

QUẢN TRỊ NGƯỜI DÙNG, NHÓM NGƯỜI DÙNG

Trịnh Tấn Đạt

Khoa CNTT - Đại Học Sài Gòn

Email: trinhtandat@sgu.edu.vn

Website: <https://sites.google.com/site/ttdat88/>



NỘI DUNG

Khái niệm cơ bản về user – group – quyền người dùng

Quản lý người dùng

Quản lý nhóm

Quản lý qua giao diện

Quyền của người dùng

I. KHÁI NIỆM CƠ BẢN

User: là người có thể truy cập đến hệ thống.

- User có **username** và **password**.
- Có ba loại user: **super user**, **system user** và **regular user**.
- Mỗi user còn có một định danh riêng gọi là **UID**.
 - **username**: khi sử dụng để login, gán quyền, v.v.. chúng ta thực hiện thông qua username, nhưng hệ thống lại hiểu và làm theo userID.
 - **userID**: Số đi kèm với username, hệ điều hành dùng số này để quản lý. Chỉ số này là không trùng lặp.

I. KHÁI NIỆM CƠ BẢN

- Từ phiên bản Linux Kernel 2.4 trở lên, UID là số nguyên 32-bit không dấu (vùng giá trị từ **0 -> 4.294.967.296**).
- Một vài UID đặc biệt và dành riêng:
 - **UID=0**: được gán cho tài khoản **root** – người dùng có đặc quyền cao nhất trong Linux.
 - **UID=65534**: thường được dành riêng cho tài khoản **nobody** – người dùng không có bất cứ đặc quyền quản trị nào. UID này thường được dành cho các cá nhân truy cập từ xa tới hệ thống qua FTP hay HTTP.
 - **UID trong khoảng 1->99**: thường được dành riêng cho các tài khoản hệ thống đặc biệt, thường được gọi là các **pseudo-users**

I. KHÁI NIỆM CƠ BẢN

- Trên 1 số bản phân phối Linux (Distro), các normal user nhận UID lớn hơn 100.
 - Ví dụ, Redhat gán UID cho normal user bắt đầu từ 500, Debian bắt đầu từ 1000.
- Ngoài ra, ta cũng nên dành riêng 1 dải UID cho các tài khoản cục bộ (*local account*) như 1000-9999, 1 dải khác cho các người dùng truy cập từ xa tới hệ thống qua mạng (*remote user*) như 10000-65534 để dễ bề quản lý cũng như giúp rà soát các hoạt động của người dùng trong các file log...

I. KHÁI NIỆM CƠ BẢN

Group: là tập hợp nhiều user lại.

- Mỗi user luôn là thành viên của một group.
- Khi **tạo một user thì mặc định một group được tạo ra.**
- Mỗi user trên linux bắt buộc phải thuộc một group nào đó (gọi là Primary Group), ngoài ra còn có thể lựa chọn tham gia vào các group khác (gọi là Secondary Group)
- Mỗi group còn có một định danh riêng gọi là **GID**.
- Định danh của group thường sử dụng giá trị bắt đầu từ 500.

II. QUẢN LÝ NGƯỜI DÙNG

- Thông tin người dùng:
 - Thông tin của người dùng chủ yếu được lưu trong tập tin `/etc/passwd`, Linux cũng có ba loại người dùng cơ bản: **supper user**, **system user**, **regular user**.
 - **Super user**: là người dùng quản trị của hệ thống Linux hoặc Unix, thường gọi với tên là người dùng root. Người dùng này được hệ thống cung cấp một định danh quản lý UID có giá trị 0.
 - **System user**: là người dùng được tạo ra khi ta cài đặt chương trình, dịch vụ hệ thống.
 - **Regular user**: tạm gọi là user thường, những user này chỉ được quyền login vào hệ thống và sử dụng tài nguyên. UID của người dùng này thường có giá trị **≥ 500** .

II. QUẢN LÝ NGƯỜI DÙNG

- **Tập tin `/etc/passwd`**

Tập tin `/etc/passwd` đóng vai trò sống còn đối với một hệ thống Unix, Linux. Mọi người đều có thể đọc được tập tin này nhưng chỉ có root mới có quyền thay đổi nó.

Mỗi tài khoản được lưu trong một dòng gồm bảy cột:

- Cột 1 : tên người sử dụng
- Cột 2 : liên quan đến mật khẩu tài khoản và “x” đối với Linux
- Cột 3,4: định danh tài khoản (UID) và định danh nhóm (GID)
- Cột 5 : tên đầy đủ của người sử dụng.
- Cột 6 : thư mục cá nhân (Home Directory)
- Cột 7 : chương trình sẽ chạy đầu tiên sau khi người dùng đăng nhập vào hệ thống

II. QUẢN LÝ NGƯỜI DÙNG

- Tài khoản được lưu trong thư mục etc/passwd

<u>oracle</u>	:	<u>x</u>	:	<u>1021</u>	:	<u>1020</u>	:	<u>Oracle user</u>	:	<u>/data/network/oracle</u>	:	<u>/bin/bash</u>
↓		↓		↓		↓				↓		↓
1		2		3		4		5		6		7

Cột 1 : tên người sử dụng

Cột 2 : liên quan đến mật khẩu tài khoản và “x” đối với Linux

Cột 3,4: định danh tài khoản (UID) và định danh nhóm (GID)

Cột 5 : tên đầy đủ của người sử dụng.

Cột 6 : thư mục cá nhân (Home Directory)

Cột 7 : chương trình sẽ chạy đầu tiên sau khi người dùng đăng nhập vào hệ thống

II. QUẢN LÝ NGƯỜI DÙNG

- Tập tin **/etc/shadow**

Tập tin **/etc/shadow** lưu trữ mật khẩu thực sự của người dùng, mật khẩu này đã được mã hóa. Ngoài thông tin mật khẩu, file này còn lưu trữ các tùy chọn mật khẩu và tùy chọn của tài khoản.

Mỗi tài khoản thường có khoảng tám cột:

II. QUẢN LÝ NGƯỜI DÙNG

- Cột 1: phải khớp với username trong file `/etc/passwd`
- Cột 2: mật khẩu đã được mã hóa
- Cột 3: số ngày từ 1/1/1970 đến ngày thay đổi mật khẩu
- Cột 4: số ngày tối thiểu yêu cầu thay đổi mật khẩu
- Cột 5: số ngày tối đa mật khẩu được sử dụng
- Cột 6: số ngày ra cảnh báo trước khi mật khẩu không còn hợp lệ
- Cột 7: số ngày quy định account bị vô hiệu
- Cột 8: ngày vô hiệu hóa tài khoản tính từ ngày 1/1/1970.

user1:\$6\$un4NjXwnJuixBhln\$51y42Tee1ubu5:16374:0:99999:7:::

User Name

Encrypted Password

lastchg days

mindays

maxdays

warn days

inactive days

disabled days

Not used

II. QUẢN LÝ NGƯỜI DÙNG

- File cấu hình người dùng :
/etc/passwd (important)

- Cú pháp:

username:password:UID:GID:comment:home directory:login

```
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
avahi:x:70:70:Avahi daemon:/:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
gdm:x:42:42::/var/gdm:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
sabayon:x:86:86:Sabayon user:/home/sabayon:/sbin/nologin
lnkkhanh:x:500:500:Khanh:/home/lnkkhanh:/bin/bash
```

II. QUẢN LÝ NGƯỜI DÙNG

- Thêm người dùng mới

- Khi 1 user được tạo mới → private group cùng tên với user đó được tạo ra.
 - Ưu điểm: Đảm bảo khi 1 file được tạo ra, file đó không thuộc về public group
- Khi 1 user được tạo mới → home directory và 1 số file được tạo ra.
 - Thư mục `/etc/skel`: chứa các file mặc định được tạo ra trong home directory cho một user khi user đó được tạo mới
- Lệnh `umask`: định giá trị mặc định cho file/thư mục do user tạo ra. Cấu hình umask được thiết lập trong file `/etc/bashrc`
 - VD: Nếu `umask=022` thì một file mới được tạo ra sẽ có quyền là: 644

CÁC THAO TÁC TRÊN NGƯỜI DÙNG

- **Tạo tài khoản người dùng**

Cú pháp : **useradd [tùy chọn] <tên user>**

Các tùy chọn:

- **-c** “thông tin người dùng”.
- **-d** <thư mục cá nhân>.
- **-m** tạo thư mục cá nhân nếu chưa tồn tại.
- **-g** <nhóm của người dùng>.

Ví dụ: Tạo user có tên nvb

```
useradd -c “Nguyen Van B” nvb  
passwd nvb
```

CÁC THAO TÁC TRÊN NGƯỜI DÙNG

- Một số option khác:
 - -p: password
 - -s: shell
 - -u: set UID
 - -g: set GID
 - -e: expire date
 - -f: set password expire during time

CÁC THAO TÁC TRÊN NGƯỜI DÙNG

- **Đổi password:**
 - Mỗi user có khả năng tự đổi passwd của chính họ, với điều kiện họ nhớ passwd cũ và phải tuân theo nguyên tắc đặt passwd của Linux.
 - User root được phép đổi passwd của tất cả các user mà không cần biết passwd cũ, cũng như không cần tuân theo nguyên tắc đặt passwd!
- **Cú pháp: *passwd* <username>**
 - **Ví dụ:** *passwd u1 //sau đó nhập 2 lần mật khẩu cho user*

CÁC THAO TÁC TRÊN NGƯỜI DÙNG

- **Thay đổi thông tin người dùng**
 - Cú pháp: `usermod [tùy chọn] <tên user>`
- **Những [tùy chọn] tương tự như lệnh `useradd`.**
 - Ví dụ: cho tài khoản `nvb` vào nhóm `admin`
`usermod -g admin nvb`

CÁC THAO TÁC TRÊN NGƯỜI DÙNG

- Một số tùy chọn của lệnh usermod:
 - **-c, comment** : thay đổi thông tin cá nhân của tài khoản người dùng
 - **-d, home_dir** : thay đổi thư mục cá nhân của tài khoản người dùng
 - **-e, expire_date** : thay đổi thời điểm hết hạn của tài khoản người dùng (YYYYMM-DD)
 - **-f, inactive_days** : thiết đặt số ngày hết hiệu lực của mật khẩu trước khi tài khoản người dùng hết hạn sử dụng
 - **-g, initial_group** : tùy chọn này thay đổi tên hoặc số khởi tạo đăng nhập nhóm người dùng

CÁC THAO TÁC TRÊN NGƯỜI DÙNG

- **-G, group** : thay đổi danh sách các nhóm phụ mà người dùng cũng là thành viên thuộc các nhóm đó. Mỗi nhóm sẽ được ngăn cách với nhóm khác bởi dấu ',' mặc định người dùng sẽ thuộc vào nhóm khởi tạo
- **-l, login_name** : thay đổi tên đăng nhập của người dùng. Trong một số trường hợp, tên thư mục riêng của người dùng có thể sẽ thay đổi để tham chiếu đến tên đăng nhập mới
- **-p, passwd** : thay đổi mật khẩu đăng nhập của tài khoản người dùng
- **-s, shell** : thay đổi shell đăng nhập
- **-u, uid** : thay đổi chỉ số người dùng

CÁC THAO TÁC TRÊN NGƯỜI DÙNG

- **Tạm khóa tài khoản người dùng**

Khóa

passwd -l <username>

usermod -L <username>

Mở khóa

passwd -u <username>

usermod -U <username>

CÁC THAO TÁC TRÊN NGƯỜI DÙNG

- **Xóa tài khoản**

- Lệnh `userdel` dùng để xóa một tài khoản. Ngoài ra, bạn cũng có thể xóa một tài khoản bằng cách xóa đi dòng dữ liệu tương ứng với tài khoản đó trong tập tin `/etc/passwd`.

Cú pháp : **`userdel [option] <username>`**

Ví dụ : **`userdel -r nvb`**

CÁC THAO TÁC TRÊN NGƯỜI DÙNG

- **Định tuổi cho mật khẩu:**
 - Mặc định, password không bị hết hiệu lực
 - Gán ngày hết hiệu lực cho password, dùng lệnh: **chage [options] username**
 - Options:
 - -m: gán số ngày ít nhất password cần phải thay đổi
 - -M: gán số ngày nhiều nhất password cần phải thay đổi
 - -i: gán số ngày password không còn sử dụng được trước khi khóa account
 - -E: password hết hiệu lực vào ngày này (YYYY-MM-DD)
 - -w: định số ngày hệ thống gửi thông báo nhắc nhở user thay đổi password

III. QUẢN LÝ NHÓM

- Thông tin của nhóm

- Thiết lập những người dùng có chung một số đặc điểm nào đó hay có chung quyền hạn trên tài nguyên vào chung một nhóm.
- Mỗi nhóm có một tên riêng và một định danh nhóm, một nhóm có thể có nhiều người dùng.
- Thông tin về nhóm lưu tại tập tin **/etc/group**. Mỗi dòng định nghĩa một nhóm, các trường trên dòng cách nhau bằng dấu “:”. Cú pháp mô tả thông tin nhóm trong file **/etc/group**.

<tên-nhóm>:<pass-của-nhóm>:<định-danh-nhóm>:<user-thuộc-nhóm>

III. QUẢN LÝ NHÓM

- File cấu hình nhóm: **/etc/group**
- Cú pháp: **Tên nhóm:mật khẩu:GID**

```
dbus:x:81:
utmp:x:22:
utempter:x:35:
avahi:x:70:
mailnull:x:47:
smmisp:x:51:
nscd:x:28:
floppy:x:19:
vcsa:x:69:
haldaemon:x:68:
rpc:x:32:
rpcuser:x:29:
nfsnobody:x:65534:
sshd:x:74:
pcap:x:77:
ntp:x:38:
slocate:x:21:
gdm:x:42:
apache:x:48:
xfs:x:43:
sabayon:x:86:
lnkkhanh:x:500:
SV:x:101:
```


CÁC THAO TÁC TRÊN NHÓM

- Tạo nhóm

Cú pháp: **groupadd <groupname>**

Ví dụ: **groupadd hocvien**

```
axenus ~ #  
axenus ~ # groupadd cats  
axenus ~ # cat /etc/group | grep cats  
cats:x:1013:  
axenus ~ # groupadd -g 999 dogs  
groupadd: GID '999' already exists  
axenus ~ # groupadd -g 998 dogs  
axenus ~ # cat /etc/group | grep dogs  
dogs:x:998:  
axenus ~ # cat /etc/gshadow | grep cats  
cat: /etc/gshadow: No such file or directory  
axenus ~ #
```

CÁC THAO TÁC TRÊN NHÓM

- Thêm người dùng vào nhóm

Cú pháp: `usermod -g <tên-nhóm> <tên-tài-khoản>`

- Sửa group:

groupmod [-n New name] [-g new groupid]

- Đổi group password:

passwd []

CÁC THAO TÁC TRÊN NHÓM

- **Hủy nhóm**

Cú pháp: **groupdel <groupname>**

Ví dụ: Xóa nhóm **hocvien**

groupdel hocvien

CÁC THAO TÁC TRÊN NHÓM

- **Xem thông tin về user và group**

- Ta có thể dùng lệnh groups hoặc id để xem thông tin về một tài khoản hay một nhóm nào đó trong hệ thống.

Cú pháp: **id <option> <username>**

Ví dụ: Ta muốn xem groupId của một user tdnhon ta dùng lệnh:

id -g tdnhon

CÁC THAO TÁC TRÊN NHÓM

Để xem tên nhóm của một user dùng lệnh: **groups <username>**

Ví dụ:

```
[root@server root]# groups root
```

```
root : root bin daemon sys adm disk wheel
```

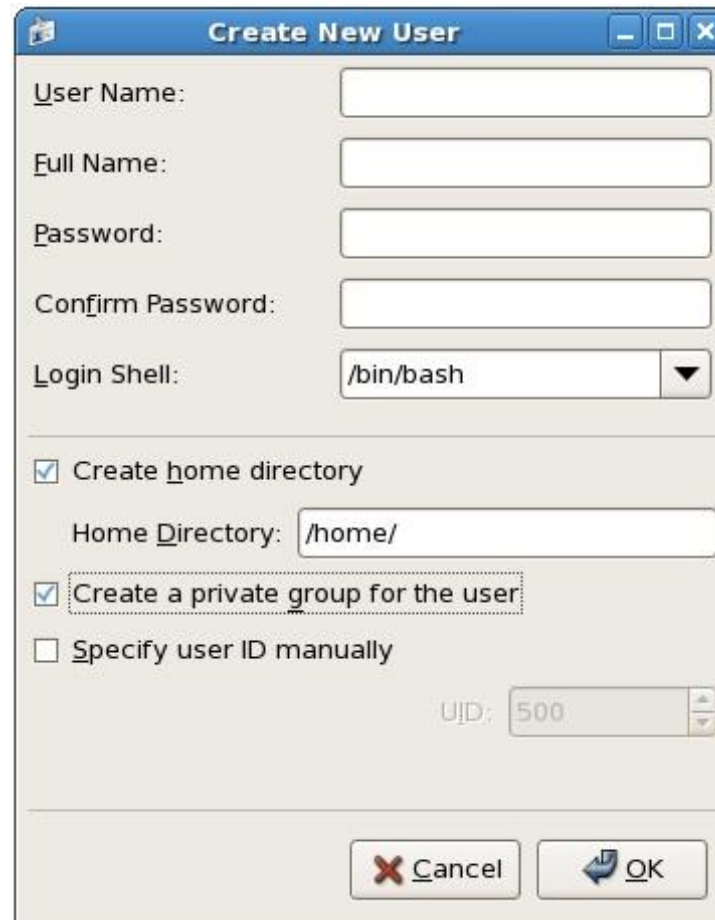
IV. QUẢN LÝ QUA GIAO DIỆN

- Linux cung cấp tiện ích **User Manager** cho phép ta có thể quản lý người dùng và nhóm linh hoạt và hiệu quả hơn.
 - Chọn **System -> Administration -> Users and Groups**
 - Giao diện quản lý người dùng trong Linux



IV. QUẢN LÝ QUA GIAO DIỆN

- **Tạo tài khoản:** chọn nút chức năng **Add User**.



The image shows a 'Create New User' dialog box with the following fields and options:

- User Name:** Text input field.
- Full Name:** Text input field.
- Password:** Text input field.
- Confirm Password:** Text input field.
- Login Shell:** Dropdown menu with '/bin/bash' selected.
- ☒ **Create home directory**
- Home Directory:** Text input field with '/home/'.
- ☒ **Create a private group for the user**
- ☐ **Specify user ID manually**
- UID:** Spin box with '500'.
- Buttons:** 'Cancel' and 'OK' at the bottom right.

IV. QUẢN LÝ QUA GIAO DIỆN

- **Thay đổi thông tin cho tài khoản:** bằng cách nhấp đôi vào biểu tượng tên account



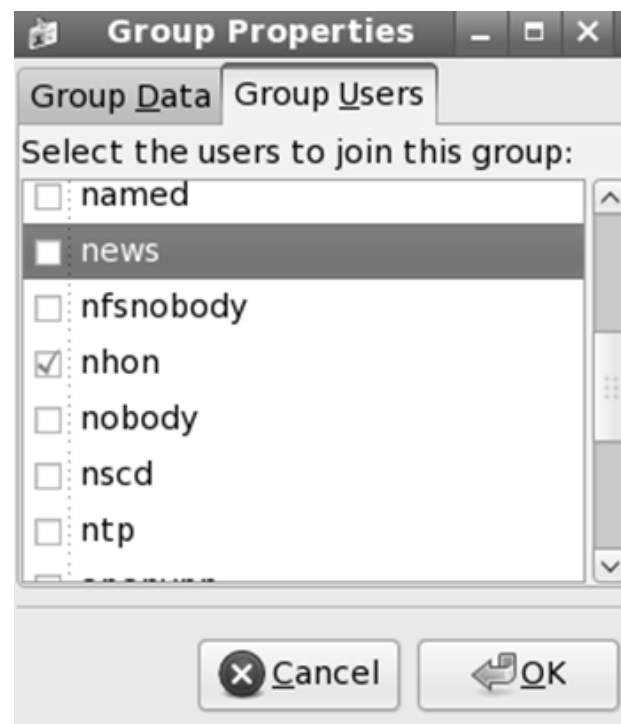
IV. QUẢN LÝ QUA GIAO DIỆN

- **Tạo nhóm:** chọn nút chức năng **Add Group**.
- Đặt tên nhóm và nhấn OK.



IV. QUẢN LÝ QUA GIAO DIỆN

- **Thay đổi thông tin cho nhóm:** nhấp đôi vào tên nhóm chọn Group Users tab để hiểu thêm hoặc loại bỏ thành viên trong nhóm.



V. QUYỀN NGƯỜI DÙNG

- Linux cho phép người dùng xác định các quyền đọc (read), viết (write) và thực thi (execute) cho từng đối tượng. Có ba đối tượng
 - **Người sở hữu** (the owner)
 - **Nhóm sở hữu** (the group owner)
 - **Người khác** (“other users” hay everyone else)

V. QUYỀN NGƯỜI DÙNG

- Quyền đọc (Read – r – 4) cho phép đọc nội dung tập tin
- Quyền ghi (Write – w – 2) dùng để tạo, thay đổi hay xóa tập tin
- Quyền thực thi (Execute – x – 1) cho phép thực thi chương trình

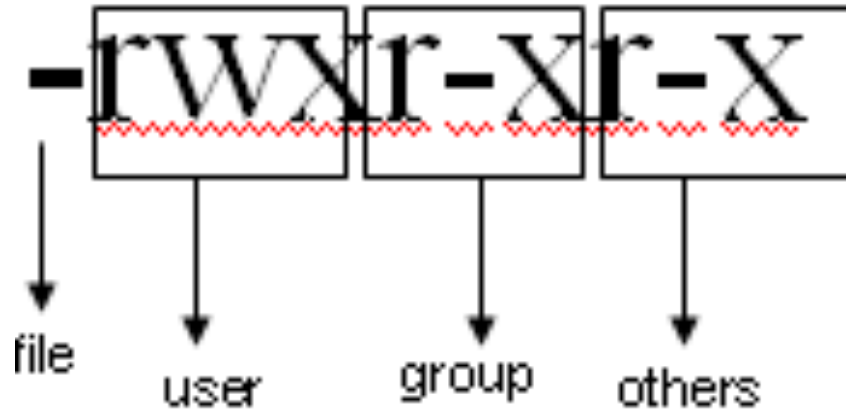
Ví dụ: lệnh **ls -l myfile**

-rw-r--r-- 1 fido users 163 Dec 7 14:31 myfile

Các ký tự **-rw-r--r--** biểu thị quyền truy cập của tập tin myfile

V. QUYỀN NGƯỜI DÙNG

```
d-rwx----- 2 root root 4096 Feb  7 17:42 orbit-root  
-rw-r--r--  1 root root    0 Dec 21 06:31 sealert.log
```

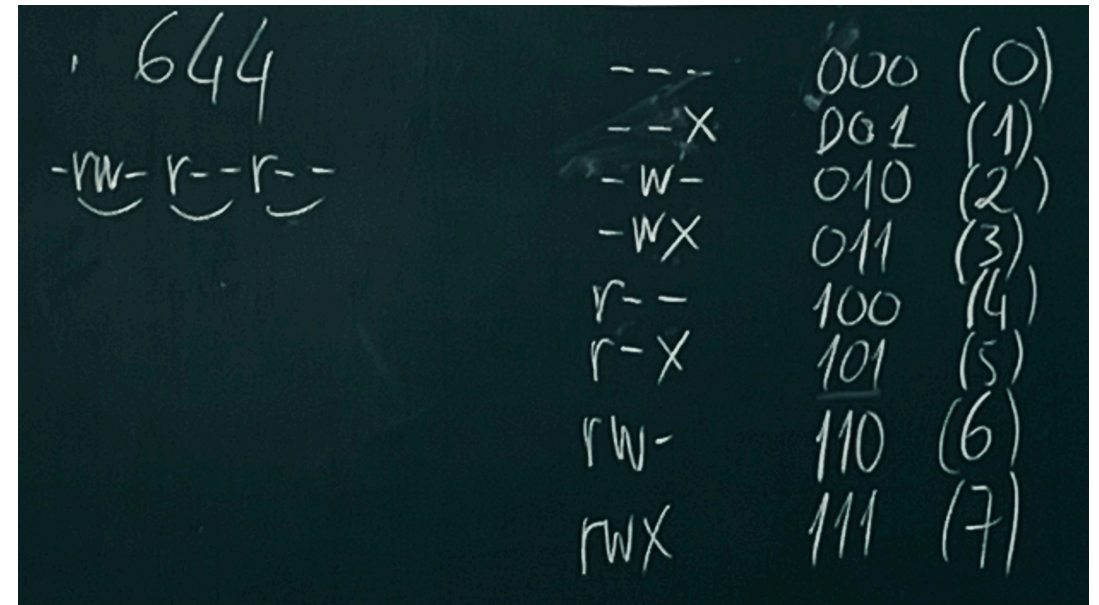


A handwritten diagram on a dark background showing the permissions `rwx`, `---`, and `---` grouped by brackets underneath. The labels "user", "group", and "other" are written below the brackets to identify each set of permissions.

V. QUYỀN NGƯỜI DÙNG

- **Tổ hợp của ba quyền trên có giá trị từ 0 đến 7**

- **0 or ---** : không có quyền
- **1 or --x** : execute
- **2 or -w-** : write-only (race)
- **3 or -wr** : write và execute
- **4 or r--** : read-only
- **5 or r-x** : read và execute
- **6 or rw-** : read và write
- **7 or rwx** : read, write và execute



---	000	(0)
--x	001	(1)
-w-	010	(2)
-wx	011	(3)
r--	100	(4)
r-x	101	(5)
rw-	110	(6)
rwx	111	(7)

Handwritten notes on the left of the table include '644' and three permission strings: '-rw-', 'r--', and 'r--', each with a smiley face drawn underneath.

V. QUYỀN NGƯỜI DÙNG

- GÁN QUYỀN CHO NGƯỜI DÙNG

- **Lệnh chmod:** cấp quyền hạn truy cập của tập tin hay thư mục

Cú pháp: **chmod** [tùy chọn] [tập tin]

Các tùy chọn:

Nhóm người dùng	Thao tác	Quyền hạn
u : user	+ : thêm quyền	r : read
g : group	- : xóa quyền	w : write
o : other	= : gán quyền	x : excute
a : all		

Ví dụ: Thêm quyền write cho nhóm trên tập tin **myfile**.

chmod g+w myfile

V. QUYỀN NGƯỜI DÙNG

- **Lệnh chown:** dùng thay đổi người sở hữu.

Cú pháp : **chown [người dùng:nhóm] [tập tin/thư mục]**

Ví dụ:

chown hv1 /bt/test.txt

Chuyển chủ sở hữu của file test.txt là người dùng hv1

V. QUYỀN NGƯỜI DÙNG

- **Lệnh chgrp:** dùng thay đổi nhóm sở hữu.

Cú pháp : **chgrp [nhóm] [tập tin/thư mục]**

Ví dụ:

chgrp users /tmp/test

Chuyển chủ sở hữu của test là nhóm users

V. QUYỀN NGƯỜI DÙNG

- **Lệnh umask:** Là lệnh cho phép thiết lập quyền mặc định của người dùng truy xuất filesystem, **mặc định giá trị umask là 022.**
 - Quyền mặc định của file hoặc thư mục được xác định là phần bù của umask xét trên ba bit quyền hạn của hệ thống dành cho người dùng.
 - **Đối với tập tin** quyền tối đa mà hệ thống tự động có thể gán là rw. Do đó, quyền tối đa của file tính theo hệ thập phân là **666.**
 - **Đối với thư mục** thì quyền tối đa của từng người dùng là **777.**
- Cú pháp lệnh umask:
- umask <giá trị>**

V. QUYỀN NGƯỜI DÙNG

- Chúng ta có thể thay đổi những giá trị mặc định trong file sau:
 - **/etc/login.defs** : file chứa thông số mặc định khi tạo user hoặc tạo group.
 - **/etc/skel/** : Tất cả những file là thư mục con trong này sẽ được copy sang HOME của user mới.