Отчет по лабораторной работе №9

**Отчет о мониторинге и настройке системных журналов**

Лупупа Чилеше

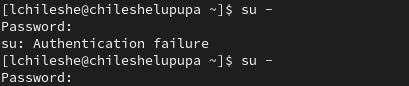
Цель работ

Цель данной лабораторной работы – изучение основ управления режимами SELinux, восстановления контекста безопасности файлов, настройки нестандартного расположения файлов веб-сервера и работы с переключателями SELinux. В ходе выполнения работы студенты научатся изменять режимы работы SELinux, корректировать контексты безопасности с помощью restorecon, настраивать SELinux для работы веб-сервера и управлять SELinux-переключателями.

Выполнение лабораторной работы

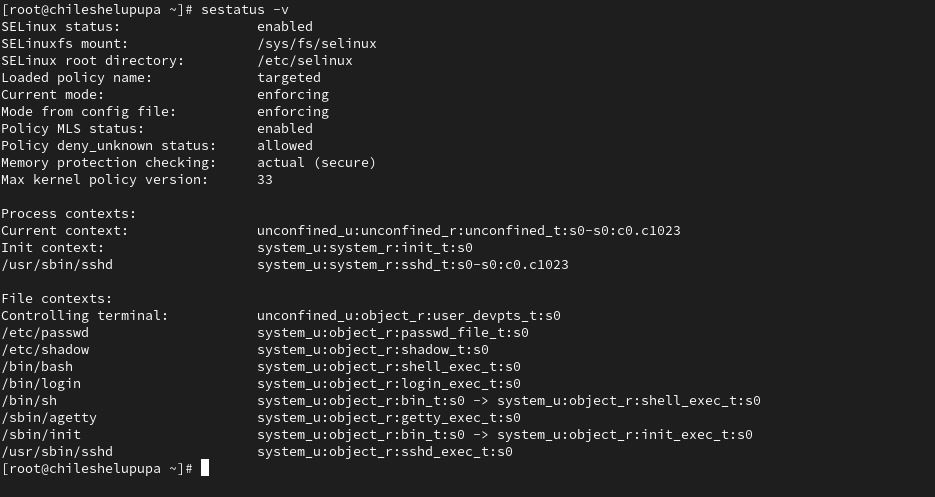
**Управление режимами SELinux**

**Запуск терминала и получение прав администратора**

* Выполнена команда su.
* 

**Просмотр состояния SELinux**

* Команда sestatus -v вывела информацию:



* SELinux status: показывает, включена ли SELinux.
* Current mode: текущий режим (Enforcing, Permissive, Disabled).
* Policy version: используемая политика безопасности.
* Loaded policy: загруженный набор правил безопасности.
* Mode from config file: режим, установленный в конфигурации

**Определение текущего режима работы**

* Команда getenforce показала Enforcing (принудительный режим).

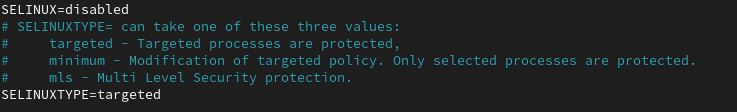


**Изменение режима на Permissive**



* + setenforce 0 изменил режим на Permissive.
  + getenforce подтвердил изменение.

**Отключение SELinux через конфигурационный файл**

****

* В файле /etc/sysconfig/selinux установлено SELINUX=disabled.
* После перезагрузки система подтвердила отключение (getenforce вернул Disabled).

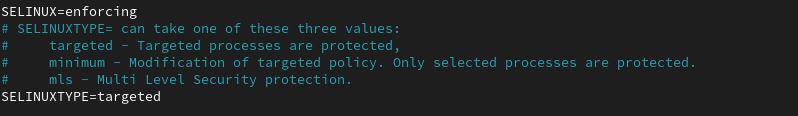


**Попытка включения SELinux без перезагрузки**



* setenforce 1 не сработал, так как отключенный SELinux требует перезагрузки.

**Возвращение режима Enforcing**



* В файле /etc/sysconfig/selinux установлено SELINUX=enforcing.
* После перезагрузки система запустилась в режиме Enforcing, возможно с предупреждением о необходимости восстановления меток.



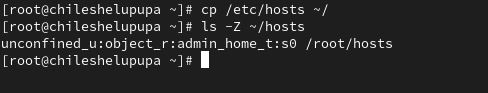
**Использование restorecon для восстановления контекста безопасности**

**Просмотр контекста файла /etc/hosts**

****

* ls -Z /etc/hosts показал net\_conf\_t.

**Копирование файла и изменение контекста**



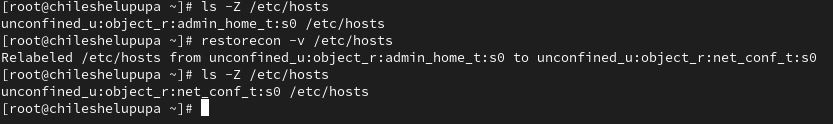
* cp /etc/hosts ~/ создал копию с контекстом admin\_home\_t.

**Перемещение файла обратно и проверка контекста**



* mv ~/hosts /etc сохранило admin\_home\_t.

**Исправление контекста**



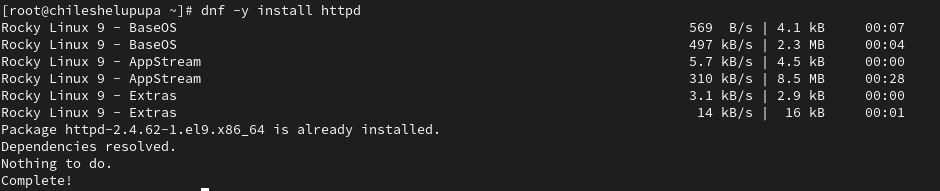
* restorecon -v /etc/hosts восстановил net\_conf\_t.

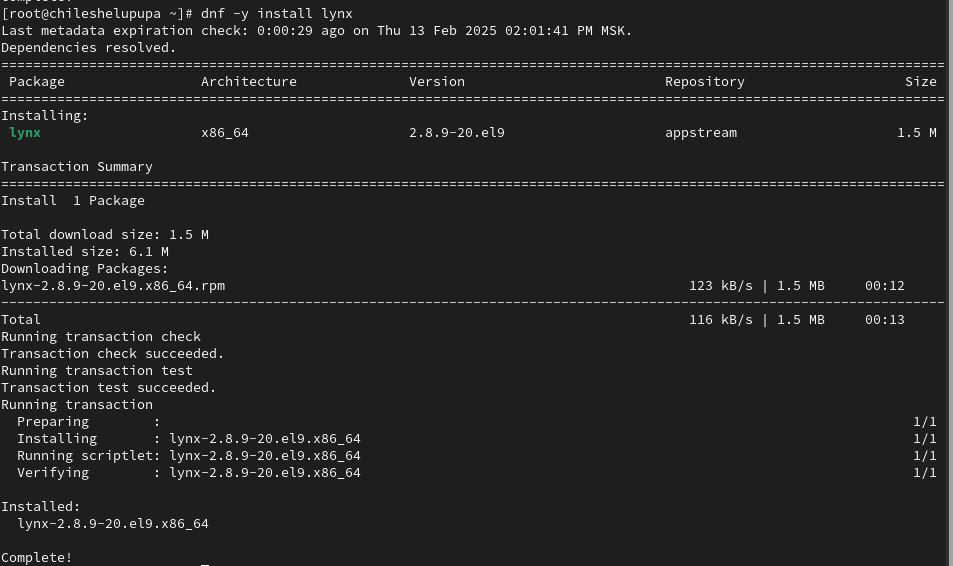
**Массовое исправление контекста**

* touch /.autorelabel и перезагрузка инициировали перемаркировку файловой системы

**Настройка контекста для нестандартного расположения веб-файлов**

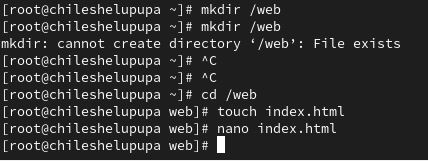
**Установка Apache и текстового браузера**



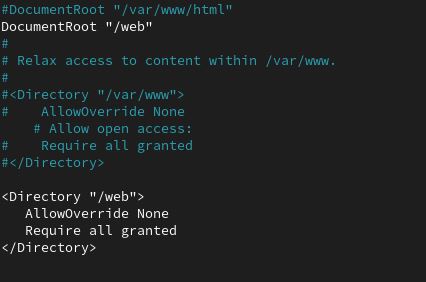


* dnf -y install httpd lynx.

**Создание каталога и конфигурация Apache**

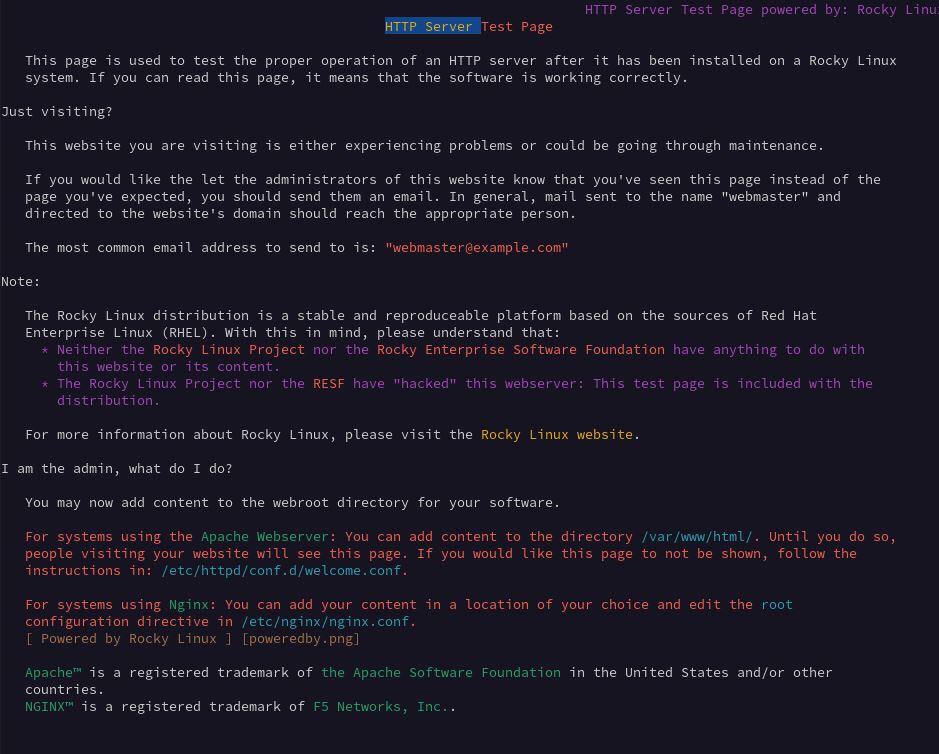


* mkdir /web, добавлен index.html.



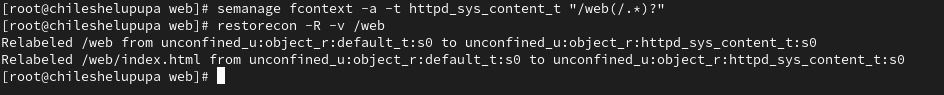
* В /etc/httpd/conf/httpd.conf изменен DocumentRoot на /web.

**Запуск Apache и тестирование через lynx**



* systemctl start httpd, но страница по умолчанию не отображала новый контент.

**Изменение контекста безопасности**



* semanage fcontext -a -t httpd\_sys\_content\_t "/web(/.\*)?".
* restorecon -R -v /web восстановил контекст.

**Повторное тестирование через lynx**



* После перезагрузки веб-страница Welcome to my web-server отобразилась успешно.

**Работа с переключателями SELinux**

**Просмотр переключателей для FTP**

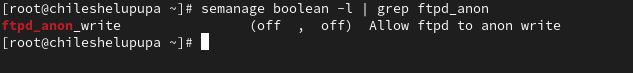


* getsebool -a | grep ftp показал ftpd\_anon\_write off.

**Изменение веменного значения**

* + setsebool ftpd\_anon\_write on временно включил параметр.

1. **Просмотр переключателей с пояснениями**



* + semanage boolean -l | grep ftpd\_anon подтвердил временное изменение.

1. **Установка постоянного значения**
   * setsebool -P ftpd\_anon\_write on сохранил изменение после перезагрузки.
2. **Проверка состояния после перезагрузки**
   * semanage boolean -l | grep ftpd\_anon подтвердил on для ftpd\_anon\_write.