



User Management



Adding New Users

ID

❑ User ID, Group ID

- % **id** liuyh
 - uid=10047(liuyh) gid=200(dcs) groups=200(dcs),0(wheel),700(ta),800(security),888(wwwadm)
- % **id** 10047
 - uid=10047(liuyh) gid=200(dcs) groups=200(dcs),0(wheel),700(ta),800(security),888(wwwadm)

❑ Super user

- root
 - uid=0(root) gid=0(wheel) groups=0(wheel),5(operator)

❑ Other Important Users

- daemon: owner of unprivileged software
- bin: owner of system commands
- sys: owner of the kernel and memory images
- nobody: owner of nothing

Steps to add a new user

1. Edit the password and group files
 - > vipw, pw
2. Set an initial password
 - > passwd liuyh
3. Set quota
 - > edquota liuyh
4. Create user home directory
 - > mkdir /home/liuyh
5. Copy startup files to user's home (optional)
6. Set the file/directory owner to the user
 - > chown -R liuyh:dcs /home/liuyh

Step to add a new user –

1. password and group file (1)

❑ /etc/passwd

- Store user information:
 - Login name
 - Encrypted password (* or x)
 - UID
 - Default GID
 - GECOS information
 - Full name, office, extension, home phone
 - Home directory
 - Login shell
- Each is separated by “:”

```
liuyh@NASA /etc $ grep liuyh passwd  
liuyh:*:1002:20:User &:/home/liuyh:/bin/tcsh
```

Step to add a new user –

1. password and group file (2)

❑ Encrypted password

- The encrypted password is stored in shadow file for security reason
 - /etc/master.passwd (BSD)
 - /etc/shadow (Linux)

```
liuyh@NASA /etc $ grep liuyh passwd
liuyh:*:1002:20:User &:/home/liuyh:/bin/tcsh
```

/etc/passwd (BSD)

```
liuyh@NASA /etc $ sudo grep liuyh master.passwd
liuyh:$1$4KQcUPbi$/nVs5bPDUXoyLLxw9Yp9D.:1002:20::0:0:User &:/home/liuyh:/bin/tcsh
```

/etc/master.passwd

```
[liuyh@yhlinux /etc] grep liuyh passwd
liuyh:x:1002:20:User &:/home/liuyh:/bin/tcsh
```

/etc/passwd (Linux)

```
[liuyh@yhlinux /etc] sudo grep liuyh passwd
liuyh:$1$4KQcUPbi$/nVs5bPDUXoyLLxw9Yp9D.:14529:0:99999:7::
```

/etc/shadow

Step to add a new user –

1. password and group file (3)

❑ Encrypted methods

- des
 - Plaintext: at most 8 characters
 - Cipher: 13 characters long
 - vFj42r/HzGqXk
- md5
 - Plaintext: arbitrary length
 - Cipher: 34 characters long started with "\$1\$"
 - \$1\$xbFdBaRp\$zXSp9e4y32ho0MB9Cu2iV0
- blf
 - Plaintext: arbitrary length
 - Cipher: 60 characters long started with "\$2a\$"
 - \$2a\$04\$jn9vc7dDJOX7V335o3.RoujuK/uoBYDg1xZs1OcBOrIXve3d1Cbm6

❑ login.conf(5), "AUTHENTICATION"

- section: passwd_format

Step to add a new user –

1. password and group file (4)

❑ GECOS

- **General Electric Comprehensive Operating System**
- Commonly used to record personal information
- “,” separated
- “finger” command will use it
- Use “chfn” to change your GECOS

```
#Changing user information for liuyh.  
Shell: /bin/tcsh  
Full Name: User &  
Office Location:  
Office Phone:  
Home Phone:  
Other information:
```


Step to add a new user –

1. password and group file (5)

❑ Login shell

- Command interpreter
 - /bin/sh
 - /bin/csh
 - /bin/tcsh
 - /bin/bash (/usr/ports/shells/bash)
 - /bin/zsh (/usr/ports/shells/zsh)
- Use “chsh” to change your shell

```
#Changing user information for liuyh.  
Shell: /bin/tcsh  
Full Name: User &  
Office Location:  
Office Phone:  
Home Phone:  
Other information:
```

Step to add a new user –

1. password and group file (6)

❑ /etc/group

- Contains the names of UNIX groups and a list of each group's member:
 - Group name
 - Encrypted password
 - GID
 - List of members, separated by “,”

```
wheel:*:0:root,liuyh  
daemon:*:1:daemon  
staff:*:20:
```

- Only in wheel group can do “su” command

Step to add a new user –

1. password and group file (7)

❑ In FreeBSD

- Use “vipw” to edit /etc/master.passwd
- Three additional fields
 - Login class
 - Refer to an entry in the /etc/login.conf
 - Determine user resource limits and login settings
 - default
 - Password change time
 - Account expiration time

```
liuyh@NASA /etc $ sudo grep liuyh master.passwd
liuyh:$1$4KQcUPbi$/nVs5bPDUXoyLLxw9Yp9D.:1002:20:0:0:User &:/home/liuyh:/bin/tcsh
```

```
liuyh@NASA /etc $ grep liuyh passwd
liuyh:*:1002:20:User &:/home/liuyh:/bin/tcsh
```

Step to add a new user –

1. password and group file (8)

- ❑ /etc/login.conf of FreeBSD
 - Set account-related parameters including
 - **Resource limits**
 - Process size, number of open files
 - **Session accounting limits**
 - When logins are allowed, and for how long
 - **Default environment variable**
 - **Default path**
 - **Location of the message of the day file**
 - **Host and tty-based access control**
 - **Default umask**
 - **Account controls**
 - Minimum password length, password aging
 - login.conf(5)

Step to add a new user –

1. password and group file (9)

```
default:\
:passwd_format=md5:\
:copyright=/etc/COPYRIGHT:\
:welcome=/etc/motd:\
:setenv=MAIL=/var/mail/$,BLOCKSIZE=K,FTP_PASSIVE_MODE=YES:\
:path=/sbin /bin /usr/sbin /usr/bin /usr/games /usr/local/sbin /usr/local/bin:\
:nologin=/var/run/nologin:\
:cputime=unlimited:\
:datasize=unlimited:\
:stacksize=unlimited:\
:memorylocked=unlimited:\
:memoryuse=unlimited:\
:filesize=unlimited:\
:coredumpsize=unlimited:\
:openfiles=unlimited:\
:maxproc=unlimited:\
:sbsize=unlimited:\
:vmemoryuse=unlimited:\
:priority=0:\
:ignoretime@:\
:umask=022:
```

Step to add a new user –

1. password and group file (10)

❑ In Linux

- Edit /etc/passwd and then
- Use “pwconv” to transfer into /etc/shadow

❑ Fields of /etc/shadow

- Login name
- Encrypted password
- Date of last password change
- Minimum number of days between password changes
- Maximum number of days between password changes
- Number of days in advance to warn users about password expiration
- Number of inactive days before account expiration
- Account expiration date
- Flags

```
[liuyh@yhlinux /etc] sudo grep liuyh passwd  
liuyh:$1$4KQcUPbi$/nVs5bPDUXoyLLxw9Yp9D.:14529:0:99999:7:::
```

Step to add a new user – 2, 3, 4

- ❑ Initialize password
 - passwd liuyh
- ❑ Set quota
 - edquota liuyh
 - edquota -p dcsq liuyh

Quotas for user liuyh:

```
/raid: kbytes in use: 705996, limits (soft = 4000000, hard = 4200000)
      inodes in use: 9728, limits (soft = 50000, hard = 60000)
```

- ❑ Ref:
<http://mail.lsp.s.tp.edu.tw/~gsyan/freebsd2001/quota.html>
- ❑ Home directory
 - mkdir /home/liuyh

Step to add a new user – 5, 6

❑ Startup files

- **System wide**

- /etc/{csh.cshrc, csh.login, csh.logout, profile}

- **Private**

- csh/tcsh ➔ .login, .logout, .tcshrc, .cshrc

- sh ➔ .profile

- vi ➔ .exrc

- vim ➔ .vimrc

- startx ➔ .xinitrc

- In this step, we usually copy private startup files

- /usr/share/skel/dot.*

- /usr/local/share/skel/zh_TW.Big5/dot.*

❑ Change onwer

- `chown -R liuyh:dcs /home/liuyh`

Remove accounts

❑ Delete the account entry

- [FreeBSD] vipw, pw userdel
- [Linux] remove the row in /etc/passwd and pwconv

❑ Backup file and mailbox

- tar jcf liuyh-home-20110927.tar.bz /home/liuyh
- tar jcf liuyh-mail-20110927.tar.bz /var/mail/liuyh
- chmod 600 liuyh-*-20110927.tar.bz

❑ Delete home directory and mailbox

- rm -rf /home/liuyh /var/mail/liuyh

Disabling login

❑ Ways to disable login

- Change user's login shell as /sbin/nologin
- Put a “#” in front of the account entry
- Put a '-' in front of the account entry
- Put a “*” in the encrypted password field
- Add *LOCKED* at the beginning of the exrypted password field
 - pw lock/unlock
- Write a program to show the reason and how to remove the restriction
- pw(8) 、 adduser(8) 、 pwd_mkdb(8)



Rootly Powers

The Root

- ❑ Root
 - Root is God, A.K.A. super-user.
 - UID is 0

- ❑ UNIX permits super-user to perform any valid operation on any file or process, such as:
 - Changing the root directory of a process with **chroot**
 - Setting the system clock
 - Raising anyone's resource usage limits and process priorities (**renice, edquota**)
 - Setting the system's hostname (**hostname** command)
 - Configuring network interfaces (**ifconfig** command)
 - Shutting down the system (**shutdown** command)
 - ...

Becoming root (1)

□ Login as root

- Console login

- Allow root login on console.

- If you don't want to permit root login in the console (in /etc/ttys)

```
ttyv1 "/usr/libexec/getty Pc"      cons25 on secure
```

```
➔ttyv1 "/usr/libexec/getty Pc"      cons25 on insecure
```

- Remote login (login via ssh)

- sshd:

```
/etc/ssh/sshd_config
```

```
#PermitRootLogin yes
```

- **DON'T DO THAT !!!**

Becoming root (2)

❑ su : substitute user identity

- su, su -, su *username*
- ※ Environment is unmodified with the exception of USER, HOME, SHELL which will be changed to target user.
- ※ “su -” will simulate as a full login.

❑ sudo : a limited su (security/sudo)

- Subdivide superuser's power
 - **Who** can execute **what command** on **which host** as **whom**.
- Each command executed through sudo will be logged

```
Sep 20 02:10:08 NASA sudo: liuyh : TTY=pts/1 ; PWD=/tmp ;  
USER=root ; COMMAND=/etc/rc.d/pf start
```

- Edit /usr/local/etc/sudoers using **visudo** command
 - **visudo can check mutual exclusive access of sudoers file**

Becoming root (3)

- sudoers format
 - **Who** can execute **what command** on **which host** as **whom**
 - The user to whom the line applies
 - The hosts on which the line should be noted
 - The commands that the specified users may run
 - The users as whom they may be executed
 - Use absolute path

Host_Alias	BSD=bsd1,bsd2,alumni
Host_Alias	LINUX=linux1,linux2
Cmnd_Alias	DUMP=/usr/sbin/dump, /usr/sbin/restore
Cmnd_Alias	PRINT=/usr/bin/lpc, /usr/bin/lprm
Cmnd_Alias	SHELLS=/bin/sh, /bin/tcsh, /bin/csh

Becoming root (4)

Host_Alias	BSD=bsd1,bsd2,alumni
Host_Alias	LINUX=linux1,linux2
Cmnd_Alias	PRINT=/usr/bin/lpc, /usr/bin/lprm
Cmnd_Alias	SHELLS=/bin/sh, /bin/tcsh, /bin/csh
Cmnd_Alias	SU=/usr/bin/su
User_Alias	wwwTA=jnlin, ystseng
User_Alias	printTA=thchen, jnlin
Runas_Alias	NOBODY=nobody
chiahung	ALL=ALL
liuyh	ALL=(ALL)ALL,!SHELLS,!SU
printTA	csduty=PRINT
wwwTA	BSD=(NOBODY)/usr/bin/more
%wheel	ALL=NOPASSWD:/sbin/shutdown

Becoming root (5)

- % `sudo -u nobody more /usr/local/etc/apache/httpd.conf`
- % `cp -p /bin/csh /tmp/csh; sudo /tmp/csh`

Cmnd_Alias	SHELLS=/bin/sh, /bin/tcsh, /bin/csh
Cmnd_Alias	SU=/usr/bin/su
liuyh	ALL=(ALL)ALL,!SHELLS,!SU

sudoers Example

- ❑ liuyh ALL=(ALL) ALL
- ❑ %wheel ALL=(ALL) NOPASSWD: ALL

```
# User privilege specification
root    ALL=(ALL) ALL
liuyh   ALL=(ALL) ALL

# Uncomment to allow people in group wheel to run all commands
# %wheel    ALL=(ALL) ALL

# Same thing without a password
%wheel  ALL=(ALL) NOPASSWD: ALL
```

Advantage of sudo

- Accountability is much improved because of command logging
- Operators can do chores without unlimited root privileges

- The real root password can be known to only one or two people
- It's faster to use sudo than to run su or login as root
- Privileges can be revoked without the need to change the root password

- A canonical list of all users with root privileges is maintained
- There is less chance of a root shell being left unattended
- A single file can be used to control access for an entire network