Account Management

Computer System and Network Administration

Department of Computer Science & Information Engineering
National Cheng Kung University
2016 Fall

Duties on Account Management

- The system administrator adds accounts for new users, removes the accounts of users that are no longer active, and handles all the account-related issues that come up in between (e.g., forgotten passwords).
- The process of adding and removing users can be automated, but certain administrative decisions (where to put a user's home directory, which machines to create the account on, etc.) must still be made before a new user can be added.

Duties on Account Management (cont.)

- When a user should no longer have access to the system, the user’ s account must be disabled.
- All the files owned by the account should be backed up and then disposed of so that the system does not accumulate unwanted baggage over time.

ID

- User ID, Group ID
  - % **id** tsaimh
    - uid=1002(tsaimh) gid=1001(imslab) groups=1001(imslab),1002(advisor)
  - % **id** 1002
    - uid=1002(tsaimh) gid=1001(imslab) groups=1001(imslab),1002(advisor)
- 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 tsaimh
3. Set quota
   > edquota tsaimh
4. Create user home directory
   > mkdir /home/tsaimh
5. Copy startup files to user's home (optional)
6. Set the file/directory owner to the user
   > chown –R tsaimh:imslab /home/tsaimh

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 ":"

```
$ grep tsaimh /etc/passwd
tsaimh:*:1001:116:User &:/home/tsaimh:/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)

```
$ grep tsaimh /etc/passwd
tsaimh:*:1001:116:User &:/home/tsaimh:/bin/tcsh
```

/etc/passwd (BSD)

```
$ sudo grep tsaimh /etc/master.passwd
tsaimh:$1$4KQcUPbi$/nVs5bPDUXoyLLxz9Yp9D.:1001:116::0:0:User &:/home/tsaimh:/bin/tcsh
```

/etc/master.passwd

```
$ grep tsaimh /etc/passwd
tsaimh:x:1001:116:User &:/home/tsaimh:/bin/tcsh
```

/etc/passwd (Linux)

```
$ sudo grep tsaimh /etc/shadow
tsaimh:$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"
  - 1xbFdBaRp$zXSp9e4y32ho0MB9Cu2iV0
- blf
  - Plaintext: arbitrary length
  - Cipher: 60 characters long started with "$2a$"
  - $2a$04$jn9vc7dDJOX7V335o3.RoujuK/uoBYDg1xZs1OcBOrIXve3d1Cbm6
- login.conf(5), "AUTHENTICATION"
  - section: passwd_format

tsaimh:*:1001:116:User &:/home/tsaimh:/bin/tcsh

Step to add a new user – 1. password and group file (4)

- GECOS
  - **G**eneral **E**lectric **C**omprehensive **O**perating **S**ystem
  - Commonly used to record personal information
  - “,” separated
  - “finger” command will use it
  - Use “chfn” to change your GECOS

```
#Changing user information for tsaimh.
Shell: /bin/tcsh
Full Name: Meng-Hsun Tsai
Office Location: Room 65B01 New CSIE Building
Office Phone: 62518
Home Phone:
Other information:
```

Step to add a new user – 1. password and group file (5)

tsaimh:*:1001:116:User &:/home/tsaimh:/bin/tcsh

- 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 tsaimh.
Shell: /bin/tcsh
Full Name: Meng-Hsun Tsai
Office Location: Room 65B01 New CSIE Building
Office Phone: 62518
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,tsaimh
daemon:*:1:daemon
staff:*:20:
```

- Only in wheel group can do "su root" 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

```
$ sudo grep tsaimh /etc/master.passwd
tsaimh:$1$4KQcUPbi$/nVs5bPDUXoyLLxw9Yp9D.:1001:116::0:0:User &:/home/tsaimh:/bin/tcsh
```

```
$ grep tsaimh passwd
tsaimh:*:1001:116:User &:/home/tsaimh:/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

```
$ sudo grep tsaimh /etc/passwd
tsaimh:$1$4KQcUPbi$/nVs5bPDUXoyLLxw9Yp9D.:14529:0:99999:7:::
```

Step to add a new user – 2, 3, 4

- Initialize password
  - passwd tsaimh
- Set quota
  - edquota tsaimh

```
Quotas for user tsaimh:
/home: kbytes in use: 705996, limits (soft = 4000000, hard = 4200000)
        inodes in use: 9728, limits (soft = 50000, hard = 60000)
```

- Home directory
  - mkdir /home/tsaimh

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.*
- Change onwer
  - chown –R tsaimh:imslab /home/tsaimh

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 tsaimh-home-20121018.tar.bz /home/tsaimh
  - tar jcf tsaimh-mail-20121018.tar.bz /var/mail/tsaimh
  - chmod 600 tsaimh-*-20121018.tar.bz
- Delete home directory and mailbox
  - rm –rf /home/tsaimh /var/mail/tsaimh

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 excrypted password field
    - pw lock/unlock

- See the following man pages for more information:

  pw(8)、adduser(8)、pwd_mkdb(8)

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 *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

```
Oct 16 22:02:48 meng sudo:   tsaimh : TTY=pts/0 ; PWD=/home/tsaimh ;
                             USER=root ; COMMAND=/bin/ls
```

  - 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 the command is executed**
  - Use absolute path

```
tsaimh          bsd1=(root) /sbin/shutdown
```

Becoming root (4)

```
Host_Alias      BSD=bsd1,bsd2

Cmnd_Alias      SHELLS=/bin/sh, /bin/tcsh, /bin/csh
Cmnd_Alias      SU=/usr/bin/su

User_Alias      wwwSA=hungwei, dsuper

Runas_Alias     WEBADM=webadm

tsaimh          ALL=(ALL) ALL
hungwei         ALL=ALL,!SHELLS,!SU
wwwSA           BSD=(WEBADM)ALL
```

% sudo –u webadmin vi /usr/local/etc/apache/httpd.conf

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.
- A single file can be used to control access for an entire network.