

資訊安全與實務操作簡介

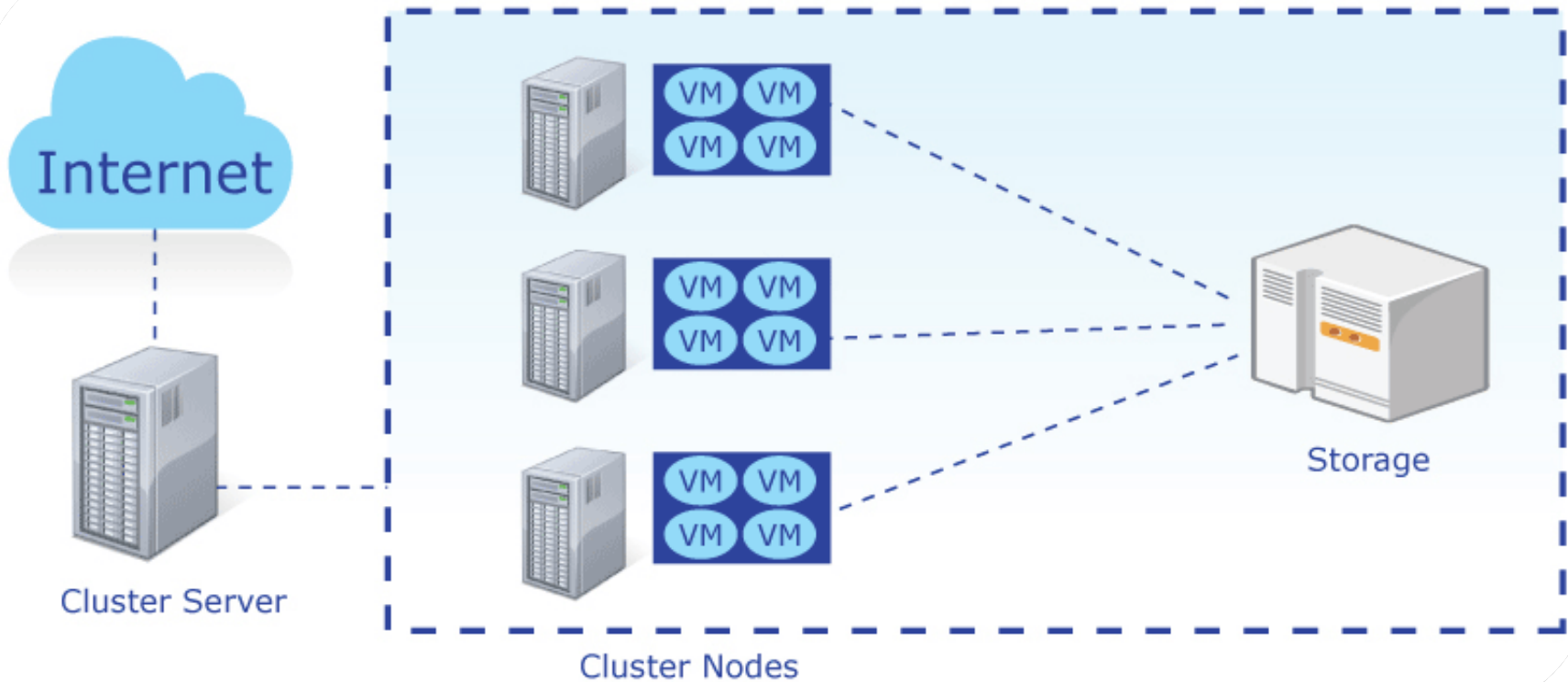
崑山科大資傳系蔡德明(VBIRD) 2017/5/25

鳥哥最近搞什麼？

- 可以遠端進行破壞性作業系統教學
 - 雲虛擬教室，提供學生連線上課使用
 - 小型辦公室環境系統，提供中小企業使用一部主機建置虛擬化環境
 - 無論如何，應該都會用到比較昂貴一些的硬體配備
 - 使用 64GB 以上大容量記憶體的主機系統
 - 與一般系統提供的虛擬化環境差異：
 - 使用 images file 模擬虛擬化系統的硬碟，使用快照來快速複製
 - 透過網頁伺服器搭配 PHP 提供會員系統，會員可以自行管理自己的硬碟，可以自行啟動/關閉/復原自己的 VM 系統。
 - 預計年底會釋出一個小型辦公環境的可安裝版本

鳥哥最近搞什麼？

- 雲虛擬電腦教室示意圖

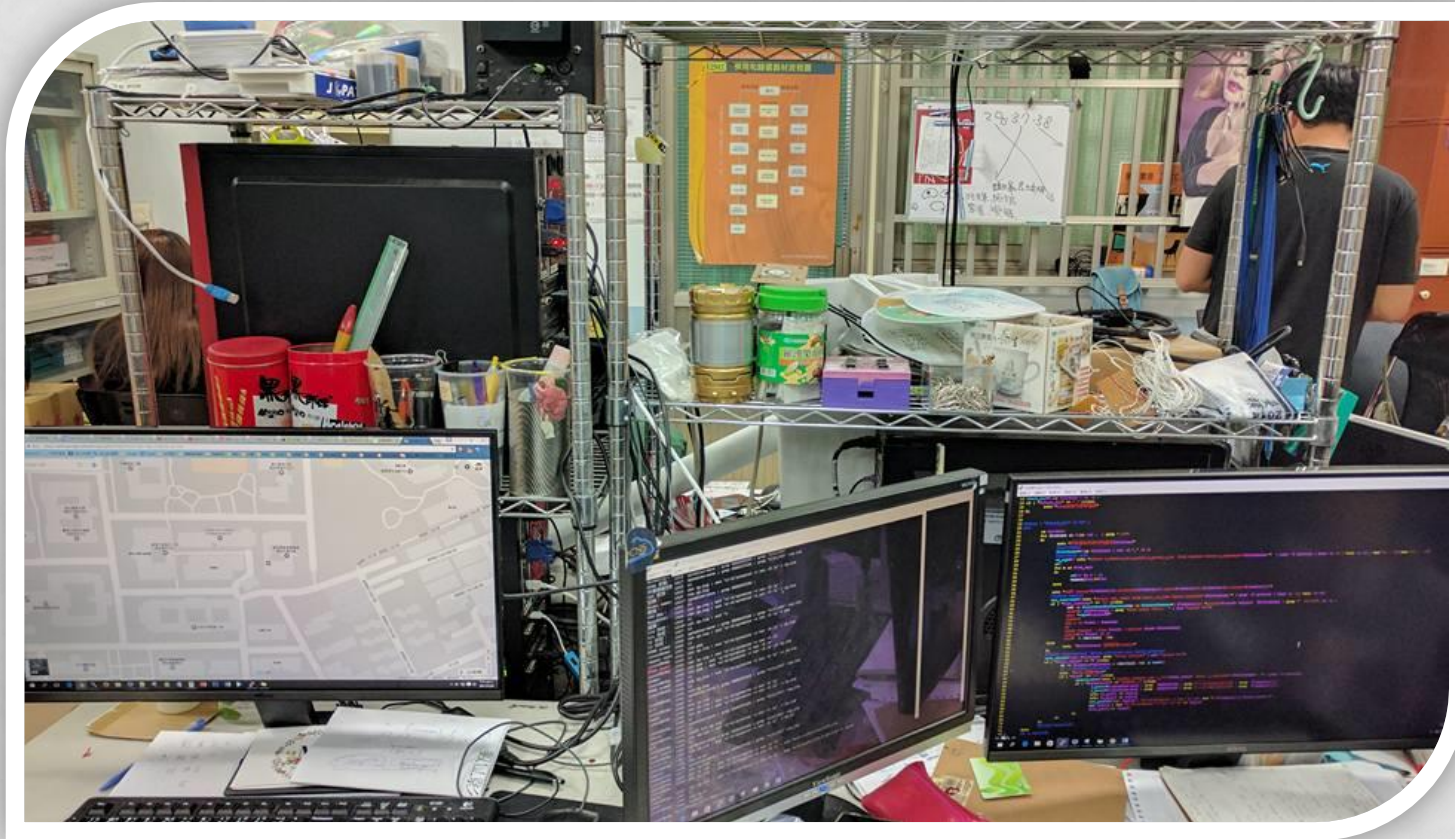


鳥哥最近搞什麼？

- 可以節省資源的 PC 系統
 - 透過 Linux 核心 patch 過後支援的 VFIO 功能
 - 讓一部實體 PC 安裝兩張顯示卡、兩個獨立的 USB 晶片
 - 就可以提供兩部邏輯上完全獨立的 VM。且由於使用獨立顯卡與獨立 USB，因此顯示效能相當良好，同時也能夠直接支援物理 USB 的直接傳輸
 - 使用 25 部實體主機就能夠提供 50 個學生來操作的環境：
 - 25 部主機需要額外的記憶體、顯示卡與 USB (所以要先看主機板)，但是額外增加的費用並沒有很高啊！
 - 而可以節省 25 部實體主機，這個省下來的 \$\$ 就很可觀了！
 - 而且因為是 VM，因此與雲系統一樣，具有方便管理的特性！

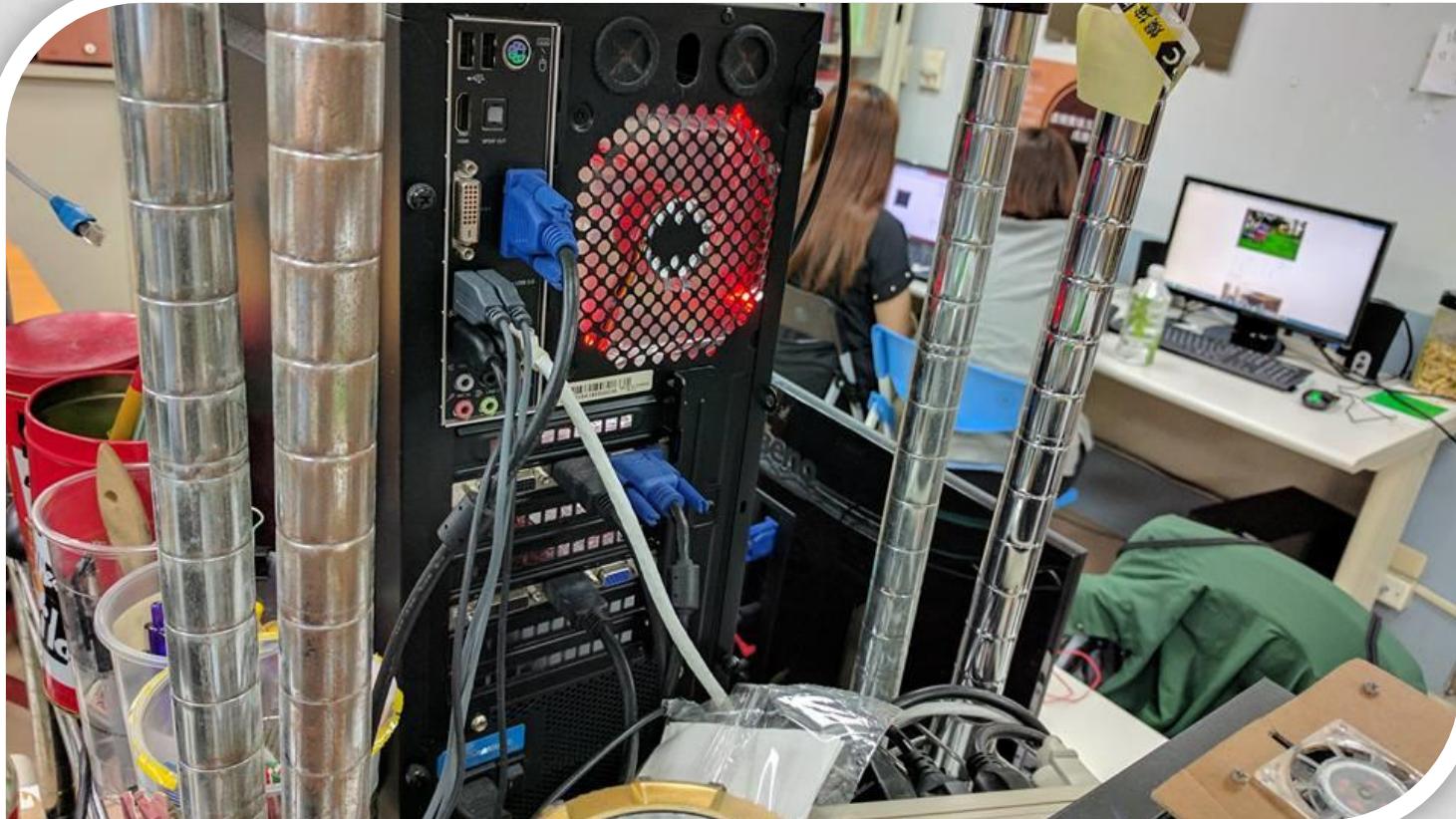
鳥哥最近搞什麼？

- 可以節省資源的 PC 系統
 - 其實，已經完整的實做在鳥哥自己的實驗室當中了！



鳥哥最近搞什麼？

- 可以節省資源的 PC 系統
 - 其實，已經完整的實做在鳥哥自己的實驗室當中了！



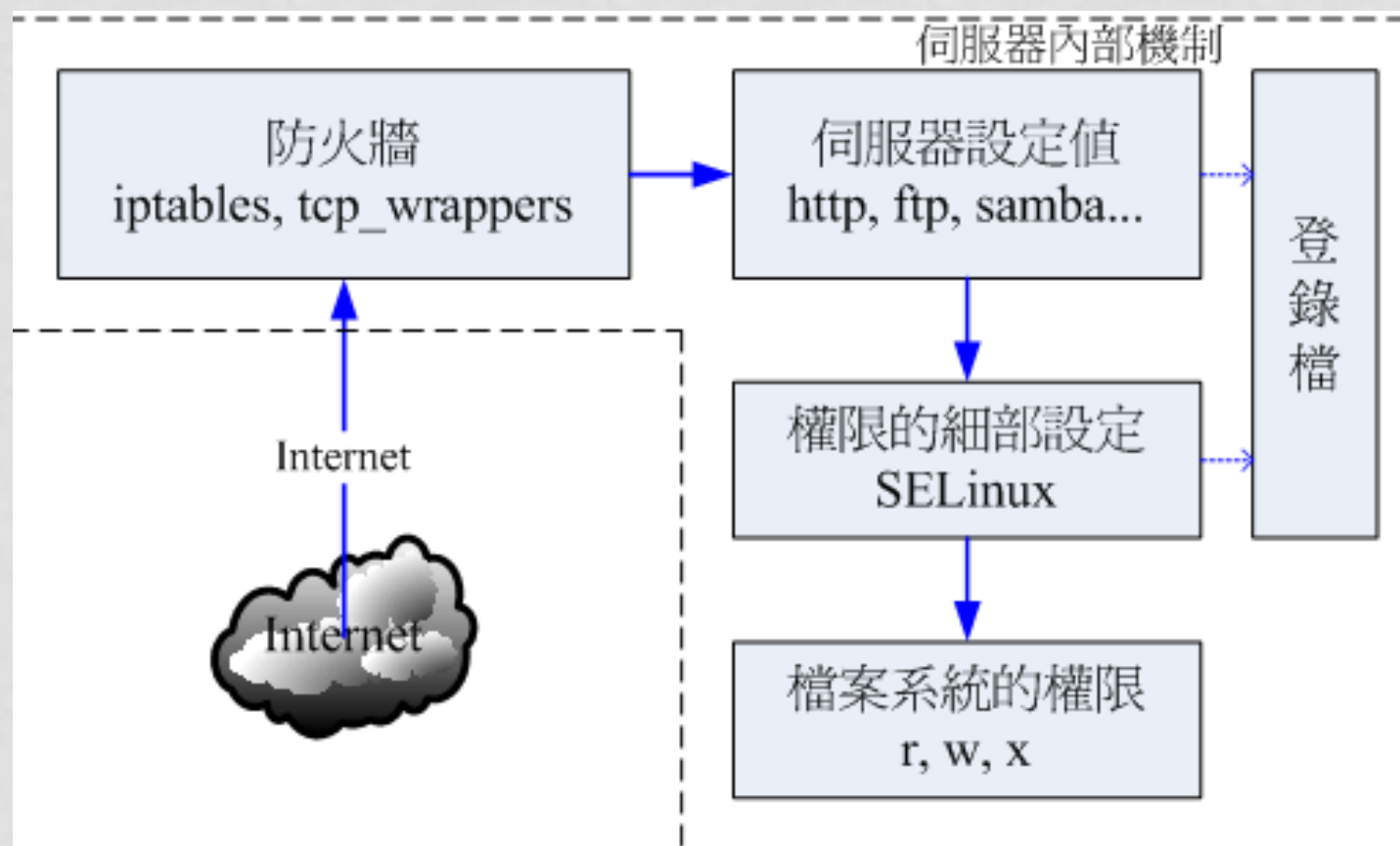
先來談談資訊安全

什麼是電腦『資訊』與『安全』

- 資訊：
 - 你的資料放置在電腦上面，該資料很重要，那就是資訊
- 安全：
 - 這些資訊可能在任何管道被不法取得，因此，如何讓你的電腦可以保障這些資訊，那就是安全。
 - 當然，也有可能是因為硬體的問題，導致資訊的損毀，這也是造成『安全』的一項隱憂。

想一想，你如何取得這些資訊

- 取得電腦資訊的基本流程架構(Linux為例)



想一想，你如何取得這些資訊

- 物理性接觸
 - 可以直接的接觸電腦，例如你的桌機、進入機房操作系統等
 - 相當於上一頁可以直接碰觸到檔案系統的狀態(個人桌機)
- 網路上取得
 - 需要網路(無論是 LAN 還是 WAN)來連線到你的桌機或伺服器
 - 上一頁的流程中，你需要經過：
 - 透過有線、無線等方式，連接到 LAN 或 WAN 之後，接觸到你的電腦
 - 你的電腦需要放行你的連線(防火牆)
 - 你的電腦要有對應的軟體服務 (遠端桌面？網頁伺服器？FTP？)
 - 認證之後進入系統取得檔案系統服務 (當然，也有可能是資料庫)

分析資安可能的危機

- 硬體：
 - 硬體一點也不重要，重要的是裡面的『資訊！』
 - 有沒有發生過『硬碟損毀』或者是不經意的『rm -rf /』呢？
 - 所以，硬體(尤其是硬碟)需要有容錯功能，而最好有備份機制
 - 另外，硬體的遺失問題也很嚴重(手機、桌機送修時的問題)
- 軟體：
 - Server一定要開放防火牆以及相對應的軟體給用戶連線
 - 那這個軟體如果出問題時，怎辦？
 - 那負責這個軟體的作業系統如果出問題，怎辦？
- 網路：
 - 服務要不要放行？資料要不要加密？這都是問題

資安基本考量

- 硬體：

- 誰可以物理接觸我的伺服器？須不須要身份管控？要不要封閉 USB 與光碟等裝置？需要加裝不斷電嘛？BIOS需要加上密碼嘛？
- 是否需要磁碟容錯的機制？是否需要磁碟備份的機制？

- 軟體：

- 使用什麼作業系統來提供相對應的服務？系統是否為正版？有沒有辦法隨時保持在最新的狀態？何時需要重新開機等
- 密碼設定難道可以依據不同的身份來簡化？相對可怕的服務是否一定要對整個 WAN 放行？相對應的軟體有沒有辦法保持最新狀態？
- 針對網路來的非官方軟體，是否完全理解以及查詢過相關的漏洞史？使用的第三方軟體是否為最新版？相關軟體使用的系統權限是否合理？

身邊常見的資安事件

事件一-磁碟損毀事件

- 鳥哥自己的家庭用桌機，從碩士班讀書到目前為止，一堆雜物都在上面
 - 某天，號稱很強的 WD 黑標硬碟突然發生怪聲音
 - 然後就...再也無法開機了！
 - 如然想到，前一次備份已經是兩年前的事....
 - 只好將硬碟整個寄到台北去進行救援

事件二-專題建置的測試系統被炸

- 導因：

- 學生在做專題期間，擔心專題電腦出事，因此使用虛擬機器模擬一個與專題相同的環境來測試
- 為了可以在家裡連線到虛擬機上面工作，因此打開恐怖的 ssh 服務
- 學生以為是虛擬機，『應該』不會被攻擊吧！
 - 所以 ssh 的埠口沒有限制進入的來源
 - 所以 root 的登入權限並沒有限制
 - 所以 root 的密碼選擇使用 123456
- 所以，指導老師就被計算機中心追殺了....
- 攻擊手法：
 - 猜到了 root 的密碼(使用輪詢方式不斷的猜測 root 密碼的手段)
 - 取得 root 權限後，安裝了許多莫名的軟體來作為跳板

事件三-搭建網頁伺服器導致被駭

- 導因：

- 學生參與暑期實習，協助廠商處理網站的建置。為了方便未來曠交給廠商進行後台管理，因此選擇 Wordpress 搭建
- 問題一：
 - 因為想說給廠商方便，所以網址、帳號、密碼通通設定相同
 - 結果...才剛剛上線，立刻被猜到密碼...還好資料通通是可公開的～
- 問題二：
 - 帳密終於設定的比較嚴謹，但隔幾天又有資安通報送到指導老師手上了...原因是，Wordpress 無論新舊版本，都有一個後台快速登入的檔案，該檔案撰寫有漏洞，導致攻擊者可以直接接觸該軟體，就此直接取得管理員權限
 - 透過 paper search 找到某些檔案，將這些不必要的資料移除就好了
 - 也可以加裝某些限制的軟體來處理

事件四-WWW懶人包的問題

- 導因：
 - 很多系所的專題、碩士生，為了方便架設網站，往往直接在 Windows 桌機系統上面就安裝 WWW 懶人包，例如 Appserv
 - 但是 Appserv 就是個第三方協力軟體，本身好像沒有自動升級的機制存在
 - 而且為了讓使用者快速上手，所以太多的功能都非常的 friendly，當然，不只對用戶 friendly，對 cracker 來說，也真是太 friendly！
 - 每年的暑假，各系的老師們，手上的資安通報都多到爆表...

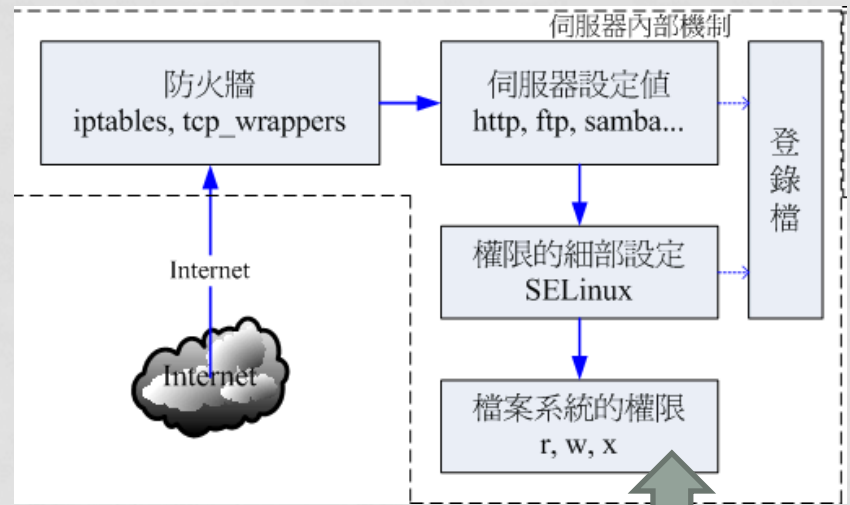
事件五-2017年初的勒索病毒事件

- 導因：

- 駭客要賺錢，所以開發了勒索病毒，讓一般桌機的『資訊』被鎖
- 主要攻擊的方式，先讓使用者點擊某些網站，並示意用戶自行安裝勒索病毒的軟體 (這個好常見啊！社交攻擊！)
- 該病毒入侵後，也會主動的攻擊區網內的 port 445，若你的 port 445 上面的軟體沒有更新，那就會被攻擊成功，你的桌機也開始被加密鎖住
- 這主要是針對 windows 沒有設定自動更新所導致的問題 (因為五月份爆發，但是該漏洞在 3 月份已經釋出更新了！)

事件六-只要有心，人人都可以是駭客

- 來自 Moto 討論區的一個小故事：
 - 早期的工程師之間討論，都用聊天室 (IRC)
 - 這是一個德國工程師在 IRC 裡面遇到的小故事！
 - [moto_phorum.htm](#)
- 來自鳥園(鳥站討論區)的一個故事：
 - 只是因為某個陸客小白般的發問，被版主打臉之後，找朋友來洗板
 - 結果導致鳥園有 5 分鐘左右被 DDoS 攻擊
 - DDoS: Deny of Service
 - 一種玉石俱焚的攻擊方法
 - 不是入侵，是讓伺服器的服務短時間內接收大量要求
 - 因為伺服器的資源被非法要求灌爆
 - 最終無法提供正常的服務給一般大眾
 - [vbird_phorum.htm](#)



本機資料的保護

本機資料的保護

- 一般檔案資料還是需要保護的：
 - 你的磁碟是否允許犯錯 (容錯)
 - 可以使用 RAID 喔！
 - 軟體磁碟陣列/硬體磁碟陣列？
 - 你的磁碟資料是否有備份？
 - 本機備份？網路備份？異機備份？？
 - 備份的頻率是多久？手動備份？自動備份？
 - 備份的工具是什麼？檔案管理員？自動分析差異備份？

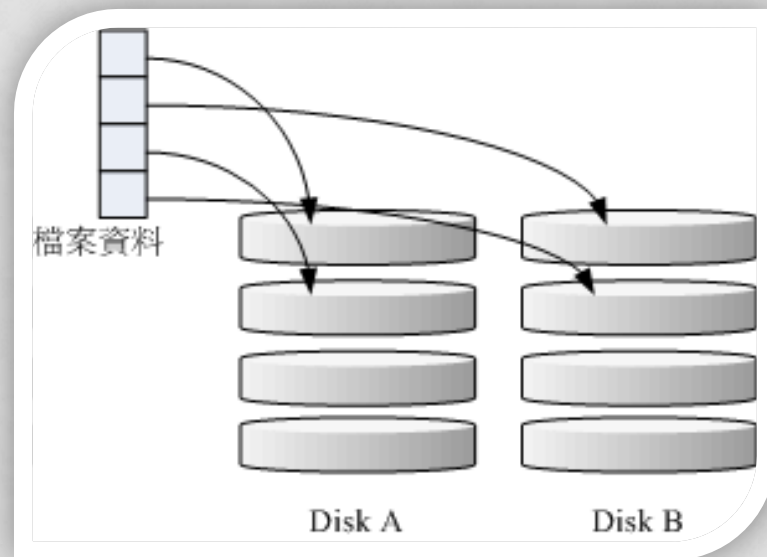
本機資料的保護

- 可以購買新伺服器的時候
 - \$\$ 充裕時：可以選購資源較大的設備 (CPU核心數較多、記憶體較多、磁碟容錯功能等)，然後透過 Linux KVM 分享資源較佳！
 - 許多 Server 收納成為 VM，那麼每個 Server 都可以使用到這個伺服器的好處了！而且，VM 還可以線上進行抽換，相當有用！
 - \$\$ 不多時：最好還是能夠考慮多顆磁碟組成的硬體磁碟陣列，透過 RAID 6 等級的保護，可以同時保有容錯與容量
 - \$\$ 很少時：最好資料放置的位置還是能有兩顆以上的磁碟組成 RAID 1 較佳
 - 那..什麼是 RAID？

本機資料的保護-RAID

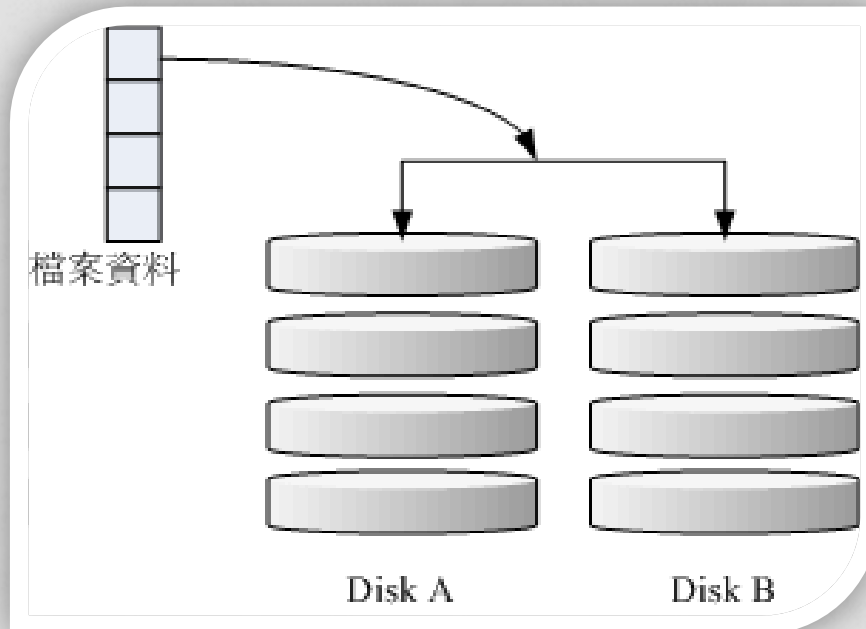
- 磁碟陣列 (RAID)

- 依據：容量、效能、容錯等需求來考量
- 除非資料一點都不重要，否則，效能最佳的 RAID 0 不要考慮！
- RAID-0
 - 效能最佳
 - 可以保有最多磁碟容量
 - 沒有容錯



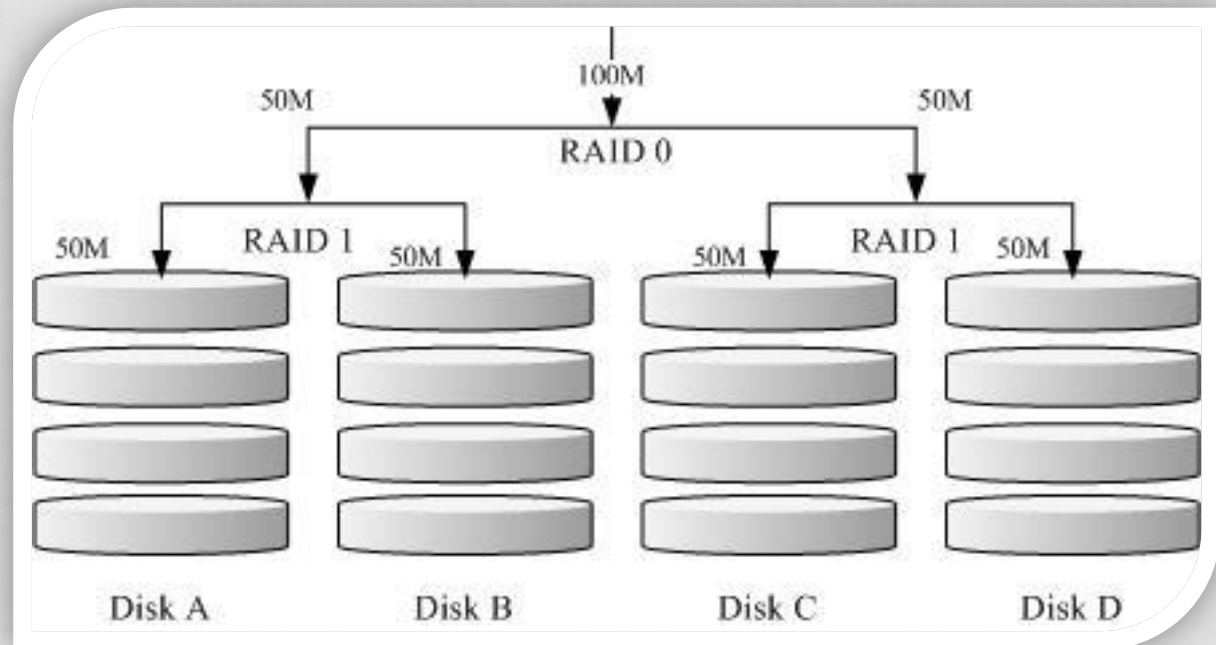
本機資料的保護-RAID

- 磁碟陣列 (RAID)
 - RAID-1
 - 寫效能尚可、讀較好些
 - 容量減半 (一半的容量做備份)
 - 容錯效果最好



本機資料的保護-RAID

- 磁碟陣列 (RAID)
 - RAID-10
 - 整合 RAID0 與 RAID1 的效果
 - 容量少一半
 - 效能有一半的磁碟總讀寫
 - 最佳容錯

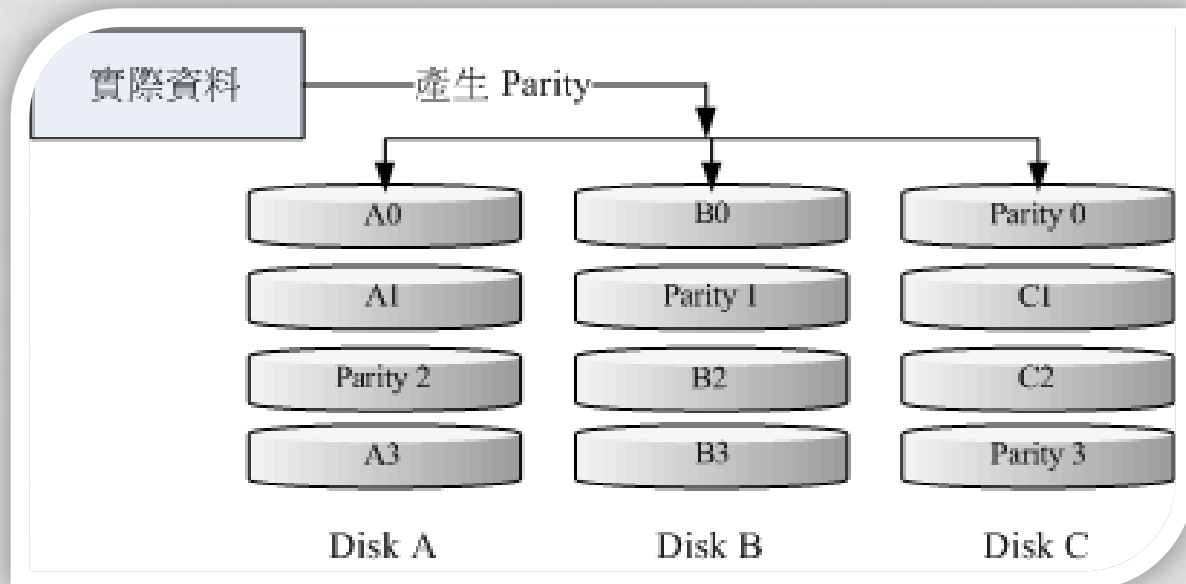


本機資料的保護-RAID

- 磁碟陣列 (RAID)

- RAID-5, RAID-6

- RAID5 少 1 顆容量，而 RAID-6 少兩顆容量
 - 讀寫效能不見得好，也需要經過計算
 - 有容錯，但是最擔心磁碟同時陣亡
 - 因此，近年來較常建議用 RAID-6



本機資料的保護-RAID

- 磁碟陣列 (RAID)
 - 實際應用的選擇：
 - RAID0 就真的不要考慮了！
 - 如果磁碟陣列上的資料需要瘋狂讀寫效能，例如作為 VM images 的來源時，建議使用 RAID-10，雖然容量少一半，但是效能肯定讓你滿意
 - 如果只是作為一般資料的讀寫，那使用 RAID-6 應該就很好了！
 - 如果資料量也不大，磁碟數也不多，那兩顆做成 RAID-1 也能容錯喔！

硬體磁碟陣列觀察

- 以 Dell 的 H7xx 及 H8xx 為例
 - 可使用 MegaRAID 軟體來線上觀察磁碟陣列的狀態

```
root@iscsi ~]# /opt/MegaRAID/MegaCli/MegaCli64 -LDInfo -LALL -aAll

Adapter 0 -- Virtual Drive Information:
Virtual Drive: 0 (Target Id: 0)
Name                : snapshot
RAID Level           : Primary-1, Secondary-0, RAID Level Qualifier-0
Size                 : 7.275 TB
Mirror Data          : 7.275 TB
State                : Optimal
Strip Size           : 256 KB
Number Of Drives per span:2
Span Depth           : 4
Default Cache Policy: WriteBack, ReadAhead, Direct, No Write Cache if Bad BBU
Current Cache Policy: WriteBack, ReadAhead, Direct, No Write Cache if Bad BBU
Default Access Policy: Read/Write
Current Access Policy: Read/Write
Disk Cache Policy    : Enabled
Encryption Type      : None
Default Power Savings Policy: Controller Defined
Current Power Savings Policy: None
Can spin up in 1 minute: Yes
LD has drives that support T10 power conditions: No
LD's IO profile supports MAX power savings with cached writes: No
Bad Blocks Exist: No
Is VD Cached: Yes
Cache Cade Type     : Read Only
```


軟體磁碟陣列的觀察

- 以鳥哥研究室的 Linux server 為例：
 - 透過 mdadm 去觀察 /dev/mdX
 - 重點就看 state 的項目即可！

```
root@kvm2 ~]# mdadm --detail /dev/md126
/dev/md126:
  Container : /dev/md0, member 0
  Raid Level : raid1
  Array Size : 927881216 (884.90 GiB 950.15 GB)
  Used Dev Size : 927881348 (884.90 GiB 950.15 GB)
  Raid Devices : 2
  Total Devices : 2

  State : active
  Active Devices : 2
  Working Devices : 2
  Failed Devices : 0
  Spare Devices : 0

  UUID : 1f3c13a8:d3cfa7fb:9c609e40:8bdcbad9
  Number Major Minor RaidDevice State
     1         8         0         0   active sync  /dev/sda
     0         8        16         1   active sync  /dev/sdb
```

LINUX SERVER 的磁碟觀察

- Linux server 提供 smartd 服務：
 - 透過 smartctl 來測試與觀察一般 SATA 磁碟的現況

```
root@iscsi ~]# smartctl --all /dev/sda
smartctl 5.43 2016-09-28 r4347 [x86_64-linux-2.6.32-696.el6.x86_64] (local build)
Copyright (C) 2002-12 by Bruce Allen, http://smartmontools.sourceforge.net

=== START OF INFORMATION SECTION ===
Device Model:          Hitachi HDS721050CLA660
Serial Number:        JP1532FL20NAXK
LU WWN Device Id:    5 000cca 39bdc7b68
Firmware Version:    JP20A50E
User Capacity:        500,107,862,016 bytes [500 GB]
Sector Size:          512 bytes logical/physical
Device is:             Not in smartctl database [for details use: -P showall]
ATA Version is:       8
ATA Standard is:      ATA-8-ACS revision 4
Local Time is:        Wed May 24 15:34:40 2017 CST
SMART support is:     Available - device has SMART capability.
SMART support is:     Enabled
```

LINUX SERVER 的磁碟觀察(續)

- Linux server 提供 smartd 服務：
 - 透過 smartctl 來測試與觀察一般 SATA 磁碟的現況
 - 可以注意看 Error logged 的輸出啊！

```
SMART Error Log Version: 0
No Errors Logged

SMART Self-test log structure revision number 1
No self-tests have been logged. [To run self-tests, use: smartctl -t]

SMART Selective self-test log data structure revision number 1
  SPAN   MIN_LBA  MAX_LBA  CURRENT_TEST_STATUS
    1       0        0       Not_testing
    2       0        0       Not_testing
    3       0        0       Not_testing
    4       0        0       Not_testing
    5       0        0       Not_testing
Selective self-test flags (0x0):
  After scanning selected spans, do NOT read-scan remainder of disk.
If Selective self-test is pending on power-up, resume after 0 minute delay.
```


本機資料的保護

- 無法購買新伺服器的時候
 - \$\$ 充裕時：可以買外接的 NAS 多磁碟的系統來備份，同樣的，請參考 NAS 的 RAID 等級，自己決定處理
 - \$\$ 不多時：可以買單顆外接式的 USB 磁碟(一定要 usb 3.0 以上)
- 本機資料保護的目的：
 - RAID 在防止磁碟發生錯誤時，還可以持續提供檔案系統支援
 - 外接式 NAS 或磁碟，主要是進行資料備份。當主機의磁碟損毀時，還可以作為資料復原的來源之用。
 - 所以，其實擁有 RAID 的主機系統，最好還是能夠額外進行備份。因為有時資料遺失，並不是因為磁碟錯誤，而是人為的操作不當
 - 網路說測試用：`rm -rf /`，一做就死掉～
 - 年初 gitlab 誤刪 310G 資料庫事件，導致救援到快死掉～

本機資料的保護-備份啦！

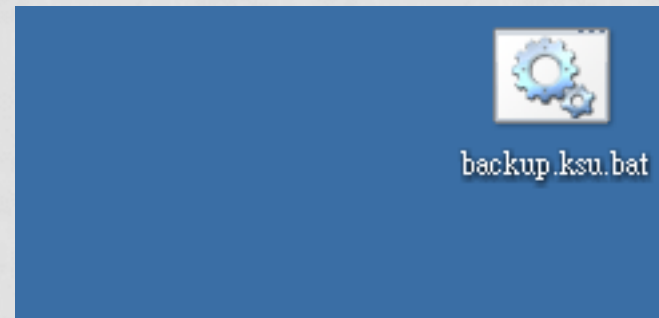
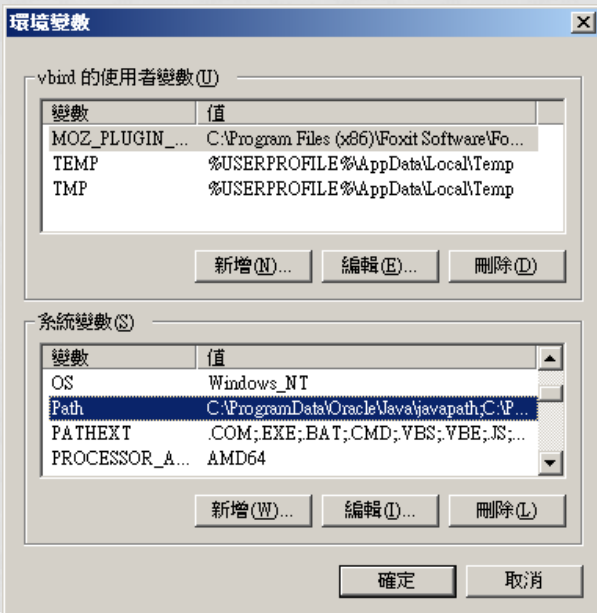
- Linux Server :
 - 可以使用 rsync 來進行備份
 - 如果可以將外接式儲存設備格式化為 xfs 或 ext4 的話，可以直接使用底下的方式來備份
 - `rsync -av /source/dir1 /source/dir2 ... /target/dir`
 - `/target/dir` 指的是外接式磁碟機所掛載的目錄
 - 如果需要定期備份，請自行使用 `/etc/crontab` 來處理
 - `rsync` 是透過比較分析新舊檔案的差異，只複製新檔案，因此處理速度比較快速

本機資料的保護-備份啦！

- Linux Server -- 異地備援
 - 可以使用 rsync 來進行備份
 - 但是遠端備份用 server 需要針對這部主機放行 ssh 的埠口 (正規埠口會在 port 22 上頭)
 - `rsync -e ssh -av /source/dir... user@SERVERIP:/target/dir`
 - 使用 user 帳號登入 SERVERIP 伺服器，放到伺服器的 /target/dir 目錄
 - 不過，如果需要自動備份，就需要用到不用密碼登入的 ssh key 功能

本機資料的保護-備份啦！

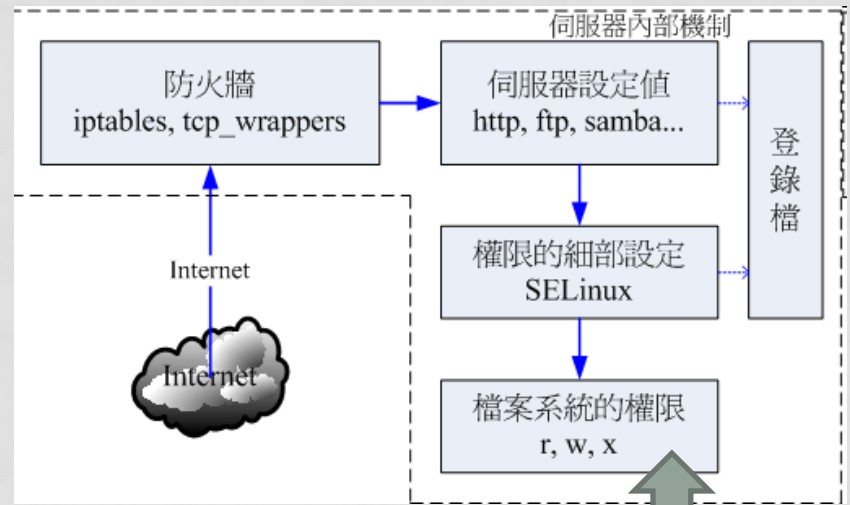
- Windows 桌機：
 - 不要傻傻使用檔案總管，請愛用 windows 版本的 rsync
 - <https://itfix.net/cwrsync>
 - 下載用戶端版本，無須使用伺服器端版本
 - <https://itfix.net/content/cwrsync-free-edition>
 - 上面為免費版，下載後直接安裝即可！
 - 請查閱 C 槽底下的目錄，將 cwrsync 的目錄貼到 PATH 變數內喔！



本機資料的保護-備份啦！

- Windows 桌機：

- 假設你的外接式硬碟格式化為 NTFS 了，然後掛載成為 Z 槽，之後你的 D 槽與 E 槽要複製到 Z 槽，可以編寫一隻批次檔，例如放在桌面下，使用 notepad++ 編輯檔名 backup.bat，內容如下：
 - rsync -rltv --del /cygdrive/d/ /cygdrive/z/D/
 - rsync -rltv --del /cygdrive/e/ /cygdrive/z/E/
 - pause
 - rsync 必須要放置於 PATH 的變數目錄內，請自行處理 windows 環境設定
 - /cygdrive/ 為 cwrsync 的磁碟槽標題代號，因此第一行為處理 d 槽
 - /cygdrive/z/D 指的是 z 槽內的 D 目錄。則 D 槽資料會放到 z 槽的 D 資料夾裡面的意思
- 放在桌面上，直接點擊兩下，就可以開始備份。第一次備份會比較久，之後只有被修改過得資料才會被重新備份，因此速度會快非常多！



繼續要講這裡

作業系統相關的保護

主機本體的物理防護

- 關於機房：
 - 重要資訊重地，不可隨意進出；
 - 進出的資訊記載很重要
 - 其實...學校就這麼小，這點很難落實。因為沒有場地啊～你懂的～
 - 不過，至少也拔掉鍵盤滑鼠，有需要在安裝上去，避免被接觸！
- 關於單一主機的實體保護：(先確定不會被搬走，密碼才有意義)
 - Case 要加鎖，電源按鈕的保護；
 - BIOS 密碼
 - 啟動裝置的維護 (硬碟、USB、光碟的開機順序！)
 - OS Loader 的密碼保護！
 - 這點是見仁見智，因為加了保護，有時候會無法遠端遙控 reboot

主機資源-帳號相關

- End user 本機登入的問題：
 - Linux：帳號的密碼一定要嚴格設定，讓系統自行判斷能不能過關。可以使用如下的方式，避免人情壓力的問題：
 - `useradd account_name`
 - `echo account_name | passwd --stdin account_name`
 - `chage -d 0 account_name`
 - 讓使用者自行設定密碼，且該密碼一定要符合系統要求！
 - 這樣比較嚴格，比較有效果！
 - 您可以建議用戶使用台灣特有的密碼『用注音拼小孩的姓名』，很難猜的啦！
- 關於離職員工：
 - 若擔心出問題，可暫時加鎖
 - `passwd -l account_name` (解鎖請自行 `passwd --help`)

主機資源-帳號相關

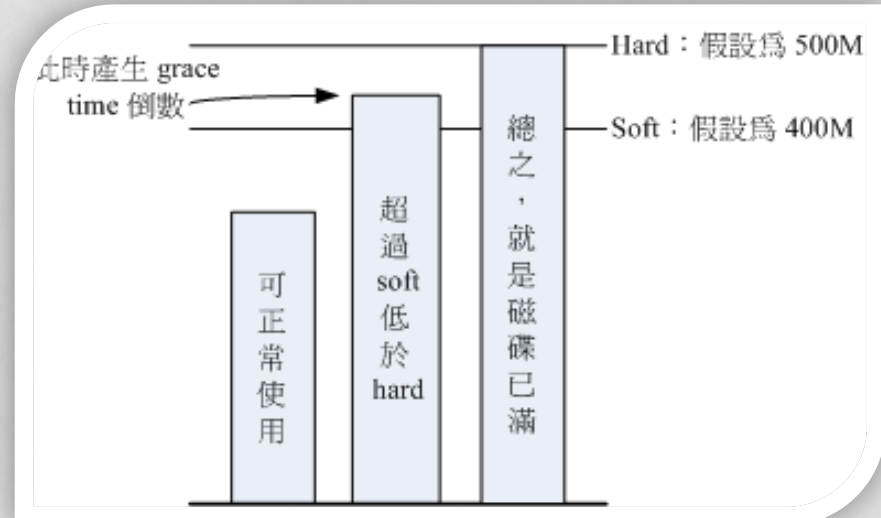
- 不取得互動 shell 的帳號(FTP/Web/Mail等帳號)：
 - 因為該帳號是單純使用某些服務 (FTP/Apache/Mail)
 - 所以該帳號不該透過 ssh 或直接在 tty1 上面登入
 - 可以讓該帳號的 shell 變成 /sbin/nologin
 - 可以修改系統預設帳號的參數設定：
 - /etc/default/useradd
 - 或直接使用 useradd
 - -s /sbin/nologin

```
File Edit View Search Terminal Help
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/sbin/nologin
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

主機資源-檔案系統

- 檔案系統的保護：

- 為了擔心檔案系統被塞爆，合理的 quota 設定是需要的
- 目前 CentOS 7 預設使用 XFS 檔案系統，可以透過 `/etc/fstab`
 - `/dev/sda2 /home xfs defaults,usrquota,grpquota 0 0`
 - 卸載再掛載就可以讓 xfs 支援 quota 了！
- 設定某個帳號的最大使用容量
 - `xfs_quota -x -c "limit -u bsoft=400M bhard=500M account" /home`



主機資源-檔案系統

- 檔案系統的保護：
 - 強者我同事說：『我的網頁程式，需要使用資料庫帳號，針對不同的目錄來設計 quota。但是，網頁程式都是使用 httpd 這個帳號，所以傳統的針對用戶設計的 quota 是無法實現的，該如何是好？』
 - XFS 檔案系統支援『project』這個 quota 設計值！只是該設計值無法與 grpquota 搭配喔！因此 /etc/fstab 要改成：
 - /dev/sda2 /home xfs defaults,usrquota,prjquota 0 0
 - 設定一個 myproject 的別名，且識別碼為 11 號，則
 - echo "myproject:11" >> /etc/projid
 - echo "11:/home/somedir" >> /etc/projects
 - 開始設定：
 - xfs_quota -x -c "limit -p bsoft=450M bhard=500M myproject" /home

主機資源-權限設定

- 系統一定會有的權限設定：
 - 包括 SUID/SGID/SBIT 等等
 - 不要隨便就『 `chmod -R 777 /` 』系統會死掉！(不問你的死掉)
 - 目錄的 `rx` 與檔案的 `rx` 是完全不一樣的概念！
 - 目錄的 `x` 是能否進入該目錄去操作相關動作的 `key` 喔！
 - 但是...針對某一個人或群組，要設定權限呢？
 - 可能是最佳解法：ACL
 - `setfacl -m u:user:perm /some/dir` 立刻生效
 - `setfacl -m d:u:user:perm /some/dir` 預設值
 - 忌諱：
 - 千萬不要 `chmod 777 /some/dir` 啊！
 - 也千萬不要亂加用戶到某些特定的群組去啊！！

主機資源-官方軟體更新

- 關於作業系統的選擇與更新：
 - Linux distributions 眾多，其中最新的可能是 Fedora / OpenSuSE / Ubuntu 等版本了！
 - 不過，如果要用來架站，最好還是選擇穩定的版本
 - 有錢用 RHEL/Ubuntu/SuSE...
 - 沒錢用 CentOS/B2D/Debian...
 - 一定要選擇還在更新支援當中的版本
 - 不過，鳥哥個人不是很愛用 X.0 版，例如 CentOS 7.0
 - 鳥哥比較愛 X.1 之後的版本，例如 CentOS 7.1
 - 所以，升級到下一階段版本，通常會在 X.1 之後才進行
 - 像 CentOS 5.x, WinXP, Win7 等，幾乎不再支援的版本，記得不要用了！要用請自行管理所需要的資安！

主機資源-官方軟體更新

- 軟體一定要使用官網釋出的版本
 - 最好不要用非官網來源的軟體
 - 若需要第三方協力軟體，亦請確認該軟體的來源可信度
 - 最好排定每日更新啊！
 - vim /etc/crontab
 - 20 3 * * * root /bin/yum -y update
 - 不過該訊息不會直接傳給你，所以最好這樣做：
 - vim /etc/aliases
 - root: root,your@email.addresss
 - newaliases
 - 可能會被判定為垃圾信，此時請自行到鳥站查詢『relayhost』吧！

主機資源-官方軟體更新

- 軟體每日更新的回報訊息範本

```
主旨: Cron <root@vbird> /bin/yum -y update
```

```
Loaded plugins: fastestmirror, langpacks
```

```
Loading mirror speeds from cached hostfile
```

```
* base: ftp.twaren.net
```

```
* extras: ftp.twaren.net
```

```
* updates: ftp.twaren.net
```

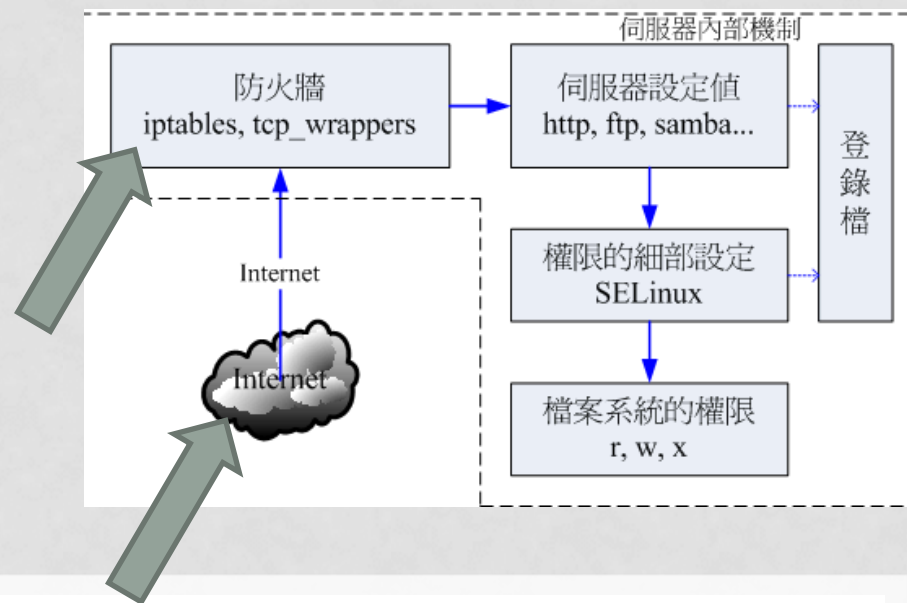
```
No packages marked for update
```

```
Resolving Dependencies
--> Running transaction check
--> Package NetworkManager.x86_64 1:1.4.0-17.el7_3 will be updated
--> Package NetworkManager.x86_64 1:1.4.0-19.el7_3 will be an update
--> Package NetworkManager-adsl.x86_64 1:1.4.0-17.el7_3 will be updated
--> Package NetworkManager-adsl.x86_64 1:1.4.0-19.el7_3 will be an update
--> Package NetworkManager-glib.x86_64 1:1.4.0-17.el7_3 will be updated
--> Package NetworkManager-glib.x86_64 1:1.4.0-19.el7_3 will be an update
--> Package NetworkManager-libnm.x86_64 1:1.4.0-17.el7_3 will be updated
--> Package NetworkManager-libnm.x86_64 1:1.4.0-19.el7_3 will be an update
--> Package NetworkManager-team.x86_64 1:1.4.0-17.el7_3 will be updated
--> Package NetworkManager-team.x86_64 1:1.4.0-19.el7_3 will be an update
--> Package NetworkManager-tui.x86_64 1:1.4.0-17.el7_3 will be updated
--> Package NetworkManager-tui.x86_64 1:1.4.0-19.el7_3 will be an update
--> Package NetworkManager-wifi.x86_64 1:1.4.0-17.el7_3 will be updated
--> Package NetworkManager-wifi.x86_64 1:1.4.0-19.el7_3 will be an update
```

主機資源-官方軟體更新

- 常問的問題之一：
 - Windows 有 update 可用，那 update 之後經常需要重新開機
 - Linux 如果 update 之後，需不需要重新開機呢？
 - 需要的條件：
 - Kernel 被 update 過了
 - 某些大家都會用到的 library 被 update 了
 - 不需要的情況：
 - 只是某些特定的軟體 update 了。一般這樣的情況下，該軟體會被自動 restart，因此是不需要重新 reboot 的！
 - 所以，上一頁回報的資訊當中，若有 update 軟體，要特別注意有沒有需要重新開機的軟體被升級了？若有，那你的 Linux server 最好還是找個比較閒的時候進行 reboot 吧！

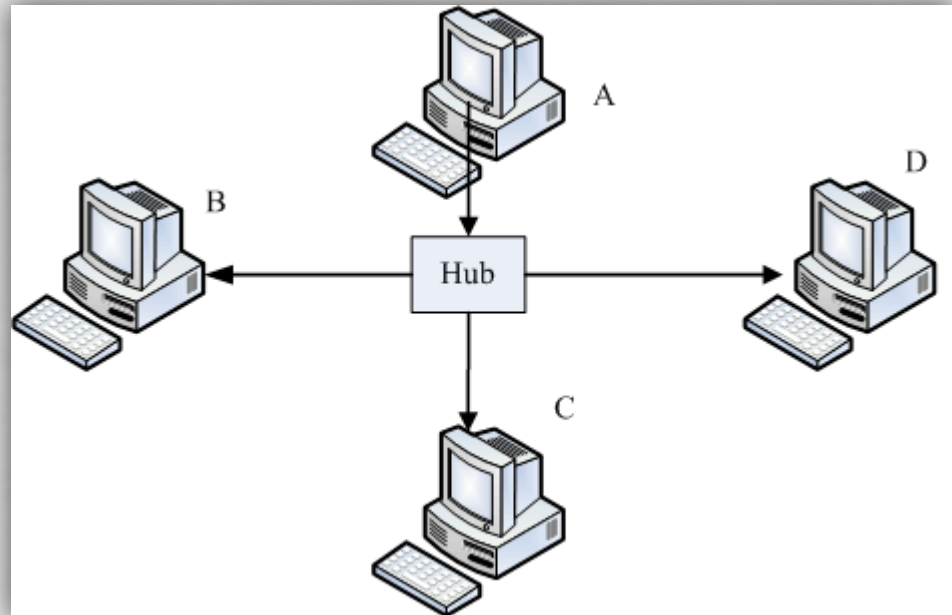
硬體： 乙太網路
軟體： TCP/IP
程式： WWW 伺服器、Browser



瞭解網路基礎

基礎網路知識

- 網路硬體設備：
 - 乙太網路都是透過網路卡互相傳遞資料
 - 透過 CSMA/CD 方式進行資料訊框的傳遞
 - CS：你的網卡傳送資料前，先監聽整個區域網路
 - MA：若沒有人在使用網路，才能夠傳送資料訊框，同時，這個訊框會傳遞給每個在區網內的網路卡。(現在你知道，為何明明沒有使用網路，hub燈卻一直閃)
 - CD：碰撞偵測，
 - 發生碰撞，
 - 重新傳送一次。



基礎網路知識

- 網際網路通訊協定 (Internet) : TCP/IP
 - 網路位址 (IP) : 你的主機在網路上的門牌
 - 除了網路卡上面由 ISP 取得的正確 IP 之外，每部主機都會有的一個特殊的內部測試 IP : 127.0.0.1
 - TCP 封包 :
 - 在這個 IP 上面，啟動的各種不同的服務，都會使用到不同的 TCP 埠口進行資料的對接與傳送。
 - 目前很多服務為了快速，也會使用 UDP 的封包格式喔！
 - 服務 : 就是提供某種網路功能的軟體程式

基礎網路知識

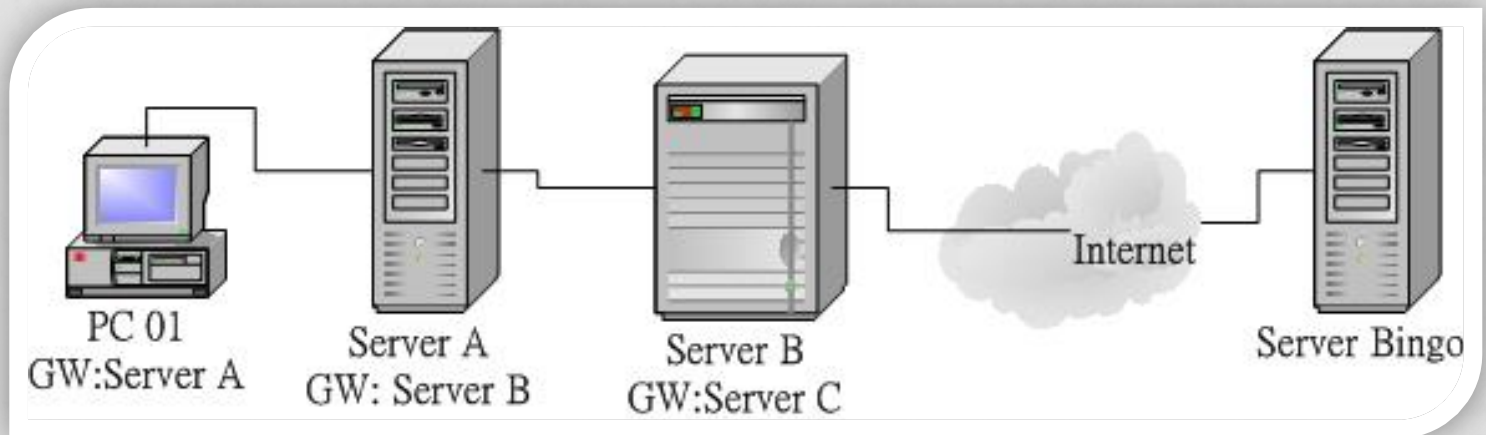
- 網際網路通訊協定的想法：
 - IP：一間銀行的位置 (只有一個啊)
 - TCP：這間銀行的窗口 (有好多個吧?)
 - 服務：在窗口後面的那個負責的人(你看過沒有人的窗口會主動幫你進行存款、提款等的任務?)

基礎網路知識

- 網路是雙向的：
 - Server：
 - Yahoo (有 IP 啊)
 - 啟動WWW伺服器軟體
 - 開啟TCP port 80監聽用戶端的請求
 - Client：
 - 你的主機 (也有 IP 啊)
 - 啟動 browser
 - 開啟 TCP port (>1024)主動向 Yahoo的 port 80 提出資料請求

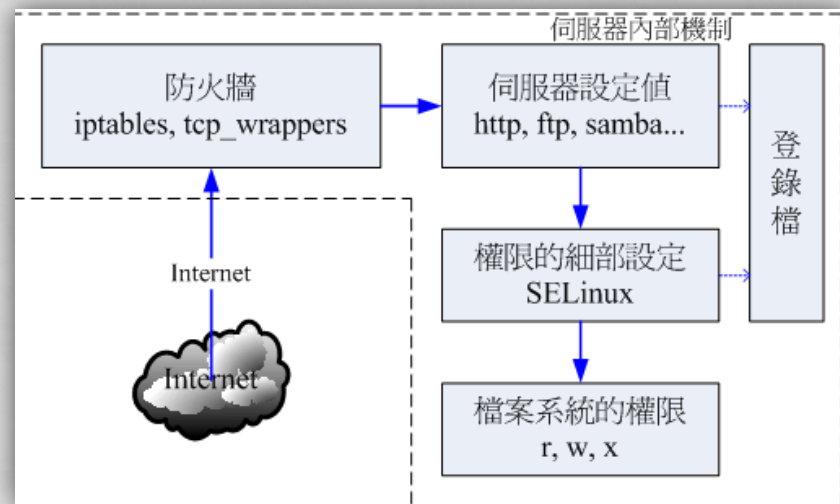
基礎網路知識

- 資料傳送的方式：
 - 區域網路內：透過資料封包的廣播
 - 區域網路外：透過路由器幫我們轉送
 - 所以，無論如何，你的資料如果不是在內網傳送，就是會透過路由器。
 - IP分享器是一種路由器
 - 無線基地台也是一種路由器
 - 目前的網路傳輸都是透過 CSMA/CD 來傳送的唷！



基礎網路所產生的困惑

- 伺服器防火牆有沒有用？
 - 針對開放的服務，殘念，防火牆沒有用
 - 你想連接到 Yahoo 的 WWW
 - Yahoo 必須要開放 port 80 讓你連進去
 - 如果 WWW 伺服器軟體有問題的話...
 - 針對不開放或有限制開放的服務，有效！
 - 你要連到 Yahoo 的 FTP
 - Yahoo 可能並沒有打開 port 21 讓你進入！
 - 抵擋住了！



基礎網路所產生的困惑

- 什麼是後門？聽說木馬程式會啟動後門？
 - 木馬：
 - 一支惡意的程式，執行它，會主動的啟動一個埠口，開始監聽 cracker(怪客) 的請求
 - 後門：
 - 因為啟動了埠口，這個埠口可能是非正規的，因此就被稱為後門。
 - 關閉的方法：
 - 從記憶體中刪除木馬程式，找到該木馬程式位於硬碟的檔名，刪除檔名才算完整(某些時刻你還得要處理登錄檔)
 - 如果沒有先從記憶體移除，直接刪除木馬檔案，則在你重新開機前，通常在記憶體內的資訊會在次寫回磁碟，所以，那個檔案又會產生在磁碟系統當中了！

基礎網路所產生的困惑

- 為何瀏覽器也要更新？
 - 網路是雙向的，你可能會瀏覽到惡意網站
 - 該網站傳遞的資料會透過你的瀏覽器傳送到你的主機上面
 - 因為是你的瀏覽器向對方要求資料的，所以這個資料會主動的被你的瀏覽器接收下來！
 - 恭喜你！中標了！

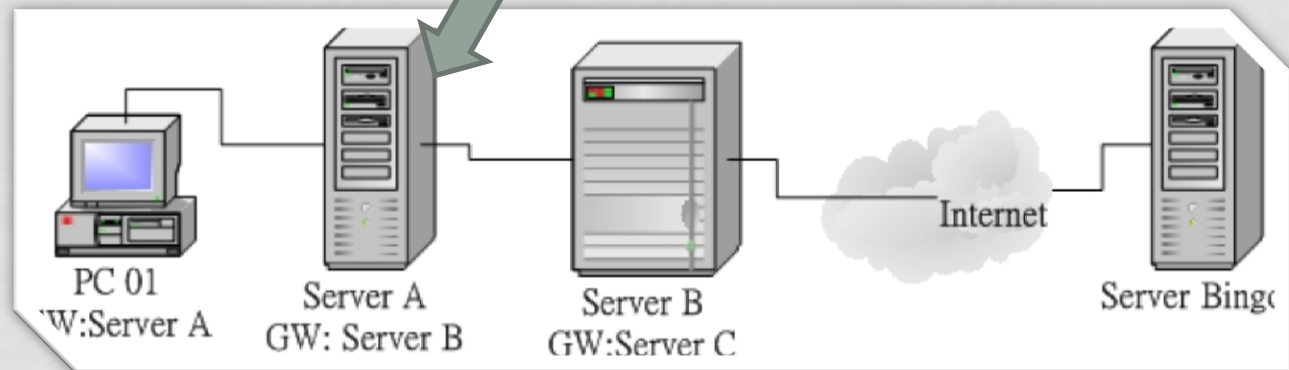
基礎網路所產生的困惑

- 為何你主機上記錄的帳號、密碼可能被竊取
 - 為了方便以後登入某些網站，你的登錄資料可能會被記載到硬碟的快取 (cookies)
 - 是你的瀏覽器允許伺服器軟體向你的硬碟搜尋相關的記錄檔案
 - 如果該伺服器軟體是惡意的呢？其他的 cookies 小檔案也會被搜尋到喔！
 - 恭喜你！資料被取得啦！天天收到莫名其妙的 email 就是這樣來的！

基礎網路所產生的困惑

- 為何不要在即時通訊軟體上面傳送重要資料？
 - CSMA/CD 會主動的將資料發送給所有網卡
 - 正確的情況下，你的網卡會丟棄不是自己的封包
 - 那，如果你的主機上面安裝了特殊監聽軟體呢？
 - 封包會被接收下來而不是丟棄
 - 解析封包，重組資料
 - 得到你的訊息了！

假設我在這裡丟一隻
監聽軟體呢？

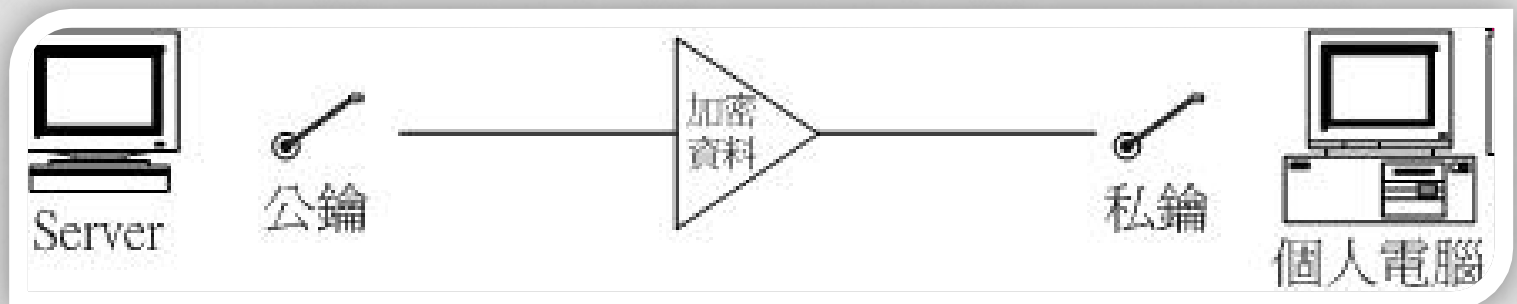


基礎網路所產生的困惑

- 為何不要使用免費的無線基地台？
 - 網路傳送時，如果是非本地端資料則交給路由器幫你轉送，也就是說，你的資料一定會通過他
 - 如果我在無線基地台上面安裝一個監聽程式，將所有資料封包捉下來重組？
 - 响～得到你的訊息了！
 - 其實就是跟剛剛一樣的情況了！

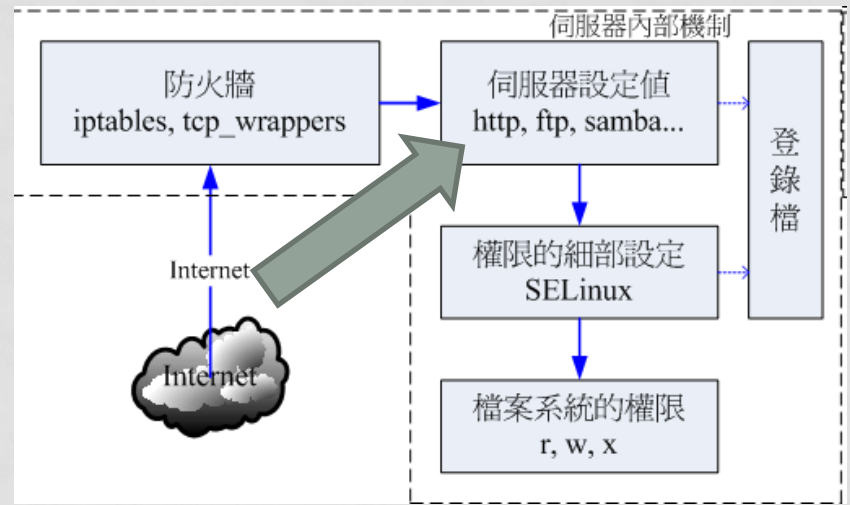
基礎網路所產生的困惑

- 為何資料要加密？
 - 既然 CSMA/CD 會大量廣播、路由器都可能被加裝監聽軟體，那我在傳出的資料加密，總不會被竊聽了吧？這就是加密的由來！
 - Server \leftrightarrow Client 之間傳遞資料前
 - 先產生互信的加密機制
 - 資料在 Internet 上面跑，是經過編碼的亂碼
 - https, ssh, ftps, pop3s 等，就是加密過的
 - 不是加密就安全了！某些協定很恐怖的！那個 ssh 就是其中之一！



基礎網路所產生的困惑

- 為何 WWW 懶人包 (例如 Appserv) 就容易被攻擊
 - 這不是 OS 官方釋出的軟體，所以 windows 也不會自動的更新
 - 為了方便『懶人』，所以提供了很多的方便設定的工具
 - 『phpmyadmin 資安』google 一下，你會下一跳
 - 『Appserv 資安』google 一下，很多經驗談啊～
 - 很多的腳本也是為了方便用戶設定，因此許多的資訊都是不設防的！相當的危險。
 - 當初 Appserv 應該定位在學習，而不是提供對外架設，使用這東西架設網站，真的是很危險的一件事。



伺服器服務的管理

服務所啟動的埠口

- 網路服務：
 - 如網路基礎當中談到的，你要連線到 server，server 就必須要啟動某個服務，這個服務會啟動某個 port，你得要透過 client 軟體連接到該 port，才可以跟 server 溝通要資料等。
 - 常見的網路服務啟動的埠口有 tcp 與 udp 兩種協定，基本上，大部分的正規服務大多使用 TCP 的！
 - 如果觀察呢？
 - Linux：netstat -tlunp
 - Windows：netstat -an

服務所啟動的埠口

- Windows 服務觀察

```
users\w...>netstat -n
使用中連線
```

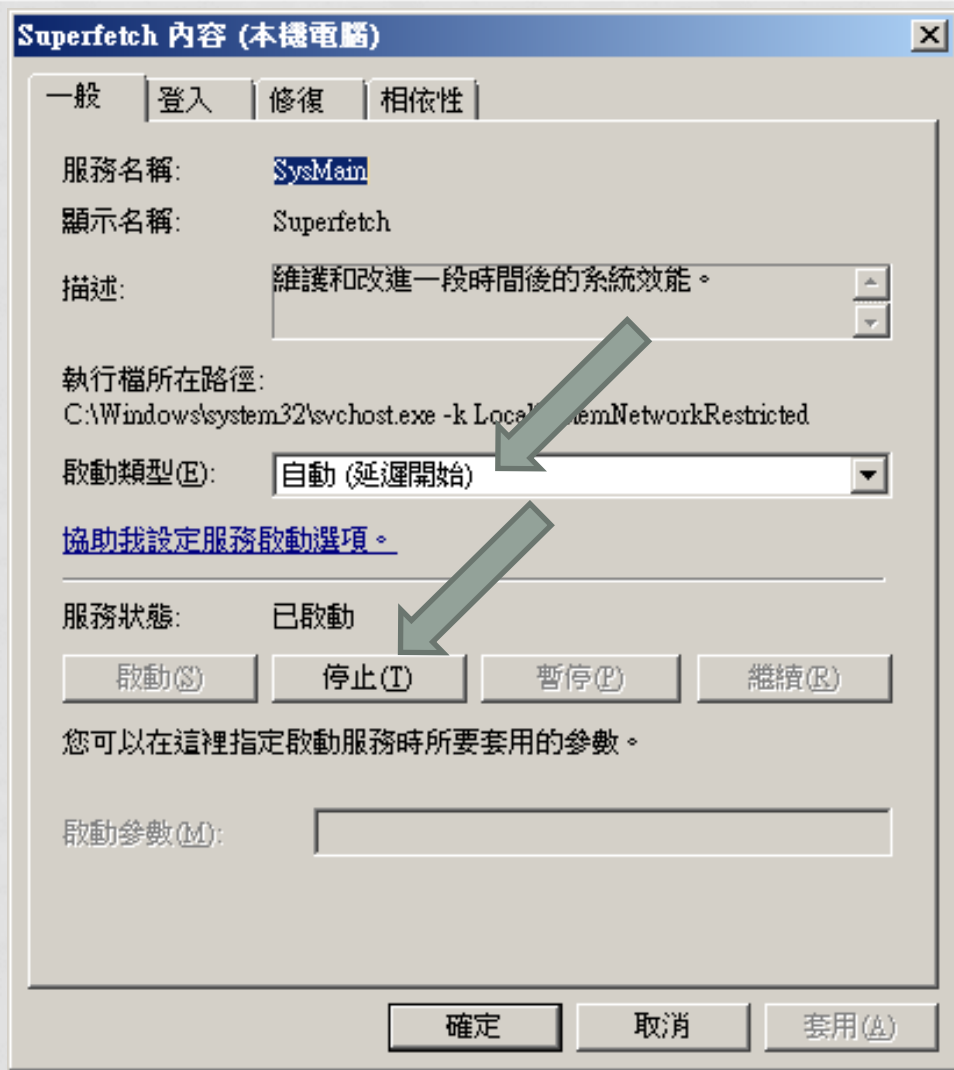
協定	本機位址	外部位址	狀態
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:8092	0.0.0.0:0	LISTENING
TCP	0.0.0.0:17500	0.0.0.0:0	LISTENING
TCP	0.0.0.0:47984	0.0.0.0:0	LISTENING
TCP	0.0.0.0:47989	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49157	0.0.0.0:0	LISTENING
TCP	127.0.0.1:843	0.0.0.0:0	LISTENING
TCP	127.0.0.1:9990	0.0.0.0:0	LISTENING
TCP	127.0.0.1:17600	0.0.0.0:0	LISTENING
TCP	127.0.0.1:49178	127.0.0.1:65001	ESTABLISHED
TCP	127.0.0.1:49188	127.0.0.1:49189	ESTABLISHED
TCP	127.0.0.1:49189	127.0.0.1:49188	ESTABLISHED
TCP	127.0.0.1:49189	127.0.0.1:49189	ESTABLISHED

需不需要關閉服務？

- 本機服務：
 - 一般本機服務中，若不清楚，先不要關閉
 - 一般網路服務中，真的用不著，就關閉吧。
 - 關閉服務的方法：
 - `systemctl list-units` 只是查詢列表
 - `systemctl stop unitname` 立刻關閉
 - `systemctl disable unitname` 下次開機不會啟動這服務

需不需要關閉服務？

- 本機服務：
 - Windows
 - 也是分兩階段
 - 一個是現在立刻
 - 一個是下次開機



需不需要關閉服務？

- 本機服務：
 - Windows
 - 由於 windows 大多會自己進行磁碟最佳化的例行工做，不過 SSD 已經是夠快了，因此，如果使用 SSD 作為系統碟，建議關閉底下服務：
 - Superfetch
 - Windows Search

需不需要關閉服務？

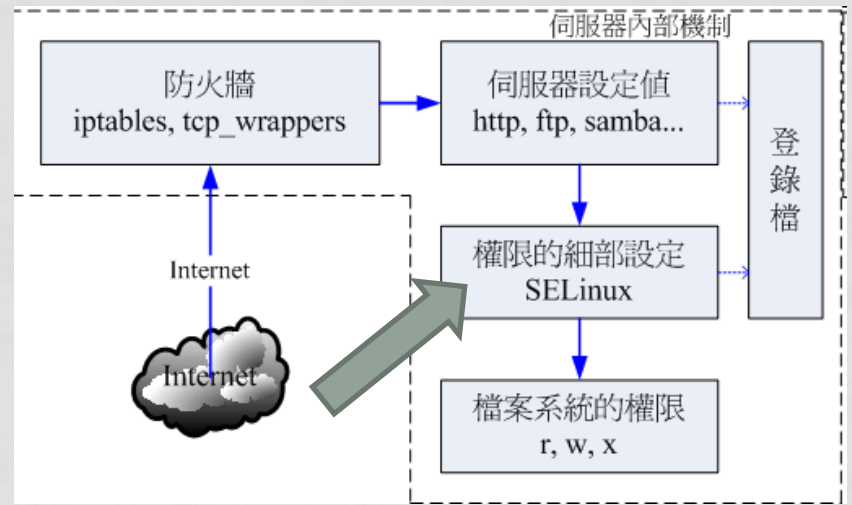
- Linux 服務狀態的觀察
 - `systemctl status daemon`

```
root@v ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since 日 2017-04-16 23:03:17 CST; 1 months 7 days ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 1191 (httpd)
    Status: "Total requests: 0; Current requests/sec: 0; Current traffic:  0 B/sec"
   CGroup: /system.slice/httpd.service
           └─ 1191 /usr/sbin/httpd -DFOREGROUND
              └─ 2928 /usr/sbin/httpd -DFOREGROUND
                 └─ 5452 /usr/sbin/httpd -DFOREGROUND
                    └─ 5453 /usr/sbin/httpd -DFOREGROUND
                       └─ 5454 /usr/sbin/httpd -DFOREGROUND
                          └─ 5455 /usr/sbin/httpd -DFOREGROUND
                             └─ 5456 /usr/sbin/httpd -DFOREGROUND
                                └─ 12671 /usr/sbin/httpd -DFOREGROUND

4月 16 23:03:05 systemd[1]: Starting The Apache HTTP Server...
```

服務怎麼進行維護？

- 一定要進行的任務：
 - 升級、升級、升級！最新的應該就代表最好的！
- 是否放行整個 Internet？
 - http 當然就是要放行
 - 但是 ssh 當然不可以放行！（要自己開後門給自己就好！）
- 服務怎麼設定？
 - 這都是 case by case
 - 但謹記：能加密就加密、內部文件就不要讓 Internet 讀到、帳號盡量想辦法不公開、



SELINUX 的使用

你都會這樣聽到

要架站喔！SELinux 先關掉再說！
不然一定無法成功架站！

.....

不要再相信沒有根據的傳說了！

SELINUX 的用途

- 某帳號有沒有權限讀取某個檔案？
 1. 先由檔名讀到 inode 號碼位置
 2. 再由 inode 內容讀到權限設定
 3. 比對用戶的 UID/GID 再與權限設定的 rwx 比對
 4. 結果就可以知道有沒有辦法讀取到這個檔案了！
- 但是總是會有人突然設定 777 的權限啊～～(讀不到嗎？這樣處理就好？傷腦筋～)
 - 所以 SELinux 會增加在 2.5 步驟內，多一個『管理網路服務』的設定值，如果你沒有通過 SELinux 的設定，那即使後面 3, 4 的權限是對的，也讀不到檔案內容！這就是基礎保護。

SELINUX 的用途

- SELinux 管理的標的：
 - 一般權限在管理『使用者所執行的 process，主要是針對使用者的 UID/GID 來設計的權限管理』
 - SELinux 主要管理的『是網路服務那隻程序能不能(1)進行某些任務或(2)讀取某些檔案』所設計的。
 - SELinux 有很多的預設值，都是針對當初推出的版本用途所設計，因此：
 - 如果你沒有額外安裝其他的軟體或者是其他的不同於官網的規劃
 - 啟用 SELinux 是完全不會影響你的架站的！

SELINUX 對程序的判斷流程

- 一隻網路程序是否可以讀到某目錄的檔案：
 - 模式：先要通過 SELinux 的運作模式
 - Enforcing 強制執行，有限制
 - Permission 寬容狀態，沒限制，但是會紀錄問題
 - Disabled 關閉沒事，沒限制、沒紀錄 (會抹除 inode 內的SELinux 資料)
 - 規則：能不能進行某項工作的放行
 - 例如 httpd 能不能讀取網際網路的資料庫？
 - 例如 ftp 有沒有放行使用者家目錄的存取權限
 - 例如 httpd 能否放行使用者家目錄的個人首頁功能等等
 - 檔案安全本文：這就與檔案的 rwx 很類似
 - 例如 http 能不能讀取 /opt/your/file ？
 - 或者是你家目錄的檔案移動到 /var/www/html 後，能否被讀取？

SELINUX 設定一般建議

- 情況一：你都使用 CentOS 7 的預設設定，修改的幅度不大，也不太用其他第三方軟體，自己開發的網頁界面比較偏向於靜態網頁，或者是單純的本機資料庫連結
 - 最好一定要開啟 SELinux 成為 Enforcing 模式！
 - 對你的架站幾乎完全不會出問題
- 情況二：CentOS 用來開發專題，這個專題的內容需要用到很多自主開發的 PHP 程式與互相呼叫服務的功能，也常常需要用到外部的第三方軟體
 - 最好開啟在 Permissive 模式，不會影響到你的系統運作
 - 而且可以在 `/var/log/messages` 裡面查閱到SELinux誤用的情況

SELINUX的模式變更

- 修改預設模式方式：
 - /etc/selinux/config
 - SELINUX=enforcing | permissive
 - Reboot
- 暫時修改 enforcing 與 permissive 模式
 - setenforce [0 | 1]
 - getenforce

```
[root@localhost ~]# setenforce 0
[root@localhost ~]# getenforce
Permissive
[root@localhost ~]# setenforce 1
[root@localhost ~]# getenforce
Enforcing
```

SELINUX 的規則觀察與設定


- 所有針對原廠系統的 SELinux 規則
 - `getsebool -a | grep keyword ←keyword` 例如 `httpd`
- 設定放行與否
 - `setsebool -P ftp_home_dir [0|1]`

```
[root@localhost ~]# getsebool ftp_home_dir
ftp_home_dir --> off
[root@localhost ~]# setsebool -P ftp_home_dir 1
[root@localhost ~]# getsebool ftp_home_dir
ftp_home_dir --> on
[root@localhost ~]# █
```

SELINUX 針對檔案的安全本文

- 安全本文的觀察
 - ll -Z
 - 可以觀察到檔案的安全本文
 - 你可以觀察預設目錄，就能知道有沒有問題

```
[root@localhost www]# ll -Z /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[root@localhost www]# █
```



移動情況的安全本文狀態與修訂

- 從 root 家目錄移動資料到 /var/www/html
 - mv index.html /var/www/html
 - ll -Z /var/www/html 會發生什麼狀況？

```
[root@localhost ~]# vim index.html
[root@localhost ~]# mv index.html /var/www/html/
[root@localhost ~]# ll -Z /var/www/html/
-rw-r--r--. root root unconfined_u:object_r:admin_home_t:s0 index.html
[root@localhost ~]# █
```

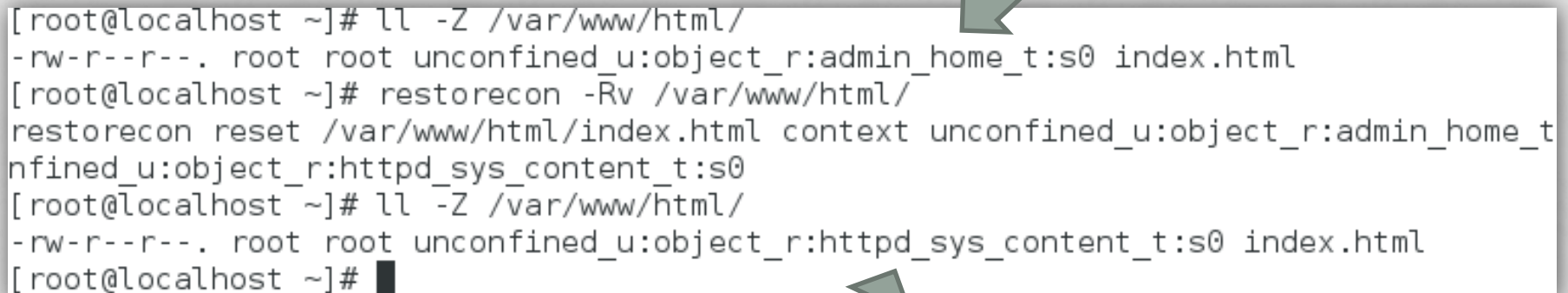


並不是系統預設認定的 httpd_sys_content_t 喔！
所以這個檔案不會讓 httpd 程序讀取的！

移動情況的安全本文狀態與修訂

- 從 root 家目錄移動資料到 /var/www/html
 - 因為是系統的預設目錄，系統會保留預設目錄的相關設定參考
 - 所以可以使用『復原』的方式來處理即可

```
[root@localhost ~]# ll -Z /var/www/html/
-rw-r--r--. root root unconfined_u:object_r:admin_home_t:s0 index.html
[root@localhost ~]# restorecon -Rv /var/www/html/
restorecon reset /var/www/html/index.html context unconfined_u:object_r:admin_home_t
nfinfined_u:object_r:httpd_sys_content_t:s0
[root@localhost ~]# ll -Z /var/www/html/
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 index.html
[root@localhost ~]# █
```



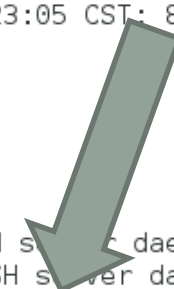
例外狀況的排除

- 例如將 sshd 放行到 2222 這個埠口時，有啟動 SELinux 的情況下，可能會無法處理！

- vim /etc/ssh/sshd_config
- systemctl restart sshd
- systemctl status sshd

```
#  
Port 22  
Port 2222  
#AddressFamily any  
#ListenAddress 0.0.0.0  
#ListenAddress ::
```

```
[root@localhost ~]# systemctl status sshd  
● sshd.service - OpenSSH server daemon  
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor pr  
   Active: active (running) since Thu 2017-05-25 11:23:05 CST; 8s ago  
     Docs: man:sshd(8)  
           man:sshd_config(5)  
   Main PID: 3435 (sshd)  
    CGroup: /system.slice/sshd.service  
            └─3435 /usr/sbin/sshd -D  
  
May 25 11:23:05 localhost systemd[1]: Started OpenSSH s...c daemon.  
May 25 11:23:05 localhost systemd[1]: Starting OpenSSH s...er daemon...  
May 25 11:23:05 localhost sshd[3435]: error: Bind to port 2222 on 0.0.0.0 f  
May 25 11:23:05 localhost sshd[3435]: error: Bind to port 2222 on :: failed  
May 25 11:23:05 localhost sshd[3435]: Server listening on 0.0.0.0 port 22.  
May 25 11:23:05 localhost sshd[3435]: Server listening on :: port 22.  
Hint: Some lines were ellipsized, use -l to show in full.
```



例外狀況的排除

- 其實在 `/var/log/messages` 會告訴你如何處理！
 - 不知為啥這一版的 SELinux 錯誤排版很亂～
 - 所以找關鍵字『`run sealert`』重新跑一次輸出！

```
May 25 11:23:06 localhost setroubleshoot: SELinux is preventing /usr/sbin/sshd from name_bind access on the tcp_socket port 2222. For complete SELinux messages. run sealert -l 93c79b52-b575-470f-bc28-3f8485e1b673
```

```
May 25 11:23:06 localhost python: SELinux is preventing /usr/sbin/sshd from name_bind access on the tcp_socket port 2222.#012#012***** Plugin bind_ports (92.2 confidence) suggests ***
*****#012#012If you want to allow /usr/sbin/sshd to bind to network port 2222
#012Then you need to modify the port type.#012Do#012# semanage port -a -t PORT_TYPE -p tcp 22
22#012 where PORT_TYPE is one of the following: ssh_port_t, vnc_port_t, xserver_port_t.#01
2#012***** Plugin catchall_boolean (7.83 confidence) suggests *****#012#012If
you want to allow nis to enabled#012Then you must tell SELinux about this by enabling the 'n
is_enabled' boolean.#012#012Do#012setsebool -P nis_enabled 1#012#012***** Plugin catchall (1
.41 confidence) suggests *****#012#012If you believe that sshd should
be allowed name_bind access on the port 2222 tcp_socket by default.#012Then you should report
this as a bug.#012You can generate a local policy module to allow this access.#012Do#012allo
w this access for now by executing:#012# grep sshd /var/log/audit/audit.log | audit2allow -M
mypol#012# semodule -i mypol.pp#012
```

例外狀況的排除

- 其實在 `/var/log/messages` 會告訴你如何處理！
 - 依據說明，選擇最大可信度的項目，按照說明去執行錯誤克服！就搞定了！

```
.oot@localhost ~]# sealert -l 93c79b52-b575-470f-bc28-3f8485e1b673
SELinux is preventing /usr/sbin/sshd from name_bind access on the tcp_socket port 2222.

**** Plugin bind_ports (92.2 confidence) suggests ****

If you want to allow /usr/sbin/sshd to bind to network port 2222
Then you need to modify the port type.
Do
# semanage port -a -t PORT_TYPE -p tcp 2222
   where PORT_TYPE is one of the following: ssh_port_t, vnc_port_t, xserver_port_t.

**** Plugin catchall_boolean (7.83 confidence) suggests ****

If you want to allow nis to enabled
```

例外狀況的排除

- 如果發生無法確認的問題
 - 先將 SELinux 啟動到 permissive 狀態
 - `setenforce 0`
 - 然後將錯誤狀況再次實現一次，如果錯誤排除，就是 SELinux ！
 - 請到 `/var/log/messages` 找到相關的錯誤訊息，並加以排除
 - 將 SELinux 再次啟動到 Enforcing 狀態
 - `setenforce 1`
 - 再次實現已經成功的狀態，是否保持成功？若無法保持，代表該解決方案可能不太正確，請再次執行上述程序數次，應該就能處理您的問題了！

多人共管伺服器的管理

怎麼管理SERVER

- 導因：
 - 很多時候，你會用到許多朋友一起管理你的 server
 - 對方會需要切換成為 root 來管理系統
 - 你要告訴對方 root 的密碼嘛？
- 請愛用 sudo 來處理
 - 確認 visudo 裡面有這行：
 - %wheel ALL=(ALL) ALL
 - 將你的朋友加入 wheel 群組
 - usermod -a -G wheel username
 - 這個用戶未來使用 『 sudo su - 』 輸入自己的密碼，就可以變身了！

真的沒問題嘛？

- 其實，所有操作 su 或 sudo 均會被紀錄到 /var/log/secure 檔案內
 - 透過分析該檔案就好了！

```
May 25 11:35:13 localhost sudo: student : TTY=pts/0 ; PWD=/home/student ; USER=root ; COMMAND  
=/bin/su -  
May 25 11:35:13 localhost su: pam_unix(su-l:session): session opened for user root by student  
(uid=0)
```

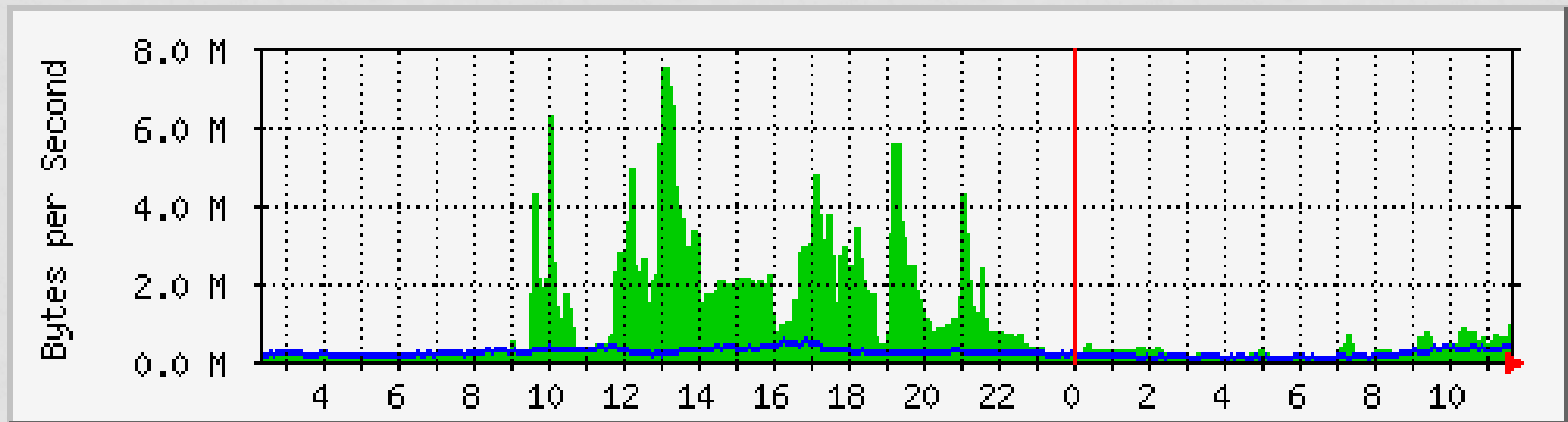

APACHE 服務管理

APACHE 服務設定

- 基礎設定方面
 - Option 內，盡量不要放行 indexes，可避免某些錯誤！
 - 許多系統偵測的腳本，盡量不要對外公開
 - 例如多年前的 awstate 事件
 - 我個人都將 awstate 或者是 MRTG 圖示，通通放置到需要驗證的目錄
 - 使用 Apache 標準認證的方式就可以了！

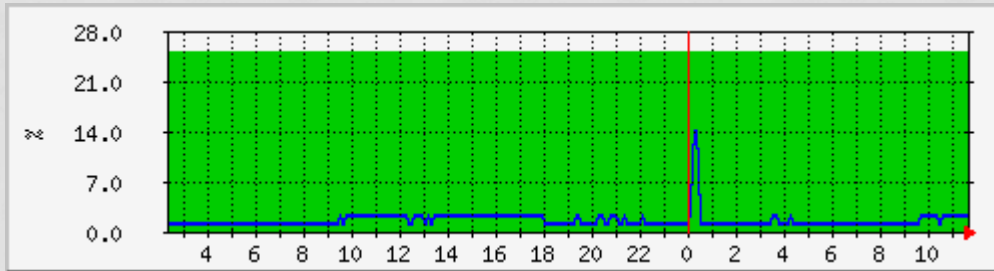
統計系統資訊

- 例如流量統計表

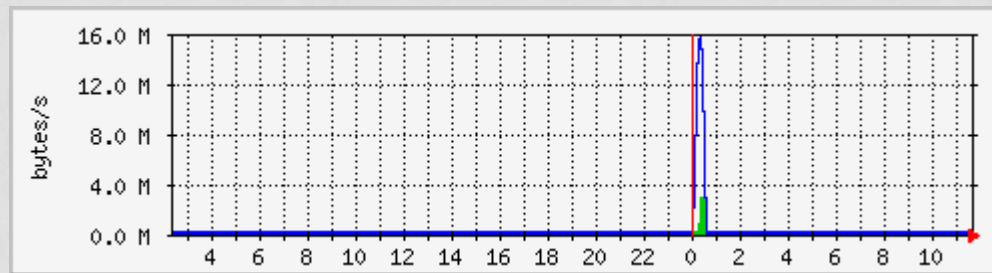


統計系統資訊

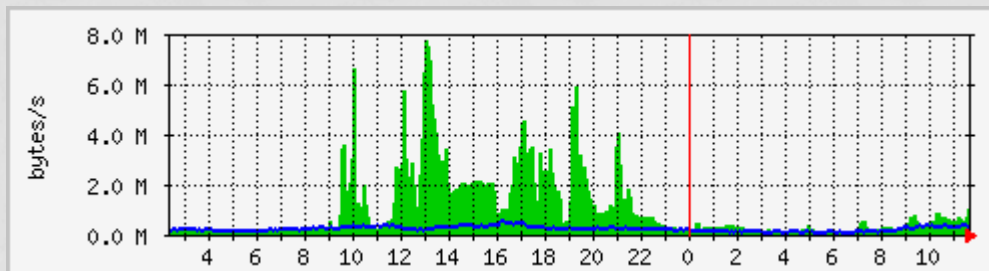
- 例如系統資源表單



CPU 與記憶體



磁碟 I/O 狀態



網路狀態

MRTG 的分析

- 因為系統有很多的分析工具了 (sar)
 - 網路分析：
 - `iostat=$(LANG=C sar -n DEV ${timer} | grep Average | grep 'eth0' | awk '{print $5, $6}')`
 - `in=$(echo "scale=3; $(echo ${iostat} | cut -d ' ' -f 1)*1024" | bc)`
 - `out=$(echo "scale=3; $(echo ${iostat} | cut -d ' ' -f 2)*1024" | bc)`

MRTG 的分析

- 因為系統有很多的分析工具了 (sar)
 - CPU 分析：
 - `cpustat=$(LANG=C sar -u ${timer} | grep Average | awk '{print $6, $8}')`
 - `cputotal=$(echo "scale=3; 100 - $(echo ${cpustat} | cut -d ' ' -f 2)" | bc)`
 - `testing=$(echo $cputotal | cut -d '.' -f 1)`
 - `["$testing" == ""] && cputotal="0${cputotal}"`
 - `cpuiowait=$(echo ${cpustat} | cut -d ' ' -f1)`

MRTG 的分析

- 因為系統有很多的分析工具了 (sar)
 - 磁碟分析：
 - `iostat=$(LANG=C sar -d ${timer} | grep Average | grep 'dev252-0' | awk '{print $4, $5}')`
 - `out=$(echo "scale=3; $(echo ${iostat} | cut -d ' ' -f 1)*512" | bc)`
 - `in=$(echo "scale=3; $(echo ${iostat} | cut -d ' ' -f 2)*512" | bc)`

MRTG 的分析

- 系統既有的工具，不用 snmp 了！
 - 效能也很好，也不需要額外的服務！
 - 不過就是要記得，你的輸出不要放在對外公開的環境內！
 - 除非是某些政策需要公開
 - 否則就不要公開！

要不要放行 3306 呢？

- 你用 MySQL 時，3306 要放行防火牆嘛？
 - 你的 Apache 是讀取本機的 MySQL 3306
 - 所以讀取的是 lo 這個 127.0.0.1
 - 所以防火牆當然不需要針對 3306 放行！

SQL INJECTION

- 這是啥？
 - 使用者輸入 input 欄位時，給予怪異的 SQL 語法！
 - 正常的語法是這樣：
 - `select login_name, realname from userinfo where login_name = '$login_name' and login_pass = '$login_pass'`
 - 一般 login_name 就是帳號，帳號通常沒啥問題對吧！
 - 如果 login_name 的欄位被輸入：
 - `myname' or 'x'='x'`
 - 整個 SQL 會變成：
 - `select login_name, realname from userinfo where login_name = 'myname' or 'x' = 'x' and login_pass = '$login_pass'`
 - 很可能就會繞過正常的檢查程序！

SQL INJECTION

- 怎麼預防：
 - 在登入，或者是比較重要的第一層關卡，透過比較嚴格的字元比對判斷，就可以拒絕大部份的困擾！
 - 例如，帳號要求只能是數字、底線、英文、減號，再透過 PHP 內部程式碼的正規表示法比對，去除錯誤的字碼，不許登入或註冊，就可以避免大部分登入時產生的錯誤！
 - 不過，程式開發人員，就得要知道哪些項目是最重要的 input 資訊

SQL INJECTION

- 怎麼預防：

- 其實還有很嚴重的單引號問題！可以透過呼叫底下的程式碼處理：

```
foreach ($_POST as &$inp){
    $inp=str_replace("'", "''", $inp);
    $inp=str_replace("<", "&lt;", $inp);
}
foreach ($_GET as &$inp){
    $inp=str_replace("<", "&lt;", $inp);
}
foreach ($_REQUEST as &$inp){
    $inp=str_replace("<", "&lt;", $inp);
}
```

基礎保護

日誌分析

- 一定要有安裝日誌分析
 - Watchlog 原廠資料就很完整了！
 - 鳥哥自己也有做分析

```
75 ruser=admin rhost=110.255.22.163
  1 ruser=admin rhost=117.204.155.123
  9 ruser=admin rhost=67.108.232.221.broad.wh.hb.dynamic.163data.com.cn
75 ruser=admin@ksu.edutw rhost=110.255.22.163
75 ruser=data rhost=110.255.22.163
  1 ruser=ftp rhost=124.29.211.186 user=ftp
  1 ruser=ftp rhost=host-94-100-224-52.magtinet.ge user=ftp
75 ruser=guest rhost=110.255.22.163
75 ruser=ksu rhost=110.255.22.163
  9 ruser=ksu rhost=67.108.232.221.broad.wh.hb.dynamic.163data.com.cn
  3 ruser=ksu rhost=dns70.online.tj.cn
75 ruser=ksu.edutw rhost=110.255.22.163
  9 ruser=ksu.edutw rhost=67.108.232.221.broad.wh.hb.dynamic.163data.com.cn
  9 ruser=ksu.edutw123 rhost=67.108.232.221.broad.wh.hb.dynamic.163data.com.cn
75 ruser=ksu@ksu.edutw rhost=110.255.22.163
75 ruser=ksuedutw rhost=110.255.22.163
  9 ruser=ksuedutw rhost=67.108.232.221.broad.wh.hb.dynamic.163data.com.cn
  2 ruser=ksuedutw rhost=dns70.online.tj.cn
  9 ruser=ksuedutw123 rhost=67.108.232.221.broad.wh.hb.dynamic.163data.com.cn
75 ruser=test rhost=110.255.22.163
```

日誌分析

- 日誌分析裡面常見的資料：
 - RAID 是否健康？磁碟系統是否健康？
 - 檔案系統容量是否足夠？
 - 最近誰用了 sshd ！
 - 登入資訊 (last) 是否有問題？
 - /var/log/secure 的資料是否有錯誤
 - /var/log/messages 單日產生的錯誤訊息是否過多？
 - /var/log/httpd/error_log 單日產生的錯誤訊息是否過多？
 - 有沒有 yum 新的軟體？這些軟體安裝後是否需要重新開機？
 - 備份狀態有沒有順利進行？

日誌分析的判斷

- 關於系統異常的偵測：
 - 異常行為：
 - 不正常斷線？不正常重新開機？多餘的網路連線？過高的 CPU 使用率
 - 登錄檔的遺失；
 - 檔案權限無預警的變更；
 - 多餘且無法確認的隱藏檔；
 - suid/sgid 檔案的增加；
 - 基本的偵測工具：
 - http://www.rootkit.nl/projects/rootkit_hunter.html
 - <http://www.tripwire.com/>


服務狀態

- 服務的啟動與否？
 - 沒用到的網路服務一定就得要關閉
 - 有用到的網路服務記得最好啟動 SELinux 去管理
 - 資料是否需要公開？不公開就請放在 Internet 瀏覽不到，或者是有低階認證的環境中 (例如 Apache 的 basic 認證)
 - 某些可怕的服務可以代管就代管 (例如 mail server)
 - 某些可取得 shell 的服務只開自己的後門
 - 例如 sshd 這個服務，最好不要對 Internet 啟動
 - 最好取消 root 登入權
 - 最好只對某些點放行連線權

防火牆規劃

- 盡可能簡單明瞭，方便自己未來測試與訂正
 - 一定使用 INPUT 是 DROP 的政策
 - 重要服務千萬不可對 Internet 放行
 - 一定要經常監控 log 檔案的分析

```
[root@localhost ~]# iptables-save
# Generated by iptables-save v1.4.21 on Thu May 25 12:18:36 2017
*filter
:INPUT DROP [24958:3554710]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [1807902:252719137]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -s 192.168.0.254/32 -j ACCEPT
-A INPUT -s 192.168.0.0/24 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 172.16.0.0/16 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 21 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 555 -j ACCEPT
COMMIT
# Completed on Thu May 25 12:18:36 2017
```



分享分享-桌機怎麼裝？

主機的安裝到上線

- 1. 安裝前準備：
 - 準備好硬體，先不要接網路線；
 - 選擇較新的且來源沒問題的作業系統來安裝；
 - 事先規劃好未來的主機用途，以決定各個 partition：
 - C 槽要多大？是否要 D、E 槽？
 - 資料很重要時，要不要透過磁碟陣列 (RAID)？
 - 若可能，事先下載 service pack (sp)
 - 確認無誤後，準備安裝....

主機的安裝到上線（續）

- 2. 開始安裝與 post-install procedure :
 - 依照主機的服務目的、未來規劃，開始進行 partition ；
 - 不需要的服務就不要安裝到主機上面 ；
 - 設定管理員密碼嚴格一些 ；
 - 安裝完畢並重新開機後：
 - 檢查開啟的服務，沒有必要的就關閉 ；
 - 關閉開機就啟動的服務
 - 安裝好你的各項硬體驅動程式

主機的安裝到上線（續）

- 3. 各種必要軟體與 sp 的安裝：
 - 找到系統的 sp ，安裝他
 - 找尋個人防火牆，或者直接啟用 Windows 防火牆系統
 - 最好將主機放置於防火牆 (IP 分享器) 後端
 - 安裝防毒軟體、防木馬軟體等
 - 設定好網路參數
 - 接上網路線，進行連線測試，先進行各項 update 任務

主機的安裝到上線（續）

- 4. 各種應用軟體的安裝與更新：
 - 不是只要安裝妥當就好
 - 記得一定要進行 update ！
 - 記得一件事：Excel 使用不當也會中標 (巨集功能)

主機的安裝到上線（續）

- 5. 登錄檔修訂 (Optional)
 - 我的 C 槽只有軟體與快取檔，並沒有資料
 - 我的 my document 在 D 槽
 - 我的桌面也在 D 槽
 - 收信軟體也在 D 槽
 - 工作所需要的各種表單，也在 D 槽

主機的安裝到上線（續）

- 6. 進行全系統備份
 - 此時你的系統非常的乾淨！
 - 若可能的話，請管理員將你的系統整個備份一下
 - 例如使用 ghost 之類的免費軟體進行備份
 - 以後系統死掉，使用 ghost 復原即可！

主機的安裝到上線（續）

- 7. 隨時進行重要資料的鏡像備份
 - 我的資料都在 D 槽，與 C 槽的軟體無關
 - 重要的備份，其實就是備份 D 而已。
 - 每次都使用檔案總管？作一次備份要到達天荒地老...
 - 使用 `cwsync`，可進行鏡像備份，速度快，效果好！
 - 另外，不要過份相信硬碟，硬碟在現今的環境中，它不過是個消耗品...

主機的安装到上线 (續)

- 8. 良好的操作習慣 (老實說，鳥哥也不見得作的到)
 - 不要以為自己的主機不會淪陷！
 - 不要隨便點選莫名的網站
 - 不要太信任任何一個網站所需要你提供的重要資料
 - Browser 的設定很重要，非必要的功能就關掉。
 - 多認識一些網路基礎，對你未來瞭解如何抵擋 cracker 是相當有幫助的
 - 木馬與蠕蟲無所不在
 - USB 是重大的資安問題！包括資料外洩、病毒傳遞等

敬請多多指教！