Отчет по лабораторной работе №9

Отчет о мониторинге и настройке системных журналов

Лупупа Чилеше

Содержание

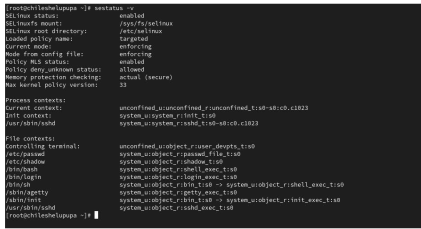
# 1 Цель работы

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.

# 2 Выполнение лабораторной работы

## 2.1 Управление режимами SELinux

1. Запуск терминала и получение прав администратора Выполнена команда su.
2. Просмотр состояния SELinux Команда sestatus -v вывела информацию:



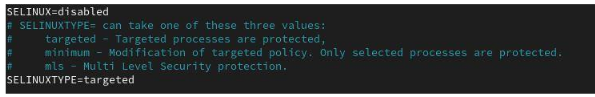
* SELinux status: показывает, включена ли SELinux.
* Current mode: текущий режим (Enforcing, Permissive, Disabled).
* Policy version: используемая политика безопасности.
* Loaded policy: загруженный набор правил безопасности.
* Mode from config file: режим, установленный в конфигурации

1. Определение текущего режима работы Команда getenforce показала Enforcing (принудительный режим).
2. Изменение режима на Permissive

fig:

setenforce 0 изменил режим на Permissive. getenforce подтвердил изменение.

1. Отключение SELinux через конфигурационный файл



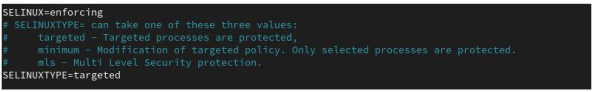
В файле /etc/sysconfig/selinux установлено SELINUX=disabled. После перезагрузки система подтвердила отключение (getenforce вернул Disabled).

1. Попытка включения SELinux без перезагрузки

fig:

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

1. 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.

# 3 Использование restorecon для восстановления контекста безопасности

1. Просмотр контекста файла /etc/hosts

fig:

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

1. Копирование файла и изменение контекста



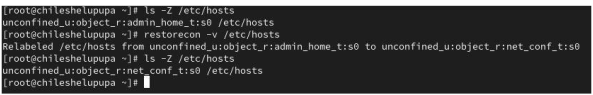
cp /etc/hosts ~/ создал копию с контекстом admin\_home\_t.

1. Перемещение файла обратно и проверка контекста

fig:

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

1. Исправление контекста



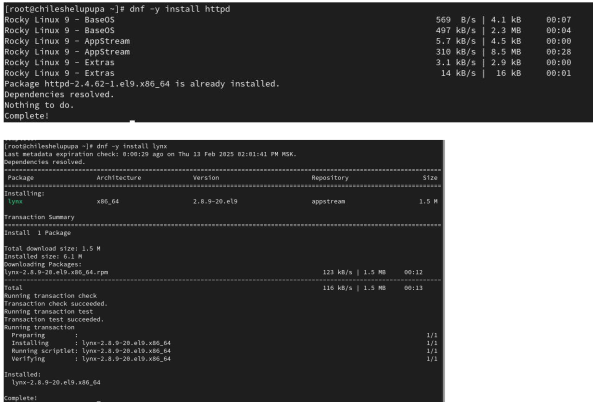
restorecon -v /etc/hosts восстановил net\_conf\_t.

1. Массовое исправление контекста

touch /.autorelabel и перезагрузка инициировали перемаркировку файловой системы

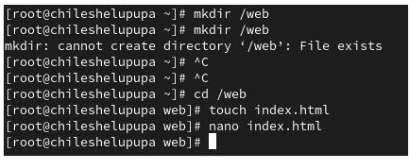
# 4 Настройка контекста для нестандартного расположения веб-файлов

1. Установка Apache и текстового браузера

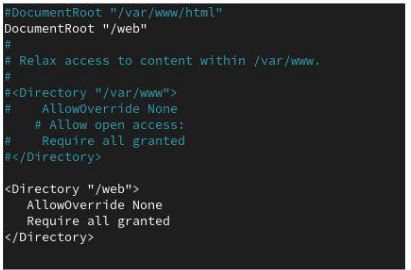


dnf -y install httpd lynx.

1. Создание каталога и конфигурация Apache

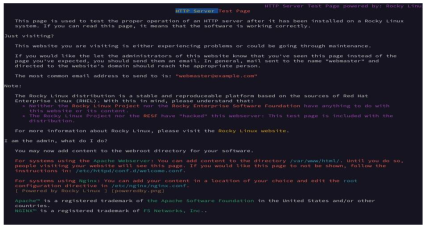


mkdir /web, добавлен index.html.



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

1. Запуск Apache и тестирование через lynx



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

1. Изменение контекста безопасности

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

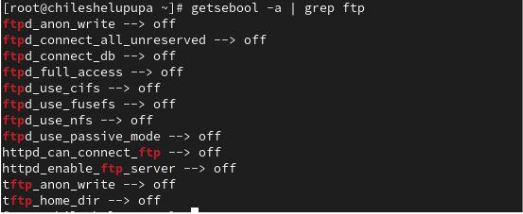
5.Повторное тестирование через lynx



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

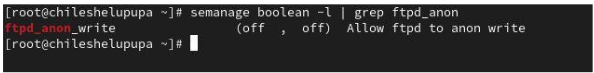
# 5 Работа с переключателями SELinux

1. Просмотр переключателей для FTP



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

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.