流量偵測 MRTG for summit 48si

write by 黃國順

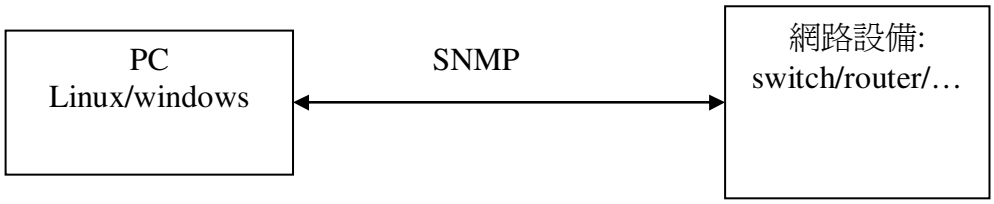
對於網管人員來說隨時了解所負責維護的伺服器運作情形是很重要的，最好我們能有一套軟體隨時監視伺服器主機的網路使用情形、CPU 使用率等資訊，因為當主機的 CPU 使用率過高的時候，系統可能呈現不穩定的狀態，或是網路流量過高的時候，可能就是被攻擊或是成為攻擊別人幫手的時候。

目前網路上有一套蠻好用軟體可以用來偵測主機的資料流量，這也是各大伺服器常使用的軟體，就是 MRTG (Multi Router Traffic Grapher) 這一套軟體。我們可以藉由 MRTG 來取得下列資訊並繪製成易讀的圖形供網管人員參考：

- 網路卡或是 router 某個介面的整體流量
- 伺服器 CPU 使用率
- RAM 使用率

要瞭解 MRTG 的運作，就必須瞭解一下 SNMP (Simple Network Management Protocol) 這個協定，因為 MRTG 是透過 SNMP 協定來監控流量的。所以，所有的 MRTG 所偵測的裝置都必須符合 SNMP 的協定。那什麼是 SNMP 呢？簡單的說，就是一種可以提供裝置（主機設備）的各類資訊的一種協定，諸如：網路流量、主機名稱、CPU 用量等等的資訊都可以藉由此一協定來提供。不過，由於不同廠牌的裝置可能會有無法相容的情況，因而後來又有所謂 MIB (Management Information Base) 的協定產生。不論如何， MRTG 就是藉由 SNMP 這個協定來監測與取得相關的資訊以製作圖表的！詳細的 SNMP 資訊可以在 http://www.net-snmp.org/ 查得。

基本上 MRTG 運作時便是透過 SNMP 的通訊協定，向某些指定的主機詢問相關的資料後，當主機傳遞數值給 MRTG 程式後，MRTG 再將資訊繪製成網頁上的圖表。由於 MRTG 是以 SNMP 協定來向主機要求資料，因此，您要使用 MRTG 來製作圖表時，必須先確定您的機器（或者說是設備）必須支援 SNMP 協定。SNMP 除了可以向網路設備查詢資料(read)外，亦可利用 write 功能設定網路設備。



以下分成 Linux 及 windows 系統分別說明：

◆ Linux 系統

1. MRTG 的安裝

因 MRTG 是以 Perl 程式寫成的，並且執行時會用到 zlib 、 gd 及 png 的函式庫（zlib 用來繪製圖表、gd 用來壓縮圖表），加上前面提到的 SNMP 及最後結果的 http 網頁輸出，因此首先要確定 Linux 主機中是否已經含有下列的套件：

perl (perl-5.0xx 以上)
zlib (zlib-1.1.3-xx 以上)
gd (gd-1.3.xx 以上)
libpng
apache
snmp
mrtg

我們可以藉由 rpm 來確認：

rpm -qa perl
rpm -qa zlib
rpm -qa gd
rpm -qa libpng
rpm –qa mrtg
rpm –qa httpd
rpm –qa |grep snmp
net-snmp.*.rpm
net-snmp-utils.*.rpm

建議利用 APT 自動下載安裝或由光碟中自行安裝：

apt-get update
apt-get install mrtg
apt-get install snmp-utils

若全部已安裝好則可進行下面步驟。

2. 利用 snmpwalk 來測試 summit 48si

執行下列命令：

snmpwalk –v 1 –c **public xxx.xxx.xxx.xxx**

xxx.xxx.xxx.xxx 是 summit 48si 的 IP，public 是 summit 48 預設的 community name(很多網路設備預設都是 public)

正常的話會出現許多資料。

若要測試遠端機器要注意的是 snmp 是以 UDP port=161 來傳送查詢封包，所以若有使用防火牆的話需把關於 snmp 的規定打開。redhat 預設的防火牆設定在/etc/sysconfig/iptables 中

請加入下面這一行

-A RH-Lokkit-0-50-INPUT -p udp -m udp --dport 161 -i eth0 -j ACCEPT

並執行/etc/init.d/iptables restart 重新啟動 iptables

3. mrtg 設定

(1)利用 cfgmaker 建立/etc/mrtg/mrtg.cfg 檔

執行下列命令：

```
cd /etc/mrtg
cfgmaker --global 'WorkDir: /var/www/html/mrtg' \
--global 'Options[_]: bits,growright' \
--global 'Language: big5' \
--output /etc/mrtg/mrtg.cfg \
public@xxx.xxx.xxx.xxx
```

xxx.xxx.xxx.xxx 為 summit48si 的 IP
public 為 summit48si 預設的 snmp community name
執行上面的命令後便會產生新的設定檔/etc/mrtg/mrtg.cfg

(2)修改 mrtg.cfg 內容作中文化（不改亦可），或其它設定。
利用 cfgmaker 建立的 mrtg.cfg 會把設備所有的實體 port、vlan port 等 interface 寫好在 mrtg.cfg 中並且只把目前有在使用的 interface 開啟。
我們要作的修改是找出 firewall 連接的對應 interface 並且只要修改 title
例如修改第 port 50 的說明

vi /etc/mrtg/mrtg.cfg

找到有關 port 50 設定的地方：

Target[163.17.149.252_50]: 50:public@163.17.149.252:
SetEnv[163.17.149.252_50]: MRTG_INT_IP="" MRTG_INT_DESCR="Summit48si-Port 50"
MaxBytes[163.17.149.252_50]: 125000000
Title[163.17.149.252_50]: **Traffic Analysis for 50 -- Summit48si**
PageTop[163.17.149.252_50]: **<H1>Traffic Analysis for 50 -- Summit48si</H1>**
<TABLE>
<TR><TD>System:</TD> <TD>Summit48si in </TD></TR>
<TR><TD>Maintainer:</TD> <TD>support@extremenetworks.com, +1 888 257 3000</TD></TR>
<TR><TD>Description:</TD><TD>Summit48si-Port 50 </TD></TR>
<TR><TD>ifType:</TD> <TD>ethernetCsmacd (6)</TD></TR>
<TR><TD>ifName:</TD> <TD>1/50</TD></TR>
<TR><TD>Max Speed:</TD> <TD>1000.0 Mbits/s</TD></TR>
</TABLE>

只要修改
Title[163.17.149.252_50]: Summit48si-Port 50 to WebGuard C320 DMZ Port
PageTop [163.17.149.252_50]: Summit48si-Port 50 to WebGuard C320 DMZ Port
只是修改為比較易懂的說明即可，這樣未來產生的網頁比較易懂。

(3)執行/usr/bin/mrtg../etc/mrtg/mrtg.cfg 三次直到沒有錯誤。

(4)利用 browser 檢查是否產生流量圖網頁：
ls /var/www/html/mrtg/ #檢查是否產生需要的 html 檔
http://127.0.0.1/mrtg/163.17.149.252_50.html

(5)mrtg 另附一個 indexmaker 程式可協助產生 index.html，因此請先將原來 index.html 備份
執行下列命令：

cp /var/www/html/mrtg/index.html /var/www/html/mrtg/index.html.old

執行下列命令：
indexmaker --output=/var/www/html/mrtg/index.html\
--title='XX 國小 MRTG 圖'\
/etc/mrtg/mrtg.cfg

修改/var/www/html/mrtg/index.html 在<head>內加入
<meta http-equiv="Content-Type" content="text/html; charset=big5">

(6)設定每隔 5 分鐘執行一次
crontab –e
加入下面設定
*/5 * * * * /usr/bin/mrtg /etc/mrtg/mrtg.cfg > /dev/null 2>&1

(7)利用 browser 檢查是否產生流量圖網頁

http://127.0.0.1/mrtg/index.html

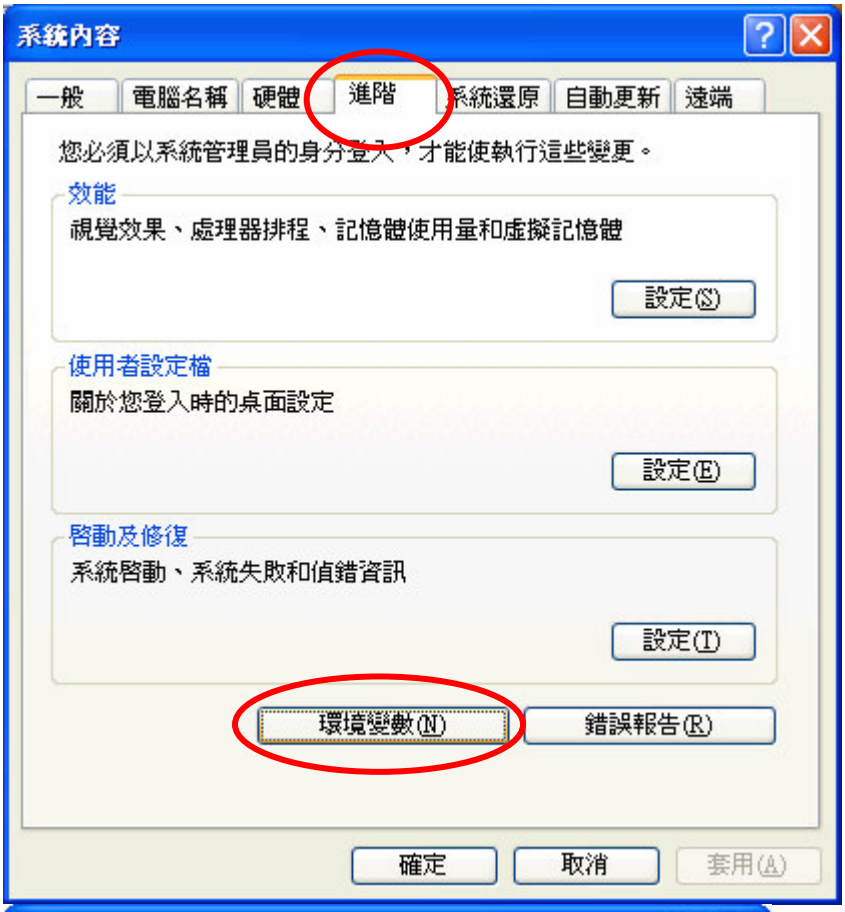
若 browser 不會自動切換成中文，則需修改 Apache 設定檔
/etc/httpd/conf/httpd.conf
中的兩個參數
LanguagePriority tw en da nl et fr de el it ja kr no pl pt pt-br ltz ca es sv
AddDefaultCharset big5

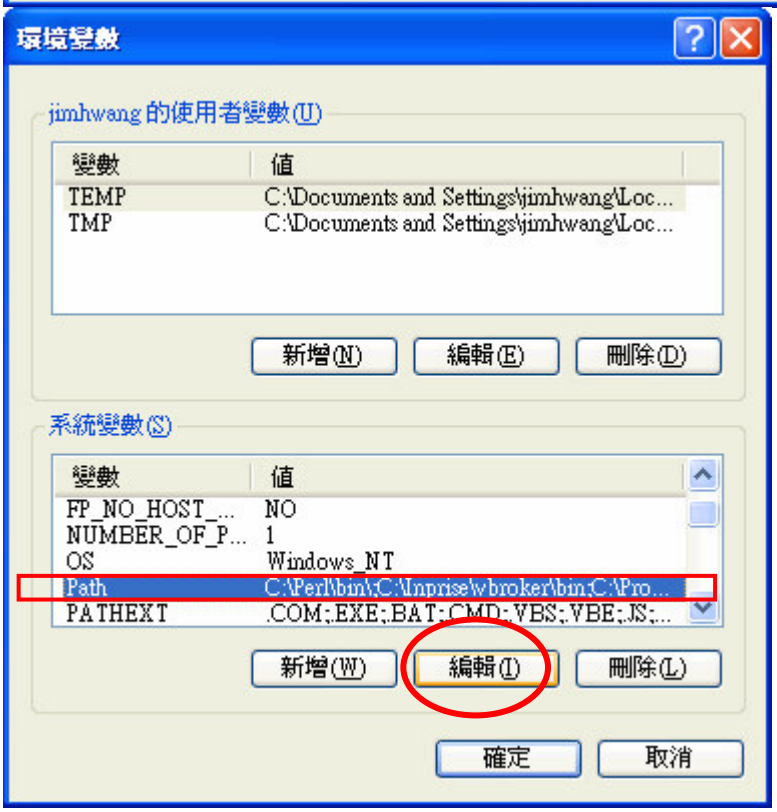
◆ windows 系統

(1)安裝 active perl

由於 mrtg 是以 perl 寫成所以並沒有辦法直接在 windows 上執行所以我們要先安裝 active perl，請至下面網址自行下載:
http://www.activestate.com/Products/ActivePerl/
下載 windows 版本 ActivePerl-5.8.4.810-MSWin32-x86.msi 後安裝。

(2)設定環境變數
windows XP、2000
[控制台]->[系統]->[進階]->[環境變數]->[系統變數]->變輯 Path，加入
C:\Perl\bin\;


系統內容
一般
電腦名稱
硬體
進階
系統還原
自動更新
遠端
您必須以系統管理員的身分登入，才能使執行這些變更。
效能
視覺效果、處理器排程、記憶體使用量和虛擬記憶體
設定(S)
使用者設定檔
關於您登入時的桌面設定
設定(E)
啟動及修復
系統啟動、系統失敗和偵錯資訊
設定(T)
環境變數(N)
錯誤報告(R)
確定
取消
套用(A)


環境變數
jimhwang 的使用者變數(U)
變數
值
TEMP
C:\Documents and Settings\jimhwang\Loc...
TMP
C:\Documents and Settings\jimhwang\Loc...
新增(N)
編輯(E)
刪除(D)
系統變數(S)
變數
值
FP_NO_HOST_...
NO
NUMBER_OF_P...
1
OS
Windows_NT
Path
C:\Perl\bin\;C:\Inprise\vbroker\bin;C:\Pro...
PATHEXT
.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;...
新增(W)
編輯(I)
刪除(L)
確定
取消

(2)下載 mrtg
請至 http://people.ee.ethz.ch/~oetiker/webtools/mrtg/pub/mrtg-2.10.14.zip 下載後，解開至 c:\mrtg\
[開始]->[執行]->輸入 cmd，開啟"命令提示字元"視窗

執行下列命令：
mkdir c:\mrtg\output

cd c:\mrtg\bin

perl cfgmaker public@xxx.xxx.xxx.xxx --global "WorkDir: c:\mrtg\output" --global "Options[_]: bits,growright" --global "Language: big5" --output c:\mrtg\bin\mrtg.cfg

xxx.xxx.xxx.xxx 是 summit 48si 的 IP，public 是 summit 48si 預設的 community name(很多網路設備預設都是 public)

(3)修改 c:\mrtg\bin\mrtg.cfg，請參考前面 linux 系統 mrtg 設定(2)之步驟。

(4) 執行 perl mrtg mrtg.cfg 三次。

(5)利用檔案總管檢查 c:\mrtg\output 是否產生流量圖網頁(一大堆 xxx.xxx.xxx.xxx_xx.html 檔)

(6)利用 indexmaker 程式產生 index.html：
執行下列命令：

perl indexmaker c:\mrtg\bin\mrtg.cfg --output=c:\mrtg\output\index.htm --title="XX 國小 MRTG 圖"

修改/var/www/html/mrtg/index.html 在<head>內加入
<meta http-equiv="Content-Type" content="text/html; charset=big5">

利用瀏覽器檢查 c:\mrtg\output\index.htm 檔是否正常

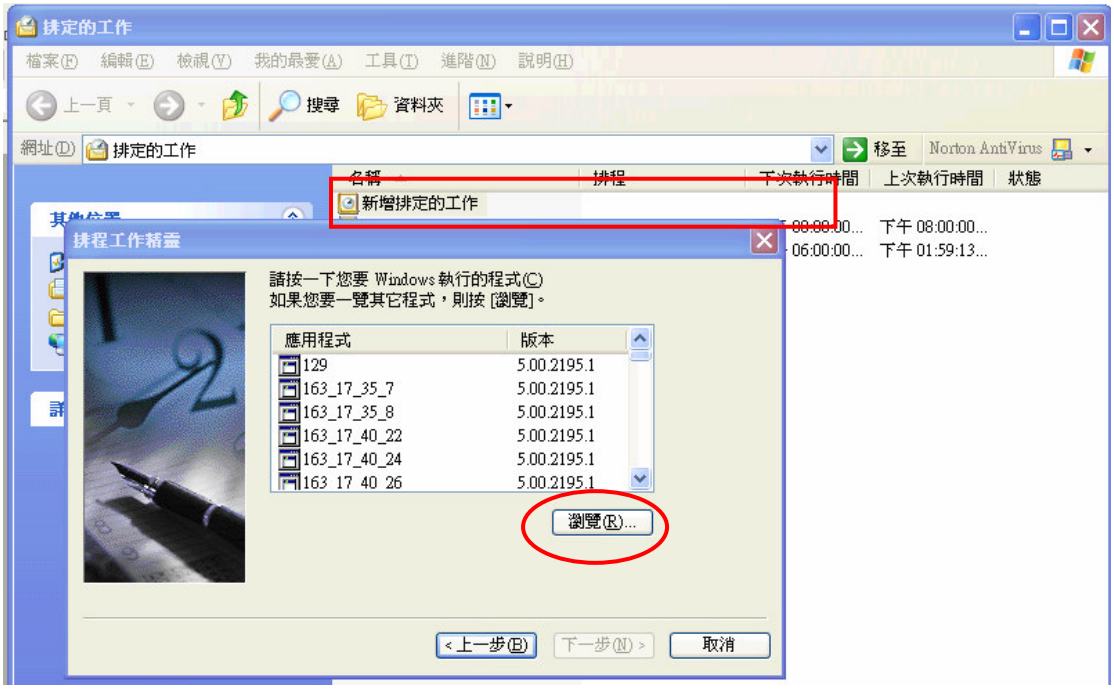
(7)windows 沒有 crontab 可以設定程式每 5 分鐘執行一次，所以要改用別的方法：
首先修改 c:\mrtg\bin\mrtg.cfg 檔，在最後的地方加入下面這一行：

RunAsDaemon: yes

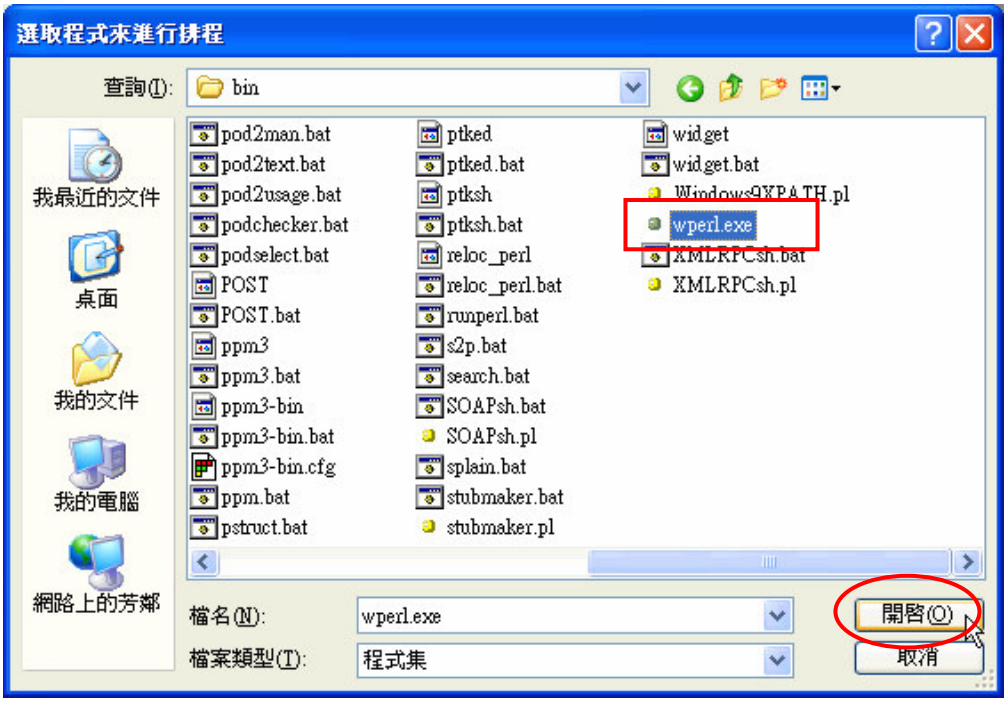
接著執行下列命令:
start /Dc:\mrtg\bin wperl mrtg --logging=eventlog mrtg.cfg

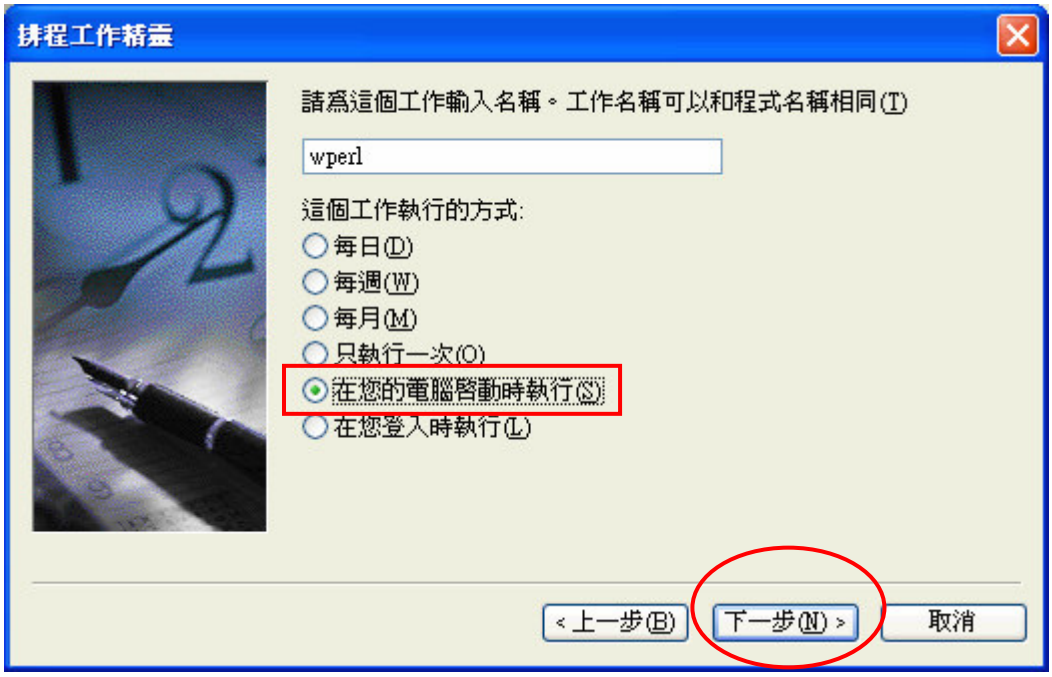
這樣便會每隔一段時間去產生新的 mrtg 流量圖了，不過還要注意的是若您執行上面的命令後又修改了 mrtg.cfg 檔內容，就必須先利用 windows 工作管理員將 wperl.exe 這個 process 結束處理程序後再重新執行上面的命令才行。

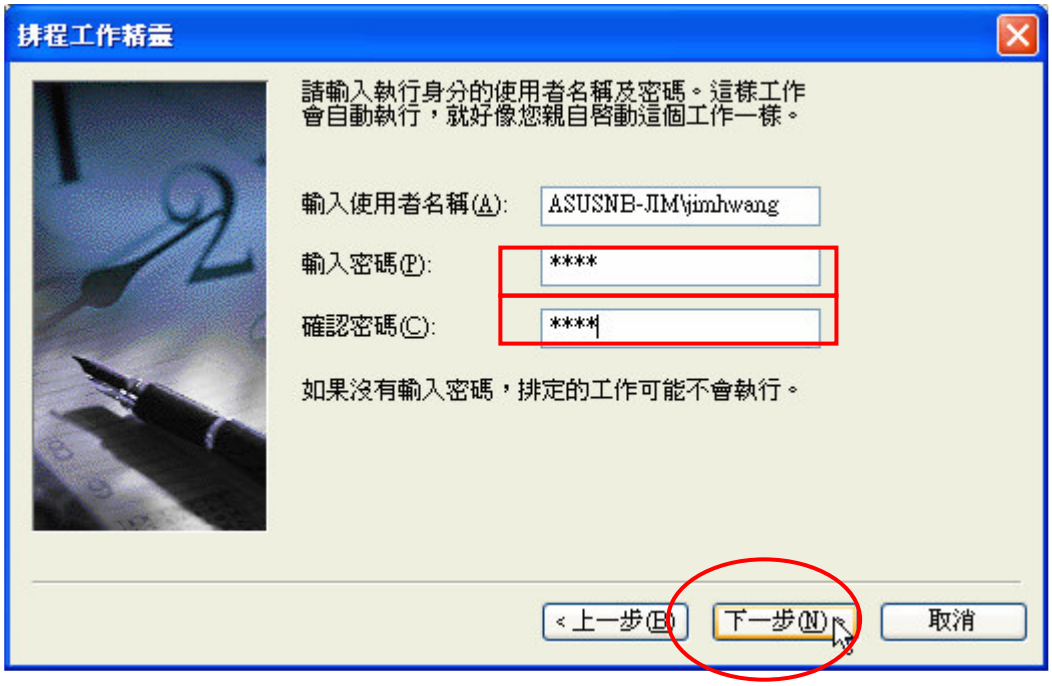
若要設定成開機時啟動則必需啟動[控制台]->[排定的工作]->[新增排定的工作]。

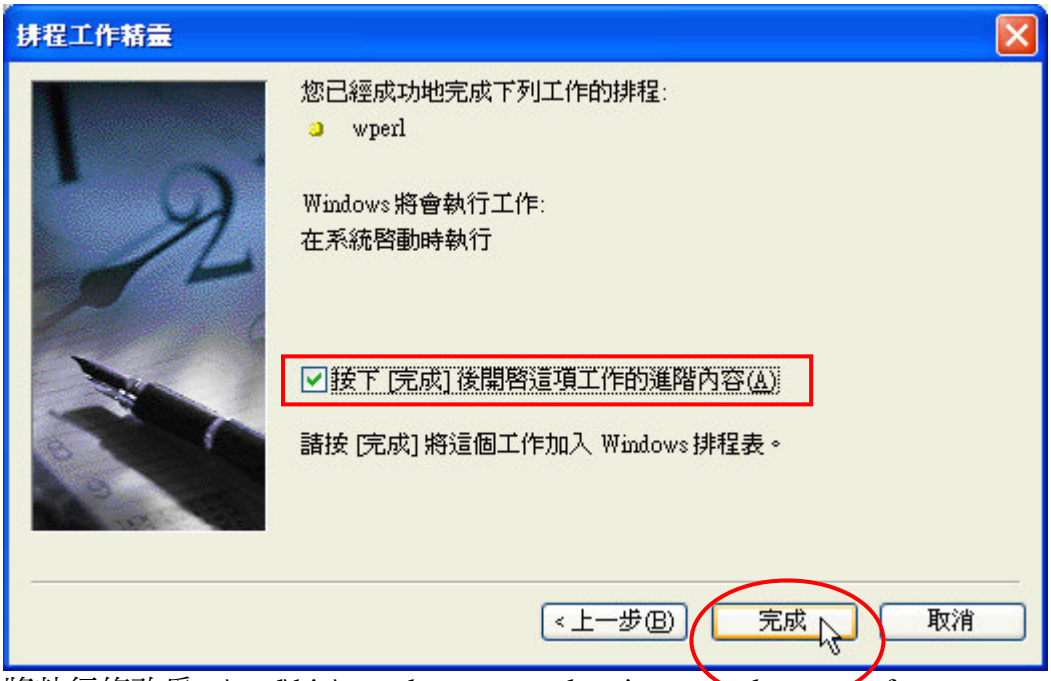


選取 c:\perl\bin\wperl

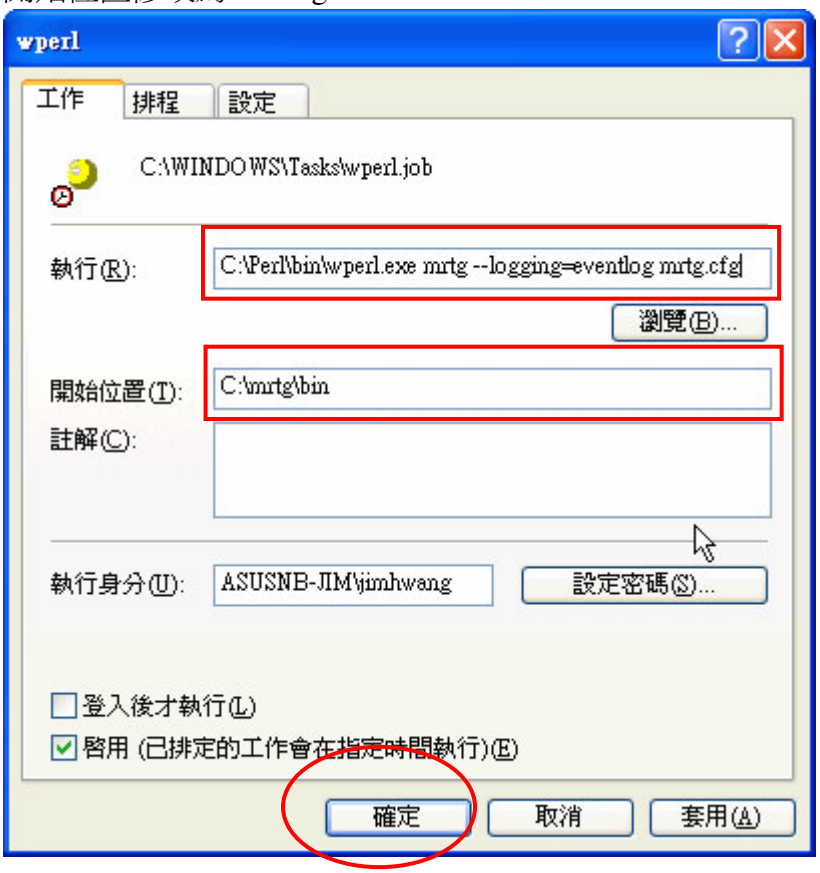



排程工作精靈
請為這個工作輸入名稱。工作名稱可以和程式名稱相同(T)
wperl
這個工作執行的方式:
每日(D)
每週(W)
每月(M)
只執行一次(O)
在您的電腦啓動時執行(S)
在您登入時執行(L)
< 上一步(B)
下一步(N) >
取消


排程工作精靈
請輸入執行身分的使用者名稱及密碼。這樣工作會自動執行，就好像您親自啓動這個工作一樣。
輸入使用者名稱(A):
ASUSNB-JIM\jimhwang
輸入密碼(P):
****
確認密碼(C):
****
如果沒有輸入密碼，排定的工作可能不會執行。
< 上一步(B)
下一步(N)
取消



將執行修改爲 c:\perl\bin\wperl.exe mrtg --logging=eventlog mrtg.cfg
開始位置修改爲 c:\mrtg\bin



(8)設定 IIS，將 c:\mrtg\output 加入成為網站可瀏覽的目錄。

◆ 附錄：mrtg.cfg 組態檔參數

Workdir 輸出目錄
LoadMIBs 載入 MIB 檔案
Language 語系
Target[xxx]:yyy:public@host_address:
　未來將產生 xxx.html
　yyy 查詢參數
　public snmp community string
MaxBytes[xxx]:nnn
　Y 軸最大值為 nnn，若有多項值可為 MaxBytes1[xxx]，MaxBytes2[xxx]
Title[xxx]:title string
PageTop[xxx]:<H1>string </H1>
AbsMax[xxx]:nnn 若監測值超過 MaxBytes 時，則以 nnn 代替
Option[xxx]:以下為可使用的選項
　growright 繪圖起點為左邊
　bit 以 bit 為計量單位,預設為 byte
　nopercent 無百分比資訊
　integer 以整數為單位
　gauge 估計的方法使用在偵測對象為磁碟容量、cpu loading、溫度時使用
　absolute 配合 gauge 使用
　unknaszero 設備斷線時,因無法量到資料,使用此參數將設為 0
kilo[xxx]:nnn 設定 K 的定義如 1000 或 1024
Ylegend[xxx]:Y 軸的說明
ShortLegend[xxx]:設定單位如 MB/s、KB/s
Legend[xxx]:量測資料的說明,若有多條可用 Legend1[xxx]、Legend2[xxx]
LegendI[xxx]、LengendO[xxx]:統計圖表下方 In 、Out 文字。另外顯示時若與數字太近可使用 string