



第 14 章

使用者與群組管理

無
礙
隊
友

Linux

第 14 章 使用者與群組管理

14-1 在 Linux 上的使用者與群組

使用者和群組形成接觸 Linux 的系統安全。每一個系統的使用者都有他自己的帳號、目錄、密碼和預設的群組。在 multiuser 多人同時使用的作業系統中，建立帳號讓我們可以分辨不同的使用者。如果沒有帳號，系統將很難分辨哪個檔案屬於哪一個使用者，或者哪個使用者可以使用哪個資源。在 Linux 上我們使用使用者的 ID 或 UID 來分辨他們。UID 通常被核心來辨別是哪一個使用者。UID 是用數字編號來表達使用者，它讓我們在系統上很輕易的就可以辨別是哪一個使用者。而使用者帳號是儲存在 `/etc/passwd` 的檔案中。這個檔案由每一個使用者的 UID、使用者名稱、密碼、和群組 ID、目錄和預定的 shell 所組成。我們使用群組就可以很輕易的就分配或限制一群指定的帳號和設定群組的存取檔案權限。

使用者帳號的檔案 `/etc/passwd`

`/etc/passwd` 是使用者的資訊文字資料庫。它包含了每一個使用者進入作業系統時的帳號與資訊。每一個使用者都有下列的欄位。

<使用者名稱> : <密碼> : <UID> : <GID> : <全名> : <家目錄> : <預設 shell>

我們使用 `more /etc/passwd` 就可以看出 `/etc/passwd` 的內容。

```
[root@flash chaiyen]# more /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
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
```



```
ident:x:98:98:pident user:/:/sbin/nologin
radvd:x:75:75:radvd user:/:/bin/false
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
apache:x:48:48:Apache:/var/www:/bin/false
squid:x:23:23:/:/var/spool/squid:/dev/null
named:x:25:25:Named:/var/named:/bin/false
pcap:x:77:77:/:/var/arpwatch:/sbin/nologin
amanda:x:33:6:Amanda user:/var/lib/amanda:/bin/bash
junkbust:x:73:73:/:/etc/junkbuster:/bin/bash
mailman:x:41:41:GNU Mailing List Manager:/var/mailman:/bin/false
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash
ldap:x:55:55:LDAP User:/var/lib/ldap:/bin/false
postfix:x:89:89:/:/var/spool/postfix:/bin/true
pvm:x:24:24:/:/usr/share/pvm3:/bin/bash
chaiyen:x:500:500:/:/home/chaiyen:/bin/bash
justin:x:501:501:/:/home/justin:/bin/bash
ju:x:502:502:/:/home/ju:/bin/bash
```

我們可以發現 root 的使用者 UID 為 0，而其 GID 也為 0，root 超級使用者的目錄是在 /root，而 root 預設使用的 shell 為 /bin/bash。我們使用者 chaiyen 的使用者 UID 為 500 而 GID 也為 500，而 chaiyen 的目錄是在 /home/chaiyen，而使用者 chaiyen 預設的 shell 是 /bin/bash。

<使用者名稱> : <密碼> : <UID> : <GID> : <全名> : <家目錄> : <預設 shell>

- 使用者名稱：我們使用使用者名稱來登錄作業系統，而且我們可以藉由使用者名稱來辨別使用者的帳號。使用者名稱在命名時不可有空白，開頭使用字母或數字。
- 密碼：這個欄位包含了使用者的密碼加密。加密的密碼是由 passwd 指令所產生，而且不是放在 /etc/passwd 的檔案中。
- UID：每一個使用者在作業系統都有一個 UID，UID 是數字的使用者編號帳號，我們的系統核心就是使用使用者編號來辨別不同的使用者，在 Linux 中，使用者 chaiyen 的 UID 為 500，而唯一不變的超級使用者，他的使用者編號 UID 為 0。
- GID：每一個在系統的使用者都有屬於他的預設群組，而這檔案是在 /etc/group 中。我們使用在 /etc/passwd 的檔案來辨別 GID 使用者群組編號。
- 全名：我們可以給每一個使用者帳號全名。當我們使用 email 的時



後，會使用到使用者名稱和使用者全名。

- 家目錄：每一個帳號或使用者都有他自己的家目錄。在家目錄中，我們使用者可以建立或儲存檔案在這預設的位置。這樣也可以方便我們自己管理自的檔案和程式。
- 預設 shell：我們每一個使用者預設的 shell 是在/bin/bash。當我們登錄作業系統時，就會啟動我們預設的 shell，我們就可以在 shell 下達指令。Shell 一般是安裝在/etc/shells 的地方。在這欄位，我們需要提供執行 shell 的路徑。

14-1-1 選取使用者編號

每一個使用者都有他自己獨一無二的使用者編號。使用者編號是從 0 到 65535，而我們的使用者編號可以不用連號。一般而言，我們的使用者編號在 100 以內是分配給系統帳號，例如 0 號 UID 是 root、1 號 UIDadm 是 bin、2 號 UID 是 daemon、3 號 UID 是 adm.....。我們的 Linux 新增使用者是從使用者編號 500 開始。例如第一位使用者 chaiyen，他的使用者編號為 500，第二位使用者 justin，他的使用者編號為 501.....。

我們使用 `more /etc/passwd` 來觀看/etc/passwd 檔。我們可以看到第 0 號 UID 是 root、1 號 UIDadm 是 bin、2 號 UID 是 daemon。

```
[root@flash Net_SSLeay.pm-1.15]# more /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
adm:x:3:4:adm:/var/adm:/sbin/nologin
```

我們的 Linux 新增使用者是從使用者編號 500 開始，例如第一位使用者 chaiyen，他的使用者編號為 500，第二位使用者 justin，他的使用者編號為 501。

```
chaiyen:x:500:500:~/home/chaiyen:/bin/bash
justin:x:501:501:~/home/justin:/bin/bash
ju:x:502:502:~/home/ju:/bin/bash
```

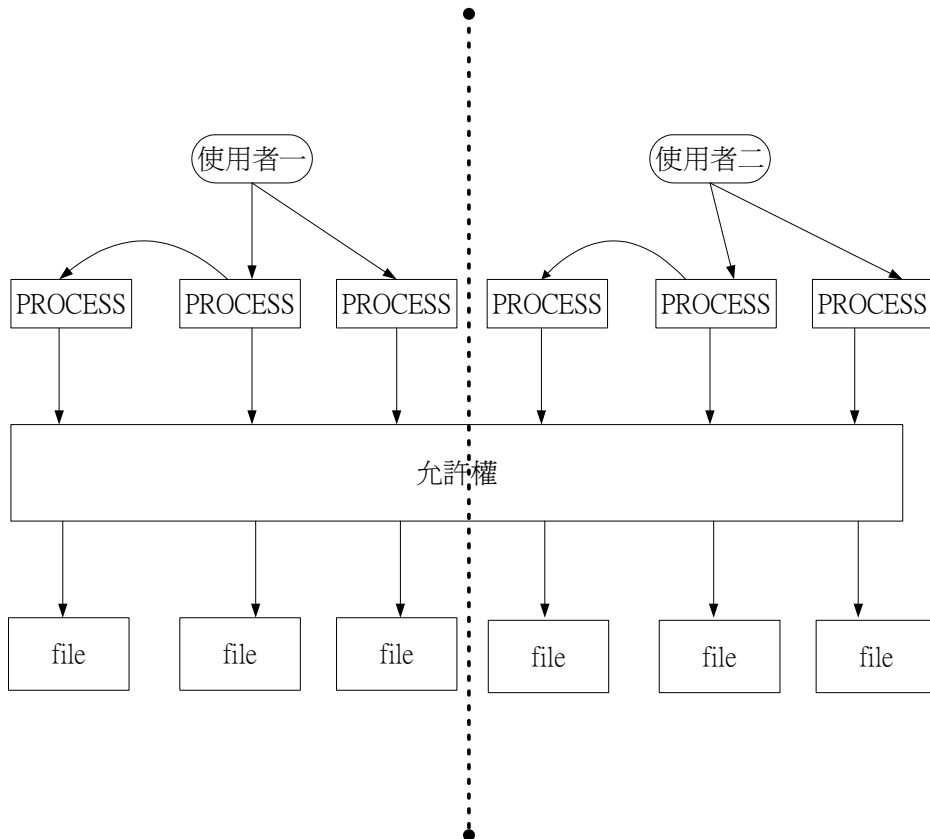


14-1-2 家目錄

我們將我們使用者的目錄建立在/home 的目錄下，讓我們每一個使用者都有他自己的家目錄，一般是在/home/使用者。在我們的/home 目錄下，有我們的使用者目錄chaiyen、justin 和 ju。

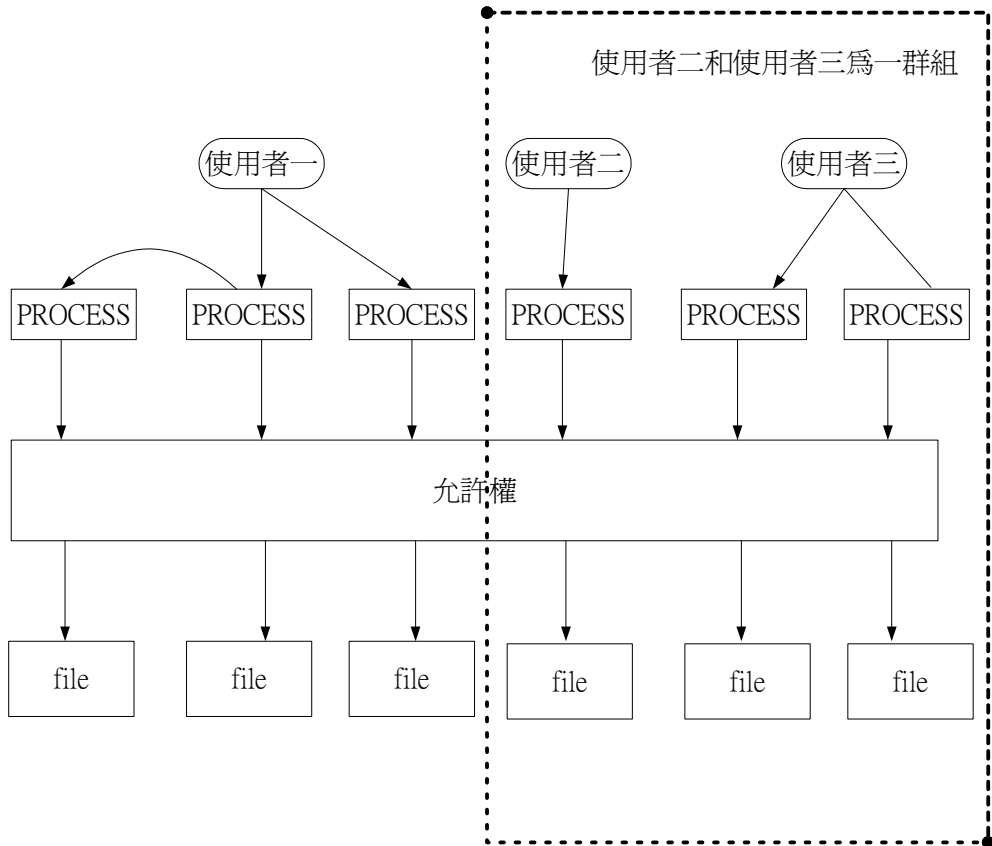
```
[root@flash home]# ls  
chaiyen  cvsroot  ju  justin  projects
```

我們每一個使用者，他們有他們自己的行程，還有他們自己所允許存取的檔案。



14-1-3 /etc/group 檔

/etc/group 檔定義 Linux 系統上的使用者群組。使用群組名稱可以將數個類似的使用者群組在一起，方便我們使用群體的運作。在圖中我們將使用者二和使用者三組成在一個群組。我們可以使用超級使用者來讓組群組。我們可以讓某些檔案屬於某一個群組，就可以不用一個個的來設定每個使用者他們存取這些檔案的權限。



<群組名稱> : <密碼> : <GID> : <使用者串列>

我們使用 `more /etc/group` 就可以觀看系統上的使用者群組。

```
[root@flash home]# more /etc/group
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
tty:x:5:
disk:x:6:root

chaiyen:x:500:
justin:x:501:
ju:x:502:
```

<群組名稱> : <密碼> : <GID> : <使用者串列>

- 群組名稱：使用群組名稱讓我們可以辨別群組名稱。群組名稱在命名時不可有空白，開頭使用字母或數字。
- 密碼：這個欄位包含了使用者群組的密碼。一般群組是不用密碼的。
- GID：GID 為群組的群組編號，它可以讓系統核心來辨別群組，因此每一個群組都有它自己的 GID。
- 使用者串列：使用者串列為組成群組的每一個使用者。

GID 的編號從 0 到 65534，每一個群組都有它自己的 GID。我們為不同的每個使用者設定不同 UID，而他們也會有他們預設的 GID。例如使用者 `chaiyen` 他的 UID 為 500，而 `chaiyen` 的 GID 也是 500。這個機制讓每一個使用者都有他自己的 UID 和 GID。



14-2 建立使用者

建立使用者的工作一般是由超級使用者 root 來負責。一般使用者是沒有權限來建立新的使用者。

建立使用者的帳號有選取使用者的 UID、選取使用者的群組、在/etc/passwd 建立登錄、設定使用者的密碼、建立使用者的家目錄/home/使用者。這些過程，我們可以在 shell 上下達 adduser 指令或 useradd 指令就可以執行了。

我們使用 useradd 指令新增使用者 goodman。

```
root@flash:~ - Shell - Konsole
工作階段 編輯 檢視 設定 說明
[root@flash root]# useradd goodman
```

我們使用 adduser 指令新增使用者 juju。

```
root@flash:~ - Shell - Konsole
工作階段 編輯 檢視 設定 說明
[root@flash root]# adduser juju
```

當我們新增使用者時會和下列目錄有關。

目錄	說明
/home	當建立使用者時，會建立/home 的子目錄為使用者的家目錄。
/etc/skel	放置登錄 shell 時所初始化的檔案，包含.bash_profile、.bashrc、和 bash_logout。還有一些檔案，例如 KDE 的視窗 .kde 檔案、Gnome 的 Desktop 檔案。
/etc/shells	放置 shell 的地方，如 BASH、TCSH
/etc/passwd	放置使用者資料的地方。
/etc/group	放置群組資料的地方。
/etc/shadow	密碼加密的檔案。
/etc/gshadow	群組密碼加密的檔案。
/etc/login.defs	使用者預設登錄的定義。

這是 skel 目錄下的檔案。

```
/etc/skel  
/etc/skel/.kde  
/etc/skel/.kde/Autostart  
/etc/skel/.kde/Autostart/Autorun.desktop  
/etc/skel/.kde/Autostart/.directory  
/etc/skel/.gtkrc  
/etc/skel/.bash_logout  
/etc/skel/.bash_profile  
/etc/skel/.bashrc  
/etc/skel/.emacs
```

14-2-1 使用系統工具建立使用者

Linux 提供我們 `useradd` 指令來新增使用者。

語法：

指令：`useradd` 參數

參數：

- c <備註>：將備註文字加入 `passwd` 的備註欄位中。
- d <登入目錄>：指定使用者登入時的開始目錄。
- e <有效期限>：指定帳戶的有效期限。
- f <緩衝天數>：指定在密碼過期後多久就關閉該帳戶。
- g <群組>：指定使用者所屬的群組。
- G <群組>：指定使用者所屬的附加群組。
- m：自動建立使用者的目錄。
- M：不自動建立使用者的目錄。
- n：不建立以使用者名稱為名的群組。
- r：建立系統帳號。
- s <shell>：指定使用者登入後使用的 shell。
- u <uid>：指定使用者 ID。



我們使用 `useradd -D` 來顯示系統帳號的預設值。

```
root@flash:~ - Shell No 3 - Konsole
工作階段 編輯 檢視 設定 說明
[root@flash root]# useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
[root@flash root]#
```

我們使用 `useradd justinwu` 來增加使用者 `justin`。

```
root@flash:/home - Shell - Konsole
工作階段 編輯 檢視 設定 說明
[root@flash home]# useradd .justinwu
[root@flash home]#
```

我們使用 `useradd -u 1201 -g chaiyen -d /home/goodgirl goodgirl` 來建立 `goodgirl` 使用者，我們在建立 `goodgirl` 使用者同時，我們設定 `goodgirl` 的使用者 UID 為 1201 設定 `goodgirl` 是屬於 `chaiyen` 群組 設定 `goodgirl` 的家目錄是 `/home/goodgirl`。

```
root@flash/bin - Shell - Konsole
工作階段 編輯 檢視 設定 說明
[root@flash bin]# useradd -u 1201 -g chaiyen -d /home/goodgirl goodgirl
```

我們使用 `vi` 來編輯 `/etc/passwd` 的檔案。

```
root@flash/bin - Shell - Konsole
工作階段 編輯 檢視 設定 說明
postfix:x:89:89::/var/spool/postfix:/bin/true
pvm:x:24:24::/usr/share/pvm3:/bin/bash
chaiyen:x:500:500::/home/chaiyen:/bin/bash
justin:x:501:501::/home/justin:/bin/bash
ju:x:502:502::/home/ju:/bin/bash
juju:x:504:504::/home/juju:/bin/bash
nana:x:505:505::/home/nana:/bin/bash
goddess:x:506:506::/home/goddess:/bin/bash
ii:x:510:510::/home/ii:/bin/bash
juj:x:511:511::/home/juj:/bin/bash
big:x:520:520::/home/big:/bin/bash
big5:x:525:525::/home/big5:/bin/bash
justinwu:x:526:526::/home/justinwu:/bin/bash
wu:x:527:527::/home/justinwu:/bin/bash
goodboy:x:1200:500::/home/goodboy:/bin/bash
goodgirl:x:1201:500::/home/goodgirl:/bin/bash
-- INSERT --
56,46 Bot
```

我們可以使用 `useradd -D` 來改變當我們使用 `useradd` 指令時的動作。我們使用 `useradd -D -b /home/chaiyen -s /bin/tcsh` 來設定當我們使用 `useradd` 指令新增使用者時會設定使用者的目錄是從 `/home/chaiyen` 目錄開始，並且設定使用者的 shell 是 `/bin/tcsh`。

```
[root@flash bin]# useradd -D -b /home/chaiyen -s /bin/tcsh
```

我們使用 `useradd -D` 來顯示系統帳號的預設值。

```
[root@flash bin]# useradd -D
GROUP=100
HOME=/home/chaiyen
INACTIVE=-1
EXPIRE=
SHELL=/bin/tcsh
SKEL=/etc/skel
```

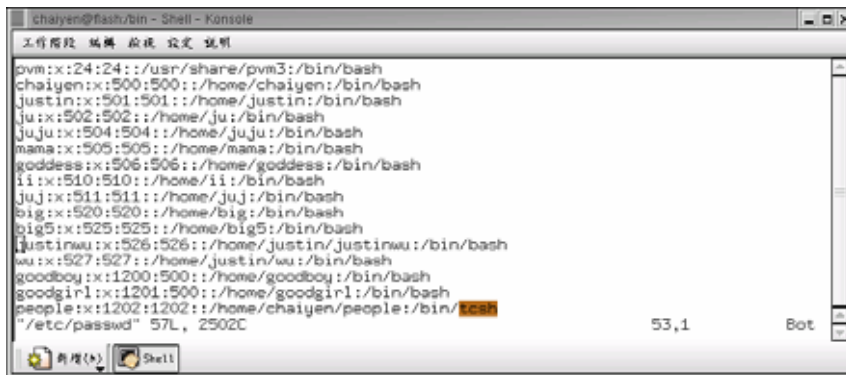
我們新增使用者 `people`。

```
[root@flash bin]# useradd people
```

我們使用 `vi /etc/passwd` 來編輯使用者資訊。

```
[root@flash bin]# vi /etc/passwd
```

我們可以看到 `people` 的家目錄是 `/home/chaiyen/people` 而其預設的 shell 是 `/bin/tcsh`。



```
chaiyen@flash/bin - Shell - Konsole
工作階段 編輯 前後 設定 說明
pvm:x:24:24::/usr/share/pvm3:/bin/bash
chaiyen:x:500:500::/home/chaiyen:/bin/bash
justin:x:501:501::/home/justin:/bin/bash
ju:x:502:502::/home/ju:/bin/bash
juju:x:504:504::/home/juju:/bin/bash
mama:x:505:505::/home/mama:/bin/bash
goddess:x:506:506::/home/goddess:/bin/bash
ii:x:510:510::/home/ii:/bin/bash
juj:x:511:511::/home/juj:/bin/bash
big:x:520:520::/home/big:/bin/bash
big5:x:525:525::/home/big5:/bin/bash
justinwu:x:526:526::/home/justin/justinwu:/bin/bash
wu:x:527:527::/home/justin/wu:/bin/bash
goodboy:x:1200:500::/home/goodboy:/bin/bash
goodgirl:x:1201:500::/home/goodgirl:/bin/bash
people:x:1202:1202::/home/chaiyen/people:/bin/tcsh
"/etc/passwd" 57L, 2502C
53,1 Bot
```



我們可以使用 `useradd -D` 來改變當我們使用 `useradd` 指令時的動作。

語法：

指令：`useradd -D 參數`

參數：

- b <目錄>：使用指定的目錄當作家目錄的所在位置。
- g <群組名稱或 GID>：使用指定的群組當作預設的群組。
- s <shell>：使用指定的 shell 當作是預設的 shell。

14-2-2 改變使用者的名稱

我們可以改變使用者名稱。我們可以編輯 `/etc/passwd` 的檔案和 `/etc/shadow` 的檔案來更改使用者的名稱。

這是 `goodgirl` 的目錄，我們要將 `goodgirl` 的名稱改為 `badgirl`。

```
drwx----- 3 goodgirl chaiyen 4096 8月 21 11:05 goodgirl
```

我們使用 `vi /etc/passwd` 來編輯。

```
[root@flash bin]# vi /etc/passwd
```

我們將使用者 `goodgirl` 改成 `badgirl`。

```
goodgirl:x:1201:500:~/home/badgirl:/bin/bash
```

```
badgirl:x:1201:500:~/home/goodgirl:/bin/bash
```

當我們使用 `ls-l` 來觀看 `goodgirl` 目錄時使用者 `goodgirl` 就變成使用者 `badgirl`。

```
drwx----- 3 goodgirl chaiyen 4096 8月 21 11:05 goodgirl
```

```
drwx----- 3 badgirl chaiyen 4096 8月 21 11:05 goodgirl
```

我們然後使用 `mv /home/goodgirl /home/badgirl` 將 `goodgirl` 目錄改成 `badgirl`。

```
[root@flash home]# mv /home/goodgirl /home/badgirl
```

這時就可以更改目錄的名稱。



```
[root@flash home]# ls
badgirl  chaiyen  goddess  goodman  ju  juju  projects  wuchaiyen
big      cvsroot  goodboy  ii        juj  justin  wu
```

我們最後修改/etc/shadow 檔案，將 goodgirl 改成 badgirl。這樣使用者名稱就修改好了。

```
[root@flash chaiyen]# vi /etc/shadow
goodgirl:!!!:11920:0:99999:7:::
badgirl:!!!:11920:0:99999:7:::
```

14-2-3 改變使用者的密碼

只有超級使用者 root 可以改變使用者的密碼。我們可以使用 passwd 指令來修改。我們在修改使用者密碼時可以不用知到被修改使用者的密碼。

語法

指令：passwd 參數 使用者

參數：

- d：刪除密碼。
- f：以亂數產生密碼以強制解開鎖定的帳戶，和-u 參數一起使用。
- l：鎖定帳戶。
- S：顯示密碼相關資訊。
- u：解除帳戶鎖定。

我們使用 passwd badgirl 來修改或新增使用者 badgirl 的密碼。我們需輸入兩次密碼來作確認。

```
[root@flash chaiyen]# passwd badgirl
Changing password for user badgirl.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```



我們使用 `passwd -l badgirl` 來將使用者 `badgirl` 的帳號鎖定。

```
[root@flash chaiyen]# passwd -l badgirl
Locking password for user badgirl.
passwd: Success
```

我們使用 `passwd -u badgirl` 來解開 `badgirl` 的帳號。

```
[root@flash chaiyen]# passwd -u badgirl
Unlocking password for user badgirl.
passwd: Success.
```

我們使用 `passwd -d badgirl` 就可以將使用者 `badgirl` 的密碼刪除。

```
[root@flash chaiyen]# passwd -d badgirl
Removing password for user badgirl.
passwd: Success
```

我們使用 `passwd -S badgirl` 來了解密碼加密的資訊。

```
[root@flash chaiyen]# passwd -S badgirl
Password set, MD5 crypt.
```

14-2-4 改變使用者的家目錄

我們將之前的家目錄搬到現在的家目錄，我們可以使用 `mv` 指令。

語法

指令：`mv 參數 來源檔案或目標 目的檔案或目標`

參數：

-b：若需覆寫檔案時，則先覆寫先前檔案。

-f：若目前的檔案或目錄與目前的檔案或目錄重複則直接覆寫現有的檔案或目



錄。

-i : 覆寫先前詢問使用者。

-u : 移動或更改檔名時，若目的地檔已存在且檔案日期比來源檔案新，則不覆寫目的地檔。

-v : 執行時顯示詳細的資訊。

-V <備份方式> : 指定備分的方式有 simple、numbered 或 existing。

--help : 顯示線上說明。

--version : 顯示版本資訊。

我們要將/home 目錄下的 goodman 目錄改成 badman。

```
[root@flash home]# ls
badgirl  chaiyen  goddess  goodman  ju  juju  projects  wuchaiyen
big      cvsroot  goodboy  ii       juj  justin  wu
```

我們使用 mv /home/goodman /home/badman 來改變目錄的名稱。

```
[root@flash home]# mv /home/goodman /home/badman
```

這時我們就可以看到 goodman 目錄已經名稱改為 badman 了。

```
[root@flash home]# ls
badgirl  big      cvsroot  goodboy  ju  juju  projects  wuchaiyen
badman   chaiyen  goddess  ii       juj  justin  wu
```

14-2-5 改變使用者的 shell

我們可以使用 chsh 指令來更改使用者所使用的 shell。我們可以在 shell 上執行各式的指令，每一種 shell 它的所有功能和所能作的事都不是一樣的。

我們使用 chsh 來改變使用者的 shell，我們然後輸入 tcsh，這樣使用者所使用的 shell 就會改成 tcsh。

```
[root@flash home]# chsh
Changing shell for root.
New shell [/bin/bash]: /bin/tcsh
Shell changed.
```



在/etc/shells 下有許多的 shell,可以供我們選擇。Sh 是最原始的 shell。csh tcsh zsh 是 C shell 由 Berkeley UNIX 的 Bill Joy 所建立,也是 bash 之後最多人使用的 shell。bash 為 Bourne Again Shell,是我們預設的 Shell,其原始碼是公開的。

```
[root@flash home]# more /etc/shells
/bin/sh
/bin/bash
/sbin/nologin
/bin/bash2
/bin/ash
/bin/bsh
/bin/tcsh
/bin/csh
/bin/ksh
/bin/zsh
```

我們可以使用 chsh 指令來變更我們使用的 Shell。我們在登入系統時,作業系統會自動幫我們設定好 shell。我們可以使用 chsh 指令來更改 shell 環境。

語法

指令 : chsh 參數

參數 :

- s <shell 名稱> : 更改使用者的 shell。
- l : 顯示目前系統可使用的 shell。
- u : 顯示線上說明。
- v : 顯示版本的資訊。

我們使用 chsh -l 顯示系統可以使用的 shell。

```
[root@flash home]# chsh -l
/bin/sh
/bin/bash
/sbin/nologin
/bin/bash2
/bin/ash
/bin/bsh
/bin/tcsh
/bin/csh
/bin/ksh
/bin/zsh
```



我們使用 `chsh -s /bin/zsh` 來更改使用者目前的 shell。

```
[root@flash home]# chsh -s /bin/zsh
Changing shell for root.
Shell changed.
```

14-3 刪除使用者或消去使用者資格

假如我們要將一些使用者刪除，讓它不能登入使用我們作業系統的資源，我們就要刪除使用者。當我們要降低使用者使用我們電腦的時間、CPU 的使用率、硬碟空間，則我們就要限制使用者使用這些資源的權力。或者當使用者違反我們的規定時，我們要降低授給他使用電腦的權力。

我們可以使用 `userdel` 指令來刪除使用者帳號。

語法

指令：`userdel 參數 使用者`

參數：

`-r`：刪除使用者及其所登入的目錄。

這是還未刪除使用者 `ii` 前的目錄。

```
[root@flash home]# ls
badgirl  big      cvsroot  goodboy  ju  juju  projects  wuc
badman  chaiken goddess  ii      juj  justin  wu
```

我們使用 `userdel -r ii` 來刪除 `ii` 這個使用者，及刪除其目錄。

```
[root@flash home]# userdel -r ii
```

這是 `ii` 目錄也同時被刪除了。

```
[root@flash home]# ls
badgirl  big      cvsroot  goodboy  juj  justin  wu
badman  chaiken goddess  ju      juju  projects  wuchaiken
```

我們也可以使用 `userdel wu` 來刪除使用者 `wu`。

```
[root@flash home]# userdel wu
```



當我們要修改使用者帳戶時可以使用 `usermod` 指令。

語法

指令：`usermod` 參數

參數

- c <說明>：修改使用者帳戶的說明文字。
- d <登入目錄>：修改使用者登入時的目錄。
- e <有效期限>：修改使用者的有效期限。
- f <緩衝天數>：修改在密碼過期多久就關掉使用者帳戶。
- g <群組>：修改使用者所屬的群組。
- G <群組>：修改使用者所屬的附加群組。
- l <帳戶名稱>：修改使用者的帳戶名稱。
- s <shell>：修改使用者登入後使用的 shell。
- u <uid>：修改使用者的 UID。

14-4 密碼安全與 Shadow 密碼

我們 Linux 都是使用 MD5 來加密。由於 `passwd` 並不安全，因此 Linux 會有投影密碼的功能 `shadow` 檔案。

`/etc/passwd` 這個檔案可以給所有使用者讀取，而且包含了標準的 `passwd` 檔欄位。`/etc/shadow` 包含了使用者、密碼、每個帳號的密碼資訊，而且只有 `root` 超級使用者才可讀取。

`/etc/shadow` 包含下列的欄位。

<使用者名稱>：<密碼>：<最後改變時間>：<允許更動時間>：<允許更改所需的時間>：<警告>：<超過的時間>：<帳號的使用期限>：<保留>

- 使用者名稱：在 `/etc/passwd` 中使用者的名稱。
- 密碼：使用者加密的密碼。



- 最後修改時間：密碼最後被修改的時間，從 7/1/1970 開始的天數。
- 允許更動時間：使用者允許修改的密碼更動的時間。當允許使用者可以隨時修改，則設定為-1。
- 允許更改所需的時間：使用者在改變密碼後，下次更改密碼所需的時間。如果我們設定 99999 則可永久不用更改。
- 警告：密碼必需更動前多少天就開始警告使用者。
- 超過的時間：超過密碼必需變動日期後多少天，就停指該帳號的使用。
- 帳號的使用期限：從 7/1/1970 年開始這個帳號可使用的天數。
- 保留：這是 shadow 的保留欄位。

我們使用 vi 來編輯/etc/shadow 就可以看到 shadow 的格式。

```
[root@flash home]# vi /etc/shadow
junkbust:!!:11845:0:99999:7:::
mailman:!!:11845:0:99999:7:::
mysql:!!:11845:0:99999:7:::
netdump:!!:11845:0:99999:7:::
ldap:!!:11845:0:99999:7:::
postfix:!!:11845:0:99999:7:::
pvm:!!:11845:0:99999:7:::
chaiyen:$1$zwysmLzh$QL4lcx/1U8EzUw.FRlnsq1:11901:0:99999:7:::
justin:$1$CYpjEQnU$1DJwZ5X3rdrxpg98ybhJ1:11904:0:99999:7:::
juju:!!:11919:0:99999:7:::
mama:$1$wMAJR1HL$ssIQSq6nPrfWp3Di cUV8M/:11919::99999:::
goddess:$1$0IChNjNA$2uuLDi saR5dVtY0p0za0F/:11919::99999:::
juj:$1$70.8GQan$tftTWkvzvfysAMEclr9dP/:11919:0:99999:7:::
justinwu:!!:11920:0:99999:7:::
goodboy:!!:11920:0:99999:7:::
badgirl:$1$Ma/ZNYZ3$n1AUaQkXm.Q1g3BzUze5U1:11920:0:99999:7:::
```

14-5 群組管理

我們可以使用 shell 指令來管理我們的群組。在系統上管理群組的為/etc/group 檔案。在/etc/group 檔案中，每一行都是一個群組。

我們使用 more /etc/group 就可以觀看系統上的使用者群組。



```
[root@flash home]# more /etc/group
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
tty:x:5:
disk:x:6:root
chaiyen:x:500:
justin:x:501:
ju:x:502:
```

<群組名稱> : <密碼> : <GID> : <使用者串列>

- 群組名稱：使用群組名稱讓我們可以辨別群組名稱。群組名稱在命名時不可有空白，開頭使用字母或數字。
- 密碼：這個欄位包含了使用者群組的密碼。一般群組是不用密碼的。
- GID：GID 為群組的群組編號，它可以讓系統核心來辨別群組，因此每一個群組都有它自己的 GID。
- 使用者串列：使用者串列為組成群組的每一個使用者。

GID 的編號從 0 到 65534，每一個群組都有它自己的 GID。我們為不同的每個使用者設定不同 UID，而他們也會有他們預設的 GID。例如使用者 chaiyen 他的 UID 為 500，而 chaiyen 的 GID 也是 500。這個機制讓每一個使用者都有他自己的 UID 和 GID。



我們可以使用 `groupadd` 指令來建立群組。

語法：

指令：`group` 參數 群組名稱

參數：

- f：強制建立已存在的群組。
- g <群組識別碼>：設定新建立群組的識別碼。
- o：重複使用群組的識別碼。
- r：建立系統群組。

我們使用 `groupadd` 指令來新增 `engineers` 群組。

```
[root@aasir chaiyen]# groupadd engineers
```

我們可以使用 `groupdel` 來刪除群組。

語法：

指令：`groupdel` 群組名稱

我們使用 `groupdel` 指令來刪除 `engineers` 群組。

```
[root@aasir chaiyen]# groupdel engineers
```

我們可以使用 `groupmod` 來改變群組的識別碼或名稱。

語法：

指令：`groupmod` 參數 群組名稱

參數：

- g <群組識別碼>：設定群組識別碼。
- o：重複使用群組識別碼名稱。
- n <新群組名稱>：設定群組名稱。

我們使用 `groupmod` 指令設定群組 `engineers` 的識別碼為 550。



```
[root@aasir chaiyen]# groupmod -g 550 engineers
```

我們使用 `groupmod -n` 指令將 `engineers` 群組名稱改為群組名稱 `teachers`。

```
[root@aasir chaiyen]# groupmod -n teachers engineers
```

我們可以使用 `chgrp` 指令來變更檔案與目錄的所屬群組。

語法

指令：`chgrp` 參數 所屬群組

參數：

-c：僅回報異動的部份。

-f：不顯示錯的訊息。

-h：只對符號連結的檔案作修改，而不動到原始檔案。

-R：遞迴處理。

-v：顯示指令執行的過程。

--help：說明

--reference = <參考檔案或目錄>：將所指定檔案或目錄所屬群組設成和所屬目錄或參考的檔案的群組相同。

--version：顯示版本。

我們使用 `mkdir` 來建立 `/home/engineers` 目錄。

```
[root@aasir chaiyen]# mkdir /home/engineers
```

我們將 `/home/engineers` 目錄群組設為 `engineers`。

```
[root@aasir chaiyen]# chgrp engineers /home/engineers
```

我們設定 `/home/engineers` 的群組可以讀寫執行。

```
[root@aasir chaiyen]# chmod g+rwx /home/engineers
```



14-6 使用者磁碟空間

我們可以分配給使用者固定的磁碟的空間。當有很多使用者建立檔案時，他就使用了我們磁碟的空間，而我們的磁碟空間資源就會被逐漸使用光，因此我們可以建立磁碟的分配 quota 給指定的使用者，限制他們無限量的使用我們的磁碟資源。

我們可以使用 quotacheck 和 quotaon 指令來分配磁碟資源。

我們在新增使用者時會將家目錄設在/home 的目錄下，我們現在就是要限制每個使用者的使用空間。我們首先編輯/etc/fstab 這個檔案(當我們啟動系統時，就會以/etc/fstab 這個檔案來掛載各別的分割)。我們家目錄/home，就是一個分割點，這在我們安裝作業系統時，將硬碟分割成/home 的掛載點(mount)。我們使用 vi 來編輯。

```
root@flash:~ - Shell - Konsole
工作階段 編輯 檢視 設定 說明
[root@flash root]# vi /etc/fstab
```

我們在第三行設定我們的/home 掛載點的/home 目錄下有磁碟分配 quota，我們在標籤為/home 的地方的 default 後面輸入 usrquota,grpquota。在改完/etc/fstab 檔案後，我們要增加 quota.user 和 quota.group 檔給/home 這個分割區，讓我們可以藉由 aquota.user 和 aquota.group 來分配磁碟空間給使用者或群組使用。

這是修改/etc/fstab 前的檔案情況。我們可以按照我們在磁碟分割時的設定，以及使用者家目錄的設定來作修正。

```

LABEL=/                /                ext2    defaults    1 1
none                  /dev/pts         devpts  gid=5,mode=620 0 0
LABEL=/home           /home            ext2    defaults,usrquota,grpquota 1 2
none                  /proc            proc    defaults    0 0
none                  /dev/shm         tmpfs   defaults    0 0
LABEL=/usr            /usr             ext3    defaults    1 2
/dev/hda2             /swap            swap    defaults    0 0
/dev/cdrom            /mnt/cdrom       iso9660 noauto,owner,kudzu,ro 0 0
```

這是修改/etc/fstab 檔後的檔案情況。我們在標籤為/home 的地方的 default 後面輸入 usrquota,grpquota。

```
root@flash:~ - Shell - Konsole
工作階段 編輯 檢視 設定 說明
LABEL=/                /                ext2    defaults    1 1
none                  /dev/pts         devpts  gid=5,mode=620 0 0
LABEL=/home           /home            ext2    defaults,usrquota,grpquota 1 2
none                  /proc            proc    defaults    0 0
none                  /dev/shm         tmpfs   defaults    0 0
LABEL=/usr            /usr             ext3    defaults    1 2
/dev/hda2             /swap            swap    defaults    0 0
/dev/cdrom            /mnt/cdrom       iso9660 noauto,owner,kudzu,ro 0 0
```



我們可以使用 `quotacheck` 指令來建立我們的 `aquota.user` 及 `aquota.group` 的兩個檔案，並且檢查我們的系統。

```
[root@flash root]# quotacheck -agv
quotacheck: Scanning /dev/hda3 [/home] done
quotacheck: Checked 10 directories and 23 files
```

我們到 `/home` 目錄下就會發現 `aquota.group` 和 `aquota.user` 的檔案。

```
[root@flash home]# ls -l
total 40
-rw----- 1 root root 7168 8月 22 17:22 aquota.group
-rw----- 1 root root 7168 8月 22 17:20 aquota.user
```

我們可以使用 `edquota -u` 指令來設定使用者使用磁碟空間的限制與分配(使用 Disk quota 面版)。我們使用 `edquota -u chaiyen` 來設定使用者 `chaiyen` 的使用磁碟空間。

```
[root@flash root]# edquota -u chaiyen
```

`/dev/hda3` 是檔案系統掛載的裝置，我們的磁碟是分成許多區塊，每個區塊有許多的節點來連到其它的區塊(節點 `node` 是其它區塊的位置)。

`hard` 就是強制的限制，當超過 `hard` 就會被強制限制。`soft` 就是警告，當超過 `soft` 所設定的數量時，警告就會出現。第三欄位的 `soft` 和第四欄位的 `hard` 是表示目前的使用空間。預設的 `soft` 為 0，預設的 `hard` 為 0，這表示使用者 `chaiyen` 沒有受到磁碟空間的限制，可以無限使用磁碟空間。第五欄位是表示使用者 `chaiyen` 目前所使用的節點 `inodes` 數目為 10(有就是有 10 個檔案)。第六行的 `soft` 為設定節點的警告數量，第七行的 `hard` 是設定節點的數量限制。

```
Disk quotas for user chaiyen (uid 501):
Filesystem      blocks      soft      hard      inodes      soft      hard
/dev/hda3       40           0         0         10          0         0
```

我們將區塊警告設為 1000，將區塊限制設為 10000。這樣當 `chaiyen` 使用區塊到 1000 時，系統就會發出警告。

```
Disk quotas for user chaiyen (uid 501):
Filesystem      blocks      soft      hard      inodes      soft      hard
/dev/hda3       40        1000     10000     10          0         0
```

我們可以使用 `quota -u -v` 來顯示使用者磁碟的使用量。在第二欄位 `blocks` 區塊為 40 表示目前使用者 `chaiyen` 已經使用了 40 個區塊，*星號是表示警告已經使用超過警告的數量。在這裏 `quota(soft limit)` 是 10。




```
[root@flash home]# quota -u -v chaiyen
```

```
Disk quotas for user chaiyen (uid 501):
  Filesystem  blocks  quota  limit  grace  files  quota  limit  grace
  /dev/hda3   _ 40*   10    10000 00:01   10     0     0
```

我們可以使用 `quota -v` 指令查看 root 的磁碟分配情況。

```
Disk quotas for user root (uid 0):
  Filesystem  blocks  quota  limit  grace  files  quota  limit  grace
  /dev/hda3   12332   0      0      0      16     0      0
```

我們使用 `edquota -t` 就可以編輯每個檔案系統的軟時間期限。

```
[root@flash chaiyen]# edquota -t
```

第二欄位是當區段 Block 超過 soft 警告的時間七天，其多餘的區塊就會被清出。

```
Grace period before enforcing soft limits for users:
Time units may be: days, hours, minutes, or seconds
  Filesystem      Block grace period      Inode grace period
  /dev/hda3       7days                    7days
```

我們可以使用 `repquota -a` 指令觀看整個磁碟分配的情況。

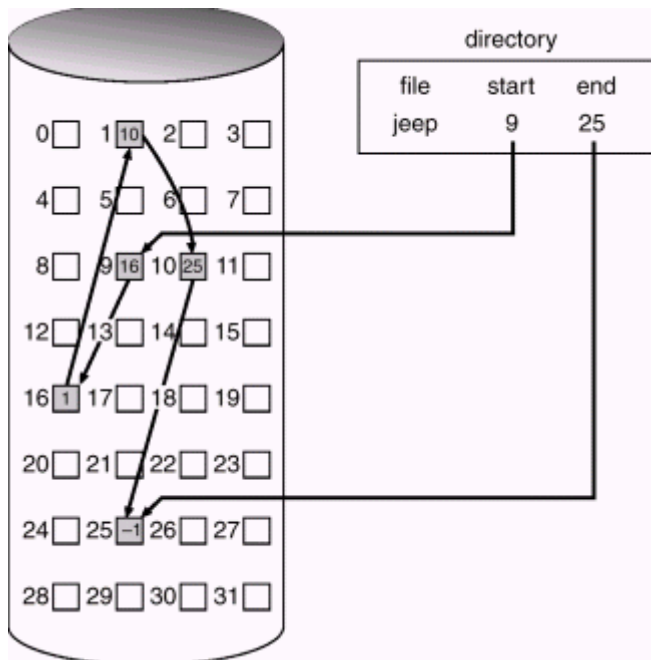
```
[root@flash chaiyen]# repquota -a
*** Report for user quotas on device /dev/hda3
Block grace time: 7days; Inode grace time: 7days
      Block limits            File limits
User    used  soft  hard  grace  used  soft  hard  grace
-----
root    --  12332   0    0      0      16    0    0
justin  --    40    0    0      0      10    0    0
chaiyen +-   40   10   30  none    10    0    0
```



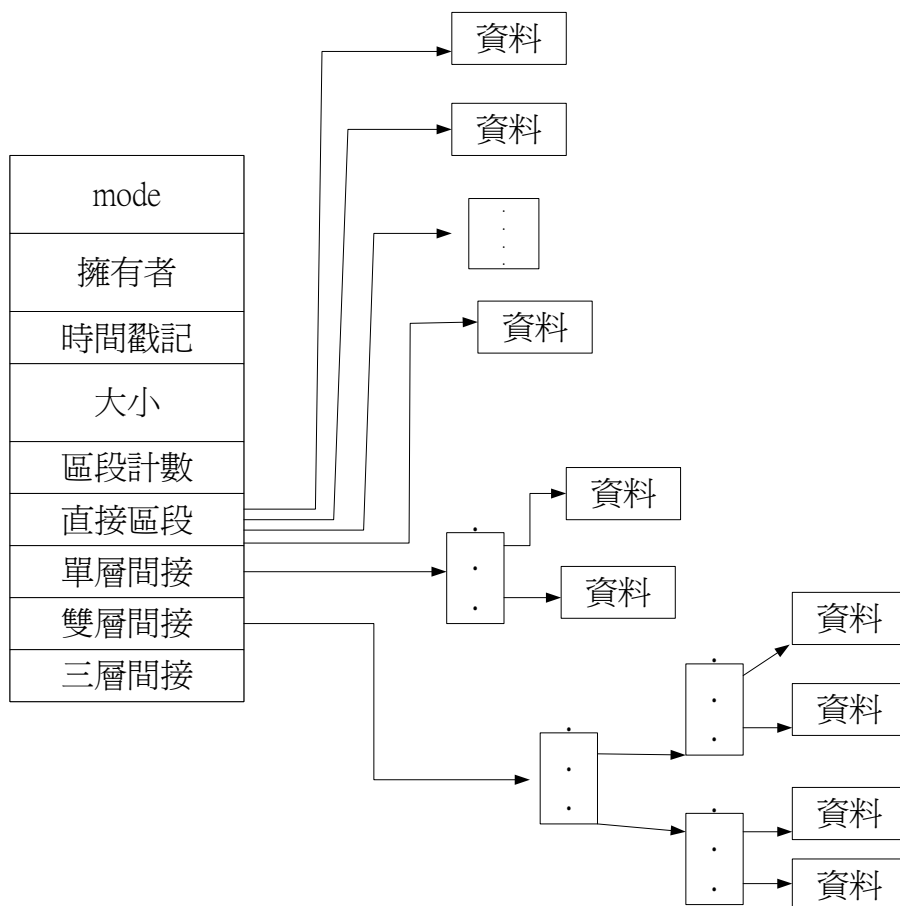
補充：

檔案概念

檔案是用鍊結的方式來表示，因為將硬碟分割成目錄和檔案，目錄標示著所有檔案的資訊，包括檔案的開始與結尾，在下圖中，檔案的開始是在 9 的地方，而結尾是在 25 的地方，結尾以負 1 來表示，而檔案中包含了下一個檔案的位址指標。



這是 Unix 也是 Linux 的檔案格式 inode，inode 裏面包含了擁有者、使用者可以存取的人的權限、也有時間戳記，裏面包含了何時這個檔案被修改；也包含了檔案的大小。每一個檔案的區段大小為 4k，在 Linux 中系統的方式為保存裝置目錄中的前 15 個索引區段指標，而指標的前 12 個指向直接區段，因此只要檔案小於 48k 的，就可以直接存取，速度較快；而單層間接及雙層間接和三層間接的第一個指向結點，裏面的內容是下一層的位址，這樣可以讓我們的檔案指標指向更多的檔案。在 32 位元的檔案指標最多可以達到 4G 位元組。



我們可以使用 quota 查詢磁碟空間使用及限制的情況。

語法

指令：quota 參數 使用者

參數：

- g：列出群組空間限制。
- q：列出超過限制部份。
- u：列出使用者磁碟空間限制。



- v : 顯示該使用者或群組在所有掛入檔案系統中的磁碟空間限制。
- V : 版本資訊。

我們可以使用 `edquota` 來編輯使用者或群組的磁碟分配 `quota`。

語法

指令 : `edquota` 參數

說明 :

- u : 編輯使用者 `quota`。
- g : 編輯群組 `quota`。
- p : 複製原型到每指定使用者的 `quota`。
- t : 編輯每個檔案系統的軟時間期限。

當我們要檢查磁碟使用空間及限制我們可以使用 `quotacheck` 指令。

語法

指令 : `quotacheck` 參數 檔案系統

參數 :

- a : 掃描/etc/fstab 檔案中加入 `quota` 設定的分割區。
- d : 顯示詳細的指令執行過程。
- g : 計算每個群組識別碼佔用的目錄和檔案數目，並建立 `aquota.group` 檔案。
- R : 排除根目錄所在的分割區。
- u : 計算每個使用者識別碼佔用的目錄和檔案數目，並建立 `aquota.user` 檔案。
- v : 顯示指令執行過程。



當我們要關閉磁碟使用空間限制我們可以使用 `quotaoff` 指令。

語法

指令： `quotaoff` 參數 檔案系統

參數：

- a：關閉/etc/fstab 檔案中加入 quota 設定的分割區。
- g：關閉群組的磁碟使用空間限制。
- u：關閉使用者的磁碟使用空間限制。
- v：顯示指令執行過程。

```
root@flash~ - Shell - Konsole
工作階段 編輯 檢視 設定 說明
[root@flash root]# quotaoff -agv
/dev/hda3 [/home]: group quotas turned off
```

我們可以使用 `quotaon` 開啟磁碟使用空間限制。。

語法

指令： `quotaon` 參數 檔案系統

參數：

- a：開啟/etc/fstab 檔案系統中加入 quota 設定的分割區。
- g：開啟群組的磁碟使用空間限制。
- u：開啟使用者的磁碟使用空間限制。
- v：指令執行過程。

```
[root@flash root]# quotaon -agv
/dev/hda3 [/home]: group quotas turned on
```



我們可以使用 repquota 顯示磁碟空間限制的情況。

語法

指令 : repquota 參數 檔案系統

參數 :

- a : 顯示我們在/etc/fstab 檔案系統中加入 quota 設定的分割區使用情況。
- g : 顯示所有群組的磁碟空間限制情況。
- u : 顯示所有使用者的磁碟空間限制。
- v : 顯示該使用者或群組的空間限制情況。



課後練習

1. 我們提供郵件伺服器的空間給使用者。我們希望使用者使用者空間不超過 40MB，但是我們又允許最高到 50MB，我們要怎麼樣才能實作這個空間？
 - (A). 啟動 grace period；設定 soft limit 到 40MB，設定 hard limit 到 50MB。
 - (B). 啟動 grace period；設定 soft limit 到 50MB，設定 hard limit 到 40MB。
 - (C). 啟動 grace period；設定 soft limit 到 50MB，設定 hard limit 到 50MB。
 - (D). 啟動 grace period；設定 soft limit 到 40MB，設定 hard limit 到 40MB。
2. 老版想要看每一個使用者在這系統上的磁碟使用，下列何者指令可以讓我們了解？
 - (A). quotareport -a
 - (B). quotareport -all
 - (C). quotashow -a
 - (D). repquota -a
3. 假如我們想在/home 目錄組態磁碟空間的分配，下列何者會加到我們/etc/fstab 的選項中？
 - (A). usrquota
 - (B). quota
 - (C). grpquota
 - (D). userquota
4. 下列何者運用相同的 quota 規則給 chaiyen 到使用者 justin？
 - (A). /usr/sbin/edquota -u chaiyen Justin
 - (B). /usr/sbin/appquota -p chaiyen Justin
 - (C). /usr/sbin/appquota -up chaiyen Justin
 - (D). /usr/sbin/edpquota -up chaiyen Justin
5. 我們有好幾個系統使用者。我們希望限制他們的磁碟空間在家目錄中，但是他們又要大量的暫時空間，我們要如何限制他們磁碟空間的使用率，但又讓他們無限制的



使用/tmp 目錄？

- (A). 使用 edquota /home 來編輯使用者 quota
- (B). 掛載/tmp 目錄到不同的分割區然後使用 edquota 在這包含/home 目錄的分割區
- (C). 使用 edquota 來指定這家目錄
- (D). 使用 quotacheck -agv

6.當使用 Linux 作業系統使用者管理時，下列何者是不需要的資訊？

- (A). 全名
- (B). 使用者名稱
- (C). 預設的 shell
- (D). 使用者的家目錄

7.下列 userdel 指令的選項可以刪除使用者和其家目錄？

- (A). -d
- (B). -r
- (C). -h
- (D). -a

8.下列何者為個別使用者的 KDE 視窗組態？

- (A). /etc/X11/.kde
- (B). /etc/skel/.kde
- (C). ~/.kde
- (D). /home/.kde



【答案】

1. A 2. D 3. A 4. A 5. B 6. A 7. B 8. C

