

第七章 使用者帳號管理



學習目標

- 了解Linux的帳號與群組
- 新增使用者帳號與群組
- 刪除帳號與群組
- 驗證帳號建立是否正確
- 認識檔案與目錄的權限

章節大綱

7-1 新增群組

7-3 認識檔案與目錄的權限

7-2 新增使用者帳號

備註：可依進度點選小節

使用者帳號管理

- 多人使用環境是Linux的主要特色
- 為多個使用者建立多個帳號(User)
- 群組的設計，可讓系統管理者為有相同特性的使用者訂定更彈性的管理模式



3

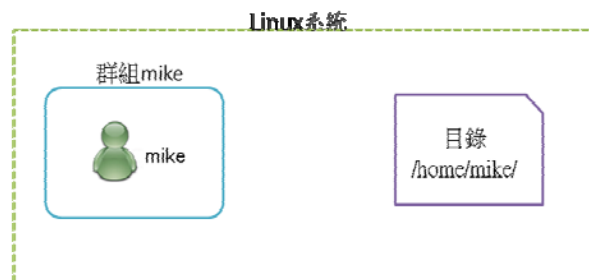
7-1 新增群組

- 一個群組皆對應一個編號，稱為GID(Group ID)
- 每個群組的GID皆不相同
- groupadd指令，再指定一個群組名稱
 - groupadd rd

4

7-2 新增使用者帳號

- 管理者必需為使用者建立帳號，並為其設定密碼
- useradd指令新增一個新的帳號
 - useradd mike



5

7-2 新增使用者帳號

- Linux的帳號
 - 每個帳號至少要有一個所屬群組
 - Linux的帳號資料
 - 帳號名稱
 - 密碼
 - 帳號編號
 - 所屬群組編號
 - 註解
 - 家目錄
 - 登入時使用的Shell
 - 帳號都要有家目錄
 - 系統環境設定檔
 - 電子信箱郵件

6

7-2 新增使用者帳號

● useradd指令規格

- useradd指令除了能快速建立帳號，其選項提供了許多客製的功能，如指定GID、指定群組、指定家目錄與指定該帳號預設使用的shell，都可透過選項來達到，指令的規格如下：

```
useradd [ 選項 ] 帳號名稱
```

7

7-2 新增使用者帳號

● useradd指令規格

- 欲建立的帳號名稱是useradd指令的參數，記得放在最後即可，若使用任何選項時，會在系統中自動建立一個群組，這個新群組與帳號名稱同名，並自動指派一個未使用的使用者編號（UID）。

```
[root@fc ~]# useradd testuser
[root@fc ~]# id testuser          ( 使用 id 指令列出該帳號的資訊 )
uid=503(testuser) gid=505(testuser) groups=505(testuser)
( 新建立帳號 testuser 所屬群組為 testuser 群組 GID 505 )
```

8

7-2 新增使用者帳號

● useradd指令規格

● 建立新帳號並指定已存在的群組

- 使用-g選項可指定新建立帳號並指定群組，-g加上空白後給予群組名稱或GID，唯該群組必須是已存在，讀者先依本章範例建立一個新的群組rd後，建立一個新帳號eric並指令群組為rd：

```
(若尚未建立群組 rd，請先以 groupadd 建立)
[root@fc ~]# groupadd rd
[root@fc ~]# useradd -g rd eric           (建立帳號 eric)
[root@fc ~]# id eric
uid=504(eric) gid=503(rd) groups=503(rd)
(成功建立帳號 eric，且群組為 rd)
```

9

7-2 新增使用者帳號

● useradd指令規格

● useradd [選項] 帳號名稱

選項用法	說明
-c 註解	指定帳號的註解說明文字，若註解內容有空白，可在文字內容兩邊使用單引號，如-c 'Hank Thomas'
-g 主要群組名稱或GID	指定帳號的主要群組
-G 附加群組名稱或GID	指定帳號所屬的附加群組
-d 目錄	指定家目錄
-e 日期	設定新建立的帳號使用到期日，過了該日期帳號即無法使用
-u UID	指定帳號的UID編號

10

7-2 新增使用者帳號

● useradd指令規格

● 指定附加群組

- 在實務上，一個帳號不一定只能指定於單一個群組，例如帳號tom的所屬群組為rd，也能讓tom再屬於另外的群組，就像一個經理（帳號）可以屬於業務部（群組），也能屬於行銷部（另一附加群組）。
- 要讓一個帳號tom除了主要群組rd外，再指定附加群組manager，可以使用-G（大寫）選項達成，筆者先以groupadd建立第二個群組manager，再使用選項-g與-G建立新帳號tom：

```
[root@fc ~]# groupadd manager
[root@fc ~]# useradd -g rd -G manager tom
          (除了主群組 -g 外，再使用 -G 增加附屬群組)
[root@fc ~]# id tom
uid=505(tom) gid=503(rd) groups=503(rd),504(manager)
(tom的主要群組為 rd，附加群組有 manager)
```

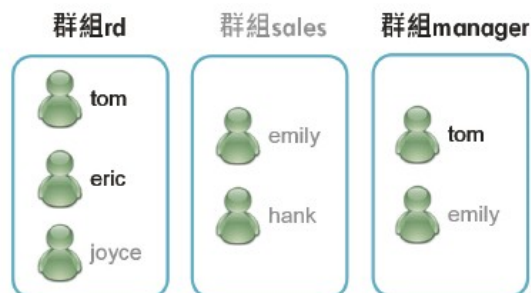
11

7-2 新增使用者帳號

● useradd指令規格

● 指定附加群組

- 目前主機帳號與群組情形應該如下示意圖，黑色部份是已建立完成的工作，讀者可以試著建立灰色未建立的群組與帳號：



12

7-2 新增使用者帳號

● 查詢使用者相關資訊

- 利用id指令，在id指令後加上帳號名稱

```
[root@fc ~]# id mike
```

```
uid=501(mike) gid=501(mike) groups=501(mike)
```

13

7-2 新增使用者帳號

● 刪除帳號

- 利用指令userdel(User Delete)
- 將帳號資訊從系統設定檔中移除(但不移除帳號所屬群組)
- userdel指令空白後，加上帳號名稱
 - [root@mylinux ~]# userdel mike
 - [root@mylinux ~]# id mike
 - id: mike: 此用戶不存在
- 在刪除帳號時，一併刪除該帳號的家目錄所有檔案
 - userdel -r mike

14

7-2 新增使用者帳號

● 變更帳號資料

- usermod指令是用來修改使用者帳號
- usermod指令的常用選項說明：

選項用法	說明
-c 註解	改變帳號的註解說明
-g 主要群組名稱或GID	改變帳號的主要群組
-G 附加群組名稱或GID	改變或增加附加群組
-d 目錄	改變家目錄
-e 日期	變更帳號的使用到期日，過了該日期帳號即無法使用
-l 帳號名稱	變更原帳號的名稱
-u UID	變更帳號的UID編號

15

7-2 新增使用者帳號

● 刪除群組

- 刪除一個群組，可用groupdel (group delete)
- 只能刪除沒有使用者指派的群組
 - groupdel 群組名稱

● 查詢使用者的群組

- groups指令可用來查詢使用者的群組資訊
- 想知道使用者tom所屬的群組有那些
 - [root@fc ~]# groups tom
 - tom : rd manager
 - (列出tom的群組為rd，另一群組為manager)

16

7-2 新增使用者帳號

● 停止帳號登入

- 可以使用userdel將帳號從系統裏刪除
- 只想讓帳號暫停使用，使其無法登入：
 - 修改/etc/passwd中帳號的密碼欄位
 - 利用chsh改變該帳號的shell

17

7-3 認識檔案與目錄的權限

- 每個檔案與目錄都擁有各自的權限設定
- 權限的代表的意義

r w x	r w x	r w x
-------	-------	-------

擁有者權限 群組權限 其他人權限

● 使用ls -l指令來觀察輸出結果

```
[root@fc ~]# ls -l myfile
-rwxrwxr-- 1 root root 0 2009-02-19 21:09 myfile
```

18

7-3 認識檔案與目錄的權限

● 權限字母有r、w、x與-（減號）

- r：可讀，可使用如cat編輯器讀取檔案內容，但無法修改。
- w：可寫入，也代表可以修改、新增資料或刪除檔案。
- x：此檔案可被執行
- 減號-：減號代表不允許該權限

19

7-3 認識檔案與目錄的權限

● 變更檔案權限chmod

- 使用chmod指令來達成
- chmod 權限表示法 檔案(對象)
 - 用三組八進位的方式表示
 - 語意描述法

20

7-3 認識檔案與目錄的權限

● 變更檔案權限chmod

● 權限表示法

● 八進位的方式

● r代表4、w代表2、x代表1

數字表示法	權限
0	---
1	--X
2	-W-
3	-WX
4	r--
5	r-X
6	rw-
7	rWX

21

7-3 認識檔案與目錄的權限

● 解讀權限

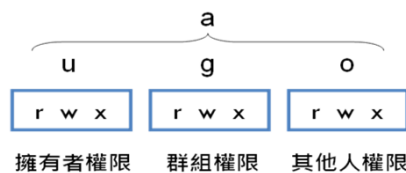
- 644代表rw-r--r--，擁有者可讀寫、群組可讀、其他人可讀
- 755代表rwxr-xr-x，擁有者可讀寫可執行、群組可讀可執行、其他人可讀可執行。
- 660代表rw-rw----，擁有者可讀寫、群組可讀寫、其他人無權限
- 754代表rwxr-xr--，擁有者可讀寫可執行、群組可讀可執行、其他人可讀。

22

7-3 認識檔案與目錄的權限

● 語意描述法

- 使用幾個字母、加減號與等號組成很方便使用的語意描述法，字母u、g、o、a
- u代表user也就是該檔案的擁有者（權限第一組）
- g 代表group，該檔案的群組（權限第二組）
- o代表other，除了擁有者與群組人員外的其他人（權限第三組）
- a代表all，代表所有人，也可說是上述ugo的集合



23

7-3 認識檔案與目錄的權限

● 改變權限

- 語法： `chmod 755 檔案`
- 為擁有者(u)加上可執行權限(x)
 - `chmod u+x 檔案`
- 一次為擁有者(u)與群組(g)加上可讀(r)與可執行(x)權限
 - `chmod ug+rx 檔案`
- 為所有人加上r權限
 - `chmod a+r 檔案`

24

7-3 認識檔案與目錄的權限

● 目錄的權限

● r :

- 代表可以列出該目錄的檔案清單，可以利用ls指令列出該目錄的內容。

● w :

- 代表至該目錄中的檔案與目錄都可以異動，如寫入檔案、建立、刪除、與更名檔案與目錄。

● x :

- 代表可進入該目錄中，也就是使用cd指令進入該目錄。

25

7-3 認識檔案與目錄的權限

● 變更檔案擁有者chown

- 使用chown (change owner) 將檔案的擁有權變更為其他使用者

● 指令用法：

- chown 使用者帳號 檔案或目錄

● 亦可以一併更變擁有群組

- chown 使用者帳號. 群組 檔案或目錄

- chown 使用者帳號:群組 檔案或目錄

26

7-3 認識檔案與目錄的權限

● 變更檔案所屬群組chgrp

- 使用chgrp (change group) 將檔案的擁有權變更為其他使用者
- 指令用法：
 - chgrp 群組名稱 檔案或目錄
- 利用chown即可變更檔案的所屬群組，不用多背一個chgrp指令

27

本章結束

Q&A討論時間

28