Linux帳號權限之管理

鳥哥

2015/11/03

開始之前-如何取得一個雲端系統？

- 點選桌面上的 gocloud64 軟體
- 輸入帳號密碼為：
  - mynckuxx / nckuuser
- 選擇正確的 HDD 來開機
- 就會出現 Linux 系統桌面了

開始之前-如何登入 Linux 呢？

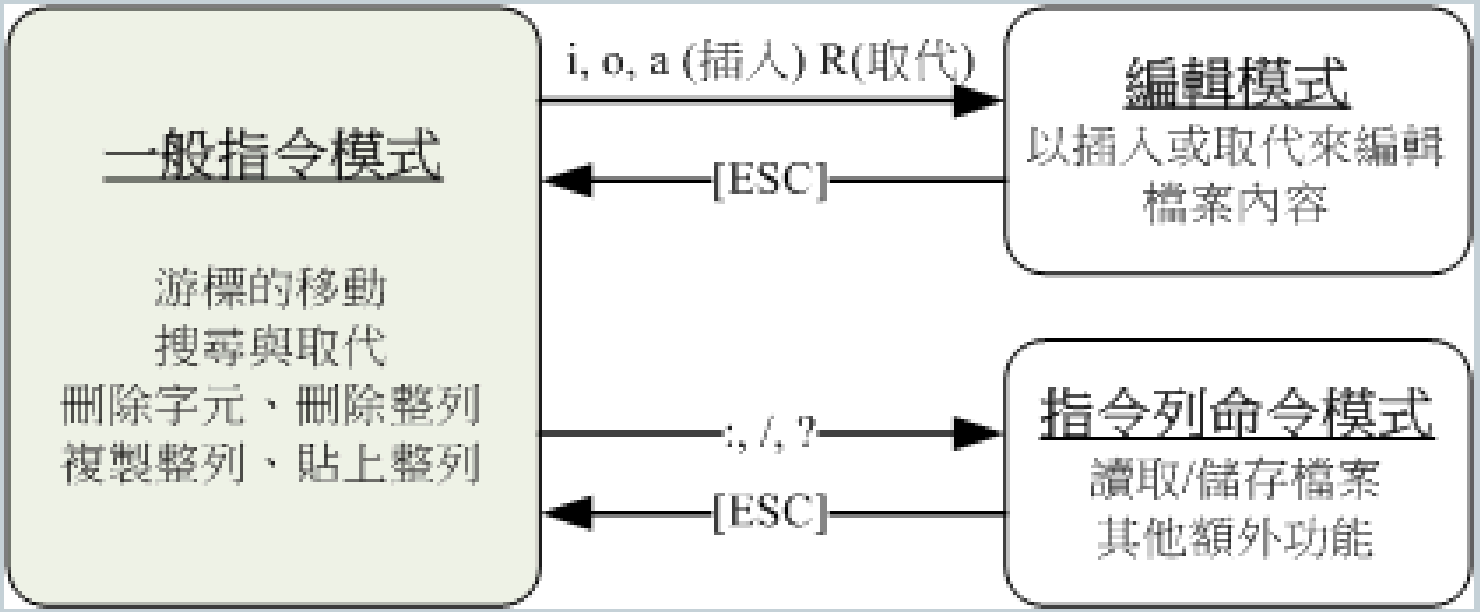
- 圖形界面：
  - 點選出現的帳號，輸入鳥哥告訴你的這個密碼
  - 然後你就依序處理你的登入流程即可
- 文字界面：
  - 可以按下 [Alt]+[Ctrl]+[F2]~[F6]
  - 出現 login: 時，輸入剛剛提到的帳號
  - 出現 password: 時，輸入剛剛提到的密碼
  - 出現 [username@hostname ~]$ 就是登入了！

開始之前-常用的終端機熱鍵有哪些？

- 請愛用 [tab] 按鈕
  - 指令補齊
  - 檔名補齊
  - 選項補齊
- 請愛用 history 查詢
- 請愛用 上/下/左/右 按鍵來修改你的指令內容
- 請愛用 command --help 來查詢可用選項與功能

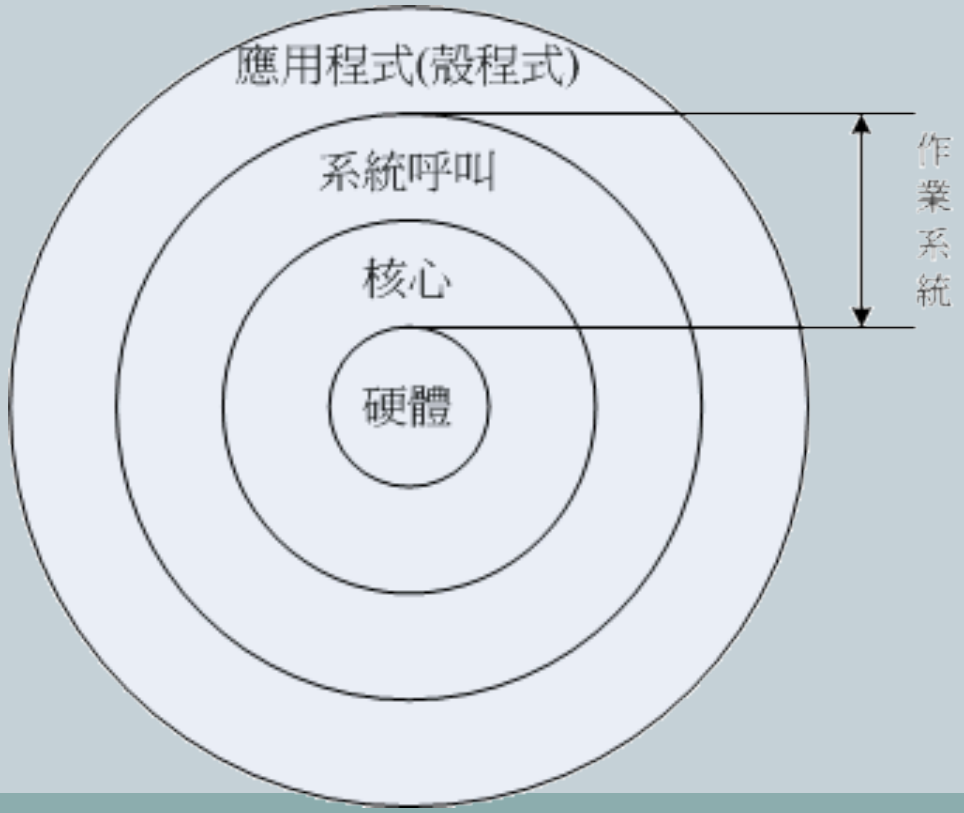
開始之前-學一下 vim 吧

- vim filename



為什麼 Linux 版本這麼多？

- 其實僅有 http://www.kernel.org 有提供 Linux 耶
- Linux 與硬體、軟體間的關係為：



那什麼是Red Hat/Fedora/SuSE/Debian/CentOS?

- Linux kernel + Software + Tools + Installation
  - Distributions
- 硬要分類的話：
- 伺服器請用 CentOS/Debian 等

	RPM 軟體管理	DPKG 軟體管理	其他未分類
商業公司	RHEL (Red Hat 公司) SuSE (Micro Focus)	Ubuntu (Canonical Ltd.)	
社群單位	Fedora CentOS OpenSuSE	Debian B2D	Gentoo

為什麼架站需要學系統？

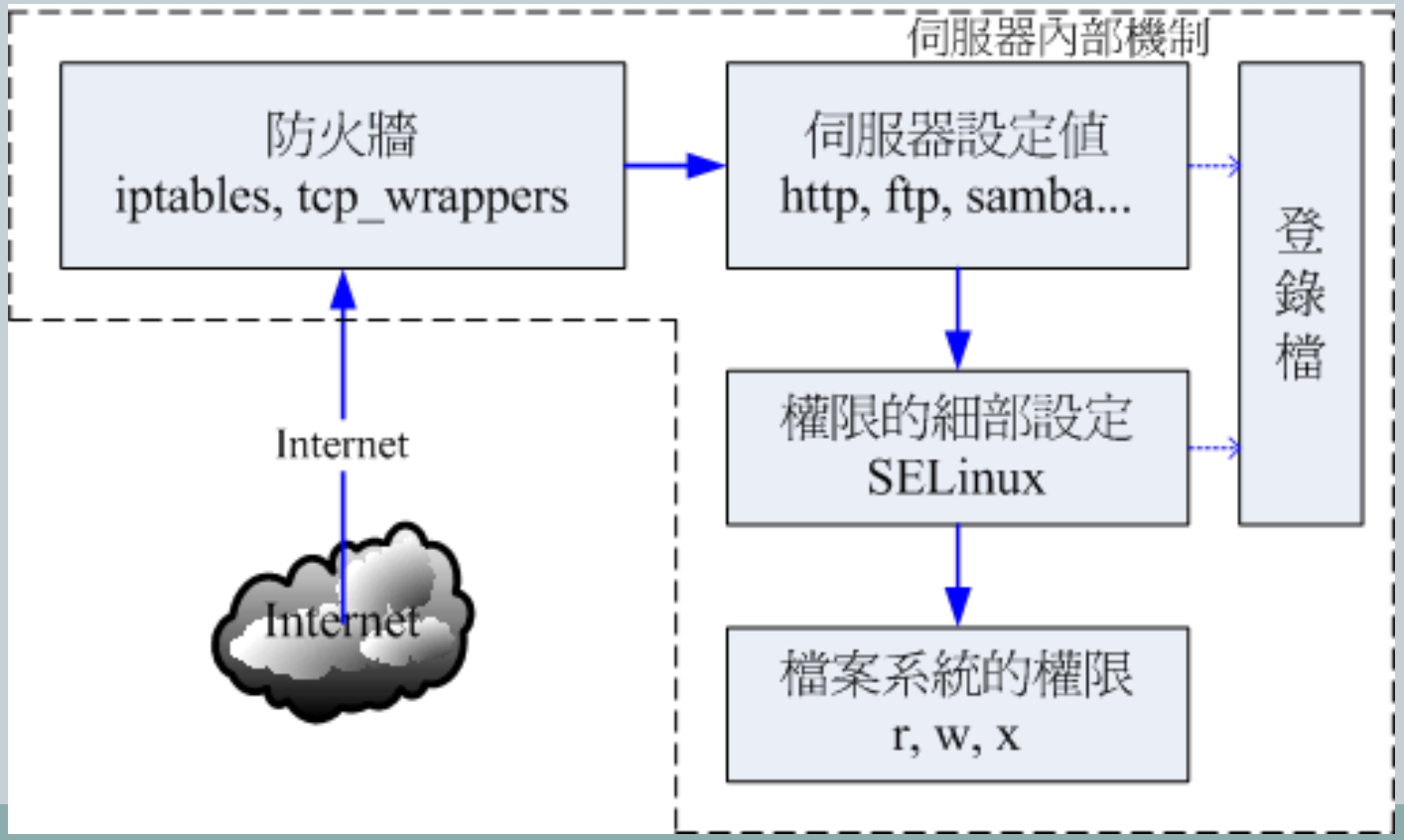
- 以 apache 這個 WWW 為例：
  - 你總是得要有足夠的磁碟空間，但，如何規劃分割槽？
  - 你總是得要提供某些人管理，但如何設計帳號？
  - 你總是得要啟動這個服務，但如何安裝？如何啟動？
    - 新的 systemd 與舊的 systemV 差很多很多....
  - 你總是得要學會防火牆的管理
  - 你總是得要學會核心提供的某些防火牆功能
  - 系統總有出錯的時候，出錯時，你總得要分析錯誤發生的原因然後去克服它！
  - 所以！學Linux系統總是沒錯的！

為什麼需要學會管理權限？

- 回到最原始的話題，架站的目的是要幹麻？
  - 分享你的檔案系統
  - 分享你的網頁資料/照片/成果
  - 儲存你的重要資料
  - 提供用戶上傳/下載你需要的資料
  - 所以，無論如何，就是需要『資料！』
- 因此：
  - 資料放在哪裡？誰能夠讀寫？誰只能讀？誰不能有權限？
  - 如何讓一群人可以讀寫？如何讓一個人可以讀寫？
  - 權限有哪些？目錄/檔案的權限是否相同？
  - 就得要了解了解！

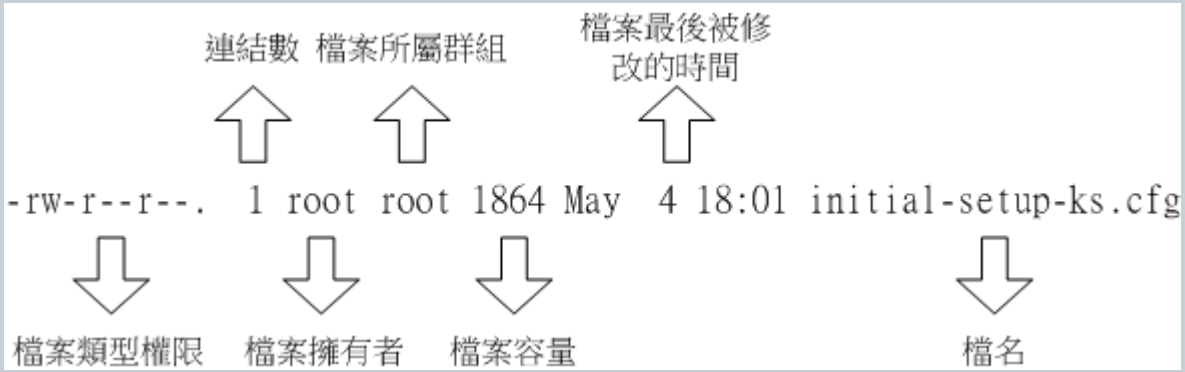
能不能說說權限/架站間的流程關係？

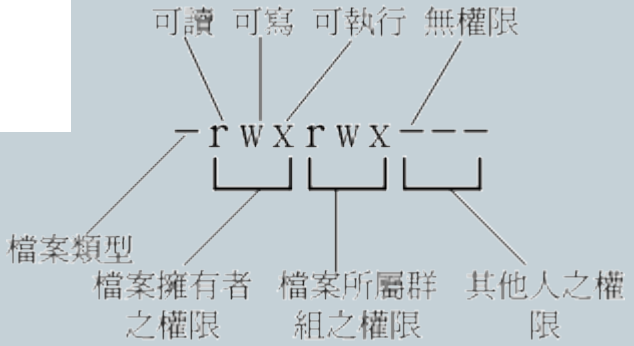
- 來看看目前 CentOS 這個東西用了什麼步驟讓妳可以存取資料呢？



Linux 的權限有哪些？

- 請打開一個終端機，輸入 ll 這個指令來瞧一瞧
- 請注意『身份』有哪些？
- 請注意每種身份的權限有哪些？
- 請注意基本的檔案格式有哪兩個？





權限在不同檔案類型上，有何差異？

元件	內容	疊代物件	r	w	x
檔案	詳細資料data	文件資料夾	讀到文件內容	修改文件內容	執行文件內容
目錄	檔名	可分類抽屜	讀到檔名	修改檔名	進入該目錄的權限(key)

來看看真的了解了嗎？

- 有個檔案 /dir1/file1
- 有個目錄 /dir2
- 回答問題：
  - 要讀到 file1 需要有什麼權限？
  - 要可寫入 file1 需要有何權限？
  - 需要執行 file1 呢？
  - 要將 file1 複製到 /dir2 又需要什麼權限？
  - 要刪除 file1 又需要什麼權限？

來認真玩一玩

- 開始之前：如何切換身份？
  - su -
  - sudo su -
- 使用 root 身份，建立如下資料
  - cd ~dic
  - cp /etc/hosts .
  - chmod ooo hosts
- 使用 dic 帳號觀察
  - 能不能讀/寫/執行/刪除該檔案？
  - 與前幾個表格對照思考一下！

那群組又有什麼功能？

- 系統的權限其實主要都是針對『使用者』喔！
- 但如果是為了方便起見，規定『某一群使用者』能夠使用的權限，不是比較單純嗎？
  - 舉例來說，規定電腦社的社員都可以進出計中
  - 則：只要看使用者有沒有加入電腦社即可判斷！
  - 所以，最終能夠進入計中的，當然就是加入電腦社的『使用者』
- 依據不同的班級/社團，規範不同的權限，再將使用者加入到它應該去的班級/社團，這樣就搞定了！

一個重要的群組

- 目前 CentOS 7 當中，一個用戶能不能使用 sudo 這個指令，與他有沒有加入 wheel 群組有關喔！
- 那如何建立一個使用者後，讓他加入 wheel 群組呢？
  - 建立使用者： useradd 帳號
  - 增加群組： usermod -a -G 群組 帳號

專題常用帳號/群組類型

- 建立三個用戶，讓三個用戶加入到某個次要群組去就對了啊！
  - 建立群組： groupadd
  - 建立用戶： useradd / passwd

專題組員彼此間的資料共享呢？

- 上述三個用戶要共享 /srv/project 要怎麼辦？
  - 建立目錄
  - 修改權限
  - 測試一下
    - 很重要！第一個使用者建立的資料，第二個使用者能不能讀/寫呢？
    - 要如何處理？這就是共享目錄的重要性！
- 這個問題經常發生於 SAMBA 的資料分享中！！！

如何保障檔案系統不會被充爆？

- 所以分割就很重要啊！
  - 要注意，一般用戶可以讀寫的區段，最好都獨立分割
  - 重點是 /usr, / 這兩個不要被搞到 100% 的使用率...
  - /tmp, /var, /home 當然最好就是要獨立分割啊！
- 所以 quota 就很重要啊！
  - 放行檔案系統支援 /etc/fstab 加入 usrquota,grpquota
  - 將 /home 卸載再掛載
  - 開始設計：
    - xfs_quota -x -c "limit -u bsoft=250M bhard=300M user1" /home
  - 檢查看看： xfs_quota -x -c "report -ubh" /home

大量建立帳號要如何處理？

- 透過腳本處理
- for ... do ... done
  - useradd
  - passwd --stdin
  - xfs_quota -x -c "limi....

針對單一用戶來設計權限的可行性？

- 例如 /srv/project 中，某一個用戶需要登入查閱而已，其他權限不可放行。那你又該如何處理？
  - 只能透過 acl 來處理！
  - setfacl -m u:帳號:權限 目標檔案
  - getfacl 目標檔案

最後來想想

- 你有一整個班級的學生，每個學生要有自己的帳號，這個帳號可以在家目錄裡面建立各自的網頁！
- 為了系統安全，每個學生只能有 100MB 的空間
- 若要讓學生的資料可以被瀏覽到，那麼學生家目錄的權限該如何設計？
- 全部的資料寫成腳本的可行性呢？

結論

- 對於架站來說，帳號管理/權限管理是相當重要的！
- 其實，權限也是離不開檔案系統的！
- 要活用Linux預設的實體帳號可以使用的很多功能！
  - 包括 apache 的每個用戶均可取得個人首頁的功能！
  - 包括 FTP 讓每個用戶可以獨立上傳/下載資料～
  - 包括讓 FTP 與 WWW 結合～
  - 包括讓 SAMBA 與 WWW 結合
  - 包括讓專題共享所需目錄等等
- 有空來幫鳥哥 debug 吧！
  - http://linux.vbird.org/linux_basic