

HỆ ĐIỀU HÀNH LINUX CĂN BẢN

Lê Ngọc Sơn

Inson@fit.hcmus.edu.vn

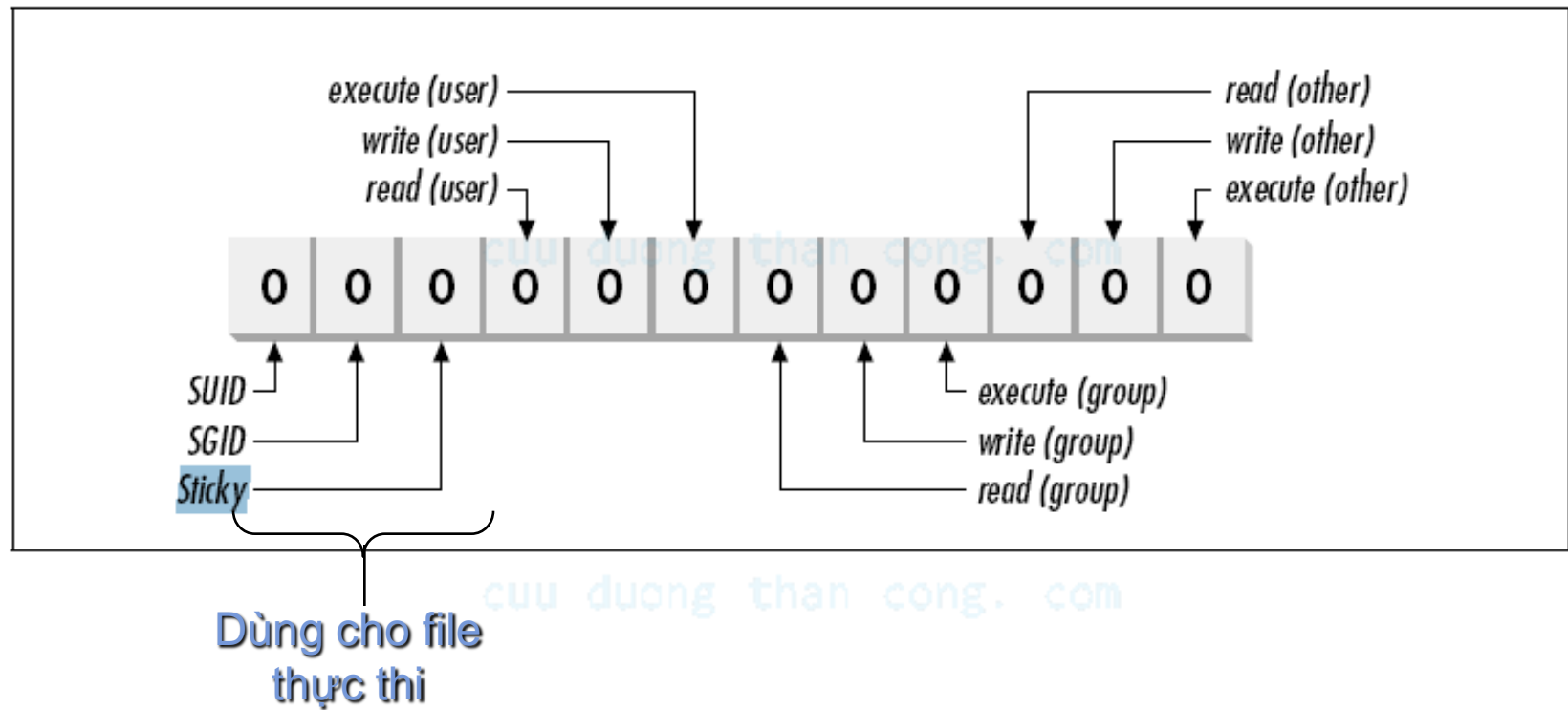
GIỚI THIỆU VỀ FILE PERMISSION

- Linux là một hệ điều hành đa người dùng, do đó vấn đề phân quyền truy xuất trên hệ thống file là rất quan trọng.
- Để xem được quyền hạn ứng với một file cụ thể, ta có thể dùng lệnh `ls -l`.

```
[sv@dhcppc3 ~]$ ls -l
total 8
--w-rw-r-- 1 sv sv 9 2008-08-27 09:10 sv.txt
```



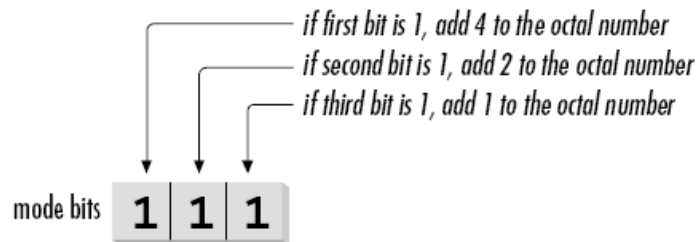
CẤU TRÚC PHÂN QUYỀN



BIỂU DIỄN DƯỚI DẠNG SỐ

Octal Value	Permissions	Octal Value	Permission Sets
4	Read	7	r w x
2	Write	6	r w -
1	Execute	5	r - x
		4	r - -
		3	- w x
		2	- w -
		1	- - x
		0	- - -

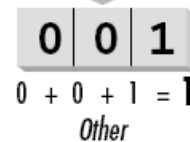
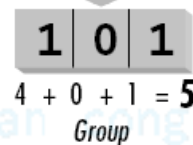
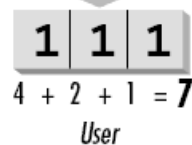




mode bits =

1	1	0	1	1	1	1	0	1	0	0	1
---	---	---	---	---	---	---	---	---	---	---	---

 octal number = **6751**



- Ba loại người dùng ứng với file permission:
 - User/Owner (u): Người nắm quyền sở hữu file, có thể thay đổi bằng lệnh chown
 - Group users (g): Những người dùng nằm trong group sở hữu user [cuu duong than cong. com](https://fb.com/tailieudientucntt)
 - Others (o): Những người dùng còn lại

[cuu duong than cong. com](https://fb.com/tailieudientucntt)



Ý NGHĨA CÁC QUYỀN

- Các từ viết tắt r,w,x; giá trị - tượng trưng cho không có quyền hạn tại vị trí đó. Ví dụ: r-x là không có quyền w.

Permission	Mnemonic	File permission	Directory permission
Read	r	Examine the contents of the file.	List directory contents.
Write	w	Write to or change the file.	Create and remove files in the directory.
Execute	x	Run the file as a program.	Access (cd into) the directory.

- Chữ cái đầu tiên là d: thư mục; -: tập tin; ngoài ra còn có các ký tự đặc biệt khác.

```
[root@dhcppc3 ~]# ll
total 216
-rw-r--r-- 1 root root    0 2008-08-20 12:31 abc.txt
-rw----- 1 root root 1266 2008-08-13 22:13 anaconda-ks.cfg
-rw-r--r-- 1 root root 30650 2008-08-20 12:47 danh sach.txt
drwxr-xr-x 2 root root  4096 2008-08-13 16:43 Desktop
drwxr-xr-x 3 root root  4096 2008-08-20 12:32 dir3
```


- Quyền hạn ngoài việc được thể hiện bằng chuỗi ký tự rwx, còn có thể được ký hiệu bằng số (777).
- Toàn bộ quyền truy xuất được chia thành 3 nhóm ứng với 3 loại người dùng. Mỗi nhóm được viết thành một số.

cuu duong than cong. com



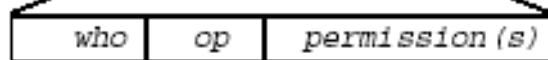
LỆNH CHMOD

- Để thay đổi quyền hạn trên file, ta sử dụng lệnh chmod, cú pháp:
- `chmod [mode] filename`
- Ghi chú: chỉ có superuser (các user quản trị) hoặc user sở hữu tập tin/ thư mục mới có thể chmod cho tập tin/thư mục.
- Lệnh chmod có thể hoạt động ở cả dạng chuỗi (rwx) lẫn cả dạng số (764).

cuu duong than cong. com



`chmod mode filename`



r Read
w Write
x Execute

= Set permissions
- Remove access
+ Give access

u User or owner of the file
g Group to which the file belongs
o Others outside owner and group
a All of the above

Mục mode trong câu lệnh chmod gồm có 3 phần. Phần đầu chỉ nhóm người dùng, phần sau là toán tử, cuối cùng là quyền hạn.

VÍ DỤ 1:

- **Xóa quyền read của group với file dante:**

```
$ ls -l dante
```

```
-rw-r--r-- 1 user2 staff 2 Jun 11  
1:44 dante
```

```
$ chmod g-r dante
```

```
$ ls -l dante
```

```
-rw---r-- 1 user2 staff 2 Jun 11  
1:44 dante
```



VÍ DỤ 2:

- Thêm quyền execute cho owner, thêm quyền read cho group và others với file dante:

- `$ ls -l dante`

```
-rw----- 1 user2 staff 2 Jun 11 1:44  
dante
```

```
$ chmod u+x,go+r dante
```

```
$ ls -l dante
```

```
-rwxr--r-- 1 user2 staff 2 Jun 11 1:44  
dante
```



VÍ DỤ 3:

- Cho mọi người dùng quyền read và write (a: all user)

```
$ chmod a=rw dante
```

```
$ ls -l dante
```

```
-rw-rw-rw- 1 user2 staff 2 Jun 11 1:44  
dante
```

Hoặc có thể dùng dạng số:

```
chmod 666 dante
```

Có thể dùng tham số -R để set quyền đệ qui (cho tập tin và thư mục con của 1 thư mục)



QUYỀN MẶC ĐỊNH

- Quyền mặc định ban đầu (initial default permission) là quyền được tự động set cho file/directory khi chúng được tạo ra.
- Quyền mặc định của một **tập tin** là 666 (rw-rw-rw-)
- Quyền mặc định của một **thư mục** là 777 (rwx rwx rwx).



UMASK

- Có thể thay đổi quyền mặc định của tập tin/ thư mục bằng cách thay đổi giá trị biến umask
- Giá trị umask gồm 4 số bát phân
- Giá trị mặc định của umask là 0022 hoặc 0002



- umask hoạt động tương tự một bộ lọc.
- Khi tính giá trị default permission cho một file, thư mục mới tạo ra hệ thống sẽ lấy (initial default permission) AND (NOT umask).
- Nhắc lại: Initial Default permission of:
 - File: 666
 - Directory: 777



VÍ DỤ 1

- Default **file** permission

umask of 022

Resulting file permission

r	w	—	r	w	—	r	w	—	(666)
—	—	—	—	w	—	—	w	—	(022)
r	w	—	r	—	—	r	—	—	(644)

- Default **dir** permission

umask of 022

Resulting dir permission

r	w	x	r	w	x	r	w	x	(777)
—	—	—	—	w	—	—	w	—	(022)
r	w	x	r	—	x	r	—	x	(755)



VÍ DỤ 2:

- Default file permission

umask of 123

Resulting file permission

r	w	—	r	w	—	r	w	—	(666)
—	—	X	—	w	—	—	w	X	(123)
r	w	—	r	—	—	r	—	—	(644)

(*not 543!*)

- Default dir permission

umask of 123

Resulting dir permission

r	w	X	r	w	X	r	w	X	(777)
—	—	X	—	w	—	—	w	X	(123)
r	w	—	r	—	X	r	—	—	(654)

THAY ĐỔI GIÁ TRỊ UMASK

- Xem giá trị umask:

```
$ umask
```

```
0022
```

- Đổi giá trị umask sang 027

```
$umask 027
```

Chỉnh trong /etc/profile hoặc /etc/bashrc, thêm dòng
umask 022 → umask cho tất cả các user.



CÁC QUYỀN HẠN ĐẶC BIỆT

- **Các quyền đặc biệt cho các tập tin thực thi và các thư mục dùng chung**
 - **Set user ID : `suid`**
 - **Set group ID : `sgid`**
 - **Sticky bit**

cuu duong than cong. com



SET USER ID

- Khi user thực thi một file, user có thể “mượn” quyền của **user làm chủ file đó** để thực thi. Ví dụ user sv thực thi một file do user root làm chủ, trong quá trình thực thi chương trình “mượn” tạm quyền của root để làm việc.
- Khi file được set “set user id” thì sẽ hiện ký tự s tại mục quyền hạn execute (thay cho ký tự x) của owner. Nếu file chỉ có quyền “set user id” mà không có quyền execute, ký tự s sẽ chuyển thành S (viết hoa).

```
$ ls -l /bin/su /usr/bin/passwd
```

```
-rwsr-xr-x 1 root root 18452 Jul 2 2003 /bin/su
```

```
-r-s--x--x 1 root root 13476 Aug 7 2003 /usr/bin/passwd
```

- Root và owner có thể set suid bằng câu lệnh chmod, với giá trị 4000 hoặc ký tự s:
- Ví dụ:

```
# chmod 4755 <executable_file>
```

```
# chmod u+s <executable_file>
```

SET GROUP ID

- Tương tự như suid, file nếu có quyền sgid khi user khác thực thi file này sẽ “mượn” tạm quyền hạn của group quản lý file đó.
- File có quyền sgid sẽ thể hiện ký tự “s” ở quyền execute của group. Nếu group không có quyền execute, ký tự S sẽ viết hoa.
- Ví dụ:

```
$ ls -l /usr/bin/slocate /usr/bin/write  
-rwxr-sr-x 1 root slocate 9 Jul 2 2003 /usr/bin/slocate  
-rwxr-sr-x 1 root tty 13476 Aug 7 2003 /usr/bin/write
```


SET GROUP ID

- User root hoặc người sở hữu file có thể set group id qua lệnh chmod, sử dụng giá trị 2000 hoặc chuỗi g+s:
- `$ chmod 2755 <executable_file>`
- `$ chmod g+s <executable_file>`
- Khi một directory được set Group ID. Mọi tập tin được tạo ra (dù do bất kỳ ai tạo) đều được chuyển quyền sở hữu về cho group đang sở hữu thư mục đó

STICKY BIT PERMISSION

- Dùng để bảo vệ tập tin trong các thư mục public. Khi một thư mục được set sticky bit:
 - Chỉ có owner hoặc root được phép xóa files/rename trong thư mục
 - Các user khác vẫn có quyền tạo/ ghi file nhưng không được phép xóa/rename.
- Sticky bit thể hiện qua ký tự “t” ở phần quyền execute của others, nếu others không có quyền x, ký tự T sẽ viết hoa.
- Set sticky bit:

```
$ chmod 1755 <directory>
```

```
$ ls -ld /tmp
```

```
drwxrwxrwt 8 root root 4096 Jul 2 2003 /tmp
```

CHOWN COMMAND

- Sử dụng lệnh **chown** để đổi quyền sở hữu tập tin, thư mục cho người dùng khác.
- Ví dụ đổi quyền sở hữu tập tin data.txt cho user sv:

```
chown sv data.txt
```

- Đổi quyền sở hữu tập tin data.txt cho user sv và group ketoan

```
chown sv:ketoan data.txt
```



CHGRP COMMAND

- Chuyển quyền sở hữu tập tin cho group khác (phần owner giữ nguyên).
- Ví dụ:

chgrp sv data.txt

=> Chuyển group sở hữu tập tin data.txt từ bất kỳ group nào sang cho group sv



Q & A

cuu duong than cong. com

