



User Management

Lctseng, arr. by pschiu

ID

❑ User ID, Group ID

- % **id** lctseng (ID Name)
 - uid=10554(lctseng) gid=1130(cs) groups=1130(cs),0(wheel),2000(taever),2012(security)
- % **id** 10047 (UID)
 - Same as above

❑ Super user (defined by uid = 0)

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

❑ Other built-in users

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



Adding New Users

Steps to add a new user

1. Edit the password and group files
 - > `vipw, pw`
2. Set an initial password
 - > `passwd lctseng`
3. Set quota (if enabled, see handbook for quota settings)
 - > `edquota lctseng`
4. Create user home directory
 - > `mkdir /home/lctseng`
5. Copy startup files to user's home (optional)
 - > `cp .tcshrc /home/lctseng`
6. Set the file/directory owner to the user
 - > `chown -R lctseng:cs /home/lctseng`

Manually to add a new user

1. Add to password and group files
 - > vipw, pw
 - > Edit /etc/master.passwd & /etc/group
2. Set an initial password
 - > passwd lctseng
3. Set quota (if enabled, see handbook for quota settings)
 - > edquota lctseng
4. Create user home directory
 - > mkdir /home/lctseng
5. Copy default files to user's home (optional)
 - > cp /usr/share/skel/dot.cshrc /home/lctseng/.cshrc
6. Set the file/directory owner to the user
 - > chown -R lctseng:cs /home/lctseng

Manually to add a new user

- 1. add user to `/etc/master.passwd`
 - 2. add user to `/etc/group`
 - 3. `mkdir /home/user`
 - 4. `passwd user`
 - 5. `chown -R user:group /home/user`
-
- In some cases, you may need this step to do that.

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 “:”

```
lctseng@NASA $ grep lctseng /etc/passwd
lctseng:*:1002:20:User &:/home/lctseng:/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)

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

/etc/passwd (BSD)

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

/etc/master.passwd

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

/etc/passwd (Linux)

```
[lctseng@linux1 /etc] sudo grep lctseng passwd
lctseng:$1$4KQcUPbi$/nVs5bPDUXoyLLxw9Yp9D.:14529:0:99999:7:::
```

/etc/shadow(Linux)

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
- sha512
 - Plaintext: arbitrary length
 - Cipher: 106 characters long started with "\$6\$"
 - \$6\$o4B4Pa/ql3PpRAQo\$196.cCzrTCOIpPqk.VX7EqR0YNtf0dRLdx5Hzl6S7uGaPz4EDJdoXnmsSf.A21xS2zimI1XsHAgICR2Pw7ols1

❑ login.conf(5), "AUTHENTICATION"

- section: passwd_format

```
passwd_format=sha512
```

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 lctseng.  
Shell: /bin/tcsh  
Full Name: User &  
Office Location:  
Office Phone:  
Home Phone:  
Other information:
```

finger

```
[pschiu@bsd1 ~]#finger pschiu
Login: pschiu                               Name: Po-Shen Chiu
Directory: /u/gcs/104/0456183                Shell: /bin/tcsh
On since 四 10月 13 15:38 (CST) on pts/33, idle 1:42, from 140.113.209.205
On since 四 10月 13 15:38 (CST) on pts/25, idle 1:42, from 140.113.209.205
On since 四 10月 13 15:38 (CST) on pts/22, idle 1:42, from 140.113.209.205
On since 四 10月 13 15:38 (CST) on pts/34, idle 1:42, from 140.113.209.205
On since 四 10月 13 15:38 (CST) on pts/42, idle 1:42, from 140.113.209.205
On since 四 10月 13 15:38 (CST) on pts/44, idle 1:42, from 140.113.209.205
On since 四 10月 13 15:38 (CST) on pts/45, idle 1:42, from 140.113.209.205
On since 四 10月 13 17:02 (CST) on pts/57, idle 0:02, from 140.113.209.205
On since 四 10月 13 15:38 (CST) on pts/20 from 140.113.209.205
Mail last read 四 10月 6 13:03 2016 (CST)
Mail forwarded to: jal@jal.tw
No Plan.
[pschiu@bsd1 ~]#
```

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 or pkg install bash)
 - /bin/zsh (/usr/ports/shells/zsh or pkg install zsh)
- Use “chsh” to change your shell

```
#Changing user information for lctseng.  
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
 - Group password: join that group which you don't belong with (rarely used)
 - GID
 - List of members, separated by “,”

```
wheel:*:0:root,lctseng,pschiu
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
 - To change editor: setenv EDITOR <editor that you want to use>
- 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
 - Expiration time

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

```
lctseng@NASA /etc $ grep lctseng passwd
lctseng:*:1002:20:User &:/home/lctseng:/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)
 - After modify, update the database
 - `$ cap_mkdb /etc/login.conf`

Step to add a new user –

1. password and group file (9)

```
default:\
:passwd_format=sha512:\
:copyright=/etc/COPYRIGHT:\
:welcome=/etc/motd:\
:setenv=MAIL=/var/mail/$,BLOCKSIZE=K:\
:path=/sbin /bin /usr/sbin /usr/bin /usr/local/sbin /usr/local/bin ~/bin:\
:nologin=/var/run/nologin:\
:cputime=unlimited:\
:datasize=unlimited:\
:stacksize=unlimited:\
:memorylocked=64K:\
:memoryuse=unlimited:\
:filesize=unlimited:\
:coredumpsize=unlimited:\
:openfiles=unlimited:\
:maxproc=unlimited:\
:sbsize=unlimited:\
:vmemoryuse=unlimited:\
:swapuse=unlimited:\
:pseudoterminals=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

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

Step to add a new user – 2, 3, 4

❑ Initialize password

- passwd lctseng

❑ Set quota

- edquota lctseng
- edquota -p csquota lctseng

Quotas for user lctseng:

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

- Ref: <https://www.freebsd.org/doc/handbook/quotas.html>
- Soft v.s hard limit

❑ Home directory

- mkdir /home/lctseng

```
[pschiu@bsd1 ~]#quota pschiu
Disk quotas for user pschiu (uid 13222):
Filesystem      usage    quota   limit   grace  files   quota   limit   grace
/net/gcs        137032  400000  420000         3324   40000  42000
/net/mail         12    100000  120000          1         2       3
[pschiu@bsd1 ~]#
```

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

- 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 lctseng:cs /home/lctseng`

Step to add a new user - adduser

❑ adduser

```
6:15pm lctseng@nctucs [~]
[W2] > sudo adduser
Password:
Username: Hi
Full name: yo
Uid (Leave empty for default):
Login group [Hi]:
Login group is Hi. Invite Hi into other groups? []: wheel
Login class [default]:
Shell (sh csh tcsh bash rbash git-shell nologin) [sh]: tcsh
Home directory [/home/Hi]:
Home directory permissions (Leave empty for default):
Use password-based authentication? [yes]:
Use an empty password? (yes/no) [no]:
Use a random password? (yes/no) [no]:
Enter password:
Enter password again:
Lock out the account after creation? [no]: |
```

❑ adduser

/etc/adduser.conf

- defaultLgroup
- defaultclass
- defaultgroups
- passwdtype
- homeprefix=/home/users/
- defaultshell
- udotdir
- msgfile
- disableflag
- upwexpire
- uexpire
- ugecos
- uidstart

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 lctseng-home-20151001.tar.bz /home/lctseng
- tar -jcf lctseng-mail-20151001.tar.bz /var/mail/lctseng
- chmod 600 lctseng-*-20151001.tar.bz

Delete home directory

- rm -rf /home/lctseng
- rm -f /var/mail/lctseng (mailbox file)

Disabling login

❑ Ways to disable login

- Change user's login shell as `/usr/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)`

FreeBSD user account related files

- /etc/master.passwd
- /etc/passwd
- /etc/pw.XXXXXXX~
- /etc/pwd.db
- /etc/spwd.db
- /etc/group
- /etc/shell
- /etc/login.conf

/etc/passwd.db /etc/spwd.db

- ❑ check master.passwd for format
 - # pwd_mkdb -C /etc/master.passwd
- ❑ create and install /etc/passwd from the master.passwd file
 - # pwd_mkdb -p /etc/master.passwd
- ❑ generate the password databases
 - # pwd_mkdb /etc/master.passwd
 - # pwd_mkdb

pw

- usage: pw [user|group|lock|unlock] [add|del|mod|show|next] [help|switches/values]
- pw groupadd
- pw groupdel
- pw groupmod
- pw useradd
- pw userdel
- pw usermod
- pw groupnext
- pw usernext
- pw lock
- pw unlock
- pw groupshow
- pw usershow



Rootly Powers

The Root

- ❑ Root
 - Root is God, also called super-user.
 - UID is 0

- ❑ UNIX permits the superuser 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 (ttyv, Alt+F1~F6)
 - 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 !!!**
- Log: /var/log/auth.log



sudo

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. (all environment variables changed)
- ❑ 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 (/var/log/auth.log)

```
Sep 20 02:10:08 NASA sudo: lctseng : 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**
 - **Syntax check**
 - **Change editor: setenv EDITOR <editor you want>**

Becoming root (3)

- sudoers format
 - **Who** can execute **what command** on **which host** as **whom**
 - The user (group) 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
 - Alias: create another name for groups of commands/hosts/users/run-as

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)

Important!

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
yench	ALL=ALL
lctseng	ALL=(ALL)ALL,!SHELL,!SU
printTA	csduty=PRINT
wwwTA	BSD=(NOBODY)/usr/bin/more
%wheel	ALL=NOPASSWD:/sbin/shutdown

Becoming root (5)

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

- ❑ Someone cannot use /bin/sh, /bin/tcsh, /bin/csh !!
- ❑ But...there still some ways can make it
 - vim/more/less commands have “shell escape”
 - Execute shell commands within these editors/pagers
 - sudo vim -> shell escape -> execute **ROOT SHELL!!**

```

16
17 ##
18 ## User alias specification
19 ##
20 ## Groups of users. These may consist of user names, uids, Unix groups,
21 ## or netgroups.
22 # User_Alias    ADMINS = millert, dowdy, mikef
/usr/local/etc/sudoers[唯讀]    [unix/SUDOERS]    nctucs.tw:/usr/home/lctseng
:!tcsh
11:01 root@nctucs [/usr/home/lctseng] >

```

Becoming root (6)

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

- ❑ Someone cannot use /bin/sh, /bin/tcsh, /bin/csh !!
- ❑ But...there still some ways can make it
 - Shell is a program, and sudoers needs to specify absolute path
 - Copy that program and executes it somewhere else
 - **ROOT SHELL!!**

```

11:02am lctseng@nctucs [~]
[W2] > cp /bin/csh /tmp/csh ; sudo /tmp/csh
11:02 root@nctucs [/usr/home/lctseng] >
  
```

sudoers Example

- ❑ `lctseng ALL=(ALL) ALL`
- ❑ `%wheel ALL=(ALL) NOPASSWD: ALL`

```
76
77 ##
78 ## User privilege specification
79 ##
80 root ALL=(ALL) ALL
81 lctseng ALL=(ALL) ALL
82
83 ## Uncomment to allow members of group wheel to execute any command
84 # %wheel ALL=(ALL) ALL
85
86 ## Same thing without a password
87 | %wheel ALL=(ALL) NOPASSWD: ALL
88
89 ## Uncomment to allow members of group sudo to execute any command
90 # %sudo ALL=(ALL) ALL
91
```

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**

Sudo log

❑ /var/log/auth.log

```
[pschiu@tbsd21 ~]#sudo cat /var/log/auth.log | grep sudo
Oct 13 17:04:11 tbsd21 sudo:    pschiu : TTY=pts/0 ; PWD=/net/gcs/104/0456183 ; USER=root ; COMMAND=/bin/cat /var/log/auth.log
Oct 13 17:05:47 tbsd21 sudo:    pschiu : TTY=pts/0 ; PWD=/net/gcs/104/0456183 ; USER=root ; COMMAND=/bin/cat /var/log/auth.log
[pschiu@tbsd21 ~]#
```



Q&A



Unix-like Env. User

Unix-like

- AIX
- Solaris, OpenSolaris
- Linux
 - Debian
 - Redhat Enterprise , CentOS
 - Arch
- Mac

- HP-UX