經濟部資訊專業人員鑑定—開放式系統類

Linux進階系統管理
日誌管理與套件管理

崑山科技大學資訊傳播系
蔡德明
(鳥哥, VBird)

分享指引

- 登錄檔
- 原始碼與Tarball
- Linux distributions提供的安裝/升級機制
- 精選範例

登錄檔

系統登錄檔

- 登錄檔所記錄的資訊：
  - 事件發生的日期與時間；
  - 發生此事件的主機名稱；
  - 啓動此事件的服務名稱 (如 samba, xinetd 等) 或函式名稱 (如 libpam ..)；
  - 該訊息資料內容。
- 與登錄檔有關的服務與指令
  - syslogd → 主程式
  - logrotate → 進行登錄檔輪替的指令

系統登錄檔案

- 系統相關登錄檔：
  - /var/log/secure：登錄有『認證』資訊的紀錄
  - /var/log/wtmp：記錄登入者的訊息資料，可用 last 讀取
  - /var/log/messages：預設系統資訊登錄的檔案(非常重要)
  - /var/log/maillog 或 /var/log/mail/*：紀錄郵件存取或往來 (sendmail 與 pop3)的使用者記錄；
  - /var/log/cron：記錄 crontab 這個例行性服務的內容的！
- 其他服務的登錄資訊
  - /var/log/httpd, /var/log/news, /var/log/mysqld.log, /var/log/samba, /var/log/procmail.log

syslogd

- 設定檔 /etc/syslog.conf 語法
  - 服務名稱[.=!]訊息等級　　訊息記錄的檔名或裝置或主機
  - mail.info　　/var/log/maillog_info
- 服務名稱
  - # auth, authpriv：主要與認證有關的機制，例如 telnet, login, ssh 等
  - # cron：就是例行性命令 cron/at 等產生訊息記錄的地方；
  - # daemon：與各個 daemon 有關的訊息；
  - # kern：就是核心 (kernel) 產生訊息的地方；
  - # lpr：亦即是列印相關的訊息啊！
  - # mail：只要與郵件收發有關的訊息紀錄都屬於這個；
  - # news：與新聞群組伺服器有關的東西；
  - # syslog：就是 syslogd 這支程式本身產生的資訊啊！

syslogd(續)

- 訊息等級
  - 1. info ：僅是一些基本的訊息說明而已；
  - 2. notice：比 info 還需要被注意到的一些資訊內容；
  - 3. warning 或 warn：警示的訊息，可能有問題， 但是還不至於影響到某個 daemon 運作的資訊；
  - 4. err 或 error ：一些重大的錯誤訊息， 例如設定檔的某些設定值造成該服務服法啓動的資訊說明！
  - 5. crit：比 error 還要嚴重的錯誤資訊！
  - 6. alert：警告，已經很有問題的等級，比 crit 還要嚴重！
  - 7. emerg 或 panic：疼痛等級，意指系統已經幾乎要當機的狀態！ 很嚴重的錯誤資訊了。

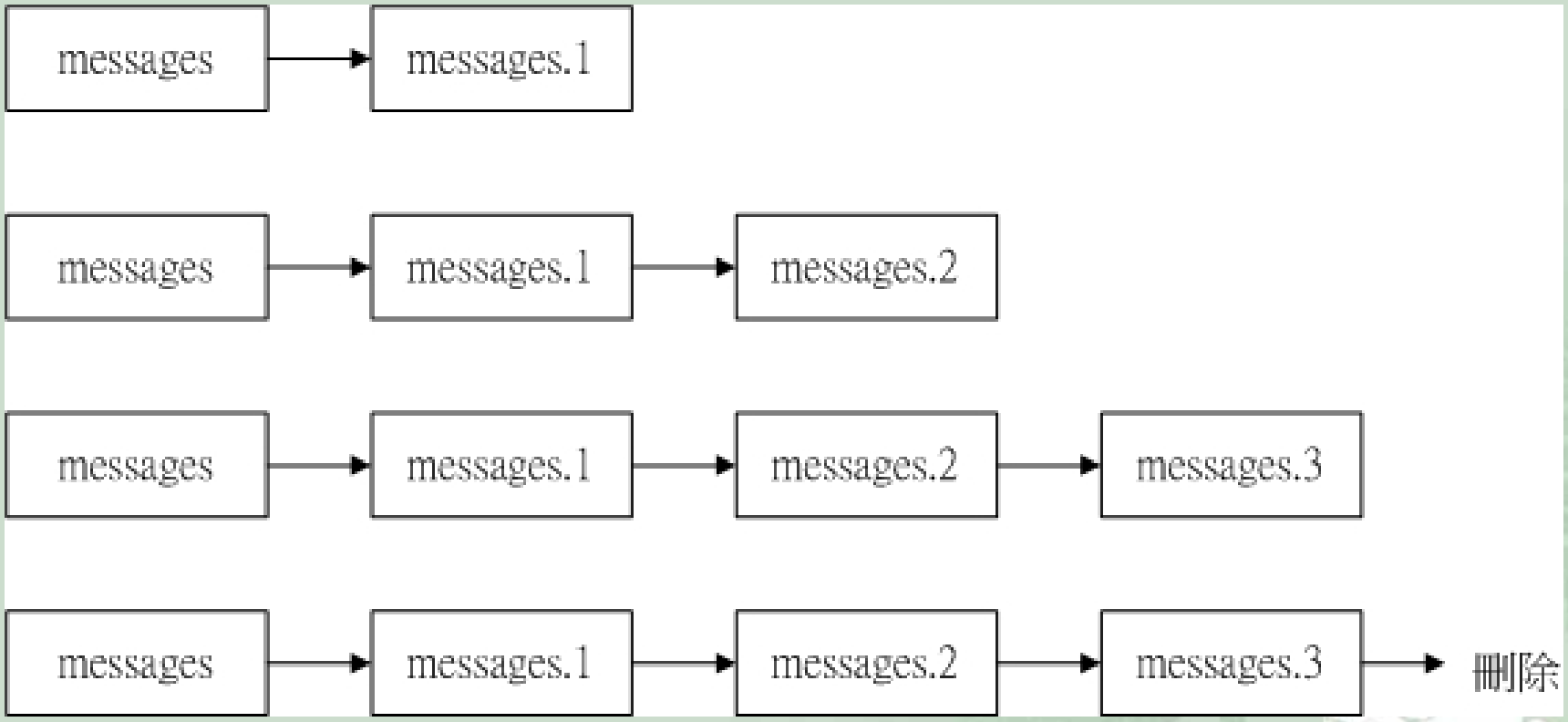
syslog.conf

- 系統預設內容
  - *.info;mail.none;authpriv.none;cron.none /var/log/messages
  - authpriv.* /var/log/secure
  - mail.* -/var/log/maillog
  - cron.* /var/log/cron
  - *.emerg *
  - uucp,news.crit /var/log/spooler
  - local7.* /var/log/boot.log
- 非同步化：如上第三行最右邊，加上 – 可增加效能(先記憶在記憶體中，與檔案系統非同步)

syslogd相關

- 登錄資訊所需要的daemons
  - syslogd
  - klogd
- 讓主機變成登錄檔伺服器
  - 伺服器：
    - 啓動 syslogd 時，加入 –r 參數(或修改 /etc/sysconfig/syslog)
    - 啓動的埠口爲 514 (UDP封包)
  - 用戶端：在 /etc/syslog.conf 內，新增一行
    - *.*　　@serverIP

登錄檔的輪替

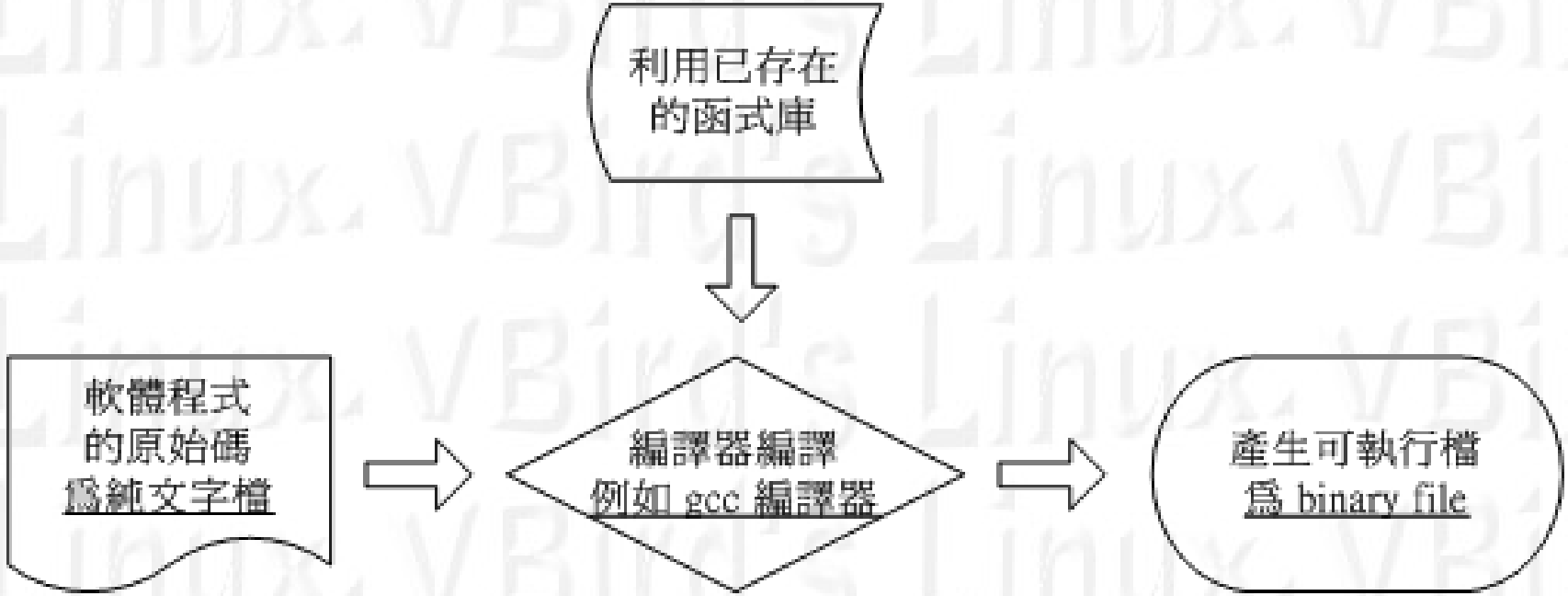

messages
messages.1
messages
messages.1
messages.2
messages
messages.1
messages.2
messages.3
messages
messages.1
messages.2
messages.3
刪除

logrotate 預設內容

- /etc/logrotate.conf 預設情況
  - weekly
  - rotate 4
  - create
  - include /etc/logrotate.d
  - /var/log/wtmp {
  - monthly
  - create 0664 root utmp
  - rotate 1
  - }
- logrotate的運作方式：使用 crontab 喔！

原始碼與Tarball

原始碼與編譯過程



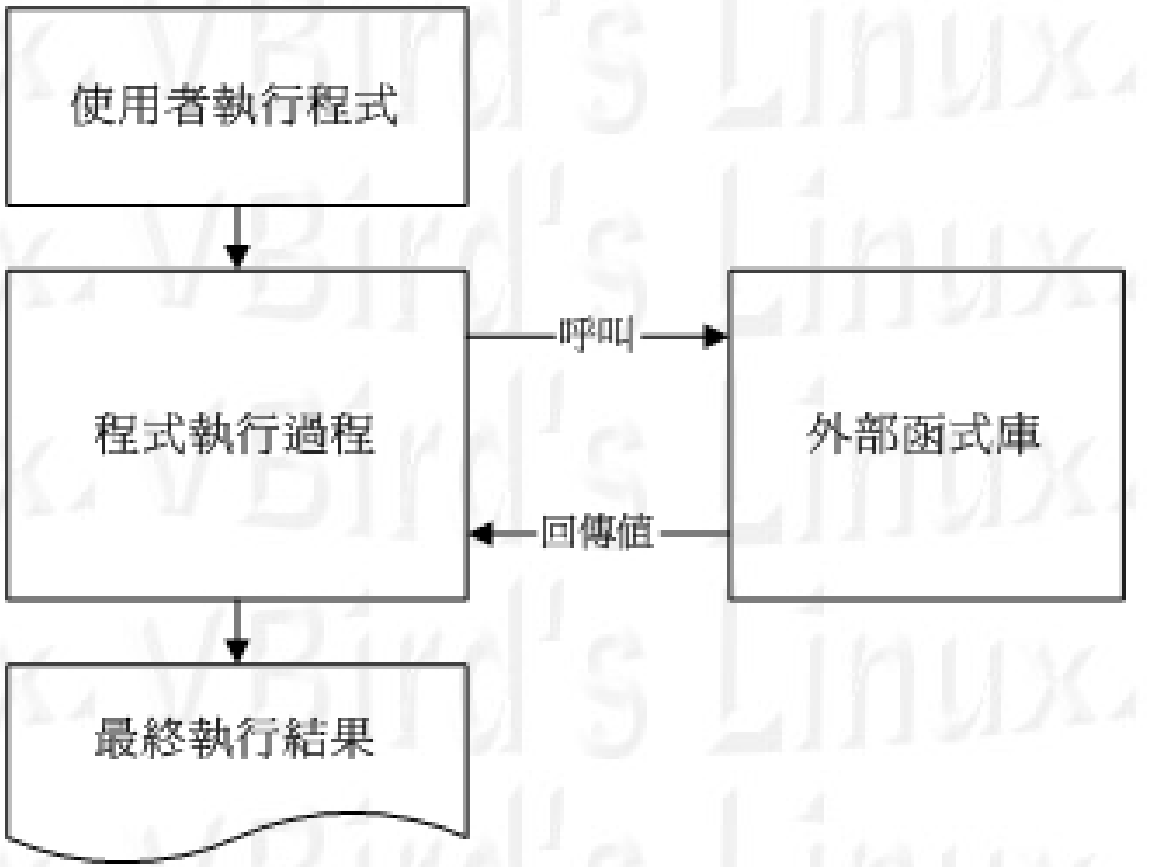
圖一、簡易的 gcc 編譯流程

- file /usr/bin/passwd
- /usr/bin/passwd: setuid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), for GNU/Linux 2.6.9, dynamically linked (uses shared libs), for GNU/Linux 2.6.9, stripped

函式庫

- 函式庫種類
  - 動態函式庫
    - 程式編譯時，並未包含動態函式庫的程式碼，而是以『指向該函式庫所在的檔名』來呼叫使用
    - 通常附檔名爲libname.so
  - 靜態函式庫
    - 程式編譯時，將此函式庫的程式碼編譯進來，可獨立執行而不需要額外呼叫
    - 通常附檔名爲libname.a
- 函式庫放置的目錄
  - /lib, /usr/lib, /usr/local/lib

動態函式庫的呼叫示意圖



圖二、程式引用函式庫的示意圖

函式庫管理

- 查詢某程式的動態函式庫
  - ldd /usr/bin/passwd
- 預先載入動態函式庫，提供系統未來之用
  - /etc/ld.so.conf →設定檔，一行一個目錄
  - ldconfig →載入上述的設定
  - ldconfig –p →顯示目前已載入的函式庫
  - /etc/ld.so.cache →函式庫的快取檔案。

編譯器與編譯

- 編譯器
  - GNU C (gcc), fortran 等等傳統程式語言
- 以gcc編譯的示意
  - gcc –o program file.c
- 如果需要編譯一套軟體，該軟體內有1000個*.c呢？可使用make
  - make 可呼叫工作目錄下的 Makefile 檔案，並據以進行編譯的流程
- 驅動程式編譯尚須的訊息
  - 因爲與kernel相關性高，所以需要kernel-devel套件。

Tarball與安裝

- 原始碼釋出的狀態
  - 由於軟體開發針對不同的作業系統，故以原始碼的形態釋出
  - 爲節省網路頻寬，將原始碼以tar壓縮成*.tar.gz，稱爲tarball
- Tarball的安裝(通常流程)
  - 解壓縮，並查閱新增目錄的INSTALL/README
  - 執行./configure (檢查系統，並建立Makefile)
  - 執行make (開始進行編譯的行爲)
  - 執行 make install(將檔案放置到目錄樹)

Linux distributions提供的安裝/升級機制

Linux distributions

- 利用Tarball的困擾
  - 安裝不容易，而且需要make/autoconfig/kernel-devel等套件
  - 升級不容易，常需要移除再升級
  - 管理不容易，不容易找到所需要的套件資料
- 發佈商的手法：
  - 先在預設的環境下將軟體編譯起來，並打包
  - 利用簡易的指令讓用戶可以直接將軟體放置到正確的目錄樹
  - 建立資料庫，方便使用者查詢到軟體的資訊與檔案
  - 可利用線上升級機制直接 online 安裝/升級/移除等
  - 常見的機制：RPM, DPKG

RPM系統

- RPM：Redhat Package Manager
  - 支援者：RedHat/Fedora/Mandriva/CentOS…等
  - SRPM/RPM
    - xxxxxxxxx.rpm　<==經過編譯且包裝完成的 rpm 檔案
    - xxxxx.src.rpm　<==包含未編譯的原始碼資訊
  - RPM檔名設定
    - rp-pppoe-　3.1　-　5　.i386　.rpm
    - 套件名稱 版本資訊 釋出次數 硬體平台 附檔名
      - i386, i686, x86_64…

RPM的優點

- RPM 檔案本身爲已經編譯過的 binary 檔案，可以讓 client 端的使用者免除重新編譯的困擾；
- RPM 檔案在被安裝之前，RPM 會先檢查系統的硬碟容量、作業系統版本等，可避免檔案被安裝錯誤
- RPM 檔案本身提供套件版本資訊、相依屬性套件名稱、套件用途說明、套件所含檔案等資訊，便於瞭解套件；
- RPM 管理的方式使用資料庫記錄 RPM 檔案的相關參數，便於升級、移除、查詢與驗證。

RPM的使用

- 安裝：
  - rpm –ivh package.rpm →全新安裝
  - rpm –Uvh package.rpm →升級(若未安裝則安裝)
  - rpm –Fvh package.rpm →升級(僅升級有安裝者)
- 查詢：
  - rpm -qa
  - rpm -q[licdR] 已安裝的套件名稱
  - rpm -qf 存在於系統上面的某個檔案
  - rpm -qp[licdR] 未安裝的某個檔案名稱

RPM的使用(續)

- 查詢的細項

```
[root@linux ~]# rpm -qa
[root@linux ~]# rpm -q[licdR] 已安裝的套件名稱
[root@linux ~]# rpm -qf 存在於系統上面的某個檔案
[root@linux ~]# rpm -qp[licdR] 未安裝的某個檔案名稱
參數：
在查詢的部分，所有的參數之前都需要加上 -q 才是所謂的查詢！
查詢主要分為兩部分，一個是查已安裝，另一個則是查某個 rpm 檔案內容。
查詢已安裝套件的資訊：
-q  ：僅查詢，後面接的套件名稱是否有安裝；
-qa ：列出所有的，已經安裝在本機 Linux 系統上面的所有套件名稱；
-qi ：列出該套件的詳細資訊 (information)，包含開發商、版本與說明等；
-ql ：列出該套件所有的檔案與目錄所在完整檔名 (list)；
-qc ：列出該套件的所有設定檔 (找出在 /etc/ 底下的檔名而已)
-qd ：列出該套件的所有說明檔 (找出與 man 有關的檔案而已)
-qR ：列出與該套件有關的相依套件所含的檔案 (Required 的意思)
-qf ：由後面接的檔案名稱，找出該檔案屬於哪一個已安裝的套件；
查詢某個 RPM 檔案內含有的資訊：
-qp[icdlR]：注意 -qp 後面接的所有參數以上面的說明一致。但用途僅在於找出
            某個 RPM 檔案內的資訊，而非已安裝的套件資訊！注意！
```

RPM的使用(續)

- 驗證：
  - rpm -Va
  - rpm -V 已安裝的套件名稱
  - rpm -Vp 某個 RPM 檔案的檔名
  - rpm -Vf 在系統上面的某個檔案
- 反安裝與重建資料庫
  - rpm -e logrotate <==解安裝 logrotate 套件
  - rpm --rebuilddb <==重建資料庫

SRPM的使用

- SRPM
  - 該檔案內僅有原始碼
  - 需要再編譯才能變成RPM
  - 可直接使用 rpmbuild 來處理
    - rpmbuild --rebuild package.src.rpm
      - 將SRPM編譯並打包成爲RPM
      - RPM檔案通常放置到/usr/src/redhat/RPMS/中
    - rpmbuild --recompile package.src.rpm
      - 編譯、打包並且『安裝』起來了！

SRPM的使用(續)

- SRPM安裝/編譯時，會用到的目錄：

/usr/src/redhat/SPEC	這個目錄當中放置的是該套件的設定檔，例如這個套件的資訊參數、設定項目等等都放置在這裡；
/usr/src/redhat/SOURCE	這個目錄當中放置的是該套件的原始檔（*.tar.gz的檔案）以及 config 這個設定檔；
/usr/src/redhat/BUILD	在編譯的過程中，有些暫存的資料都會放置在這個目錄當中；
/usr/src/redhat/RPMS	經過編譯之後，並且順利的編譯成功之後，將打包完成的檔案放置在這個目錄當中。裡頭有包含了 i386, i586, i686, noarch.... 等等的次目錄。

SRPM的重新修改與編譯

- SRPM若需要修改參數：
  - 修改*.spec檔案，在/usr/src/redhat/SPEC/中
- 重新編譯/打包的動作
  - RPM：
    - rpmbuild -bb rp-pppoe.spec <==編譯成RPM檔案
  - SRPM：
    - rpmbuild -ba rp-pppoe.spec <==打包成SRPM檔案與RPM檔案

RPM系統的線上升級

- yum軟體
  - yum server
    - 提供資料庫，讓用戶端可分析軟體相關性
    - 提供RPM檔案，直接讓使用者下載安裝
  - yum 指令
    - 下載資料庫中的軟體相關性
    - 可以直接安裝/移除/升級軟體。
    - 範例：
      - yum update →全系統升級
      - yum install package →僅安裝package
      - yum groupinstall ‘groupname’

Debian套件管理員

- 於Debian系統常用的套件管理員
  - 支援者：Debian, Ubuntu, B2D…
- 檔名設定依據：
  - program_version-revision_processor .deb
  - 軟體名稱　版本　釋出版本 硬體等級　附檔名
- 常用指令：
  - dpkg　套件管理工具，尤其是查詢方面的能力
  - atp-get　　可透過網路取得安裝/升級套件

dpkg的使用

- dpkg [動作]
  - 安裝
    - -i package　：安裝package這個軟體
    - -R /dir/　：安裝在某個目錄下的所有軟體檔案
  - 移除：
    - -r package　：移除package這個軟體(不含設定檔)
    - -P package　：移除package這個軟體(含設定檔)
  - 查詢：
    - -L package　：列出package含有的檔案名稱
    - -l keyword　：列出含有keyword的的軟體名
    - -S file　：找出file屬於那個軟體

Debian軟體的轉換

- 可以透過alien轉換不同的套件
  - 語法：
    - alien -i [來源格式] [目標格式] [選項] [套件名]
    - 格式：
      - -d：debian的.deb格式
      - -r：redhat的rpm格式

利用APT功能

- 線上升級機制：
  - 透過APT伺服器的功能
  - APT用戶端
    - /etc/apt/apt.conf　：用戶端的apt使用環境
    - /etc/apt/sources.list：適合的APT Server套件來源
  - ATP用戶端使用的工具程式
    - apt-cache　：用在查詢的指令
    - apt-get　：用在安裝/升級/移除的指令

apt-get的用法

```
[root@test root]# apt-get <options> <更新項目> <套件名稱>
參數說明：
options：關於參數有底下幾個較常見的：
    -q 不要顯示 apt-get 運作時的輸出訊息，安靜一點比較好嗎？！ ^_^
    -y 如果 apt-get 在工作過程中需要使用者回應，這個參數可以直接回答 yes
更新項目：更新的動作有底下幾個：
    update：這個動作很重要，就是我們上面有提到的，Client 端要更新與 APT Server
            套件相關性檔案的清單對應表，就得要使用這個項目了！基本上，
            每次進行 apt-get 來下載 APT Server 的檔案前，最好都先 apt-get update
    install：安裝某個套件，後面接套件名稱
    dist-upgrade：自動升級我們系統上面已經安裝的所有 RPM 套件喔
    clean：將下載自 APT 主機的的 RPM 檔案刪除哩！
    remove：移除已經安裝在我們系統的某個套件！
範例：
[root@test root]# apt-get update           # 將 RPM 檔案相關性清單更新！
[root@test root]# apt-get install tcpdump # 安裝 tcpdump 這個套件
[root@test root]# apt-get -y dist-upgrade  # 升級我們系統上面的所有 RPM 套件
[root@test root]# apt-get clean
```

精選範例

- 若要更改系統記錄檔所存放的目錄與檔案名稱，可以修改以下哪個檔案？ A
  - (A) /etc/syslog.conf
  - (B) /etc/log/syslog.conf
  - (C) /var/log/syslog.conf
  - (D) /sys/log/syslog.conf

- 以下何種檔案名稱，不是 Linux 的 Package？ C
  - (A) ssh.rpm
  - (B) ssh.deb
  - (C) ssh.pack
  - (D) ssh.tar.gz

- 某一Linux管理員修改logrotate.conf的設定，將某一log的更換條件設爲100K，但當天卻發現log的體積明明超過100K卻沒有被更換，而非得等到下一天才更換。請問可能原因爲何？ D
  - (A) logrotate程式可能罷工了
  - (B) 管理員忘記將 logrotate daemon重新啓動
  - (C) logrotate不接受100K這樣的條件
  - (D) logrotate程式是用crontab排程啓動的，預設是每天深夜才跑一次

- 請問syslogd將記錄送給其他電腦時，所使用的通訊埠爲？C
  - (A) 541
  - (B) 154
  - (C) 514
  - (D) 415

- 當妳啓動syslog服務時，有哪兩個daemon會被啓動？AD
  - (A) syslogd
  - (B) logrotate
  - (C) logwatch
  - (D) klogd

- /etc/syslog.conf有一行設定爲『mail.warn -/var/log/mail』請問下列何者正確？ B
  - (A) 有關mail的warn等級的訊息會直接輸出到檔案/var/log/mail
  - (B) 有關mail的warn等級與以上等級的訊息會儲存到buffer至一定量後輸出到檔案/var/log/mail
  - (C) 有關mail的warn等級的訊息會儲存到buffer至一定量後輸出到檔案/var/log/mail
  - (D) 有關mail的warn及warning等級的訊息會直接輸出到檔案/var/log/mail

- 若妳執行『rpm –ivh bar-1.0-1.i386.rpm』卻出現『failed dependencies: foo is needed by bar-1.0-1』，可能的問題在哪裡？C
  - (A) 該軟體已經安裝過
  - (B) 軟體相衝或不相容
  - (C) 此套件與其他套件有相依性的問題
  - (D) 套件版本無法相容

- 使用dpkg移除套件及設定檔，下列何者正確？D
  - (A) dpkg –r hdparm
  - (B) dpkg –l hdparm
  - (C) dpkg –I hdparm
  - (D) dpkg –P hdparm

- 下列套件中哪些檔案屬於原始碼安裝套件？ BC
  - (A) vsftpd-1.2.0-5.i386.rpm
  - (B) cpio-2.5-3.src.rpm
  - (C) squid-2.5.STABLE2.tar.gz
  - (D) bash_2.05-7_i386.deb

- RPM套件封裝製作中『rpmbuild –ba zip-2.3.spec』作用為何？D
  - (A) 檢查 file list
  - (B) 測試包裝 RPM 套件，但並不會產生 RPM 套件
  - (C) 執行 %Prep, %build, %insall section，並產生binary RPM軟體
  - (D) 執行 %Prep, %build, %insall section，並產生binary RPM軟體與 source RPM

- 以下關於Debian套件管理之敘述何者『不正確』？C
  - (A) Debian套件檔名的附檔名爲 .deb
  - (B) 安裝某一套件指令爲dpkg –i package.deb
  - (C) 升級某一套件的版本指令爲dpkg –u package.deb
  - (D) 列出某一套件之相關內容的指令：dpkg –l package.deb

- 修改哪一個設定檔可以指示apt-get程式，未來安裝套件時可以由國內的mirror站來下載？A
  - (A) /etc/apt/sources.list
  - (B) /etc/apt-get/sources.list
  - (C) /etc/pkg/sources.list
  - (D) /etc/dpkg/sources.list

- 在Debian Linux系統中，如下那個操作可以查詢到名爲foobar套件之全部安裝檔案清單？B
  - (A) dpkg –l foobar
  - (B) dpkg –L foobar
  - (C) dpkg –ql foobar
  - (D) dpkg –q --allfiles foobar

- 如下哪一項操作可得知ls命令所需的函式庫？B
  - (A) ldd ls
  - (B) ldd `which ls`
  - (C) ldd ‘which ls’
  - (D) ldd –q ls

- 在debian中，哪一工具可將 rpm 轉成 deb？A
  - (A) alien
  - (B) dpkg --import
  - (C) apt-get --rpm
  - (D) rpm-2-deb

- 某管理員用tarball安裝某一套件，但該套件的動態函式庫路徑並沒有出現在系統當前的設定中。妳想要預先載入該函式庫的作法爲？D
  - (A) 編輯/etc/ldd.conf，執行 ldd
  - (B) 編輯 /etc/ld.so.conf ，執行 ldd
  - (C) 編輯 /etc/ld.so.cache 即可
  - (D) 編輯 /etc/ld.so.conf ，執行 ldconfig

- 如下哪一操作可列出系統當前的動態函式庫與其路徑的對照表？A
  - (A) ldconfig -p
  - (B) ldconfig -v
  - (C) cat /etc/ld.so.conf
  - (D) cat /etc/ld.so.cache

- 如欲檢視目前系統上所有已安裝的RPM檔案屬性是否變更，該如何下達指令？B
  - (A) rpm -qa
  - (B) rpm -Va
  - (C) rpm -lqp
  - (D) rpm -pa

- 系統上有一檔名 foo，如何知道foo屬於那個rpm軟體？D
  - (A) rpm –qa foo
  - (B) rpm –Va foo
  - (C) rpm –qp foo
  - (D) rpm –qf foo

- 各家distributions都用不同的套件管理模式，下列哪些是主要的套件管理工具程式？ACD
  - (A) yum
  - (B) gzip
  - (C) rpm
  - (D) apt

- 如欲重新建置 RPM 資料庫，應如何進行指令？D
  - (A) rpm –r database
  - (B) rpm –rebuild database
  - (C) rpm –database rebuild
  - (D) rpm --rebuilddb