經濟部資訊專業人員鑑定—開放式系統類

Linux 基礎運作—帳號與程序管理

崑山科技大學資訊傳播系
蔡德明
(鳥哥, VBird)

分享指引

- Linux 的帳號與群組
- 帳號管理與身份切換
- 程序與程序管理
- 程序的nice值功能
- 精選範例

Linux的帳號與群組

帳號功能

- 登入識別碼
  - 人類容易記帳號，但作業系統記得則是識別碼(ID)
  - 將使用者ID(UID)與群組ID(GID)達成對應
    - /etc/passwd → 記錄 UID
    - /etc/group → 記錄 GID

UID範圍

- 使用者ID的意義
  - 0 →系統管理員使用的UID
  - 非爲零 →一般帳號
    - 1-499 →保留給系統用的
      - 1-99 →給系統本身用的帳號
      - 100-499 →給一些網路服務用的帳號
    - 500- →讓可登入者使用的ID

帳號記錄檔

- 帳號的參數檔案分別爲：
  - /etc/passwd →包括家目錄、UID、shell等
  - /etc/shadow →密碼相關資訊
- /etc/passwd 共有七的欄位，以『:』分開
  - 帳號名稱
  - 密碼(已經挪至/etc/shadow)
  - UID
  - GID
  - 全名(這個帳號的說明)
  - 家目錄
  - shell

密碼/etc/shadow格式

- /etc/shadow共分爲九個欄位，第一欄位需與/etc/passwd相對應
  - 帳號名稱，需與/etc/passwd 對應
  - 密碼，加密過的資料，一般使用md5加密機制
  - 最近密碼更動過的日期，使用1970/1/1累積的日數
  - 密碼不可被更動的日期：從密碼最近被更動的日期到下次能夠變更的日期
  - 密碼需重新變更的日期：多久需要重新設定一次密碼
  - 密碼變更前的警告日期：密碼需變更前的幾日發出警告
  - 密碼過期寬恕時間：過期後還能使用的日期
  - 帳號失效日：無論如何，密碼到這個設定值就會失效
  - 保留

群組功能

- 群組設定檔 /etc/group，共分四個欄位
  - 群組名稱
  - 群組密碼(移動至 /etc/gshadow)
  - GID
  - 加入此群組的使用者帳號
- 有效群組與初始群組(initial group)
  - 有效群組：新建檔案時，該檔案的所屬群組
  - 初始群組：寫在/etc/passwd內的GID
- 有效群組的切換
  - 使用 newgrp [group_name]
  - 離開 newgrp 用 exit 即可。

帳號管理與身份切換

新增使用者

```
[root@linux ~]# useradd [-u UID] [-g initial_group] [-G other_group] \
>  -[Mm] [-c 說明欄] [-d home] [-s shell] username
參數：
-u   ：後面接的是 UID ，是一組數字。直接指定一個特定的 UID 給這個帳號；
-g   ：後面接的那個群組名稱就是我們上面提到的 initial group 啦～
       該 group ID (GID) 會被放置到 /etc/passwd 的第四個欄位內。
-G   ：後面接的群組名稱則是這個帳號還可以支援的群組。
       這個參數會修改 /etc/group 內的相關資料喔！
-M   ：強制！不要建立使用者家目錄
-m   ：強制！要建立使用者家目錄！
-c   ：這個就是 /etc/passwd 的第五欄的說明內容啦～可以隨便我們設定的啦～
-d   ：指定某個目錄成為家目錄，而不要使用預設值；
-r   ：建立一個系統的帳號，這個帳號的 UID 會有限制 (/etc/login.defs)
-s   ：後面接一個 shell ，預設是 /bin/bash 的啦～
```

- 建立系統帳號 → useradd –r account
- 建立不可登入的帳號 → useradd –s /sbin/nologin account

新增使用者的參考資訊

- /etc/default/useradd
  - 指定shell, 主要家目錄, 初始群組及家目錄參考來源目錄之資料
- /etc/skel/*
  - 預設的家目錄參考來源目錄，可由 /etc/default/useradd 修改
- /etc/login.defs
  - 最大及最小的UID/GID設定
  - 密碼相關資訊的指定

密碼設定

- 密碼的設定與修改
  - 密碼設定：以root身份『passwd account』
  - 密碼修改：使用者自己下達『passwd』
- 密碼參數的查閱
  - chage –l
- 強制使用者初次登入需修改密碼的方法
  - chage –d 0 account

使用者參數修改/刪除

- 需以root身份處理
  - 刪除使用者用 userdel [-r] username
  - 修改使用者用 usermod

```
[root@linux ~]# usermod [-cdegGlsuLU] username
參數：
-c   ：後面接帳號的說明，即 /etc/passwd 第五欄的說明欄，可以加入一些帳號的說明。
-d   ：後面接帳號的家目錄，即修改 /etc/passwd 的第六欄；
-e   ：後面接日期，格式是 YYYY-MM-DD 也就是在 /etc/shadow 內的第八個欄位資料啦！
-g   ：後面接 group name，修改 /etc/passwd 的第四個欄位，亦即是 GID 的欄位！
-G   ：後面接 group name，修改這個使用者能夠支援的群組，修改的是 /etc/group 囉~
-l   ：後面接帳號名稱。亦即是修改帳號名稱， /etc/passwd 的第一欄！
-s   ：後面接 Shell 的實際檔案，例如 /bin/bash 或 /bin/csh 等等。
-u   ：後面接 UID 數字啦！即 /etc/passwd 第三欄的資料；
-L   ：暫時將使用者的密碼凍結，讓他無法登入。其實僅改 /etc/shadow 的密碼欄。
-U   ：將 /etc/shadow 密碼欄的 ！ 拿掉，解凍啦！
```

群組處理

- 群組的建立
  - groupadd [-g gid] group_name
- 群組的修訂
  - groupmod [-g gid] [-n name] group_name
- 群組的刪除
  - groupdel group_name
  - 此群組不可是某帳號的初始群組，才能被刪除

使用者身份參數自我修改

- 常見可修改/觀察的指令
  - 修改 shell 的方法：
    - chsh –s shell
  - 查閱/修改使用者的註解說明
    - finger username
    - chfn
  - 查閱使用者的UID/GID
    - id [username]
  - 查閱使用者支援的群組
    - groups

用 su 切換身份

- 使用 su 切換身份須知
  - 需要知道被切換者的密碼
  - root可切換成爲任何人，不需原使用者密碼
  - 最好加上 – 才能夠讀取使用者的環境設定檔
    - su – [username]
  - 在多人共管的環境中，可能有很多人會知道root的密碼，理論上是比較不安全些。

使用sudo操作系統指令

- 可用sudo來操作系統指令，語法如下：
  - sudo [-u username] command
- 可使用 sudo 的使用者需規範於 /etc/sudoers
  - /etc/sudoers 不可直接編輯
  - 使用visudo可編輯/etc/sudoers

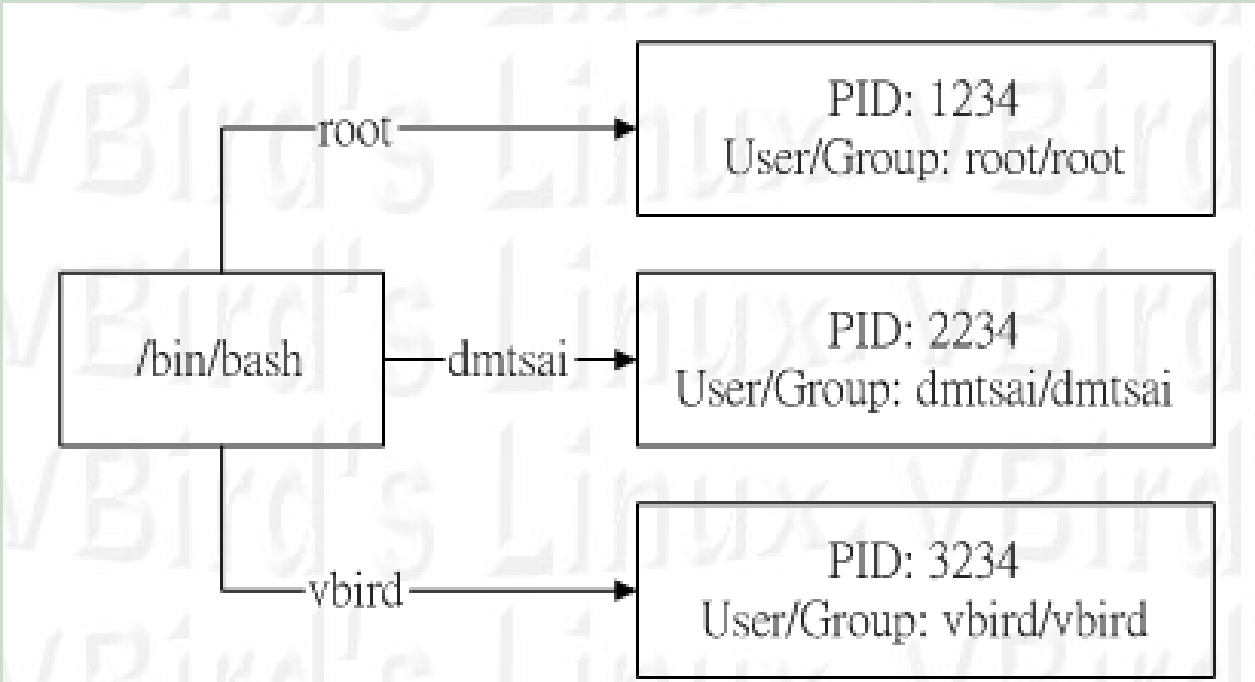
程序與程序管理

程式與程序

- 程式 (program)
  - 通常爲binary program，是作業系統可以執行的檔案資料，如/bin/ls
  - 程式通常放置於硬碟/光碟/軟碟等儲存設備
- 程序 (process)
  - program被系統觸發後，其程式碼會被載入記憶體中，同時會載入該程式所需的資料，及執行者的相關屬性/權限資訊
  - 系統會給予該段記憶區段一個識別碼，稱爲PID
  - 一個program可被同時觸發多次，彼此間不會互相干擾，因爲PID並不相同。

程序執行的範例

- 問：爲何大家登入都是使用/bin/bash，卻不會互相干擾？



圖一、程式與程序之間的差異

程序的相關性

- 系統執行的第一支程序：init (/sbin/init)
  - 此程序的PID爲 1
  - 系統所有的其他程序都由此 PID 所衍生
- 子程序與父程序
  - 被衍生的程序成爲子程序
  - 子程序會再含有一個 PPID，代表父程序的PID
  - 當父程序結束時，所有的子程序亦將被結束

程序的管理

- 使用 ps 查閱
  - ps –l
    - 只看bash自己的程序
  - ps aux
    - 看所有的程序，包含背景中的各項程序資料

- USER：屬於那個使用者帳號
- PID ：程序的號碼。
- %CPU：使用掉CPU資源百分比
- %MEM：所佔用記憶體百分比
- TTY ：是在那個終端機上面運作
- STAT：該程序目前的狀態，主要的狀態
  - R ：目前正在運作
  - S ：目前正在睡眠當中
  - T ：目前正在偵測或是停止
  - Z ：殭屍程序
- START：被觸發啓動的時間
- TIME：實際使用CPU運作時間
- COMMAND：實際指令

動態觀察程序

- 使用 top 囉

```
[root@linux ~]# top [-d] | top [-bnp]
參數：
-d   ：後面可以接秒數，就是整個程序畫面更新的秒數。預設是 5 秒；
-b   ：以批次的方式執行 top ，還有更多的參數可以使用喔！
       通常會搭配資料流重導向來將批次的結果輸出成為檔案。
-n   ：與 -b 搭配，意義是，需要進行幾次 top 的輸出結果。
-p   ：指定某些個 PID 來進行觀察監測而已。
在 top 執行過程當中可以使用的按鍵指令：
        ? ：顯示在 top 當中可以輸入的按鍵指令；
        P ：以 CPU 的使用資源排序顯示；
        M ：以 Memory 的使用資源排序顯示；
        N ：以 PID 來排序喔！
        T ：由該 Process 使用的 CPU 時間累積 (TIME+) 排序。
        k ：給予某個 PID 一個訊號 (signal)
        r ：給予某個 PID 重新制訂一個 nice 值。
```

程序樹相關性與程序的刪除

- pstree [-pu]
- 程序的刪除
  - 給予程序一個訊號(signal)，常見的訊號
    - kill –l
    - man 7 signal
      - 1) SIGHUP　　重新讀取設定檔(reload)
      - 9) SIGKILL　　強制將某程序從記憶體中移除
      - 15) SIGTERM　　嘗試以正常流程將程序關閉
    - kill -9 12345
  - 給予某指令一個訊號
    - killall -9 command

程序的nice值功能

程式的執行順序

- ps –l

```
F S   UID   PID  PPID  C PRI  NI ADDR SZ WCHAN  TTY          TIME CMD
0 S   500  4663  4662  0  76   0 -  1351 wait   pts/0    00:00:00 bash
0 R   500  4788  4663  0  78   0 -  1244 -      pts/0    00:00:00 ps
```

- PRI (Priority, 優先執行順序)
  - 越小越早被CPU所執行
  - 爲核心動態調整，不會一直是固定的
- NI (Nice, 可修改 PRI)
  - PRI(new) = RPI(old) + Nice
  - Nice越小可讓PRI變小，所以越快被CPU所執行
  - Nice 範圍爲 -20 ~ 19
  - nice 只有 root 可以設定爲負值
  - 使用者只能將nice越調越高，且只能調整自己的PID

nice值的使用

- 新執行的指令，使用 nice
  - nice –n NI command
    - ex> nice –n 10 bash
- 從已經存在的PID修改其nice值
  - renice NI PID
    - ex> renice -5 12345
  - top
    - 按下 r 即可選擇 PID 與 Nice 值了

精選範例

- 想產生一個不用登入密碼的帳號 guset ，何者正確？ BC
  - (A) 輸入 useradd guest 即可免密碼登入
  - (B) 輸入 useradd –p ‘’ guest
  - (C) 輸入 useradd guest; passwd –d guest
  - (D) 輸入 useradd guest; passwd –p ‘’ guest

- 下列何者可使使用者 foo 無法登入系統？ ABC
  - (A) useradd –s /sbin/nologin foo
  - (B) usermod –s /bin/true foo
  - (C) usermod –s /bin/false foo
  - (D) useradd –s /sbin/tcsh foo

- 若要把某個檔案的權限改爲 Owner 可讀寫，其餘可讀，應如何處理？ B
  - (A) chmod 755
  - (B) chmod 644
  - (C) chmod 722
  - (D) chmod 622

- 關於記錄使用者帳號的 /etc/passwd 下列敘述何者有誤？C
  - (A) 該檔案裡面一行代表一個使用者帳號
  - (B) 裡面記載了某一帳號登入後要使用哪一個shell
  - (C) 該檔案也記載了帳號的失效日期
  - (D) 該檔案中不會有兩個相同的使用者別碼 (UID)

- 關於程序的描述下列何者有誤？A
  - (A) 如果A程序的PID與B程序的PPID相同，則A程式是B程序的子程序
  - (B) 使用pstree可以察看每個程序之間的相關性
  - (C) 系統中執行程序所擁有的權限與該程序的執行者權限有關
  - (D) 每一個系統中執行的程序都會有一個PID，而且這個PID不會重複

- 關於SUID(SetUID)的描述下列何者有誤？B
  - (A) SUID的權限設定只對二進位檔案有效
  - (B) 一般使用者執行passwd指令來修改密碼時，passwd程序的權限就是執行者的權限
  - (C) 使用者執行具有SUID的檔案時，該檔案執行中的權限與該檔案的擁有者的權限相同
  - (D) 使用find /home –perm -4000 可查詢具有 SUID 權限的檔案

- 有關 Linux 的程序觀念，下列哪些正確？ ABC
  - (A) 所有程序都是由 init 這一個程序分出來的，或再分出來的
  - (B) 子程序都是由父程序分出來的
  - (C) 程序就是只執行中的程式
  - (D) 程序和程序之間完全獨立，無法互相溝通