Unit 4　常見的系統服務(非網路服務)

2007/12/11 建立 by VBird

1. 常見的 daemon 與服務 (service) 類型
   A. 所謂的 daemon 可以想成：『在背景中執行的一支常駐程式』，這支 daemon 可以提供某些服務
   B. 若爲網路服務，則該服務的 port 與服務名稱的對應可於 /etc/services 檔案中查得！
   C. Stand alone 服務：可單獨啓動的服務，反應速度快，但會一直佔據記憶體資源。
      i. 通常使用『 /etc/init.d/服務名稱 {start|stop|restart} 』來啓動、停止或重新啓動
   D. Super daemon：統一透過一支控管程式來處理服務的啓動，該服務只有在使用到時才會啓動。雖然比較不耗系統支援(平時沒有被啓動)，但是需要一些時間的喚醒。
      i. 這支 super daemon 稱爲『 xinetd 』
      ii. 設定檔在『 /etc/xinetd.d/服務名稱 』當中，亦可使用 chkconfig 直接設定
      iii. 最後必須使用『 /etc/init.d/xinetd restart 』來重新啓動喔！
2. 練習題一：瞭解何謂 super daemon 與其啓動方式
   A. 請使用 rpm 查詢系統是否有安裝 telnet-server 這個套件？_____
   B. 如果沒有的話，該如何安裝這個套件？_____
   C. 這個服務的啓動是依據 stand alone 還是 super daemon 的方法？_____
   D. 請問你如何啓動這個服務？_____

3. 網路校時功能：
   A. 直接以手動方式處理的話，可以使用：
      i. ntpdate tock.stdtime.gov.tw
      ii. 可配合 /etc/crontab 這個檔案的設定來定時處理即可
   B. 可利用 NTP (Network Time Protocol) 協定來即時更新系統時間：
      i. 必須安裝的套件名稱爲：『ntp』
      ii. 設定檔在：/etc/ntp.conf，可增加一行設定，約在第 16 行，『server tock.stdtime.gov.tw』即可
      iii. 啓動方式：『chkconfig ntpd on』、『/etc/init.d/ntpd start』，請察看 port 123。
4. 練習題二：請花 5~10 分鐘完成底下的練習：
   A. 如何查閱目前你的系統時間？_____
   B. 如何修改時區設定？例如由台北時間改爲美國時間？_____
   C. 如何查詢目前系統的硬體時間(BIOS)？_____
   D. 請立即進行網路校時工作：_____
   E. 啓動 NTP 協定，並且加入台灣地區的 tock.stdtime.gov.tw 在設定檔中
   F. 過大約數十分鐘後，使用底下的指令來進行觀察連線狀態：

      ntpstat、 ntptrace -n 127.0.0.1、 ntpq -p

5. 登錄檔的管理與設定；
   A. 常見的登錄檔有： (page 74)
      i. /var/log/messages：幾乎系統所有的預設資料都會被丟進這個檔案中！
      ii. /var/log/maillog ：與郵件有關的資料都放進這個檔案中
      iii. /var/lg/secure ：例如登入的資訊，安全性及 xinetd 的資料都放進這個檔案中
   B. 主要登錄的資訊爲：『何時、何地(IP 或主機名稱)、何種服務、什麼動作或資訊』
      i. Dec 11 14:55:05 localhost sshd[24738]: Accepted password for vbird from 203.71.39.249 port 2316 ssh2

C. 登錄資訊的傳遞方式(將訊息丟給誰看的意思)(page 75 說明第二段)

i. 記錄到 file 中(如上面提到的檔案)
ii. 廣播給線上的所有使用者 (例如 shutdown 機器時)
iii. 傳輸到某個終端機，例如 tty1 常有一些資訊會跑出來
iv. 亦可傳輸到某部遠端主機上面，這個就是『網路登錄主機』的情況！

D. 登錄資訊的服務與設定檔：服務名稱『syslogd 或 klogd』，設定檔『/etc/syslog.conf, /etc/sysconfig/syslog』

i. 設定檔的語法如下：

```
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
```

ii. 常見的服務名稱：

1. auth, authpriv：主要與認證有關的機制，例如 login, ssh 等需要認證的服務都是使用此一機制
2. cron：就是例行性命令 cron/at 等產生訊息記錄的地方；
3. daemon：與各個 daemon 有關的訊息；
4. kern：就是核心 (kernel) 產生訊息的地方；
5. lpr：亦即是列印相關的訊息啊！
6. mail：只要與郵件收發有關的訊息紀錄都屬於這個；
7. news：與新聞群組伺服器有關的東西；
8. syslog：就是 syslogd 這支程式本身產生的資訊啊！
9. user, uucp, local0 ~ local7：與 Unix like 機器本身有關的一些訊息

iii. 常見的等級：

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；基本上， info, notice, warn 這三個訊息都是在告知一些基本資訊而已
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， 通常藉由 err 的錯誤告知，應該可以瞭解到該服務無法啓動的問題呢！
5. crit：比 error 還要嚴重的錯誤資訊，這個 crit 是臨界點 (critical) 的縮寫
6. alert：警告警告，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。 通常大概只有硬體出問題，導致整個核心無法順利運作，就會出現這樣的等級的訊息吧！

iv. 記錄等級的相關性：

1. . ：代表『比後面還要高的等級(含該等級)都被記錄下來』的意思
2. .= ：代表所需要的等級就是後面接的等級而已，其他的不要！
3. .! ：代表不等於，亦即是除了該等級外的其他等級都記錄。

6. 登錄檔的輪替 (logrotate) 動作：

A. 例如 /var/log/messages->messages.1->messages.2 等動作

B. 可以避免登錄檔越來越大，導致登錄效能變差，或者是 filesystem 被用盡的困擾。

C. 設定檔『/etc/logrotate.conf(系統預設值)』及『/etc/logrotate.d/服務名稱』

D. /etc/logrotate.d/syslog 的範例：

```
/var/log/messages /var/log/secure /var/log/maillog /var/log/spooler /var/log/boot.log
/var/log/cron {
    sharedscripts
    postrotate
        /bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/null || true
    endscript
}
```

E. 強行進行 logrotate 的測試：『logrotate [-vf] /etc/logrotate.conf』

7. 練習題三：請花 10 分鐘左右進行底下的練習與測試。

A. 請參考 /etc/sysconfig/syslog 設定檔內容，查出那個選項會讓你的 syslogd 支援遠端登錄主機？____
B. 請讓你的 syslogd 支援遠端訊息登入，並查閱有無 port 514 的出現？

C. 請關閉你的防火牆：_____

D. 詢問鄰近同學的 IP，並修改設定檔，讓你的『任何訊息』都可以傳輸給鄰近同學

_____

E. 重新啓動 syslogd 後，請鄰近同學看看，他的 /var/log/messages 有無你的登錄資料？

F. 查閱 page 96 最後一行所提供的 logger 指令的用法

8. X Window System：簡稱爲 X ，過去的計畫所產生的版本類別爲： X11 之故！

   A. 元件與各元件的管理：

      i. X Server：管理硬體、驅動程式、額外的 3D 功能(dri, glx...)，只管繪圖不知道圖在哪裡

      ii. X client：就是圖形介面的軟體(X applications)，主要在提供繪圖數據給 X server 來繪製。

      iii. Window Manager：爲特殊的 X client，管理每個 X client 的視窗狀態，包括 titile, resize,....

   B. X Server：

      i. 目前最常用 Xorg 所提供的 X 了，網站： http://www.X.org, http://xorg.freedesktop.org

      ii. 登錄檔在 /var/log/Xorg.0.log，若有問題，請查閱這個檔案！

      iii. 設定檔在：/etc/X11/xorg.conf ，可配合 xfs (X font server) 服務來提供可使用的字型！

      iv. xfs 的設定檔在：/etc/X11/fs/config，可修改『no-listen = tcp 』讓你的 xfs 可否對 network 提供字形

      v. 可使用 X -configure 來重新製作設定檔

      vi. 可配合 /etc/sysconfig/desktop 來設定預設的桌面爲何？(page 79、page 80)

9. 練習題三：瞭解 X server/ Xclient/ Window manager 層層疊疊的作用

   A. 在 [F8] 啓動另一個 X server：_____

   B. 在該 X 當中丟入一個 xeyes 的程式：_____

   C. 在該 X 當中丟入一個 xterm 的終端機程式：_____

   D. 再丟入一個 xeyes 的程式：_____

   E. 請問此時這三個程式能不能互相瞭解對方在何處？可否進行移動等動作？_____

   F. 丟入 twm 這個 WM，再看看三個 X client 能否動作了？_____

   G. 一個一個程式給予刪除，最後關掉 [F8] 吧！_____

10. 練習題四：使用你的 X server 連線到伺服器的 X client，以取得他人的圖形介面來用。

    A. Server 端：需啓動 Xdmcp，亦即是 port 177 才能夠讓人家來連線，這裡是 X client

       i. 關閉 firewall，同時先關閉 SELinux_____

       ii. 編輯圖形介面登入的設定檔：/etc/gdm/custom.conf，找尋『[xdmcp]』在其下『Enable=true』

       iii. 重新啓動 X：『init 3』、『init 5』

       iv. 觀察是否有 port 177 在監聽？_____

    B. Client 端：這個部分需要啓動 X server 喔！

       i. 請查詢您鄰近同學的 IP，並確定他已經啓動 port 177 才行！

       ii. 如何讓你的 X server 可以給 X client 登入使用？(page 81)

       iii. 在 tty1 的地方輸入『X -query IP :1』讓新的 X 啓動在『F8』

       iv. 嘗試在 [F8] 以 student 的身份登入(預設不可以 root 登入遠端)

11. 練習題五：使用 VNC 連線進入 VNC server 端喔！

    A. Server 端：必須啓動 VNC server 才行：

       i. 先確認一下 port 177 是否已經啓動了？_____

       ii. 切換成爲某個使用者，例如 student，並且執行 vncpasswd，建立 VNC 密碼

       iii. 建立啓動的 script，將 script 清空：『cd ~/.vnc; touch xstartup; chmod 755 xstartup』

       iv. 啓動 VNC server：『vncserver -query localhost :1』

       v. 察看有無 Xvnc 的程式啓動的 port 呢？

    B. Client 端的使用：使用『vncviewer IP:5901』來連線看看！(需要在 X 畫面下喔！)

    C. 測試完畢後，在 Server 端以『 vncserver -kill :1 』來結束！

12. 循環型的工作排程， crontab 這個玩意兒！

A. 若是一般使用者，可以使用『crontab [-lre]』來編輯自己的排程工作，語法爲：

分 時 日 月 週 指令項目

B. 若是系統工作的話，則可以考慮加入 /etc/crontab 這個檔案，語法爲：(注意看，與上面語法不同)

分 時 日 月 週 使用者身份 指令項目

C. crontab 的安全性：(仔細看 page 85 的說明！很重要！！！！！)

i. /etc/cron.allow ：寫入者才能夠使用，這東西優先

ii. /etc/cron.deny ：寫入者不能夠使用，這東西較慢被檢查。

D. 還有一些系統常用來放置資料的目錄可以處理：

i. /etc/cron.hourly
ii. /etc/cron.daily
iii. /etc/cron.weekly
iv. /etc/cron.monthly

E. 如果系統不是全天候開著，注意可以啓動『anacron』這個系統服務(page 88 有詳細的說明喔！)