第五章 帳戶管理

5-1 使用者帳號/密碼

在多人使用系統環境裡，使用者必須事先擁有一個『帳戶』(Account)，才可以依此登入系統並使用系統資源。另一方面，系統管理者必須針對每一使用者的身份及工作性質，來開啟帳戶並規劃其優先等級，以及存取資源的權限如何，並當成計費的依據 (因此，稱之為 account)。簡單的說，帳戶即是使用者的身份識別，系統僅就帳戶名稱識別使用者的身份(非真實身份)。為了讓帳戶得到適當的保護而不被他人冒名頂替，一般帳戶都設有密碼，使用者必須正確輸入『帳戶/密碼』(Account/Password)，才可以登入系統。而系統也會驗證帳戶名稱與密碼是否正確，才決定是否允許登入系統，這就是使用者身份識別的依據。

5-1-1 建立帳戶

系統管理者有權限與義務幫使用者建立帳戶 (adduser 命令)，並規劃其工作環境 (容後介紹)。至於密碼方面，多半先由系統管理者設定 (passwd 命令，如 Welcome)，並郵遞傳送給使用者，當使用者首次登入系統之後，必須再重新設定自己選定的密碼(passwd 命令)。話說回來，帳戶名稱與密碼一般都儲存於系統檔案上 (如 /etc/passwd)，若是沒有經過特殊處理，萬一遭他人非法讀取該檔案，使用者的密碼便一覽無遺。因此，密碼在儲存之前都需經過某一種雜湊演算法 (如 MD5) 計算之後，得到一堆亂碼再儲存，既然亂碼無法由螢幕顯示出來，他人也無從輸入同樣的亂碼。至於雜湊演算法，它是一種單向計算公式，明文經過雜湊演算法以後，會計算出一段固定長度的雜湊值，而且無法由雜湊值倒推計算出原來的明文。如此一來，縱使他人可以看到密碼計算後的雜湊值，應該也無法 (很困難的意思) 由雜湊值計算出原來的密碼，如此便可達到保護密碼的功能。圖 5- 為建立帳戶與密碼的示意圖。

5-1-2 密碼驗證

使用者在取得帳號及密碼之後，便可登入系統，並可依照系統管理給予之權利範圍內存取系統上的資源。圖 5-2 是使用者登入的運作程序，首先經過網路連線（telent 140.127.138.32），連結主機成功之後，主機系統會傳送出 login: 與 passwd: 提示（訊號 (1) 與 (3)），要求使用者輸入帳戶名稱與密碼（訊號 (2) 與 (4)）。系統接收到帳戶及密碼之後，會將使用者所輸入的密碼經過雜湊演算法（如 MD5）計算，所得的雜湊值再與密碼檔案（/etc/passwd）上使用者的密碼比對是否相同，如果兩者相同的話，則表示密碼正確，並允許登入系統（出現提示 $）；否則顯示密碼錯誤（Login incorrect），並要求使用者重新登入。

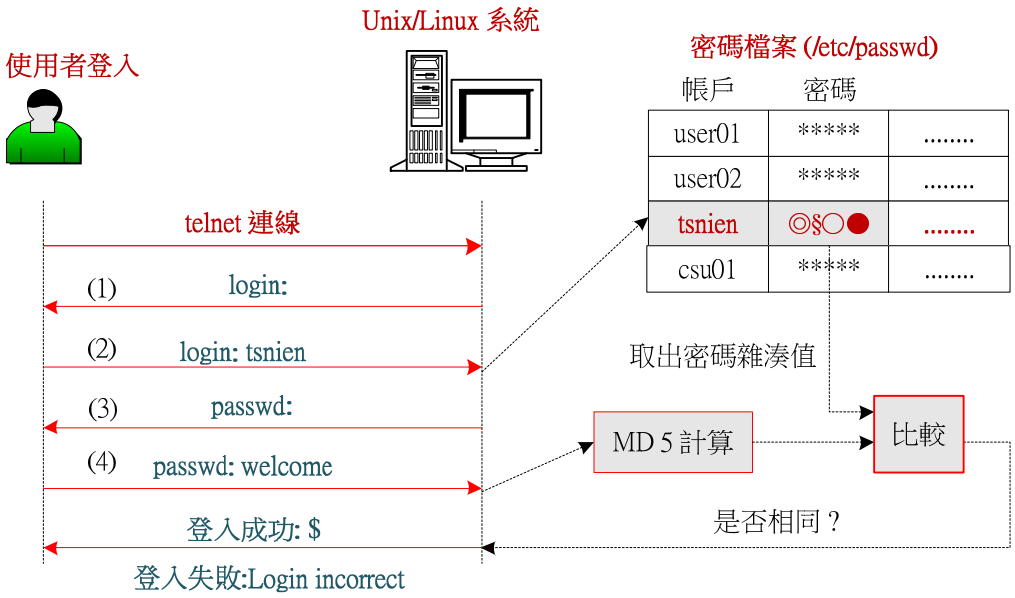


圖 5-2 系統驗證密碼

由上述運作可以看出，雖然密碼是經過雜湊演算之後，再儲存於密碼檔案上，但只要設定密碼與登入系統時所採用的雜湊演算法是一樣的話，就不會影響密碼的辨識。一般 Unix/Linux 系統大多採用 MD5 演算法，但它也可能會遭受破解，因此，多半會要求使用者在某一段時間之內（15 天左右）必須更改密碼。再者，如果利用 Telnet 登入遠端主機，所輸入的密碼是以明文方式，透過網路傳送給主機，有心人士很容易截取明文密碼，因此常會利用加密後的密碼傳送確保安全（使用 ssh 連線）；但也不見得，有興趣的讀者可參考拙著

『資訊與網路安全技術』，內有更詳細資訊安全技術的相關技術。

5-2 使用者與群組關係

就『個人電腦』（Personal computer，如 Windows XP Home）而言，並沒有所謂『群組』（Group）的概念，因為它是單人使用的系統，任何人只要能進入系統，便享有該主機上所有資源的最高權限。但對於『多使用者』（Multi-user）系統就不可如此隨便了，系統管理者必須規劃並授權每一使用者的權限，如此才能保護系統的安全性，不讓使用者越權使用或窺視不當資訊。但如要執行『對每一個使用者規劃並授與權限』，其實並不容易，它可能衍生下列兩個問題：

- **使用者人數過多：**在人數眾多的情況下，欲對每一使用者授與權限，管理者的工作負荷之重不在話下；再說，使用者可能會隨時加入或刪除，所以辨識每一使用者的權限，就更顯得複雜。
- **使用者多重角色：**一般情況，授與權限大多依照使用者所扮演著的角色而定。譬如，學生、老師、主任等不同角色，當然所給予的權利範圍是不同的。但若某一位使用者同時扮演兩個角色（譬如，老師與主任），欲規劃其權限範圍可能就有點困難。

由此可見，僅利用使用者帳戶來設定其權限是很困難的，尤其針對使用者人數超過千人以上的系統，那幾乎是不可能的事。還好，我們發現許多使用者大多有相同的工作性質，我們依照工作性質（或稱扮演角色）可將使用者分成若干個群組，再依照群組所扮演的角色授與權限，或許可以簡化許多管理上的困難點。以一般學校為例，每一系所的學生可以規劃於同一群組、老師也是一個群組、行政人員也是一群組，如此一來，整個學校的師生全部歸納於所屬系統的群組，譬如電機系學生、電機系教師、資管系學生、資管系老師、工學院主任等等群組。圖 5-3 為系統資源、群組與使用者三者的關係。首先，系統管理者製作了若干個群組，並且授與每一群組適當的權限，譬如規劃某一群組可以存取哪些資料庫記錄、讀取哪些檔案、存取磁碟儲存系統、或使用印表機等等。同時，管理者也可依照使用者的角色將

他歸類於某一群組。至於使用者應具有的權限，則視所屬群組而定，如此一來，我們只需針對群組規劃權限即可。另一方面，使用者也許同時具有多個角色，亦即同時屬於多個群組，所以該使用者在不同群組就享有不同的權限。

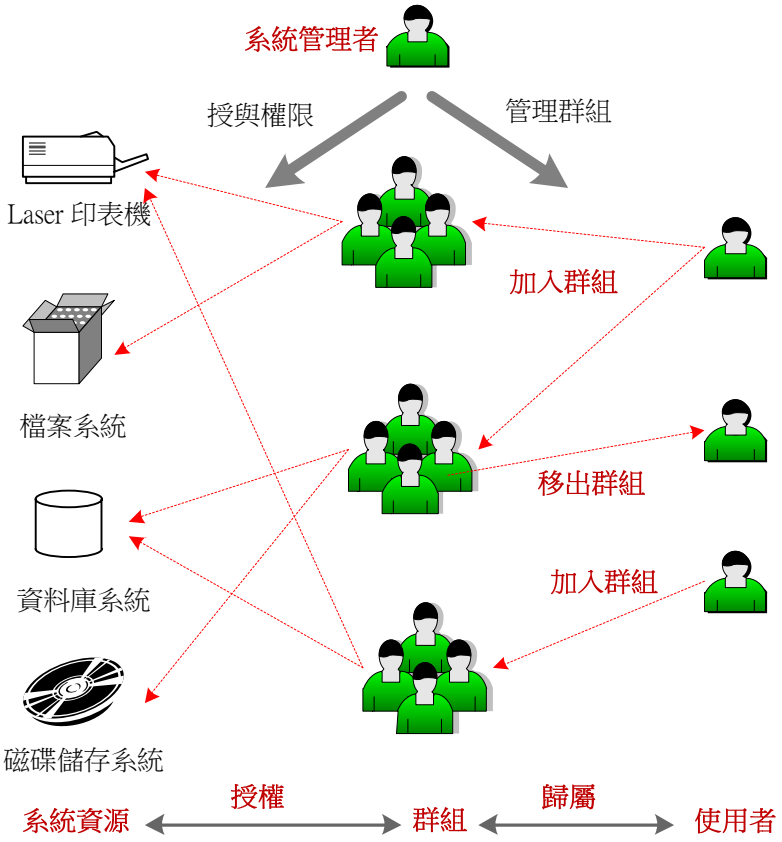


圖 5-3 系統資源、群組與使用者之關係

其實，Unix/Linux 系統對於群組與使用者之間系統資源設定的管理操作，是最為人詬病的，這或許與系統所從事的工作有所關聯吧！如果將作業系統看成一家公司，Unix 所扮演角色就如同生產工廠一般；Windows 就如同服務公司（如遊樂或保險公司）。生產工廠比較重視使用者的工作範圍，超過自己的工作範圍大多不被允許的；服務公司則會依使用者付費的多寡，來決定它可以接受服務的程度。因此，對於服務公司而言，群組與系統資源之間的連帶性比較高；對於工廠而言，群組與使用者之間的連帶性會比較高。我們可以發現，Unix/Linux 系統對於授與使用權限而言，僅區分為擁有者（owner）、群組（group）與其他（other）三種身份，而每一種身份僅可授與讀取（read）、寫入（write）與執行（execute）等三種權限，並無法針對某一特殊群組授與權限，這方面就遠不及 Windows 系統方便。

5-3 帳戶類別

5-3-1 帳戶與使用者身份

就單純的角度來看，『多使用者』(Multi-user) 系統當然允許多使用者可同時登入，並操作使用系統。若從宏觀的觀點來看，整部系統的運作是由多人共同努力，並承擔各種工作所達成。前者是系統表面上的服務導向，後者才是真正建構系統的因素。由此可見，一部系統不僅只是使用資源的使用者而已，還有更多使用者默默的為系統運作而努力；這種觀念就好像『遊樂區』一樣，使用者並不單指遊客而已，許多工作人員也是屬於使用者之一。

因此一部 Unix/Linux 系統除了管理者所建立的使用者帳戶，還有許多從事於某一特定工作的內部使用者 (又稱系統操作者，System operator)。基本上，系統操作者也需要一個帳戶來規劃它的執行權限，只不過這類使用者不需要登入程序，也沒有 Login script 與 Home directory。簡單的說，Unix/Linux 上的使用者大致上可區分為『一般使用者』與『系統操作者』二類，此二類使用者都需要帳戶來規範操作權限，一般使用者需要經過登入程序才可以啟動；而系統操作者則不需經過登入程序，只要系統需要時，透過呼叫來啟動它即可。以下分別說明這兩類使用者的屬性。

初學者多半認為『使用者』(Users) 是經過登入程序後，再使用系統資源，其實不然，系統中有許多無需登入程序就已存在的使用者，而這些使用者大多從事於某一特定的工作。之前本書曾經介紹過，一套運作中的作業系統就宛如一座工廠一般，裡面有許多工作人員隨時從事自己某一特定的工作。如果給予這個工廠某一特定管理程序及製作工具，它就可以生產出各種不同的產品。作業系統也是一樣，植入不同運作程序及軟體套件，便可提供不同的服務。譬如，一套 Unix/Linux 系統可能從事於生產管理系統、銷售管理系統、網頁伺服系統、郵件系統、甚至 CAD/CAM 等等。也就是說，系統會依照某種特殊需求，植入不同的軟體，同時也產生一個特殊操作者來執行該軟體，這類操作者會使用到系統資源，也是另一類的使用者。

由此可見，系統內可能存在許多不同性質的使用者，在此我們大略可將一部 Unix/Linux 系統的使用者屬性，區分為以下三大類型：

5-3-2 系統管理者

在系統安裝的同時，就會自動建立一個『系統管理者』(System administrator)，其帳戶名稱及所屬群組名稱皆固定為 root，屬於此群組的使用者皆享有最高權限，可以任意刪除或增加系統執行程序。為了安全起見，一般系統並不允許 root 使用者從遠端登入，僅允許在主控台 (Consol) 登入，但有時為了方便操作，或一部系統有多個系統管理者時，並不希望每一個人都以 root 帳戶登入系統，如此將很難記錄哪些命令是由何人所執行。因此，都會將某些具有管理責任的帳戶加入 root 群組上，這些帳戶可以遠端登入，也可以管理系統，而且可由記錄檔 (Log file) 上觀察出，所有帳戶所下達的命令，順便可觀察是否有越權或違規的事件發生。

既然帳戶名稱都固定為 root，密碼的保護就顯得格外重要，甚至可以說，只要知道 root 的密碼就相當於有 root 的權限了。Unix/Linux 就依照這個觀點，讓知道 root 密碼的使用者可以立即升級成管理者身份。任何帳戶執行 su(substitute user)命令，並輸入 root 密碼，即可立即升級成為 root 身份；恢復原來身份可執行 exit 命令或直接鍵入 Ctrl+D 即可，操作範例如下：

```
[tsnien@linux-1 ~]$ su
Password:######                    【輸入 root 密碼】
[root@linux-1 tsnien]#             【取代成 root 身份】
[root@linux-1 tsnien]# cd          【切換到 root 家目錄】
[root@linux-1 root]# exit          【輸入 exit 命令】
exit
[tsnien@linux-1 tsnien]$           【恢復原來身份並回原家目錄】
```

值得注意的是，雖然可以利用 su 命令，取得 root 身份，但未真正執行 root 的登入命令稿（Login script）的話，也就沒有真正進入 root 的外殼環境（Shell environment），因此許多環境變數並沒有改成 root 的環境變數，譬如 PATH 變數還是保留原來使用者的內容。

5-3-3 一般使用者

經由系統管理者所建立的帳號，稱為『一般使用者』(General Users)。系統管理者建立帳戶時，必須指定該帳戶屬於哪一群組、家目錄、以及登入外殼程式等等。使用者若需要使用某一系統資源，或在該系統上從事工作之前，都必須向系統管理者提出申請。待系統管理者評估申請者的身份後，再開啟申請者帳戶，並通知他使用系統。

值得注意的是，使用者登入系統之後，系統會針對使用者帳戶建立一個執行程序(Process)，並給予一個程序號碼(Process ID, PID)，爾後所有處理動作僅針對此 PID 運作。因此，同一個帳戶可供多人同時登入，系統會針對每一個登入（同一帳戶）給予一個獨一無二的 PID 號碼。系統是依據 PID 識別運作，多人使用同一帳戶登入後，雖然在同一家目錄下工作，但之間運作也不至於發生衝突。又有某些使用者登入系統後，僅瀏覽或參觀系統資源並不真正執行某些特定工作，此類使用者一般稱之為『訪客』(Guest)，一般系統都會建立一個 Guest 帳戶，供這些客戶登入使用。

5-3-4 系統操作者

此類使用者大多是建立系統或安裝某種軟體時，系統依其需求自動建立的帳戶。基本上，這些帳戶是無法登入的，僅於需要它執行時，系統才會去啟動它，因此稱之為『系統操作者』(System operators)。每一系統使用者大多背負著某一特殊的任務，並隨時等待執行此工作。譬如，一般系統上都有一個 lp（Line printer）使用者，專門負責列印的功能。當某一線上使用者需要列印資料時，只要將資料交付給 lp 使用者，它就會幫它印出來，該使用者

根本不用理會印表機安裝的位置（近端或遠端）與印表機驅動程式等問題；如果需要郵遞信件時，只要將信件交給 mail 操作者，它就幫您傳遞郵件，您根本不用知道郵件伺服器在哪裡；甚至，當您想要關閉主機時，只要通知 shutdown 操作者，何時關機或關機之前應傳送哪些訊息給線上使用者， shutdown 都會依照指示程序，按時關閉主機。由此可見，這類的使用者就好像工廠裡的作業員一樣，隨時等待執行某特定的工作，如果工廠裡有許多這類型的操作者，然而這些操作員都依循著某一生產程序，便可以製造出各型各類的產品。

每一個系統操作者都有一個獨立的帳戶，某些工作性質相同者也會被歸納在同一群組，並規劃其群組的權限範圍，如 bin、daemon、sys、lp 等等群組。常見系統工作者的範例如下：

- lp：列印工作者，專門負責列印的工作。
- shutdown：關機工作者，專門負責執行關機程序者。
- daemon：監督工作者，專門執行某一特殊功能的監督程式。
- named：名稱工作者，專門負責執行 DNS 名稱查詢工作者。
- apache：網頁工作者，專門負責執行 Apache 網頁伺服工作者。
- uucp： UUCP 工作者；專門負責執行 UUCP（Unix to Unix Copy）伺服工作者。

任何一部 Unix/Linux 系統安裝越多軟體套件，就將會建立越多系統工作者，也就是說，系統會針對每一個軟體套件開啟一個以上的帳戶。當需要執行某一套件時，只要呼叫它的系統操作者，再由它負責執行；操作者執行軟體套件所得到的某些結果，會傳遞給呼叫它的程序。至於目前系統有哪些系統工作者正在執行任務中，可利用 ps –ef 顯示所有程序，除了一般使用者（或 root 系統管理者）登入外，其餘皆是系統操作者；操作範例如下：

```
$ ps -ef |more
UID          PID    PPID    C STIME TTY          TIME CMD
root           1       0    0 Jul20 ?        00:00:07 init [5]
```

```
root          2     1   0 Jul20 ?        00:00:00 [ksoftirqd/0]
....
rpc        1854     1   0 Jul20 ?        00:00:00 portmap
rpcuser    1874     1   0 Jul20 ?        00:00:00 rpc.statd
...
xfs        2434     1   0 Jul20 ?        00:00:00 xfs -droppriv
-daemon
daemon     2453     1   0 Jul20 ?        00:00:00 /usr/sbin/atd
......
```

其中 rpc、rpcuser、xfs、daemon 即是系統操作者。

5-4 帳戶管理檔案

一般 Unix/Linux 系統有四個主要的帳戶管理檔案，分別是 /etc/passwd、/etc/shadow、/etc/group 與 /etc/gshadow，並且都設定成僅能『讀取』，不可修改或執行。管理者如要修改的話，則須先它設定成可寫入，完成後再改回來（利用 chmod）。以下分別介紹之。

5-4-1 帳戶檔案 - /etc/passwd

此檔案在建立系統時便已存在，管理者不用特地去產生它，而且當管理者操作增加、刪除或更新帳戶命令時，也會自動修改此檔案。當然，管理者也可以直接利用 vi 編輯此檔案來管理帳戶，但一般系統都不建議如此操作，還是利用正規管理命令(容後介紹)較為妥當。我們可以利用 # cat /etc/passwd 命令，觀察此檔案內容，如下所示：

```
# cat /etc/passed
root:BXOVk2FNVaoKs:0:0:root:/root:/bin/bash
bin:*:1:1:bin:/bin:/sbin/nologin
daemon:*:2:2:daemon:/sbin:/sbin/nologin
adm:*:3:4:adm:/var/adm:/sbin/nologin
lp:*:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:*:5:0:sync:/sbin:/bin/sync
shutdown:*:6:0:shutdown:/sbin:/sbin/shutdown
halt:*:7:0:halt:/sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail:/sbin/nologin
news:*:9:13:news:/etc/news:
uucp:*:10:14:uucp:/var/spool/uucp:/sbin/nologin
```

```
operator:*:11:0:operator:/root:/sbin/nologin
games:*:12:100:games:/usr/games:/sbin/nologin
gopher:*:13:30:gopher:/var/gopher:/sbin/nologin
ftp:*:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:*:99:99:Nobody:/:/sbin/nologin
.....
tsnien:GaB2MI0gT.psI:508:508::/home/tsnien:/bin/bash
```

其中每一行記錄（即是每一筆資料的意思）表示每一個使用者的帳戶資料。圖 5-4 是每一筆記錄中每一欄位所代表的功能，各欄位功能（欄位之間以冒號分隔）如下：

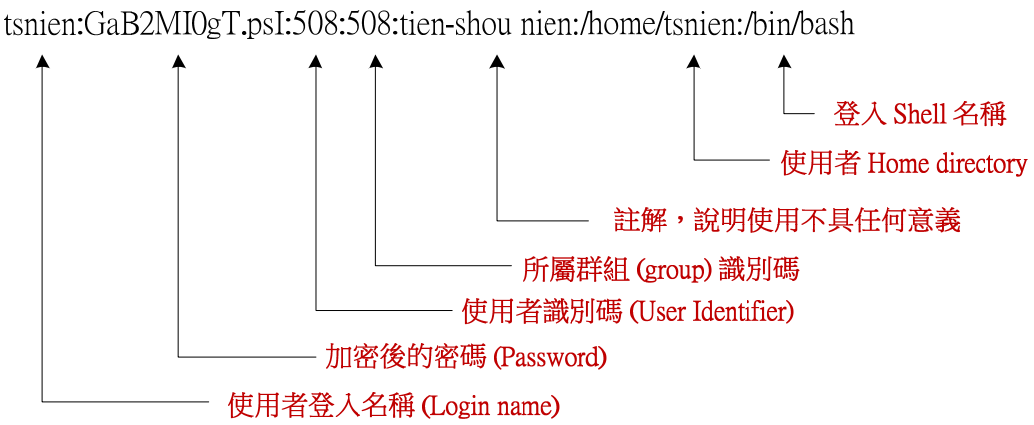


圖 5-4 帳戶檔案內容

- **使用者名稱（User name，第 1 欄位）：**使用者身份的識別名稱，又稱為登入名稱（Login name）或帳戶名稱（Account name）。名稱最長為 32 個字元，且同一系統內不可以有兩個以上名稱相同。

- **密碼（password，第 2 欄位）：**加密或雜湊演算後的密碼儲存位置。許多系統（如 Fedora core 4）並不會將密碼儲存於此欄位，而是將加密後的密碼儲存於 /etc/shadow 檔案內，此欄位顯示如下（x 的含意容後說明）：

```
csu001:x:502:502:csu students:/home/csu001:/bin/bash
```

- **使用者識別碼（User Identifier, UID，第 3 欄位）：**使用者獨一無二的識別碼。UID 號碼介於 0 ~ 65535 之間，其中 UID=0 為 root 識別碼；1 ~ 499 則保留給系統使用，大多分配給『系統操作者』帳戶使用；其餘 500 ~ 65535 則給一般使用者帳戶使用。

- **群組識別碼（Group Identifier, GID，第 4 欄位）：**使用者所屬群組的識別碼。此欄位

與 /etc/group 檔案內第三欄位相對應，表示該帳戶使用者是歸屬於哪一個群組。

✧ **註解（Comment，第 5 欄位）：**此欄位僅做說明使用，大多使用於儲存使用者的全名。

✧ **家目錄（Home directory，第 6 欄位）：**該帳戶的家目錄，使用者登入後會立即進入此帳戶。系統管理者在建立帳戶時，必須同時開啟該帳戶的家目錄，並將此目錄的擁有者設定為所建立的帳戶所有，如家目錄未建立完備，該帳戶將無法順利登入系統。

✧ **外殼（Shell，第 7 欄位）：**此欄位指定使用者登入後，執行哪一個外殼程式（如 /bin/bash），亦即指定外殼環境。

5-4-2 群組檔案 - /etc/group

由群組檔案 /etc/group 可以看出系統上已設定的群組，以及每一群組包含的使用者，檔案範例如下（# cat /etc/group）：

```
root::0:root,systexftp,service
bin::1:root,bin,daemon
daemon::2:root,bin,daemon
sys::3:root,bin,adm
adm::4:root,adm,daemon
tty::5:
disk::6:root
lp::7:daemon,lp
……
tsnien:x:508:
```

上述中，每一列表示一筆記錄，並代表一個群組的屬性，其格式如下：

groupname:password:gid:user-list

其中：

➢ **群組名稱（Group name，第 1 欄位）：**每一群組的名稱，如 bin、root 等。某些名稱是系統內定的，多半有其特殊功能。

➢ **群組密碼（password，第 2 欄位）：**目前此欄位不使用。

- **群組識別碼（Group ID, GID，第 3 欄位）**：範圍 0～65535，其中 0～99 保留給系統使用，其中 root 的 GID 為 0。此 GID 與 /etc/passwd 內的 GID（第三欄位）相同。如果使用者有獨立群組的話，則 GID 與 UID 的號碼相同。

- **使用者列表（User list，第 4 欄位）**：此群組底下的使用者。相同群組的使用者的權限大致上相同，譬如上例中，除了 root 具有超級使用者權限外，systexftp 與 service 使用者都具有相當的權限，這樣的做法是非常危險的。

5-4-3 帳戶隱藏檔 - /etc/shadow

加密或雜湊計算後的密碼是否就安全呢？這是值得深思的問題。如圖 5- 所建立的帳戶，將加密後的密碼儲存於帳戶檔案 /etc/passwd 。我們利用 ls –l 觀察此檔案的安全性如何：

```
$    ls -l /etc/passwd
-rw-r--r--    1 root root 7716 Jul 16 10:07 /etc/passwd
```

由它的存取控制碼（-rw-r--r--，0644）可以看出，雖然該檔案僅能由 root 修改，但其他所有人都可以讀取它。這是因為系統上還有許多地方必定會利用到 /etc/passwd 檔，所以無法限制他人讀取。如此一來，任何人都可以讀取所有帳戶加密後的密碼，有心人士便可以利用暴力攻擊法或字典攻擊法（請參考拙著『資訊與網路安全技術』），去猜測或破解某一特殊使用者的密碼。一般系統大多利用 MD5 演算法，有心人士只要輸入不同的密碼，再經過 MD5 計算後所得的雜湊值，比較是否與 root 欄位的密碼相同。如果相同的話，表示就已破解 root 的密碼，再利用所猜測的密碼，便可以順利以 root 身份進入系統，如此一來，不但入侵成功而且還享有最高優先權。

由此可見，將加密後的密碼存放於 /etc/passwd 檔案是不可靠的。還好一般 Unix/Linux 都可利用 Shadow 套件來解決此困厄。Shadow 套件不但可以隱藏密碼，還可以擴充密碼的功能，譬如設定帳戶有效期限、密碼更換週期等等。安裝 Shadow 套件之後，系統會另外建立一個密碼管理檔案，其名為 /etc/shadow，是儲存加密後的檔案，亦即相關密碼控制訊息。

然而，加密後的密碼就不再存放於 /etc/passwd 檔案，其中每筆記錄將變更為下列格式：(# cat /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
.....
tsnien:x:502:502::/home/tsnien:/bin/bash
```

原來儲存密碼的第二個欄位，不再儲存加密後的密碼，而以『x』取代，表示加密後密碼已移植到 /etc/shadow 檔案上。另外，觀察 /etc/shadow 檔案屬性如下：

```
$ ls -l /etc/shadow
-r--------    1 root root 8709 Jul 16 10:07 /etc/shadow
```

我們可以發現 /etc/shadow 的存取控制碼為 0400，亦即只有 root 可以讀取，其他使用者是不允許讀取的。儲存於 /etc/shadow 的加密後密碼，一般使用者是無法讀取，如此便可以增加破解密碼的困難度 (當然還可利用其他方法破解)。

欲觀察 /etc/shadow 的檔案內容，必須以 root 帳號登入系統，如下所示 (# cat /etc/shadow)：

```
root:$1$oa4Fm13y$b1aJSwPYX2JDJSIuTVDxV0:12832:0:99999:7:::
bin:*:12832:0:99999:7:::
daemon:*:12832:0:99999:7:::
adm:*:12832:0:99999:7:::
lp:*:12832:0:99999:7:::
sync:*:12832:0:99999:7:::
shutdown:*:12832:0:99999:7:::
halt:*:12832:0:99999:7:::
mail:*:12832:0:99999:7:::
....
radiusd:!!:12832:0:99999:7:::
ldap:!!:12832:0:99999:7:::
mysql:!!:12832:0:99999:7:::
.....
tsnien:$1$EvORlBb6$zhui.EoD70ir8FiWVhIj/0:12838:0:99999:7:::
```

如同 /etc/passwd 檔案一樣，每一行表示一筆記錄並對應到 /etc/passwd 檔案資料，表

示某一帳戶的密碼管理訊息。每一筆資料包含若干個欄位，欄位之間以冒號 (:) 分隔，如圖 5-5 所示。各欄位功能如下說明：

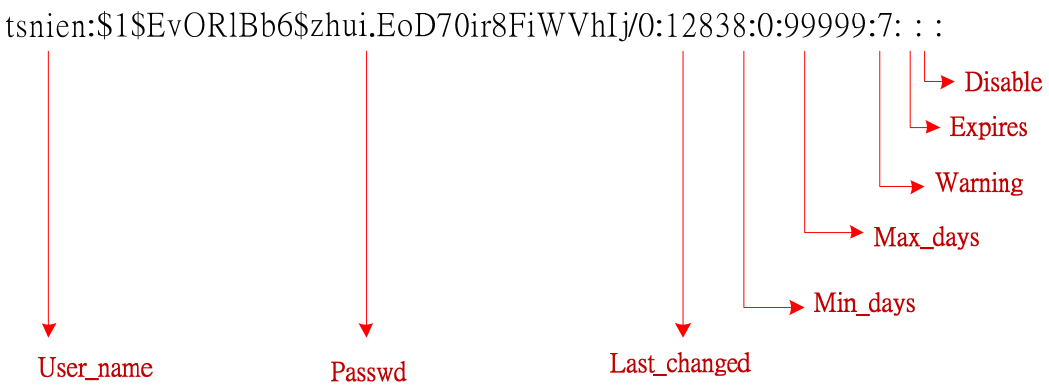


圖 5-5 /etc/shadow 各欄位功能

- **使用者名稱 (User name，第 1 欄位):** 該筆記錄的使用者名稱 (或稱帳戶名稱、登入名稱)，此欄位與 /etc/passwd 檔案相對應的使用者名稱。

- **密碼 (Password，第 2 欄位):** 儲存該帳戶的加密或雜湊演算後的密碼。如果該欄位內容是兩個驚嘆號 (!!)，表示該帳戶已被鎖定而且無法登入 (或還未開啟)；如果是一個星號 (*)，則表示該帳戶是特殊使用者，並且無法直接登入，如 lp 等等。

- **最後變更日期 (Last changed，第 3 欄位):** 儲存該帳戶密碼最後變更的日期，但不是直接儲存某年某月的日期，而是取某一日期 (如 1970 年 1 月 1 日) 到所變更日期之間的天數。

- **至少使用天數(Min days，第 4 欄位):** 密碼至少必須使用的天數。譬如若此欄位為 10，表示密碼上次變更後(Last changed 欄位)，至少必須經過 10 天之後才可以再變更密碼。此欄位一般甚少使用，大多設定為 0。

- **使用最多天數 (Max days，第 5 欄位):** 密碼最多可使用的天數，亦即在這個期間必須變更密碼。譬如若此欄位為 30，則表示上次變更密碼後 (Last changed 欄位值)，30 天內必須重新變更密碼。如果沒有特定指定可以使用幾天，可將此欄位設定成最大值

（99999），表示永遠有效的意思。

- **警告（Warning，第 6 欄位）：**密碼過期之前警告的天數。譬如若此欄位是 7，表示該密碼使用最多天數的最後 7 天內，使用者登入時，都會發出警告的訊息；如果沒有特殊指定，此欄位大多設定為 7。

- **過期天數（Expires，第 7 欄位）：**此欄位記錄著允許密碼過期變更的天數。譬如若此欄位設定為 5，表示密碼過期的 5 天內還可登入，如果再超過的話，則帳戶就會被鎖定而且無法登入（需管理者重新設定）。此欄位若為 0 表示密碼永遠有效。

- **鎖定（Disabled，第 8 欄位）：**此欄位為 0，表示該帳戶已被鎖定；否則表示未被鎖定。

5-4-4 群組隱藏檔 - /etc/gshadow

雖然目前甚少使用群組密碼，但 Shadow 套件還是建立一個群組密碼隱藏檔案 /etc/gshadow。因為甚少使用此檔案，這裡僅簡單介紹。檔案範例如下（# cat /etc/gshadow）：

```
root:::root
bin:::root,bin,daemon
daemon:::root,bin,daemo
....
tsnien:!!::
```

其中每一行表示一個群組的管理訊息，它是由四個欄位所構成，欄位之間以冒號（:）分隔，如圖 5-6 所示。各欄位功能如下：

- **群組名稱（Group name，第 1 欄位）：**與 /etc/group 相對應的群組名稱。

- **密碼（Password，第 2 欄位）：**加密後群組密碼。

- **管理者（Administrators，第 3 欄位）：**群組管理員的帳戶名稱，如果超過一位管理員，會以逗號（,）分隔。

- **成員（Members，第 4 欄位）：**群組成員的帳戶名稱；如果超過一個成員，會以逗號（,）

分隔。

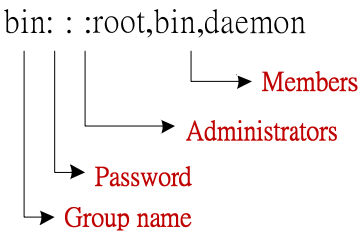


圖 5-6 /etc/gshadow 各欄位功能

5-5 帳戶管理命令

以下將介紹一些較常用的帳戶管理命令，譬如新增帳戶(useradd)、刪除帳戶(userdel)、新增群組 (addgroup)、刪除群組 (delgroup) 等功能；以上功能必須具有 root 權限者才可執行，且於執行後，系統會相對編輯 /etc/passwd、/etc/group、/etc/shadow 與 /etc/gshadow 等控制檔。當然，直接修改上述控制檔也可以達到管理帳戶的功能，但一般系統還是建議管理者執行控制命令，最好不要直接修改控制檔，以免出差錯。

5-5-1 新增使用者 - useradd

系統管理者可利用 useradd(/usr/sbin/useradd)命令新增或編輯帳戶，其命令格式如下：

```
# man useradd
        useradd [-c comment] [-d home_dir]
                [-e expire_date] [-f inactive_time]
                [-g initial_group] [-G group[,...]]
                [-m [-k skeleton_dir] | -M] [-n] [-o] [-p passwd] [-r]
                [-s shell] [-u uid] login
        useradd -D [-g default_group] [-b default_home]
                [-e default_expire_date] [-f default_inactive]
                [-s default_shell]
```

其中：

- **-c <備註>**：將備註文字填入 /etc/passwd 備註欄位中。

- **-d <家目錄>：**使用者家目錄（Home directory）位置，如 /home。
- **-e <有效期限>：**該帳戶的有效期限；-1 表示沒有限制到期日。
- **-f <緩衝時間>：**密碼到期後的緩衝時間。
- **-g <群組>：**使用者所屬群組；-G <群組> 為使用者所附加的其他群組。
- **-m：**自動建立家目錄；-M 為不自動建立家目錄；- n 則是不自動建立群組。
- **-s <shell>：**使用者起始 Shell，如 /bin/sh。
- **-u <uid>：**指定使用者識別碼（User ID）。
- **-D**：建立預設值（default）參數，如 -g（預設群組）、預設家目錄、預設到期日等等；預設值儲存於 /etc/default/adduser 檔案內。

【A. 預設值帳戶】

以下範例是完全採用內定值來產生一個新帳戶。通常系統為了方便操作，都會事先建立一些內定值，管理者如沒有特別指定，則可利用內定參數建立一個新帳戶，範例如下：(新帳戶名稱為 nien1)

```
[root@linux-1 ~]#useradd    nien1    ➔ 增加 nien1 使用者
[root@linux-1 ~]# passwd    nien1      ==➔ 設定 nien1 密碼
Changing password for user nien1.
New password: #######
Retype new password: ######
passwd: all authentication tokens updated successfully.
```

第一個命令（# useradd nien1）為增加新帳戶 nien1；第二個命令（# passwd nien1）是設定新帳戶，系統會要求重複輸入密碼兩次。執行完畢後，上述四個控制檔將會被變更其內容，範例如下：

```
# cat    /etc/passwd |grep nien1
nien1:x:618:618::/home/nien1:/bin/bash
```

```
# cat    /etc/group |grep nien1
nien1:x:618:

# cat    /etc/shadow |grep nien1
nien1:$1$ZGV1ApHR$/0aH8NbGWB8ZgBvIc2v2F/:13016:0:99999:7:::

# cat    /etc/gshadow |grep nien1
nien1:!::
```

由 /etc/passwd 檔案，可以看出已增加 nien1 記錄，並從中可以了解其屬性，如下：

- 登入名稱：nien1。
- 密碼：已隱藏至 /etc/shadow。
- 使用者識別碼（UID）：618。
- 群組識別碼（GID）：618。
- 註解：此欄位目前空白，可利用 vi 編輯其內容。
- 家目錄：/home/nien1
- 登入 Shell：/bin/bash

在 /etc/group 檔案內也會增加 nien1 記錄，則表示已增加 nien1 群組；記錄內容如下：

- 群組名稱：nien1。
- 密碼：已隱藏於 /etc/gshadow 檔案內，目前此欄位沒有使用。
- 群組識別碼（GID）：618。
- 群組成員：nien1 帳戶。

同樣於 /etc/shadow 與 /etc/gshadow 檔案內也都會增加 nien1 記錄，至於其內容下個範例再介紹。

【B. 帳戶預設檔】

上述範例增加帳戶時，大部分的參數皆是預設值，且預設值是參考到檔案 /etc/default/adduser。如變更預設檔的內容，再增加帳戶時也會依照新的預設值。該檔案範例如下：

```
#    cat /etc/default/useradd
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
# /usr/sbin/adduser -D -b /home/data
# cat /etc/default/useradd
# useradd defaults file
....
HOME=/home/data
.......
```

【C. 指定參數帳戶】

管理者也可以直接指定帳戶參數，但沒有特別指定的參數還是會引用 /etc/default/adduser 的內容。操作範例如下：

```
# useradd -u 800 -g 100 -d /home/nien2 nien2
#    passwd nien2
Changing password for user nien2.
New UNIX password:#####
Retype new UNIX password:######
passwd: all authentication tokens updated successfully.
# cat    /etc/passwd |grep nien2
nien2:x:800:100::/home/nien2:/bin/bash
#
```

上述範例中，建立新帳戶名為 nien2，其中 UID 為 800、GID 為 100、家目錄是 /home/nien2，如果家目錄不存在時，系統會新開啟該目錄。

5-5-2 刪除使用者 - userdel

刪除帳戶的命令格式如下：

```
userdel [-r] login
```

其中 –r 表示刪除使用者登入目錄及該目錄下的所有檔案。操作範例如下：

```
# userdel   -r   nien2
# cat   /etc/passwd |grep nien2
# cat   /etc/group |grep nien2
# cat   /etc/shadow |grep nien2
```

上述範例刪除 nien2 帳戶，同時可以發現於 /etc/passwd、/etc/group 與 /etc/shadow 內原有的 nien2 記錄也都被刪除了。

5-5-3 修改使用者 – usermod

建立後的帳戶可利用 usermod 命令修改其參數，命令格式如下：

```
usermod [-c comment] [-d home_dir [-m]]
                [-e expire_date] [-f inactive_time]
                [-g initial_group] [-G group [,...]]
                [-l login_name] [-p passwd]
                [-s shell] [-u uid [-o]] [-L|-U] login
```

大致上，修改帳戶的參數大多與建立帳戶命令（useradd）相同。以下範例我們先建立一個帳戶，再修改該帳戶的參數（將 UID 從 800 修改為 801），且觀察修該前後設定檔（/etc/passwd）的變化如何，操作範例如下：

```
#useradd   -u 800 -g 100 -d /home/nien2 nien2
# cat /etc/passwd |grep nien2
nien2:x:800:100::/home/nien2:/bin/bash
# usermod   -u 801 nien2
# cat   /etc/passwd |grep nien2
nien2:x:801:100::/home/nien2:/bin/bash
```

5-5-4 變更密碼 - passwd

使用者登入系統（如帳號 nien2）後，立即可以利用 passwd 命令變更密碼，操作範例如下：

```
$ passwd
Changing password for user nien2.
Changing password for nien2
```

```
(current) UNIX password:#######    ( 原來舊密碼 )
New UNIX password:######           ( 新密碼 )
Retype new UNIX password:######    ( 重複輸入新密碼 )
passwd: all authentication tokens updated successfully.
```

變更密碼時，系統會要求重新輸入原來密碼，確認是否是真正帳戶使用者。確認密碼正確後，才會允許變更密碼，並要求重新輸入新密碼一次。

【使用者遺失密碼】

對於密碼的設定，大多是系統管理者建立帳戶時，幫使用者設定好之後，再通知使用者。通常會要求使用者於第一次登入系統時，立即變更成自己選定的密碼。但使用者也有可能遺失密碼而無法登入系統，此時將求助於系統管理者。解決的方法有兩種：一者是系統管理者重新設定使用者密碼，再通知使用者使用；二者是直接刪除帳戶密碼，使用者登入後再重新設定密碼。第一種方法操作如下 (重新設定 nien2 密碼):

```
# passwd nien2
Changing password for user nien2.
New UNIX password: #####
Retype new UNIX password ######:
passwd: all authentication tokens updated successfully.
```

若直接刪除帳戶密碼，使用者可不用密碼就可以登入系統，登入後再自行設定新密碼，操作範例如下 (刪除 nien2 密碼):

```
# passwd -d nien2
Removing password for user nien2.
passwd: Success
[root@linux-1 root]#
```

5-5-5 設定密碼參數 - passwd

如果系統有安裝 Shadow 套件的話，則可針對帳戶密碼的使用期限加以限制，這些設定值將會記錄於 /etc/shadow 檔案內。設定密碼期限也是使用 passwd 命令，其格式如下：

```
passwd [-k] [-l] [-u [-f]] [-d] [-n mindays] [-x maxdays] [-w warndays]
       [-i inactivedays] [-S] [username]
```

較常用的選項有：

- -d ：刪除帳戶密碼。
- -f ：重新設定帳戶密碼。
- -l ：關閉密碼登入，限制使用者帳戶使用。
- -u ：開啟密碼登入，密碼被 –l 關閉後，可使用 –u 重新開放。
- -n mindays：設定密碼變更的最少天數。
- -x maxdays：設定密碼最多使用天數。
- -w warndays：設定密碼過期前，開始警告的天數。
- -i inactivedays：設定密碼過期後，鎖定帳戶的天數。

設定範例如下：

```
# cat    /etc/shadow |grep nien2
nien2:$1$ladMn0AI$4rMA0Fezim/IfeQQY.8a.0:13018:0:99999:7:::
# passwd    -n 8 -x 30 -w 3 -i 7 nien2
Adjusting aging data for user nien2.
passwd: Success
# cat /etc/shadow |grep nien2
nien2:$1$ladMn0AI$4rMA0Fezim/IfeQQY.8a.0:13018:8:30:3:7::
```

上述範例，設定了 nien2 帳戶的密碼參數，其中包含最小天數（-n）、最高天數（-x）、警告天數（-w）與過期天數（-i），並由設定前後的 /etc/shadow 檔案觀察出 nien2 記錄的變化。

【帳戶暫停使用】

許多情況系統管理者會暫停某些帳戶，當然也可能再重新開放。譬如有些系統的使用者

沒有繳交月租費，管理者會暫停該帳戶登入，直到該帳戶補繳費用，再重新開啟。由此可見，此情況的帳戶僅是暫停使用，而非遭到刪除。我們可用 –l 與 –u 選項來達到此功能。關閉帳戶的操作如下：

```
# passwd    -l nien2
Locking password for user nien2.
passwd: Success
```

開啟暫停帳戶的操作如下：

```
# passwd    -u nien2
Unlocking password for user nien2.
passwd: Success.
```

5-5-6 增加群組 - groupadd

增加群組的命令格式如下：

```
groupadd [-g gid [-o]] [-r] [-f] group
```

其中常用的選項有：

- -g gid ：指定群組的識別碼。
- -r ：指定新群組為系統群組。
- -f ：強制執行。無論群組名稱或識別碼是否已存在，皆強制執行產生。

以下範例是產生一個 project 群組，並指定其識別碼為 800：

```
# grep project /etc/group
# groupadd    -g 800 project
# grep project /etc/group
project:x:800:
```

5-5-7 刪除群組 – groupdel

刪除群組的操作範例如下：

```
# grep project /etc/group
project:x:800:
# /usr/sbin/groupdel project
# grep project /etc/group
[root@linux-1 ~]#
```

第一個命令是查閱 /etc/group 檔案內有一筆 project 群組記錄，執行第二個刪除群組命令之後，該筆記錄已不見了。

如同使用者帳戶一樣，也可以針對群組記錄做某些修改，其命令格式如下：

```
groupmod [-g gid [-o]] [-n group_name ] group
```

命令參數也與 groupadd 命令相同，在此便不再另述。

5-6 替代身份

5-6-1 使用者身份替代 -su

使用者登入系統後，可利用 su 命令替代其它帳戶身份，利用 exit 命令返回原登入身份。比較要注意的是，替代他人身份後，目前工作目錄並未改變，可利用 cd 命令切換到家目錄，操作如下：

```
$ whoami                          【查詢目前身份】
student01
$ pwd                             【查詢目前工作目錄】
/home/student01
$ su student02                    【替代身份 student02】
密碼：                            【輸入 student02 密碼】
$ whoami                          【查詢目前身份】
student02
$ pwd                             【查詢目前工作目立】
/home/student01
```

```
$ cd                                    【切換到家目錄】
$ pwd                                   【顯示目前工作目錄】
/home/student02
$ exit                                  【返回原身份】
exit
$ whoami                                【查詢目前身份】
student01
$ pwd                                   【查詢目前工作目錄】
/home/student01
```

5-6-2 管理者身份替代 -sudo

利用 su 替代身份時不指定身份，則是替代 root 身份，如下：

```
$ su                                    【替代身份】
密碼：                                  【輸入 root 密碼】
# whoami                                【查詢目前身份】
root
```

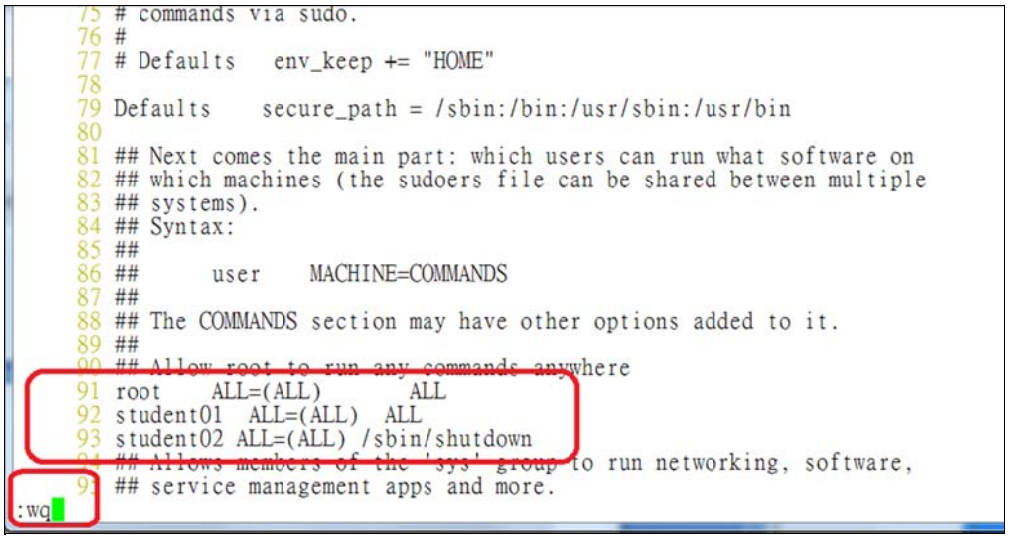
上述操作最大的缺點是需要輸入 root 密碼，root 享有最高權限，知道它的密碼就可以任意操作系統，因此它的密碼不可以隨便讓他人知道。但又有許多系統管理工作需授權與其他使用者操作，如何辦到呢？我們可以利用 sudo 命令將某些管理命令授權給某些帳戶使用。首先須先認識 sudo 的設定檔(/etc/sudoers)，它不可以直接利用 vi 編輯，須利用 visudo 命令編輯，其為了預防兩人以上同時編輯該檔案，操作如下： (執行# visudo 進入 vi 再設定 set number 命令)

```
88 ## The COMMANDS section may have other options added to it.
89 ##
90 ## Allow root to run any commands anywhere
91 root        ALL=(ALL)             ALL     【設定使用者權限】
92 ## student02 ALL=(ALL)ALL                 【設定使用者權限】
93 ## Allows members of the 'sys' group to run networking, software,
```

```
94 ## service management apps and more.
95 # %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE,
     DELEGATING, PROCESSES, LOC              ATE, DRIVERS
96
97 ## Allows people in group wheel to run all commands
98 %wheel    ALL=(ALL)          ALL       【前面有 % 表設定群組權限】
99
100 ## Same thing without a password
101 # %wheel            ALL=(ALL)          NOPASSWD: ALL
```

第 91 行內容是 root ALL=(ALL) ALL，其者 root 表示帳號名稱，第一個 ALL 表示可以在任何主機(可指定主機名稱)，第二個(ALL)表示可以替代任何帳號(可指定其它帳號名稱，第三個 ALL 表示可操作任何管理命令(可指定其它管理命令)。另外，如第 98 行，有 % 記號表示授權給該群組使用者的權利。

假設，我們要授權給 student01 如同 root 般的權限，student02 有關機的權限(/sbin/shutdown)，則利用 visudo 編輯如下：(操作# visudo)



接著，我們再利用 student01 登入系統，看是否具有與 root 相同的權限，如下：(驗證 student01 是否有增加使用者的權限(useradd)

```
login as: student01                              【利用 student01 登入】
student01@120.118.165.120's password:
Last login: Fri Feb  3 10:35:06 2017 from 120.118.165.107
$ sudo useradd student03                         【執行 useradd 命令】

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
```

```
    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for student01:                    【輸入 student01 密碼】
$ cat /etc/passwd |grep student03                 【查閱是否產生 student03】
student03:x:1002:1002::/home/student03:/bin/bash
$
```

習　題

1. 請說明密碼儲存於系統內的技巧如何？

2. 請說明系統驗證密碼是否正確的技巧如何？

3. 請說明使用者與群組之間的關係如何？（一對一、一對多、多對一或多對多的關係）

4. 請說明將使用者劃分群組的功能為何？

5. 請分別說明『一般使用者』與『系統操作者』之間有何不同？

6. 何謂『系統操作者』？並舉一例說明其功能為何？

7. 請說明 su（substitute user）命令的功能為何？舉一例說明之。

8. 請以使用者登入系統的程序，說明 /etc/passwd 檔案的功能為何？

9. 同上題，說明 /etc/shadow 檔案的功能為何？

10. 管理者如果想要授權給某一個使用者，使其具有系統管理者的權限，應如何操作？

11. 當使用者遺失密碼後，求助於系統管理者，系統管理者應如何處置？

12. 請說明正常執行 useradd 命令後，系統應完成哪些工作？

13. 請說明正常執行 userdel 命令後，系統應完成哪些工作？

14. 使用者應如何變更自己的密碼？

15. 系統管理者如何關閉與再開啟某一帳戶，其命令如何？