

## IX. Quản lý thuộc tính và quyền truy cập files

### Mục tiêu:

Thiết lập lại quyền truy cập cho một thư mục với các quyền sau:

Tất cả mọi người đều có thể truy cập vào thư mục, tất cả mọi người có thể đọc các file trong thư mục. Không ai có thể thực thi các file trong thư mục, áp dụng tất cả các quyền trên cho tất cả các thư mục con theo cách đệ quy.

#### 1. Sử dụng 1 user có quyền sudo để Đăng nhập vào Linux server của các bạn:

```
ssh user@ip_server
```

Sau đó sử dụng lệnh sau để vào quyền root:

```
sudo -i
```

#### 2. Tạo thư mục và files (môi trường) cho bài thực hành như sau:

```
mkdir /opt/myapp
```

```
mkdir /opt/myapp/testapi
```

```
touch /opt/myapp/testapifile.cc
```

```
touch /opt/myapp/testapi/api.sh
```

```
echo "ls -al ." > /opt/myapp/testapi/api.sh
```

#### - Chạy lệnh:

```
[root@localhost ~]# /opt/myapp/testapi/api.sh
```

#### - Sẽ thấy báo không có quyền chạy file: "Permission denied"

#### 3. Cấp quyền cho file chạy:

```
chmod u+x /opt/myapp/testapi/api.sh
```

#### Chạy lại file chạy:

```
[root@localhost ~]# /opt/myapp/testapi/api.sh
```

Chúng ta có thể thấy kết quả trả về.

#### - Cấp quyền cho thư mục myapp chỉ cho phép user root mới có thể truy cập được vào thư mục này:

```
chmod 600 /opt/myapp
```

#### - Sử dụng lệnh exit để thoát ra khỏi quyền root:

exit

#### 4. Giải pháp:

##### **Cấp quyền truy cập vào thư mục:**

- Chuyển tới thư mục opt bằng lệnh: `cd /opt`
- Mở tất cả các files và quyền hạn của thư mục bằng lệnh: `ls -la`
- Thử mở thư mục myapp bằng lệnh `cd myapp/`
- Nhận thông báo "Permission denied" do hiện tại các quyền truy cập bị giới hạn cho người dùng user của bạn.
- Hãy thay đổi quyền bằng cách nhập lệnh: `sudo chmod 777 myapp` và nhập mật khẩu khi được yêu cầu.
- Mở lại file và quyền hạn của thư mục bằng lệnh `ls -la`.
- Sau đó, thử mở lại thư mục bằng lệnh `cd myapp` và chúng ta đã có thể mở được thư mục.
- Thay đổi quyền truy cập cho thư mục:
- Bước tiếp theo là cấp quyền đọc và ghi cho tất cả người dùng cho thư mục này. Tuy nhiên, chúng ta cũng cần đảm bảo không ai có thể thực thi file trong thư mục.
- Hãy bắt đầu bằng cách xóa quyền thực thi bằng lệnh: `sudo chmod -f -x -R *`.
- Sau đó, cấp quyền đọc và ghi cho tất cả mọi người bằng lệnh: `sudo chmod 666 -f -R *`.
- Lưu ý là việc này cũng sẽ xóa quyền thực thi mà chúng ta đã xóa ở bước trước, nhưng chúng ta muốn hiển thị cách làm đó rõ ràng.
- Liệt kê lại files và quyền hạn của thư mục bằng lệnh: `ls -la`. Chúng ta có thể thấy rằng tất cả mọi người đều có quyền đọc và ghi.
- **Lưu ý:** Để cho phép người dùng có thể truy cập được vào các thư mục, các thư mục phải được thiết lập phân quyền đúng.