



Hệ điều hành Linux

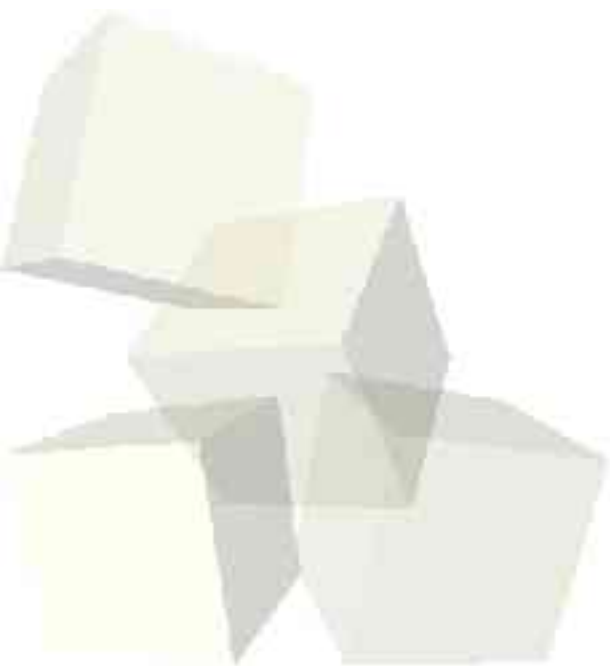
Lê Đình Long
longld@vnSecurity.net

2003



Chương 6

Quản trị căn bản





- Tài khoản superuser
- Quá trình khởi động và ngừng hệ thống
- Quản trị dịch vụ
- Quản trị tài khoản người dùng
- Quản trị hệ thống file
- Quản trị gói phần mềm
- Kiểm soát tiến trình (process)



root – tài khoản superuser

- Tài khoản có quyền cao nhất trên hệ thống
- Không bị giới hạn
- Đảm nhiệm việc quản trị và bảo trì hệ thống
- Sử dụng: không login trực tiếp

```
$ su -
```

```
Password
```

```
#
```

- Cẩn thận khi thực thi lệnh!

```
# rm -rf / usr/local/oldir
```

```
# rm -rf bad *
```



Khởi động và ngừng hệ thống

- Khởi động hệ thống
- File /etc/inittab
- Chuyển đổi runlevel
- Các file rc script
- Chế độ một người dùng (single-user)
- Ngừng hệ thống





Khởi động hệ thống

- Boot kernel
- Khởi tạo các điều khiển thiết bị
- Thực thi /sbin/init (khởi động theo Sys-V)
- init đọc và thực thi /etc/inittab
- Thực thi các file rc tùy theo runlevel





■ Định dạng

`code:runlevel:actions:command`

■ Runlevel

```
# Default runlevel. The runlevels used by RHS are:
# 0 - halt (Do NOT set initdefault to this)
# 1 - Single user mode
# 2 - Multiuser, without NFS
# 3 - Full multiuser mode
# 4 - unused
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
```

```
id:5:initdefault:
```



Chuyển đổi runlevel

- Sửa dòng initdefault trong /etc/inittab

```
id:3:initdefault:
```

- Thực thi init bằng tay

```
# init 5 (chuyển sang mode X11)
```

```
# init 3 (chuyển sang multiuser mode)
```

```
# init 1 (chuyển sang single user mode)
```

```
# init 6 (reboot)
```

- Tìm runlevel hiện tại và trước đó

```
# runlevel
```

```
N 5
```




Các file rc script

- Được đặt trong /etc/rc.d/rcN.d (N=runlevel)
- Là các shell script để khởi động/ngừng dịch vụ
- Script khởi động (start): Snnxxxx
- Script ngừng (kill): Knnxxxx
- nn = 00 – 99: quy định thứ tự được thực thi

S10network K90network K10xfS S99local

- S* và K* chỉ là các symlink đến các script thực
- Các script thực được chứa trong một thư mục tập trung: /etc/rc.d/init.d (hoặc /etc/init.d)



Cấu hình *runlevel*

- `redhat-config-services/serviceconf` (dạng đồ họa)
- `ntsysv` – giao diện cấu hình các dịch vụ cho một hoặc nhiều `runlevel` ở console

```
# ntsysv (cấu hình cho runlevel hiện tại)
# ntsysv --level 35
```

Lưu ý:

- Các thay đổi sẽ không tác động cho đến lần chuyển đổi `runlevel` kế tiếp



Bật/tắt dịch vụ bằng tay

```
# service svc_name {start|stop|restart|status}
```

```
# /etc/init.d/svc_name {start|stop|restart|status}
```

Ví dụ:

```
# service xfs restart
```

```
# /etc/init.d/xinetd stop
```

```
# service httpd start
```

```
# service portmap status
```



Chế độ single-user

- Dùng để khôi phục hệ thống, khắc phục sự cố
- Không yêu cầu login
- Truy cập thẳng vào root shell
- Chỉ có duy nhất một console

```
boot: linux single
```

```
boot: linux -s
```

```
boot: linux 1
```

```
# init 1
```



■ shutdown – ngừng hệ thống

```
# shutdown -r +10 "Rebooting to try new kernel"
```

```
# shutdown -h now (halt ngay lập tức)
```

```
# shutdown -c "No need to shutdown"
```

■ Một số cách khác

```
# reboot
```

```
# halt
```

```
# poweroff
```

Ctrl+Alt+Del



Quản trị người dùng

- User và group
- Thông tin người dùng: `/etc/passwd`
- Thông tin mật khẩu: `/etc/shadow`
- Thông tin group: `/etc/group`
- Tạo mới tài khoản
- Sửa đổi thông tin tài khoản
- Xóa tài khoản





User và group

- Tài khoản hệ thống và tài khoản người dùng
- Mỗi user có duy nhất một tên và id (uid)
- Mỗi user thuộc về ít nhất một nhóm (primary group)
- Mỗi nhóm có duy nhất một tên và id (gid)
- Tên tài khoản thường toàn chữ thường
- Tài khoản superuser có id 0 (uid=gid=0)





■ Định dạng

username:password:uid:gid:gecos:homedir:shell

- username: chuỗi ký tự bất kỳ, tên dùng để login
- password: mật khẩu đã được mã hoá (không có thông tin nếu dùng shadow)
- uid: user id
- gid: group id
- geccos: thông tin thêm về user
- homedir: thư mục home của user
- shell: chương trình sẽ được thực thi khi user login, thường là một shell (/bin/bash)



Ví dụ về */etc/passwd*

```
root:x:0:0:root:/root:/bin/bash
```

```
bin:x:1:1:bin:/bin:/sbin/nologin
```

```
daemon:x:2:2:daemon:/sbin:/sbin/nologin
```

```
nobody:x:99:99:Nobody:/:/sbin/nologin
```

```
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
```

```
student:x:500:500:Student:/home/student:/bin/bash
```



■ Định dạng

username:password:d1:d2:d3:d4:d5:d5:reserved

- username: tương ứng username trong /etc/passwd
 - password: mật khẩu đã được mã hoá
 - d1: số ngày kể từ lần cuối thay đổi mật khẩu
 - d2: số ngày trước khi có thể thay đổi mật khẩu
 - d3: số ngày mật khẩu có giá trị
 - d4: số ngày cảnh báo user trước khi mật khẩu hết hạn
 - d5: số ngày sau khi mật khẩu hết hạn tài khoản sẽ bị khoá
 - d6: số ngày kể từ khi tài khoản bị khoá
- (các giá trị số ngày tính theo mốc từ 1/1/1970)



Ví dụ về */etc/shadow*

```
root:$1$dxtC0Unf$2SCguIhTlrcnkSH5tjw0s/:12148:0:99999:7:::
```

```
bin:*:12148:0:99999:7:::
```

```
daemon:*:12148:0:99999:7:::adm:*:12148:0:99999:7:::
```

```
nobody:*:12148:0:99999:7:::
```

```
xfx:!!:12148:0:99999:7:::
```

```
student:$1$HI64tQaw$YKRSqWwWOM4vgaRYJ/hs80:12148:0:99999:7:::
```



File /etc/group

■ Định dạng

groupname:password:gid:members

- groupname: chuỗi ký tự bất kỳ, xác định tên group
- password: mật khẩu (tùy chọn)
- gid: group id
- members: danh sách thành viên, cách nhau bằng “,”
(các thành viên có groupname là secondary group)

■ Ví dụ về /etc/group

root:x:0:

bin:x:1:bin,daemon

student:x:500:



Tạo mới tài khoản

```
groupadd [-g gid] group
```

```
# groupadd student
```

```
# groupadd -g 1000 sv
```

```
useradd [-u uid] [-g group] [-G group,...]  
        [-c comment] [-d home] [-s shell] login
```

```
# useradd -g students -c "Student 001" stud001
```

■ passwd – đặt mật khẩu cho user

```
# passwd stud001
```



Sửa đổi thông tin tài khoản

```
groupmod [-g gid] [-n name] group
```

```
# groupmod -g 1001 student
```

```
usermod [-u uid] [-g group] [-G group,...]  
        [-c comment] [-d home] [-s shell] [-l  
        new_login_name] login
```

```
# usermod -u 1001 stud001
```

```
# usermod -c "Sinh vien 001" -l sv001 stud001
```



Xoá tài khoản

```
userdel [-r] login
```

-r: xoá thư mục home của user

```
# userdel -r sv001
```

```
groupdel group
```

```
# groupdel student
```





Chuyển đổi quyền sở hữu

`chown [OPTION] USER[:[GROUP]] FILE`

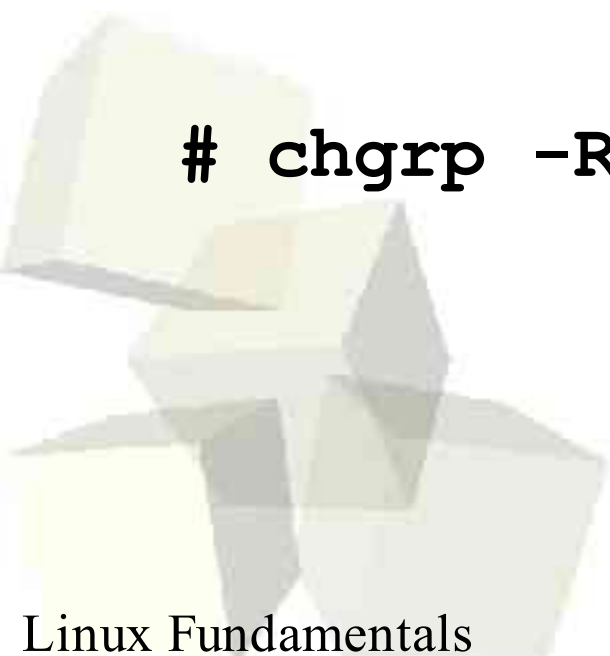
`-R`: đổi cả file và thư mục con

```
# chown -R sv001 /home/stud001
```

```
# chown -R :student /home/stud001
```

`chgrp [OPTION] [GROUP] [FILE]`

```
# chgrp -R student /home/stud*
```





Quản trị hệ thống file

- Kiểu hệ thống file
- Mount/unmount hệ thống file
- Thông tin về hệ thống file: /etc/fstab
- Tạo mới hệ thống file
- Kiểm tra và sửa chữa hệ thống file





Kiểu hệ thống file

- ext2 - kiểu chuẩn của Linux
- vfat – Windows 9x FAT32
- ntfs – Windows NT/2000/XP NTFS
- iso9660 – CD-ROM
- smbfs – hệ thống file chia sẻ dùng SMB
- nfs – Network File System
- proc – hệ thống file giả /proc
- ext3, reiserfs, xfs, jfs – hệ thống file nhật ký



Mount hệ thống file

■ Mount hệ thống file

```
mount -t fstype device directory
```

```
# mount -t ext3 /dev/hda5 /mnt/backup
```

```
# mount -t vfat /dev/hda1 /mnt/windows
```

```
# mount -t iso9660 /dev/hdd /mnt/cdrom
```

-a: mount tất cả fs mô tả trong /etc/fstab

-o: tùy chọn mount

remount: mount lại một fs đã mount

ro: read-only

rw: read/write

loop: mount thông qua loop device



Unmount hệ thống file

- Xem các hệ thống file đã mount

```
# mount
```

```
/dev/hda2 on / type ext3 (rw)
```

- Unmount hệ thống file

```
umount directory | device
```

```
# umount /mnt/backup
```

```
# umount /dev/hda1
```

```
# mount -t iso9660 /dev/hdd /mnt/cdrom
```

```
-a: unmount các fs mô tả trong /etc/mtab
```



- Giúp tự động mount các hệ thống file lúc boot
- Khai báo cho các lệnh mount ngắn gọn

```
# mount
```

```
/dev/hda2 on / type ext3 (rw)
```

- Định dạng

```
device mount-point type options
```

- Ví dụ về file /etc/fstab

/dev/hda2	/	ext3	defaults	1	1
none	/proc	proc	defaults	0	0
/dev/hda3	swap	swap	defaults	0	0
/dev/fd0	/mnt/floppy	auto	noauto	0	0
/dev/hdd	/mnt/cdrom	iso9660	noauto,ro	0	0
/dev/hdc1	/mnt/c	auto	auto	0	0



Tạo hệ thống file

- Tạo phân vùng trên đĩa

```
# fdisk /dev/hda
```

- Tạo hệ thống file mới

```
mkfs -t fstype filesys blocks
```

blocks: kích thước của fs (1024-byte blocks)

```
# mkfs -t ext3 /dev/hda6
```

```
# mkfs -t vfat /dev/hda7
```

Lưu ý:

- Tạo hệ thống file mới sẽ xóa toàn bộ dữ liệu cũ
- mkfs không hỏi trước khi tạo hệ thống file



Kiểm tra, sửa hệ thống file

- Kiểm tra tính nhất quán của hệ thống file
- Sửa chữa sau khi bị crash, mất nguồn
- Ngoại trừ hệ thống file "/", nên unmount trước khi kiểm tra, sửa chữa

```
fsck -t fstype filesys
```

```
# fsck -t ext3 /dev/hda2
```

```
-A: kiểm tra tất cả fs trong /etc/fstab
```



Quản trị gói phần mềm

- RPM – Red Hat Package Manager
- Cài đặt
- Nâng cấp
- Gỡ bỏ
- Truy vấn thông tin
- Cài đặt từ mã nguồn





Red Hat Package Manager

- Hệ thống quản lý phần mềm đóng gói do Red Hat phát triển
- Thông tin về gói được lưu trong database
- Theo dõi sự phụ thuộc giữa các gói
- Dễ sử dụng
- Sử dụng trong hầu hết các Linux distro hiện nay
- Nhược điểm: giải quyết vấn đề phụ thuộc giữa các gói là việc không dễ dàng



Cài đặt gói rpm

```
rpm -i | -U pkg-ver.arch.rpm ...
```

--force: cài đè nếu gói đã được cài

--nodeps: cài bỏ qua các gói phụ thuộc

```
# rpm -i openssh-3.5p1-6.i386.rpm
```

```
# rpm -ihv openssh-clients-3.5p1-6.i386.rpm
```

```
# rpm -ihv openssh-askpass-3.5p1-6.i386.rpm\  
openssh-askpass-gnome-3.5p1-6.i386.rpm
```

```
# rpm -Uhv xvnkb-0.2.7-2.i386.rpm
```



Nâng cấp gói rpm

```
rpm -F pkg-newver.arch.rpm ...
```

```
# rpm -Fhv xvnkb-0.2.7-2.i386.rpm
```

```
# rpm -Fhv *.rpm
```





Gỡ bỏ gói rpm

```
rpm -e pkg ...
```

```
# rpm -e openssh-3.5p1-6 openssh-clients
```

```
# rpm -e xvnkb
```



Truy vấn thông tin gói rpm

`rpm -q [query-options]`

`# rpm -qi openssh-clients`

(thông tin về nội dung gói đã cài)

`# rpm -ql fileutils`

(liệt kê các file của gói đã cài)

`# rpm -qif /bin/ls`

(thông tin về gói chứa file /bin/ls)

`# rpm -qip xvnkb-0.2.7-2.i386.rpm`

(thông tin về gói chưa được cài)

`# rpm -qa`

(liệt kê tên tất các gói được cài)



Giải quyết sự phụ thuộc

```
# rpm -ihv MagicPoint-1.09a-1.i386.rpm
error: failed dependencies:
VFlib2 >= 2.25.6-4 is needed by MagicPoint-1.09a-1
libpng.so.2 is needed by MagicPoint-1.09a-1

# rpm -ihv MagicPoint-1.09a-1.i386.rpm \
    VFlib2-2.25.6-4.i386.rpm \
    libpng-1.0.12-2.i386.rpm
```





Cài đặt từ mã nguồn

- Giải nén gói mã nguồn
- Xem thông tin trong file README
- Xem hướng dẫn cài đặt trong file INSTALL
- Các bước chung:

```
# tar zxvf source-ver.tar.gz
```

```
# cd source-ver
```

```
# ./configure
```

```
# make
```

```
# make install
```

- Hướng dẫn tùy chọn cấu hình

```
# ./configure --help
```



Điều khiển tiến trình

- Tiến trình (process)
- Liệt kê các tiến trình đang chạy
- Ngừng một tiến trình
- Theo dõi hệ thống





Tiến trình (process)

- Tiến trình là một chương trình đang chạy trong bộ nhớ
- Nhiều tiến trình chạy đồng thời ở một thời điểm
- Mỗi tiến trình được gán một chỉ số PID duy nhất
- Tiến trình cũng có quyền sở hữu và truy cập như với file
- Các loại tiến trình:
 - Daemon
 - Background
 - Foreground



ps – liệt kê tiến trình

`ps [options]`

`a`: tất cả proc trên cùng một terminal

`x`: các proc không gắn với tty điều khiển

`u`: user-format

`l`: long-format

`w`: wide output

`$ ps`

PID	TTY	TIME	CMD
728	pts/3	00:00:00	bash
1010	pts/3	00:00:00	ps

`$ ps auw`

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	728	0.0	0.6	3528	1604	pts/3	S	21:08	0:00	/bin/bash
root	1161	0.0	0.3	3548	860	pts/3	R	22:29	0:00	ps auw



kill – ngừng tiến trình

```
kill [-s signal] pid
```

```
kill -l [signal]
```

signal mặc định là SIGTERM

```
$ kill 728
```

```
$ kill -s SIGKILL 728
```

```
$ kill -KILL 728
```

```
$ kill -9 728
```

```
$ kill -l
```

1) SIGHUP	2) SIGINT	3) SIGQUIT	4) SIGILL
5) SIGTRAP	6) SIGABRT	7) SIGBUS	8) SIGFPE
9) SIGKILL	10) SIGUSR1	11) SIGSEGV	12) SIGUSR2
13) SIGPIPE	14) SIGALRM	15) SIGTERM	17) SIGCHLD
18) SIGCONT	19) SIGSTOP	20) SIGTSTP	21) SIGTTIN



killall – ngừng theo tên

```
killall [-s signal] name
```

```
# killal -HUP syslogd
```

```
# killall -9 man
```





Theo dõi hệ thống

- top: hiển thị thời gian thực thông tin sử dụng tài nguyên hệ thống
- free: hiển thị thông tin bộ nhớ sử dụng/còn trống
- uptime: thời gian sống của hệ thống
- w: xem các user còn đang login đang làm gì
- pstree: hiển thị cây tiến trình
- pgrep, pkill: tìm hoặc gửi signal đến tiến trình dựa theo tên và các thuộc tính khác
- nice, renice, snice: thay đổi mức độ ưu tiên của tiến trình



Q & A

