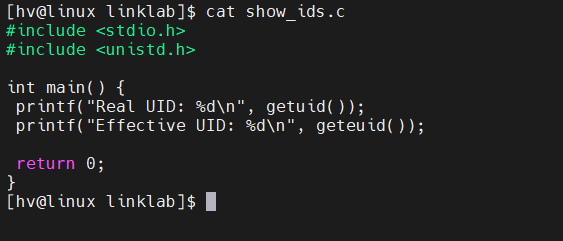


<https://chmod-calculator.com/#google_vignette>

**Minh họa SUID**

**Trong user hv**

**step 1: tạo 1 file c**



**step 2: cài trình biên dịch gcc**



**step 3: biên dịch file .c**

****

**step 4: chuyển ownership của file thành root**

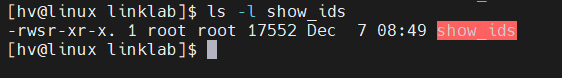
****

**step 5:**

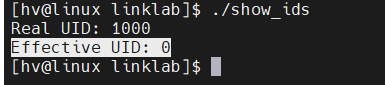
**set UID bit cho file**

**sudo chmod 4755 show\_ids**

**step 6: kiểm tra quyền file**

****

**step 7: ./show\_ids**

****

**số 0 là root**

**lưu ý: khi chưa gán suid , thì real id và effective uid trùng nhau, vì đều user thường**

**sau khi gán suid và owner là root, thì effective uid trở thành root (0) khi user thường chạy chương trình**

**suid guid stickybit**

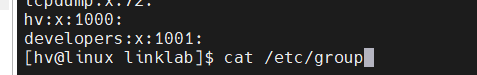
**2^2 2^1 2^0**

**Minh họa về SGID**

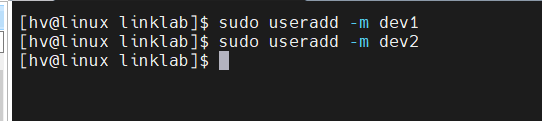
**step 1: tạo group và user**

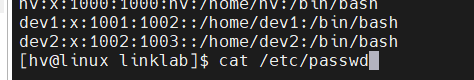
# tạo group developers



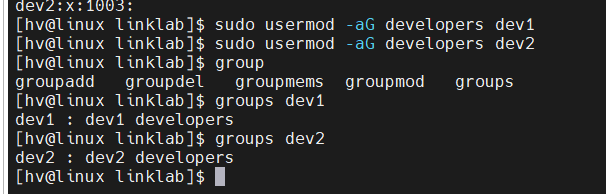


# tạo 2 user để test

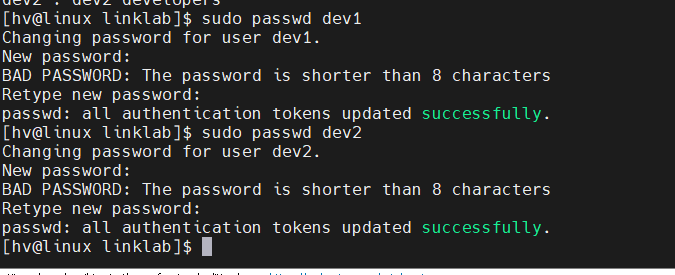




# Thêm users vao group developers



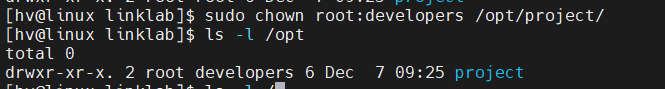
# đặt password cho users

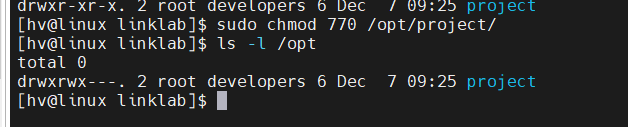


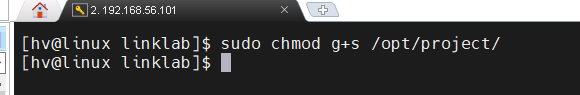
**step 2: tạo thư mục project và set quyền**

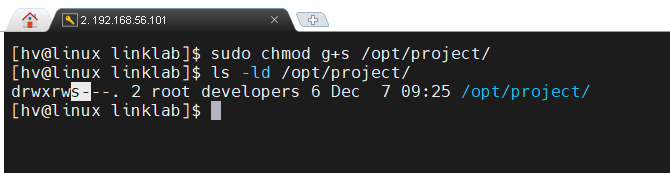
**tạo thư mục**

****

****

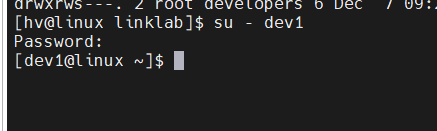
****

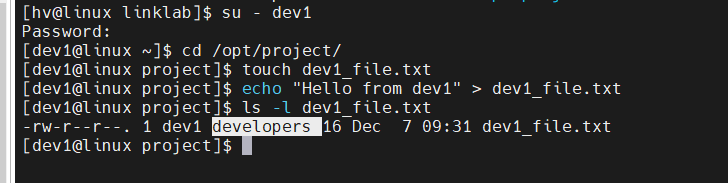
****

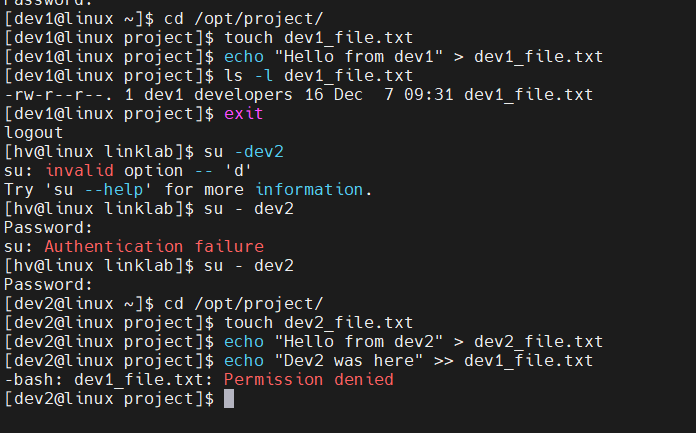
****

**Thử nghiệm**

**# đăng nhập với user dev1**

****

****

****

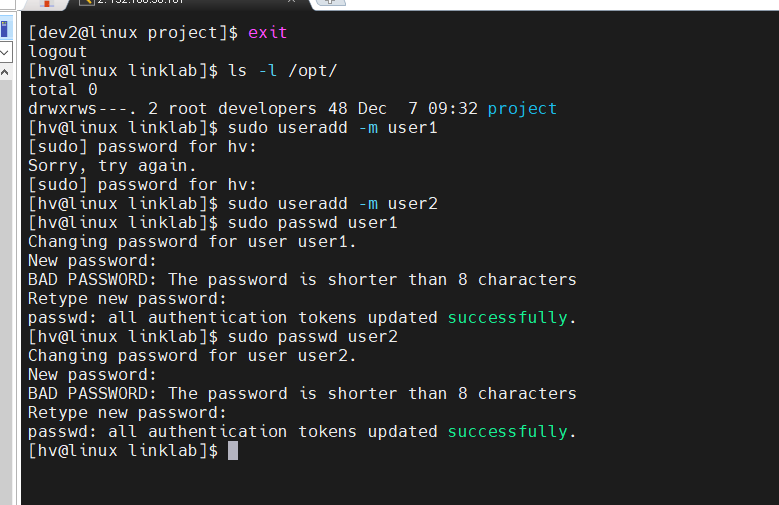
**Khi không có SGID: user tạo file mới, file mới sẽ có: owner : user tạo ra, group: primary group của user đó**

**Khi có SGID: khi tạo file trong thư mục có SGID : owner : user tạo file, group tự động là group của thư mục cha (trong ví dụ developers)**

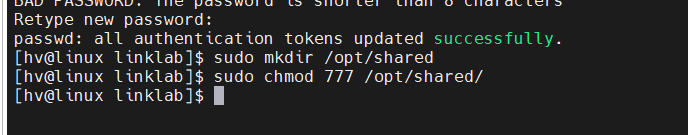
**Set quyền group mọi thành viên trong group deveopers: tạo file mới, đọc và sửa file của nhau, không cần thay đổi group thủ công**

**Ví dụ: Sticky bit**

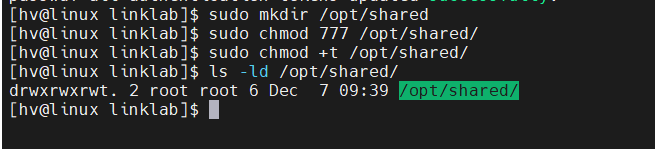
1. **Đầu tiên, tạo users để test: user1, user2**
2. **Đặt pass cho 2 user**

****

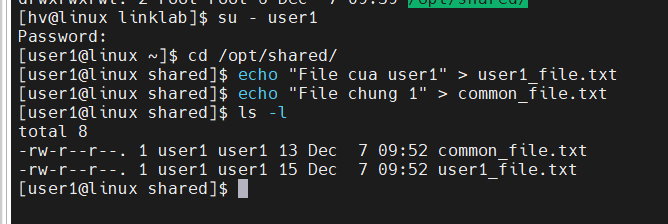
1. **Tạo thư mục /opt/shared**
2. **Gán quyền để mọi người đều chỉ thể read/write**

****

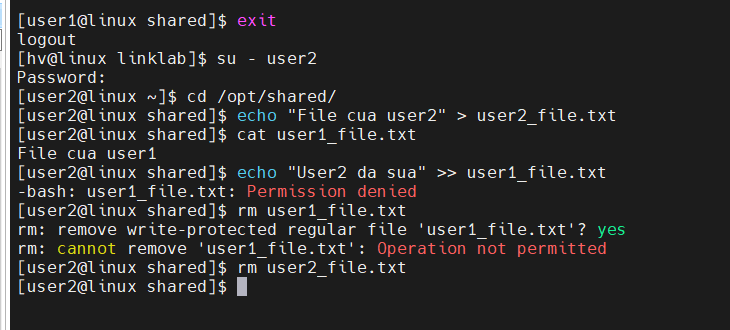
1. **Set sticky bit**

****

**Test với user 1**

****

**Test với user2**

****

**1. Không có sticky bit:**

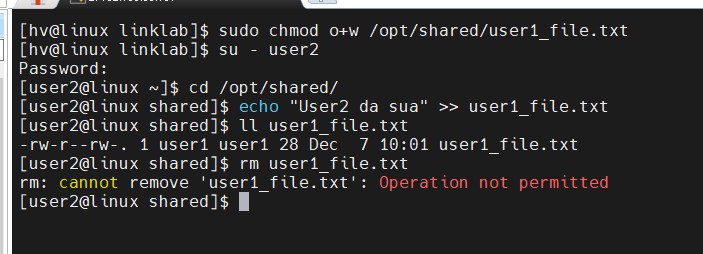
**Nếu user có quyển write vào thư mục, họ có thể xóa bất kỳ file nào trong đó, kể cả file không phải của họ**

**2. Có sticky bit:**

**Chỉ có thể xóa file khi là : owner của file , owner của thư mục, root**

**vẫn có thể đọc và sửa file ( nếu có quyền)**

**không thể xóa files của người khác**

****

**—----**

**SUID: dùng cho: file thực thi -> tác dụng khi chạy file , nó chạy với quyền của chủ file chứ không phải người chạy**

**SGID : dùng cho thư mục -> file mới tạo trong thư mục sẽ thừa kế group của thư mục , thư mục project dùng chung, files luôn có group là developers**

**Sticky Bít dùng cho thư mục , tác dụng : chỉ chủ file mới được xóa file của mình**

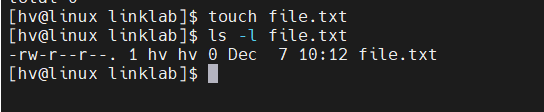
**Ví dụ : thư mục /tmp -> ai cũng được tạo file nhưng chỉ xóa được file của mình**

**ACL : cho phép set quyền chi tiết hơn so với permissions thông thường và linh hoạt hơn**

**ACL: áp dụng cho users và groups**

**Có thể set ACL mặc định cho thư mục**

**ACLs không ảnh hưởng đến permissions gốc**

****

**Mong muốn**

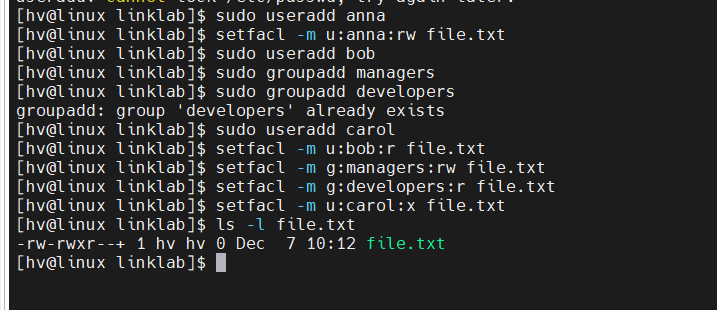
**anna có quyền read và write**

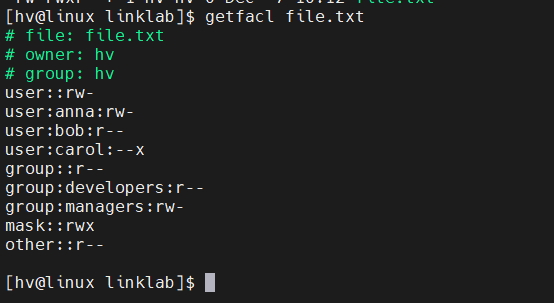
**bob chỉ được read**

**Nhóm managers được read và write**

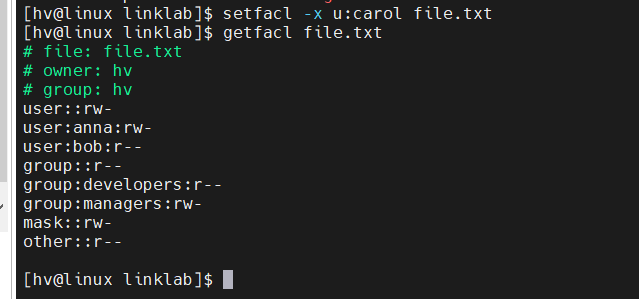
**Nhóm developers chỉ được read**

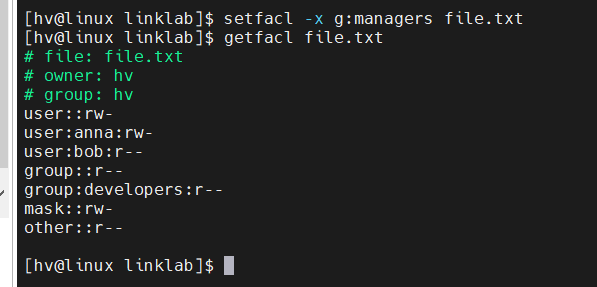
**carol được execute**

****

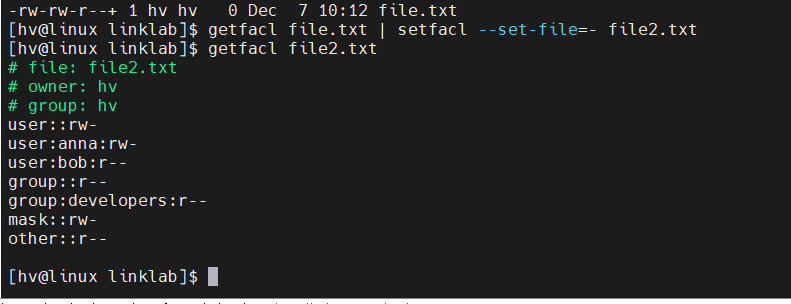
****

**xoa quyen**

****

****

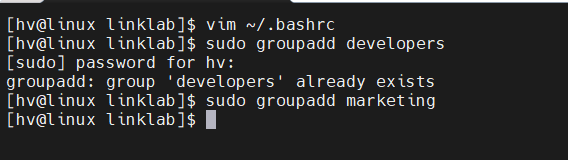
**Tạo file mới lấy acl cũ từ file.txt**

****

**Ví dụ minh họa về quyền mặc định umask**

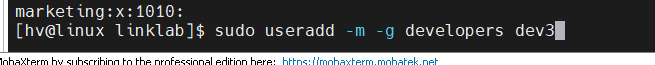
**Bước 1:**

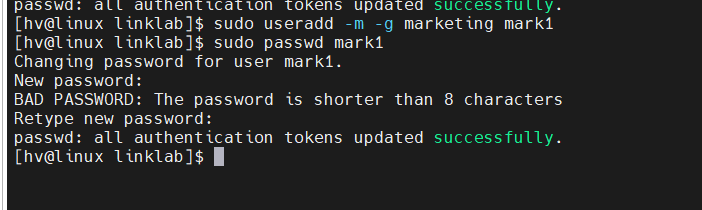
**Tạo 2 group developers và marketing**

****

**Bước 2:**

**Tạo user và thêm vào group (user dev3 và mark1)**

****

****

**Đặt password cho user dev3 và mark1**

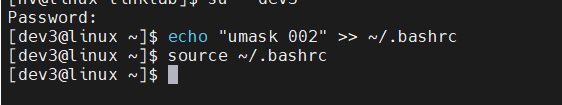
**dev3 -g thêm dev3 vào developers vào đồng xóa group dev3 chính**

**-aG: thêm vào group phụ mà không phải xóa của group chính của user đó**

**Bước 3: Set umask dev3 và mark1**

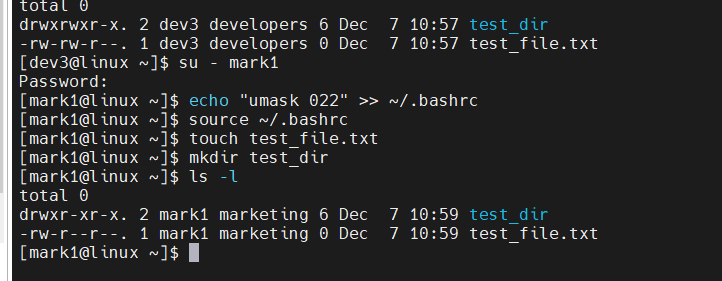
**umask của developers có umask 002**

**-> tạo file mới: 002 | 664 | 775 | User thông thường**

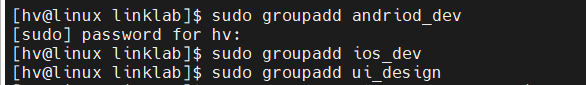
****

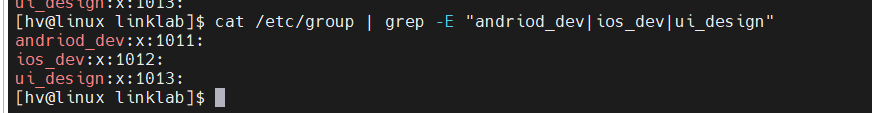
**marketing bảo mật**

**umask 022 022 | 644 | 755 | Bảo mật cao hơn**

****

**—----------**

****

****

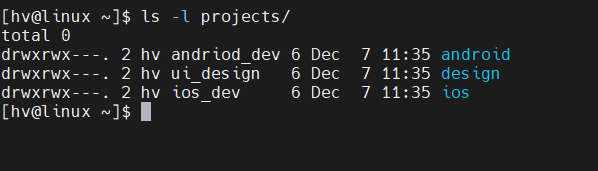
**mkdir -p projects/{android,ios,design}**

**sudo chown -R hv:andriod\_dev projects/android**

**sudo chown -R hv:ui\_design projects/design**

**sudo chown -R hv:ios\_dev projects/ios**

**chmod -R 770 projects/**

****

Bai tap:

Hay tao cac user:

* kt1, kt2 nam trong group ketoan -G
* kd1, kd2 nam trong group kinhdoanh -G
* Tao thu muc /data/{ketoan, kinhdoanh} sao cho
* Cac thanh vien khac phong ban khong truy cap duoc thu muc cua nhau
* Trong cung phong ban co the truy cap thu muc cua nhau