - проверка защиты памяти: актуальная (безопасная)

Проверяем текущий режим работы SELinux (рис. [**fig:001?**]).



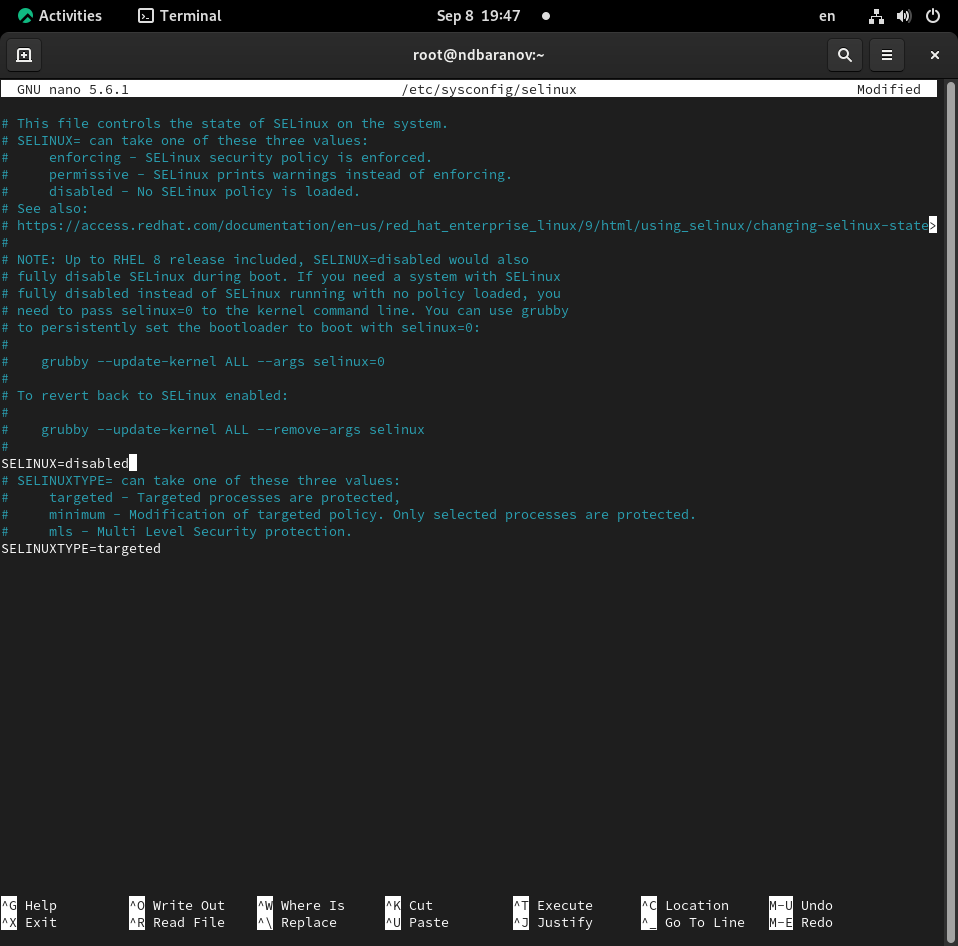
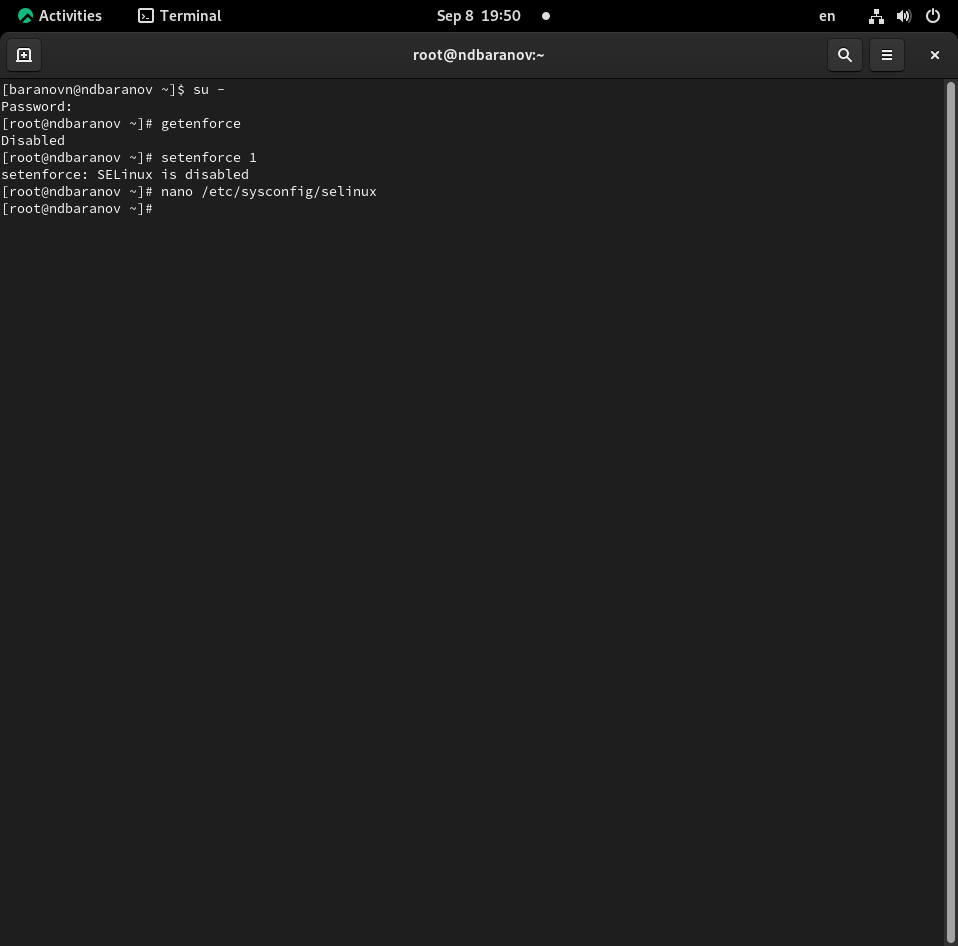
Проверка режима getenforce

Изменяем режим работы на разрешающий (Permissive) и проверяем (рис. [**fig:001?**]).

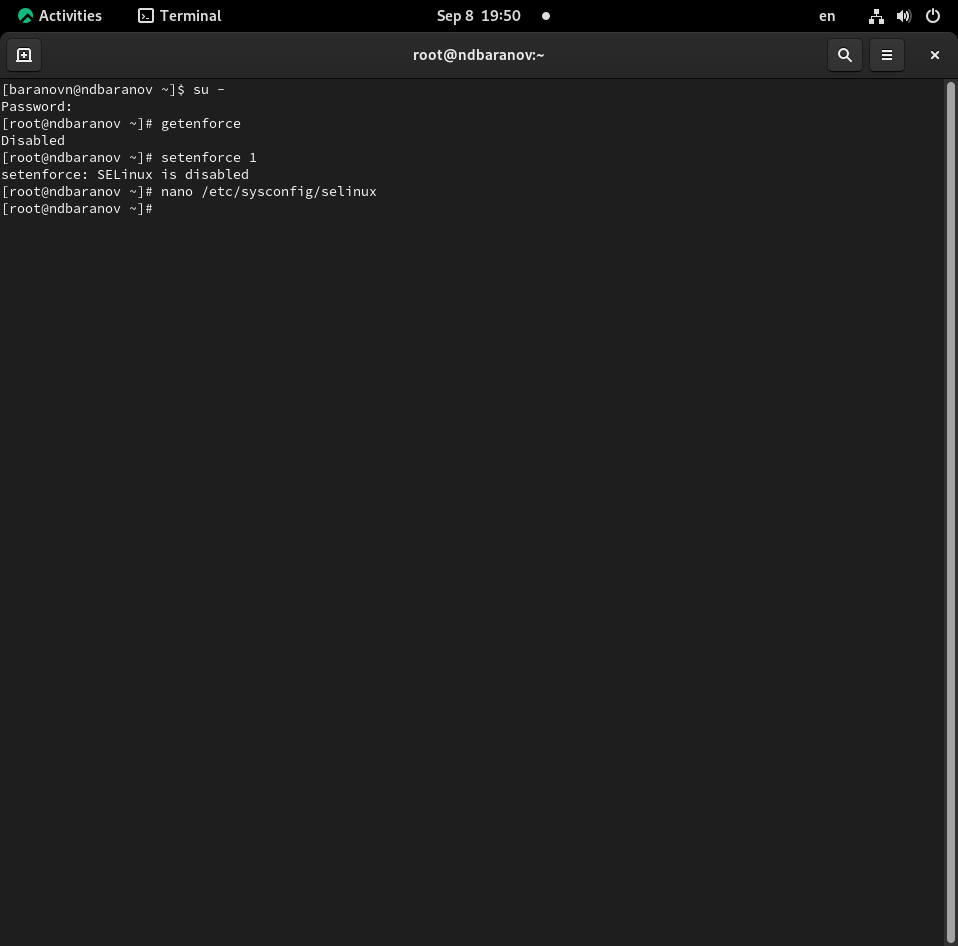


Изменение режима на Permissive

Редактируем конфигурационный файл для отключения SELinux (рис. [**fig:002?**], [**fig:003?**]).

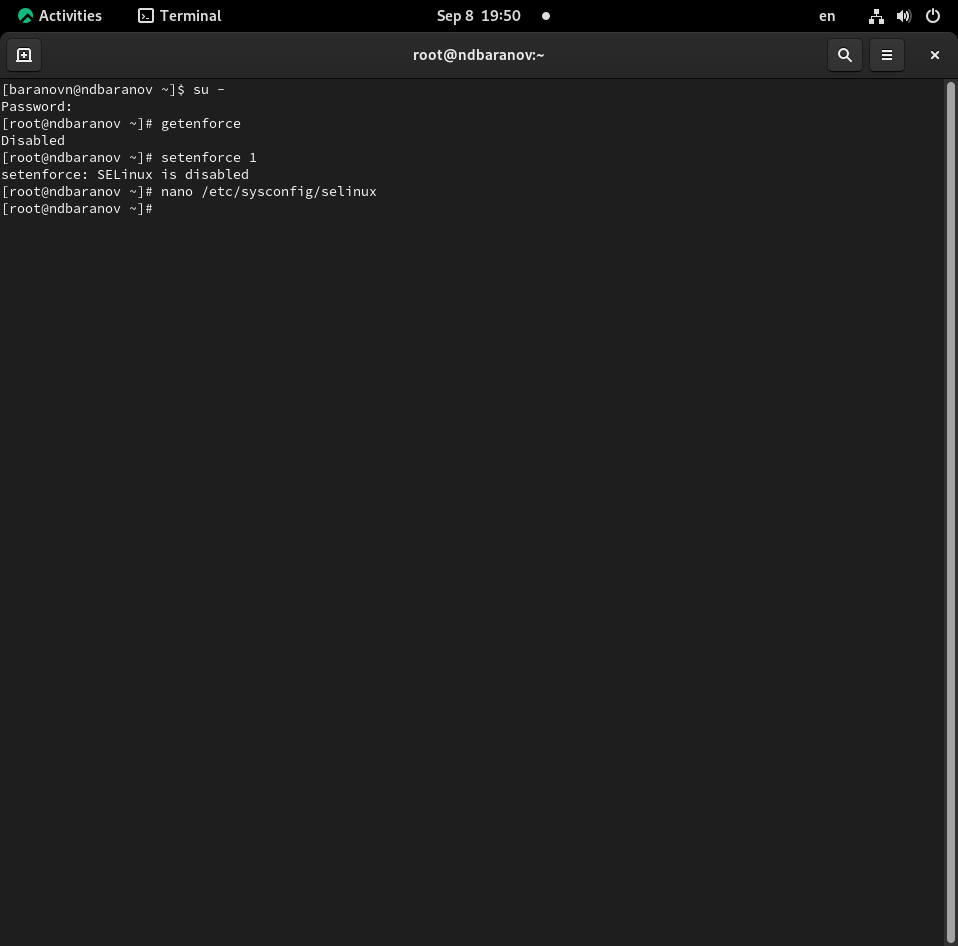
 

После перезагрузки проверяем статус SELinux (рис. [**fig:003?**]).



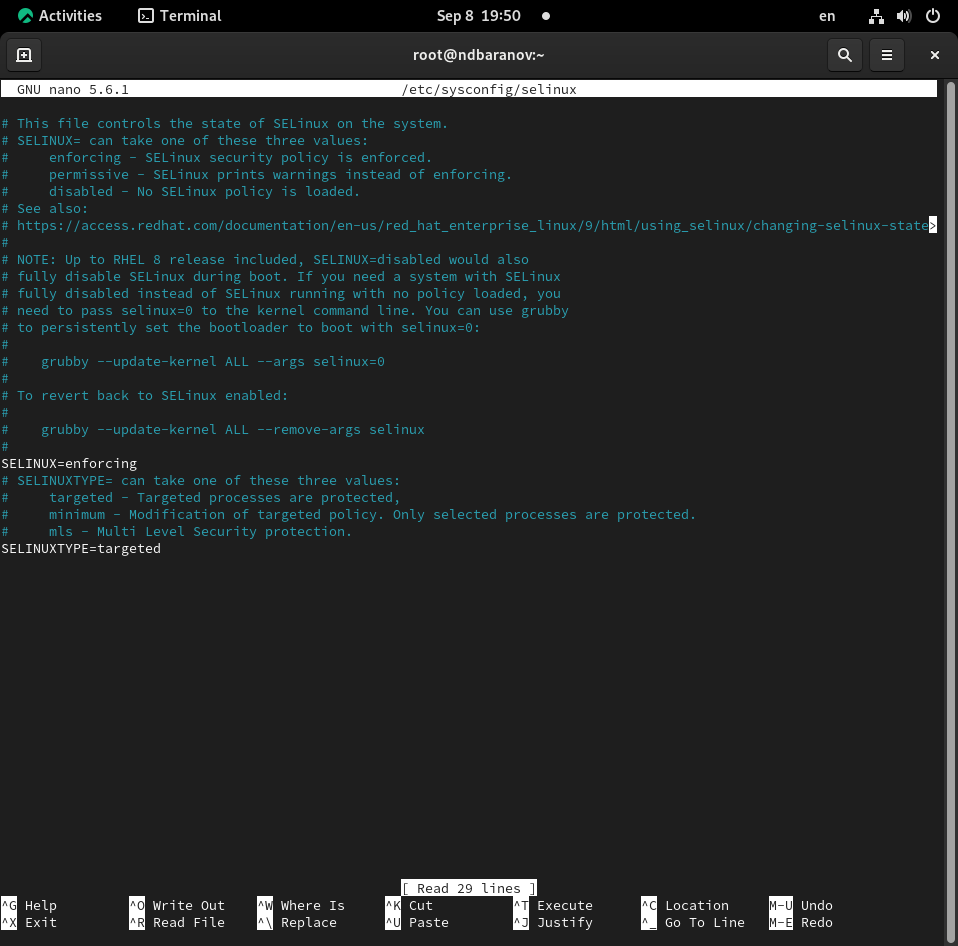
Проверка статуса после отключения

Пытаемся изменить режим работы SELinux при отключенном состоянии (рис. [**fig:003?**]).



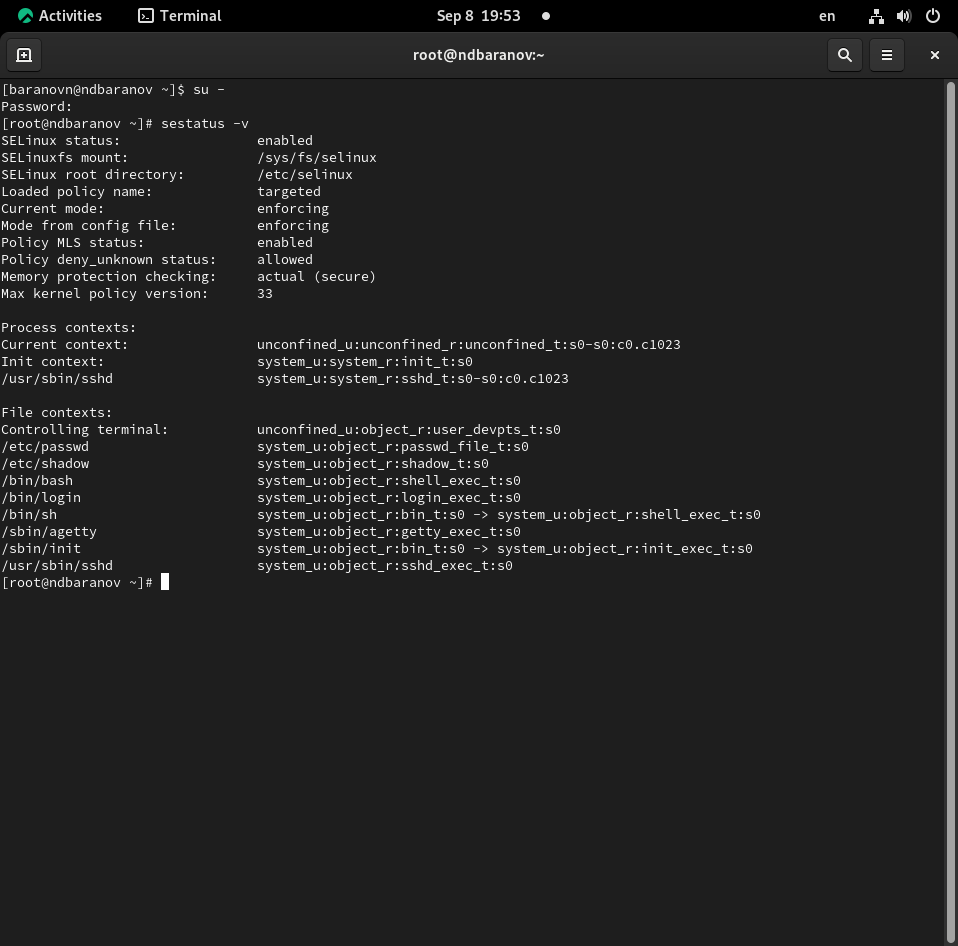
Попытка изменения режима при отключенном SELinux

Восстанавливаем режим enforcing через конфигурационный файл (рис. [**fig:004?**]).



Восстановление режима enforcing

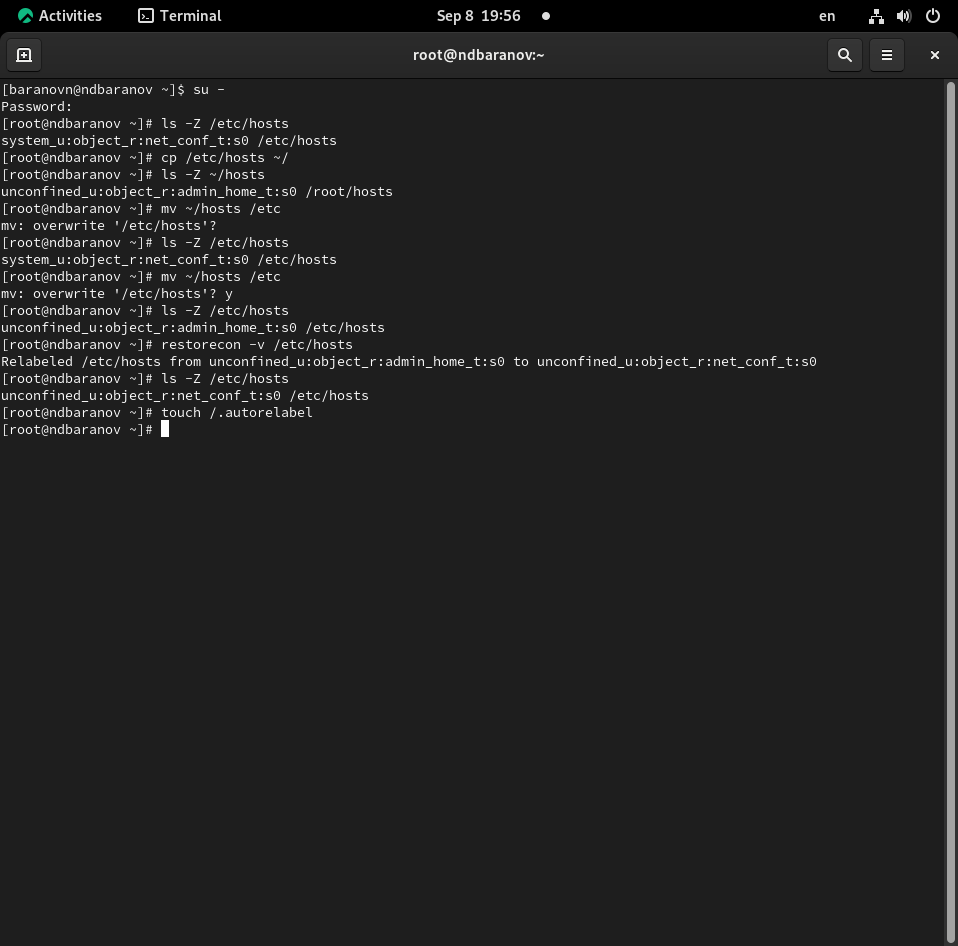
После перезагрузки проверяем статус SELinux (рис. [**fig:005?**]).



Проверка статуса после восстановления

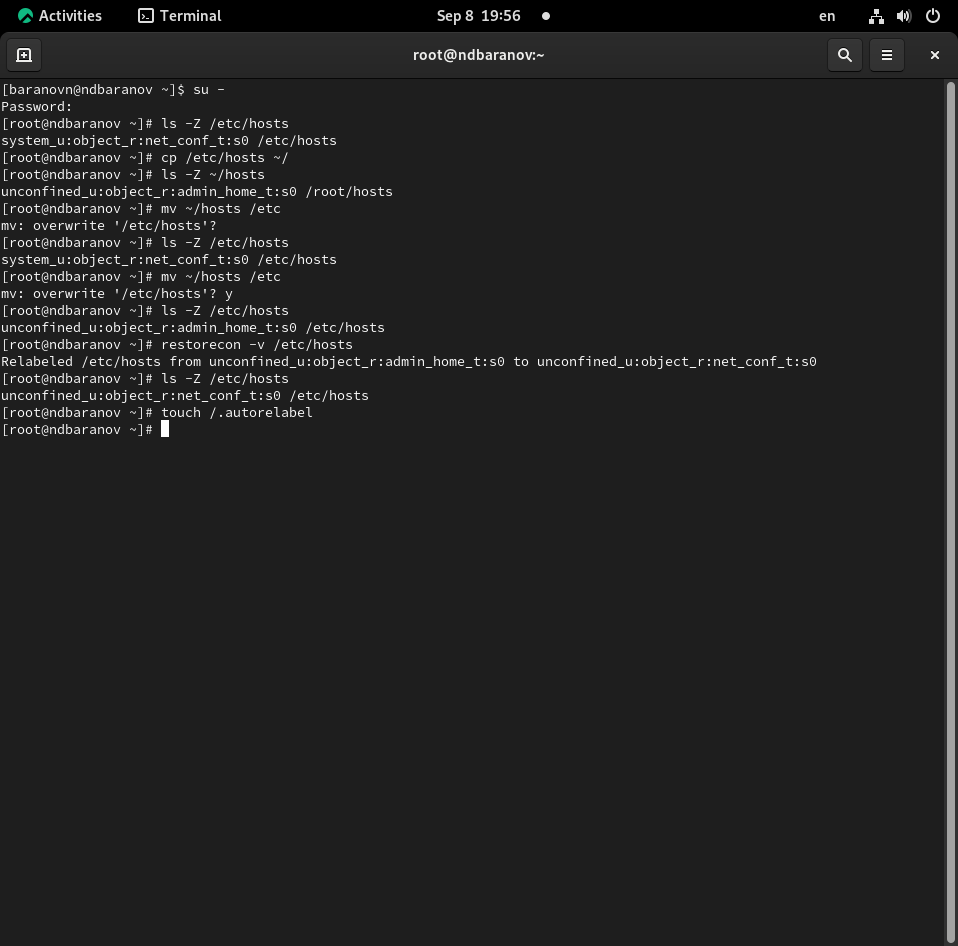
## 3.2 Работа с контекстами безопасности

Просматриваем контекст безопасности файла /etc/hosts (рис. [**fig:006?**]).



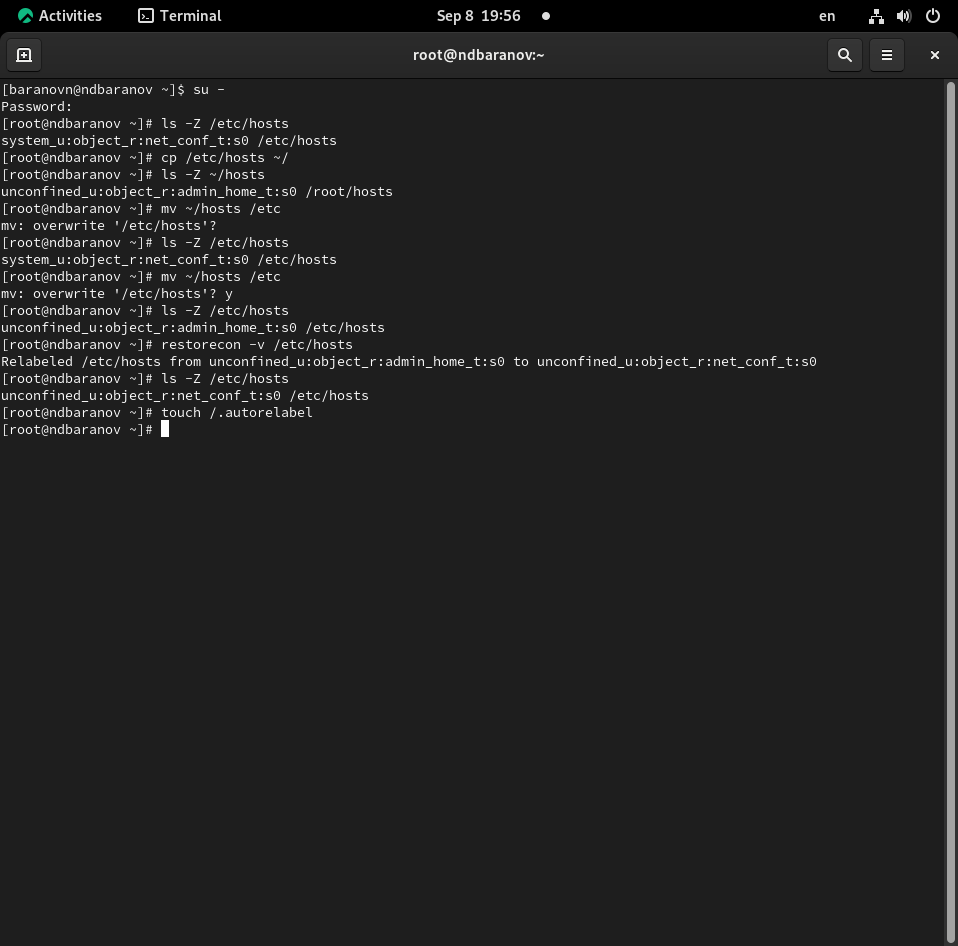
Контекст безопасности /etc/hosts

Копируем файл и проверяем изменение контекста (рис. [**fig:006?**]).



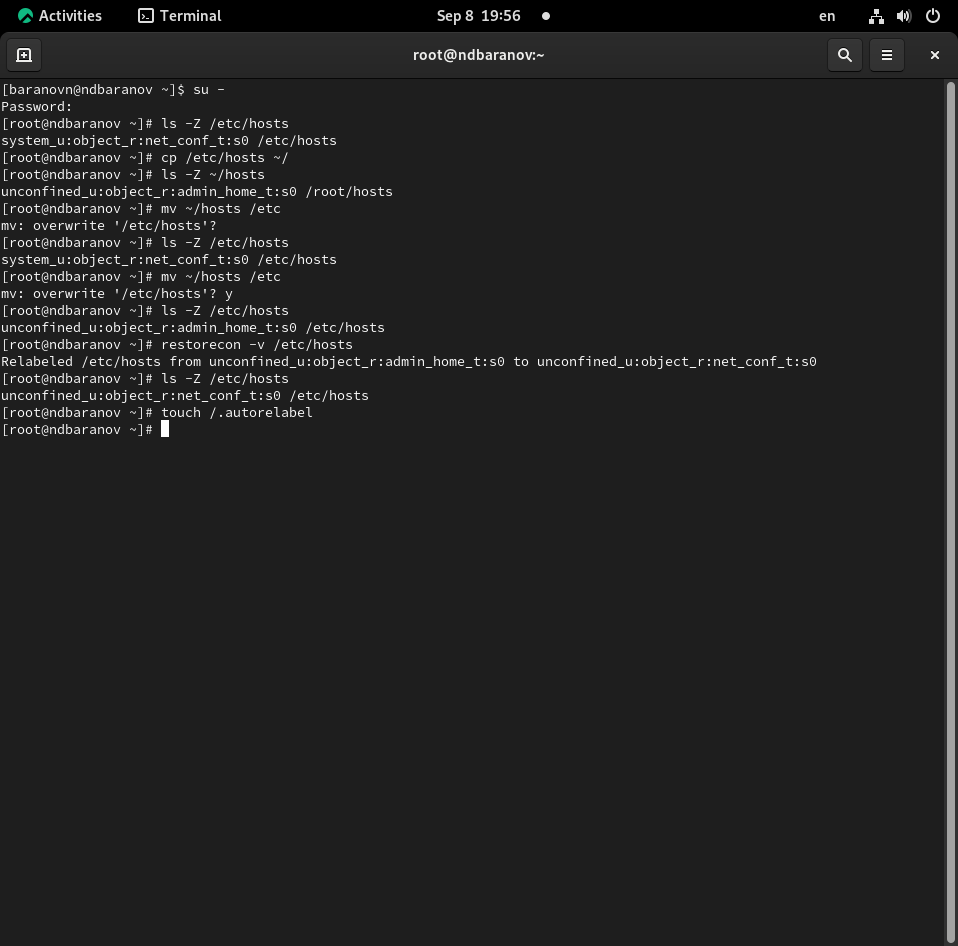
Копирование файла и проверка контекста

Перезаписываем файл и проверяем контекст (рис. [**fig:006?**]).



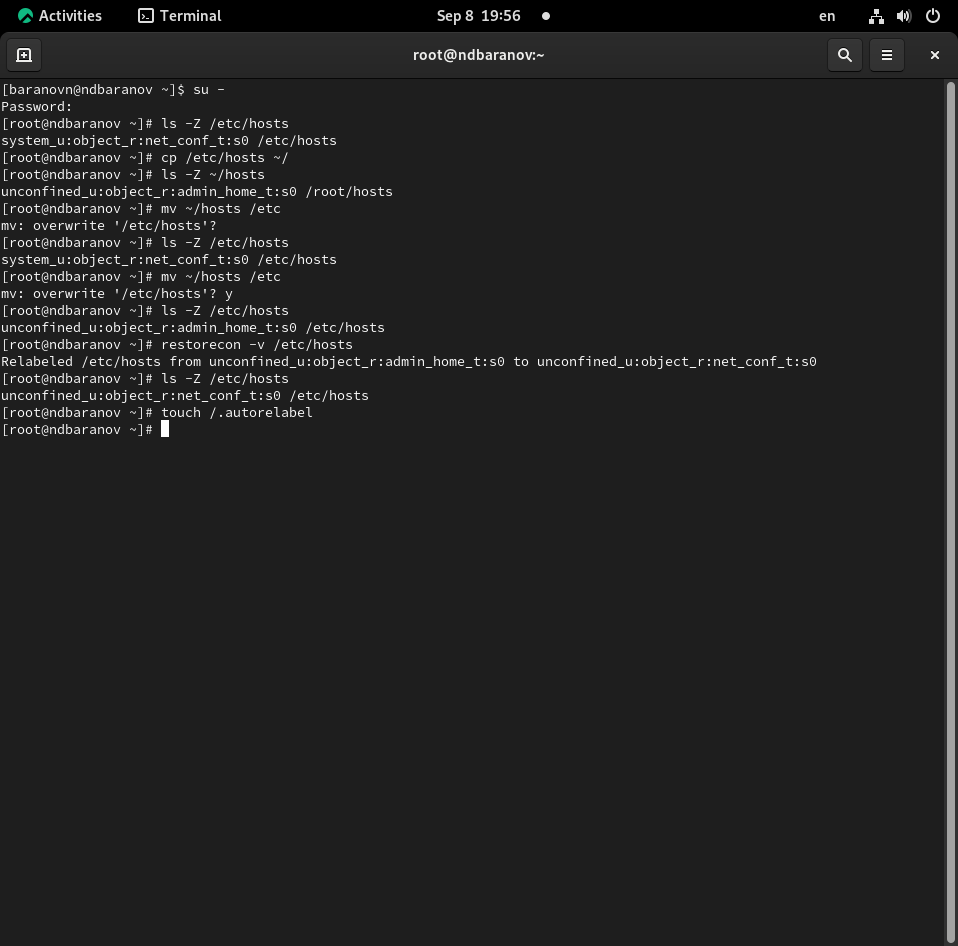
Перезапись файла и проверка контекста

Восстанавливаем правильный контекст безопасности (рис. [**fig:006?**]).



Восстановление контекста restorecon

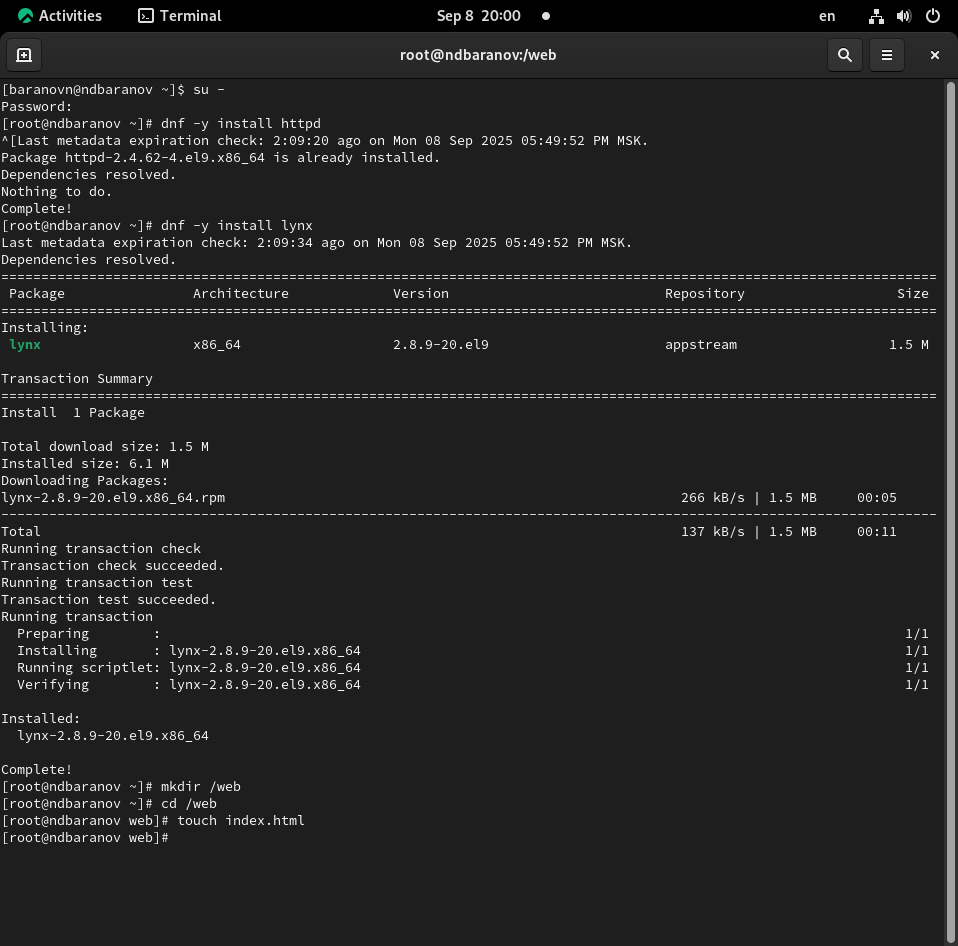
Создаем файл для массового восстановления контекстов (рис. [**fig:006?**]).



Создание файла для массового восстановления

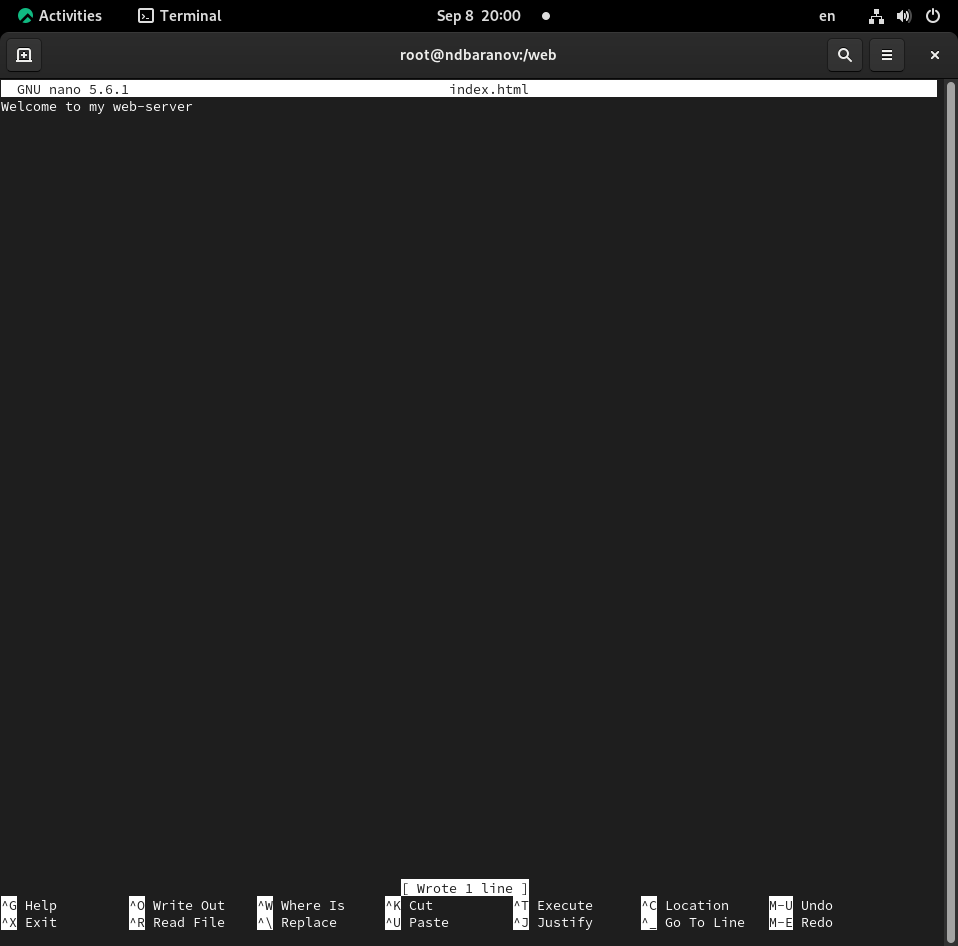
## 3.3 Настройка веб-сервера Apache с SELinux

Устанавливаем необходимое программное обеспечение (рис. [**fig:007?**]).

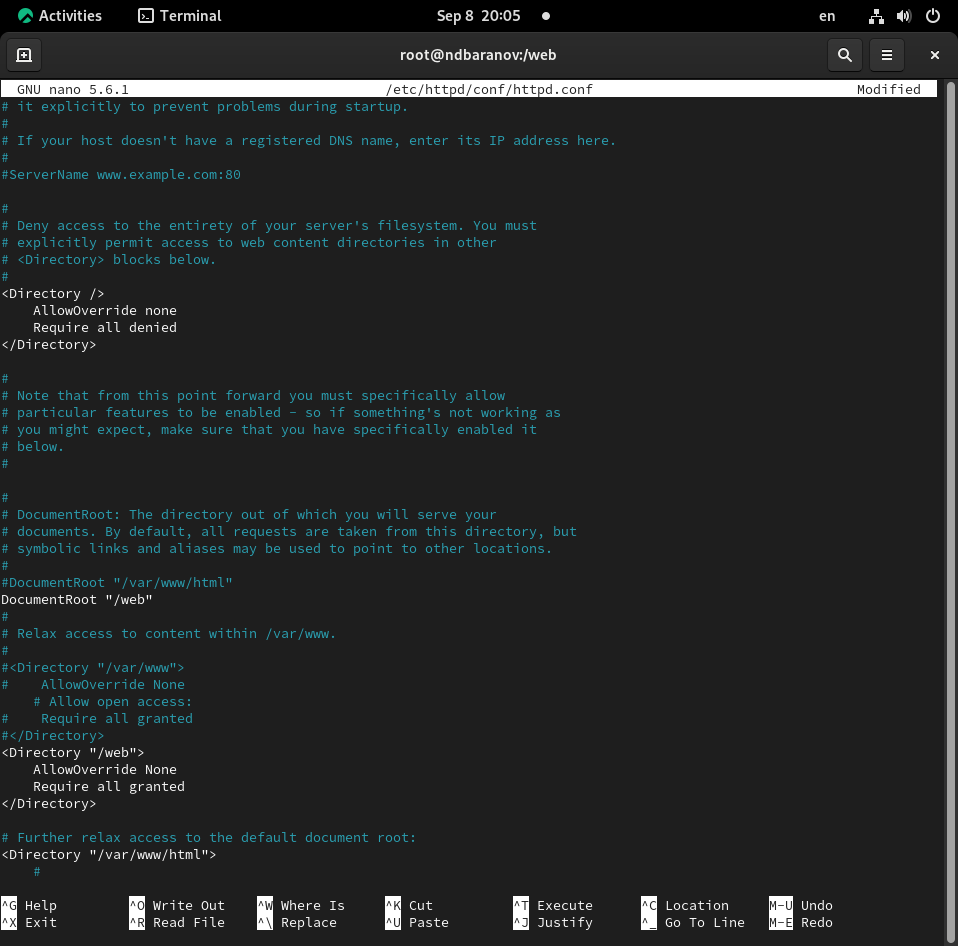


Установка httpd и lynx

Создаем каталог для веб-сервера и файл index.html (рис. [**fig:007?**], [**fig:008?**]).

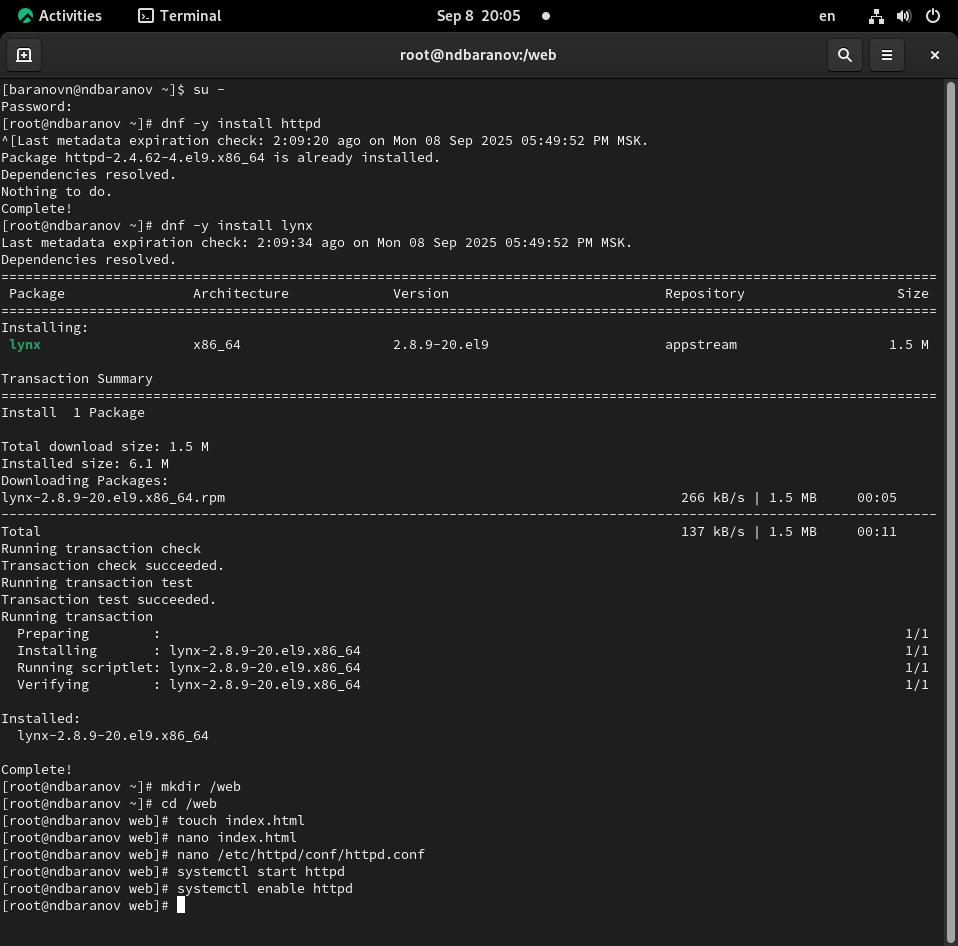
Создание каталога /web и файла index.html 

Настраиваем конфигурационный файл Apache (рис. [**fig:009?**]).



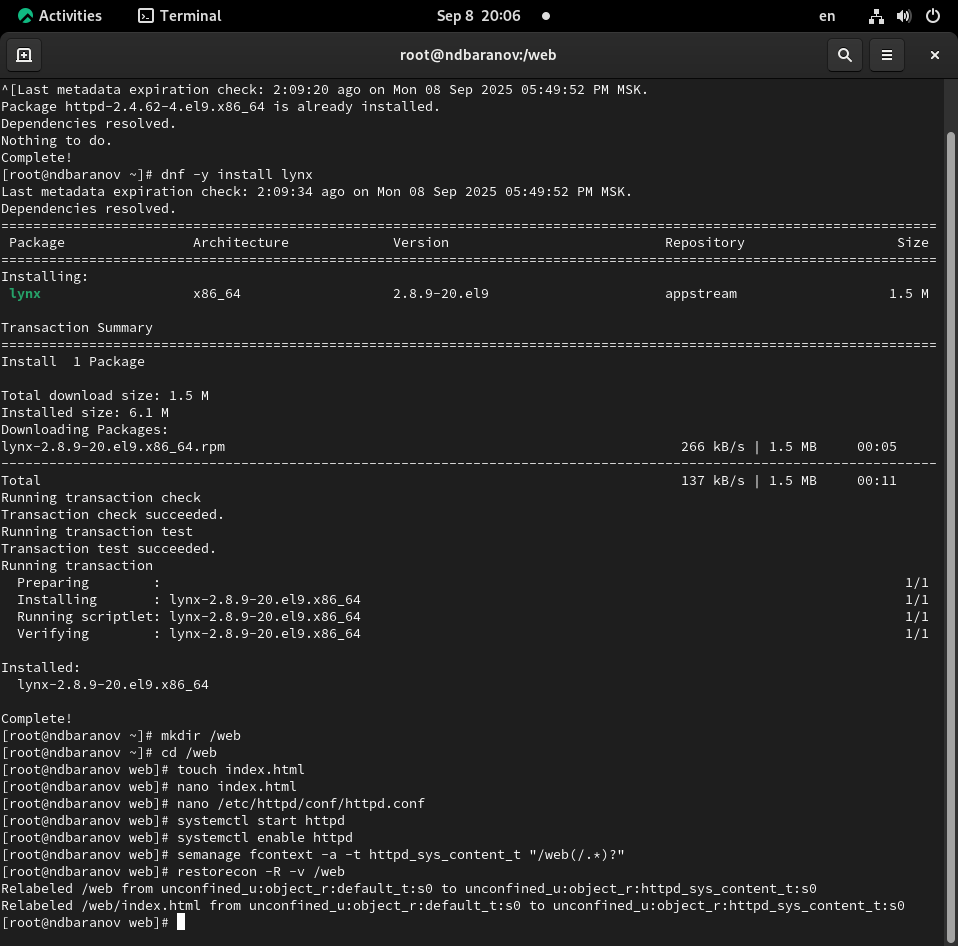
Настройка httpd.conf

Запускаем и включаем веб-сервер (рис. [**fig:010?**]).



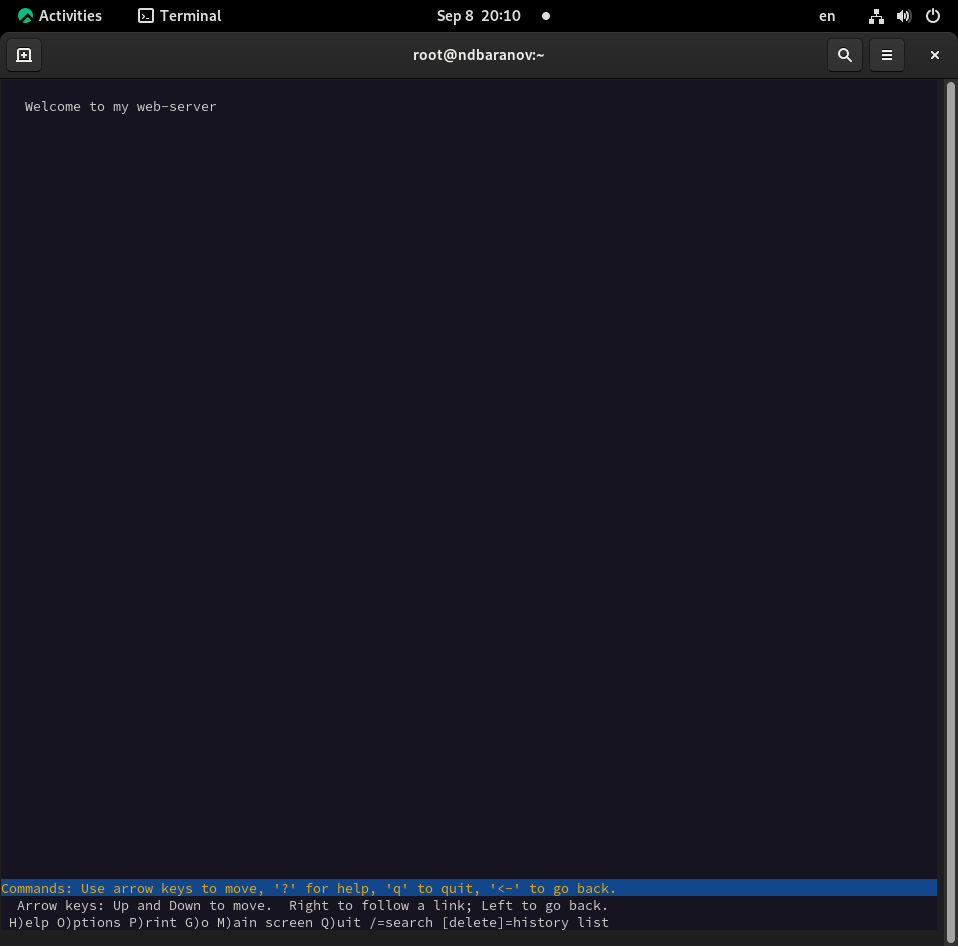
Запуск и включение httpd

Применяем правильный контекст безопасности для каталога /web (рис. [**fig:012?**]).



Настройка контекста безопасности для /web

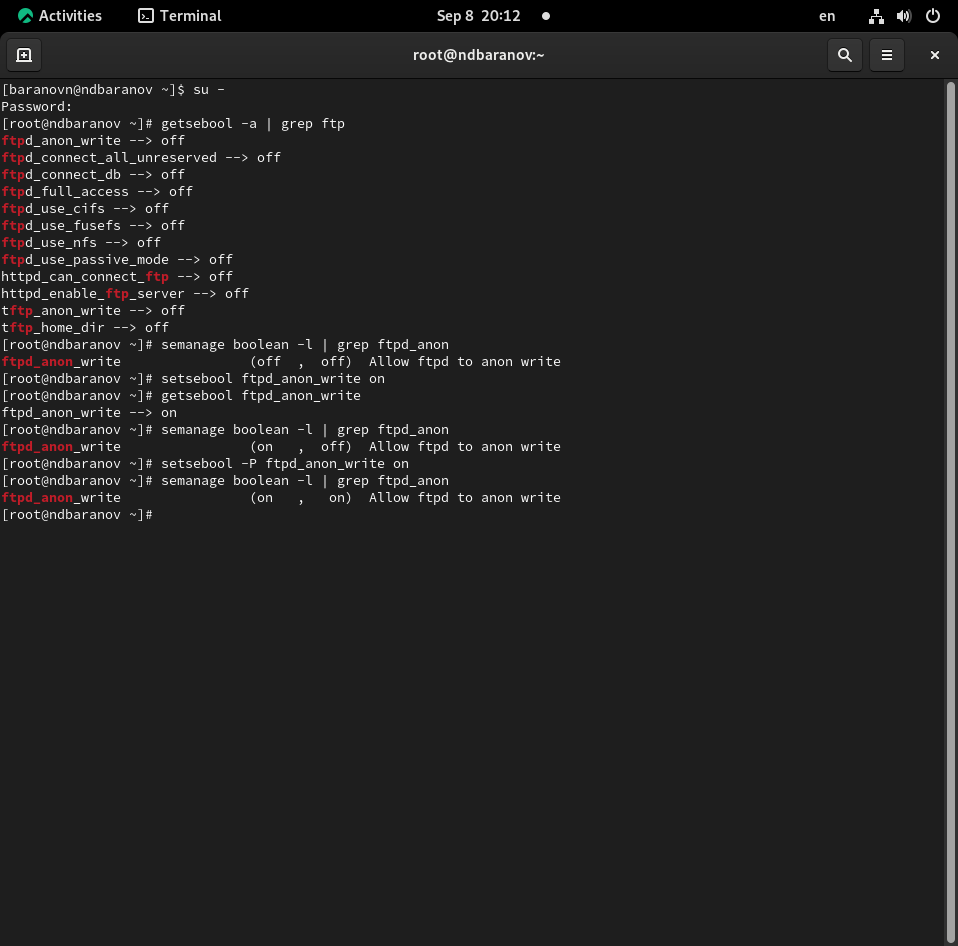
Проверяем доступ к веб-странице (рис. [**fig:013?**]).



Проверка доступа к веб-серверу

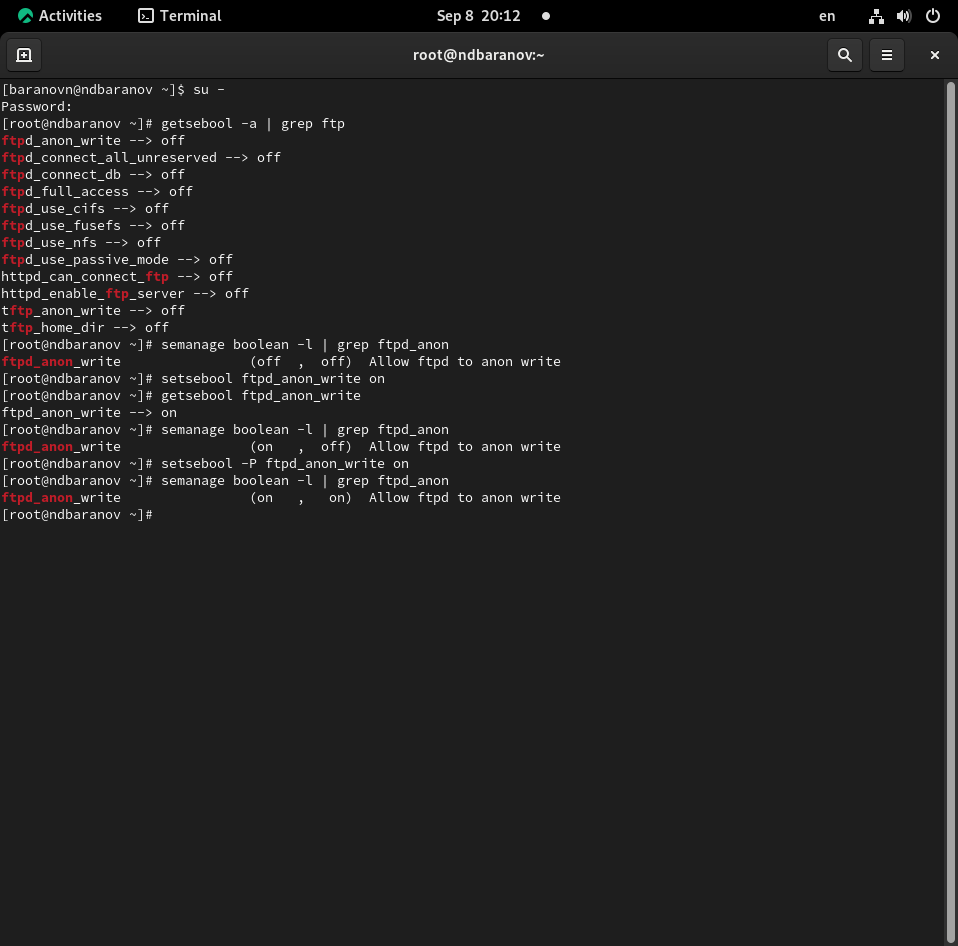
## 3.4 Управление переключателями SELinux для FTP

Просматриваем переключатели SELinux для службы FTP (рис. [**fig:014?**]).



Просмотр переключателей FTP

Изменяем значение переключателя ftpd\_anon\_write (рис. [**fig:014?**]).



Изменение переключателя ftpd\_anon\_write

**Состояние переключателя ftpd\_anon\_write после изменения:** - Время выполнения: включен (on) - Постоянная настройка: включена (on) - Описание: Allow ftpd to anon write (Разрешить анонимную запись для ftpd)

# 4. Выводы

Мы получили навыки работы с контекстом безопасности и политиками SELinux.

# Список литературы