

# Windows系統 入侵檢測與處理

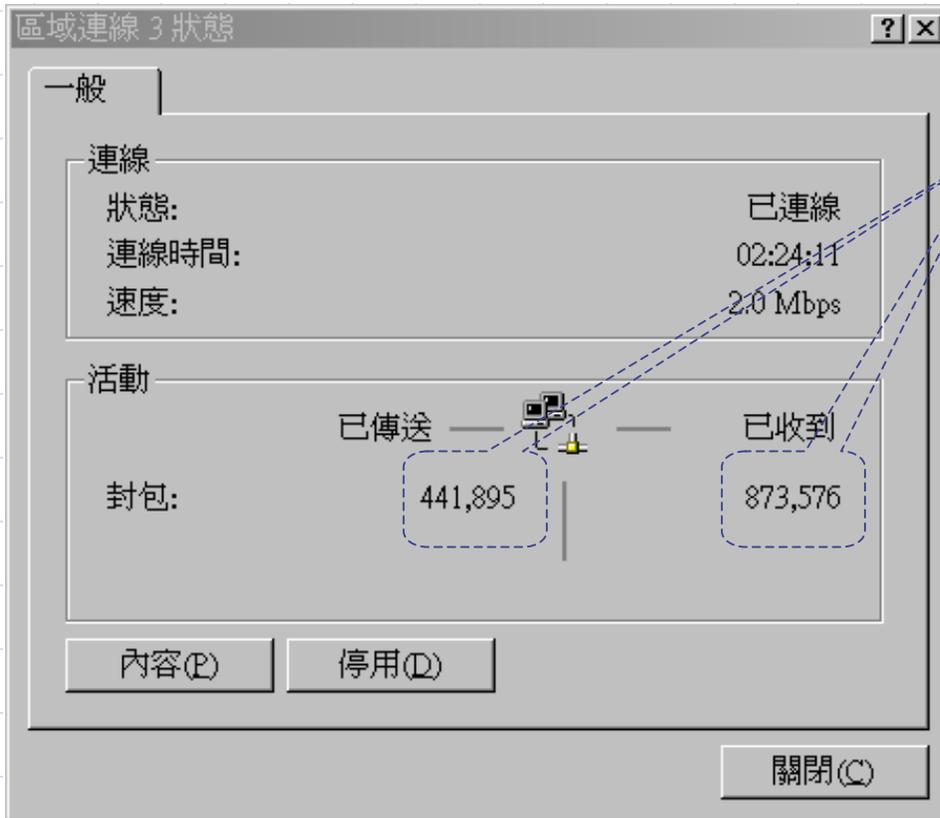
成大計網中心  
楊峻榮

2004/5/20

# 使用時機及頻率

- ◆ 主要判斷已遭或疑似入侵（ex 系統效能不佳）之檢測及處理，針對核心項目或入侵模式
- ◆ 手動方式檢測，必須加上人為判斷（ex遭入侵或破壞之經驗累積）或和別部主機交叉比對
- ◆ 當發覺系統負載及流量異常時之手動檢測
- ◆ 固定時間約二週檢測一次
- ◆ 以Windows 2000/XP/2003 為例
- ◆ 參考防毒軟體公司網頁之[手動移除病毒程序]
- ◆ 善用登錄表編輯程式，更改登錄表前先將登錄表之該資料夾匯出，以便出狀況時匯入。但若對登錄表內容不甚了解，勿輕易嘗試。
- ◆ 屬於進階使用註明或非例行之檢測，註明\*

# 傳輸狀況



開啟連線狀態視窗，在沒有傳輸資料情況下，是否在傳輸大量資料。若是，可能是DOS或DDOS攻擊。

# 連線狀態 (netstat)

開啟 開始 / 程式集 / 附屬應用程式 / 命令提示字元，在該視窗下鍵入 netstat ，看看是否有不尋常之連線。

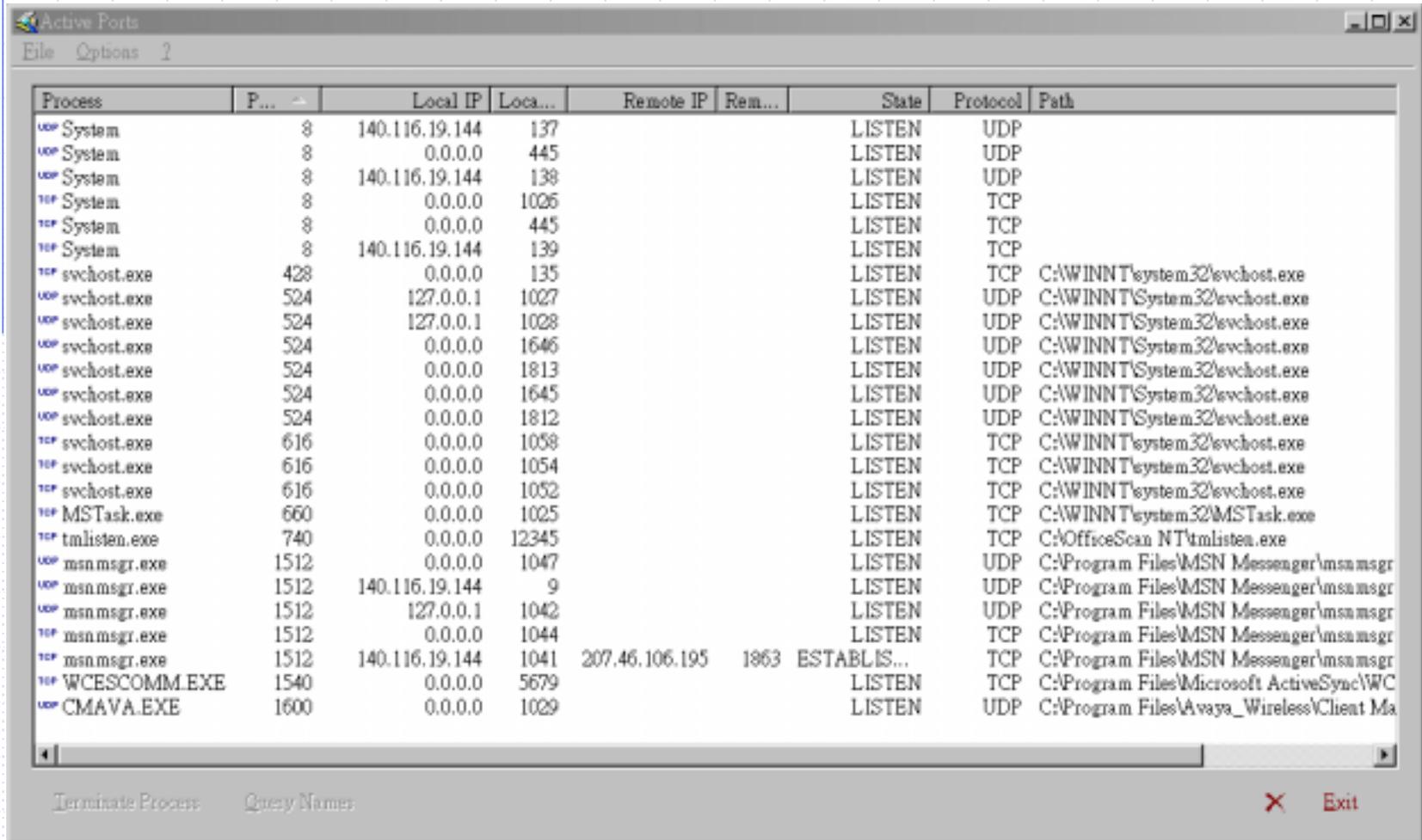
Proto	Local Address	Foreign Address	State
TCP	yang:1026	yang:20032	ESTABLISHED
TCP	yang:20032	yang:1026	ESTABLISHED
TCP	yang:3024	dec4000.cc.ncku.edu.tw:22	ESTABLISHED
TCP	yang:3613	mail.ncku.edu.tw:telnet	ESTABLISHED

其中Foreign Address表示對方的Address及port，而State之連線狀態，如此例ESTABLISHED表示已連上。

因一般人可能很難了解Services port是代表什麼及是從本機連出或由外部連進來的，一般而言Server端port的號碼是固定的，而client端是動態的。故只要發覺Foreign Address並不是您所要連線之位置，就該注意。

# 連線狀態 (active port)

Freeware軟體，主要可顯示所對應之執行程式



The screenshot shows the 'Active Ports' utility window. The window title is 'Active Ports' and it has a menu bar with 'File' and 'Options'. The main area contains a table with the following columns: Process, P... (PID), Local IP, Loca... (Local Port), Remote IP, Rem... (Remote Port), State, Protocol, and Path. The table lists various active ports and the processes that are listening on them.

Process	P...	Local IP	Loca...	Remote IP	Rem...	State	Protocol	Path
UDP System	8	140.116.19.144	137			LISTEN	UDP	
UDP System	8	0.0.0.0	445			LISTEN	UDP	
UDP System	8	140.116.19.144	139			LISTEN	UDP	
TCP System	8	0.0.0.0	1026			LISTEN	TCP	
TCP System	8	0.0.0.0	445			LISTEN	TCP	
TCP System	8	140.116.19.144	139			LISTEN	TCP	
TCP svchost.exe	428	0.0.0.0	135			LISTEN	TCP	C:\WINNT\system32\svchost.exe
UDP svchost.exe	524	127.0.0.1	1027			LISTEN	UDP	C:\WINNT\System32\svchost.exe
UDP svchost.exe	524	127.0.0.1	1028			LISTEN	UDP	C:\WINNT\System32\svchost.exe
UDP svchost.exe	524	0.0.0.0	1646			LISTEN	UDP	C:\WINNT\System32\svchost.exe
UDP svchost.exe	524	0.0.0.0	1813			LISTEN	UDP	C:\WINNT\System32\svchost.exe
UDP svchost.exe	524	0.0.0.0	1645			LISTEN	UDP	C:\WINNT\System32\svchost.exe
UDP svchost.exe	524	0.0.0.0	1812			LISTEN	UDP	C:\WINNT\System32\svchost.exe
TCP svchost.exe	616	0.0.0.0	1058			LISTEN	TCP	C:\WINNT\system32\svchost.exe
TCP svchost.exe	616	0.0.0.0	1054			LISTEN	TCP	C:\WINNT\system32\svchost.exe
TCP svchost.exe	616	0.0.0.0	1052			LISTEN	TCP	C:\WINNT\system32\svchost.exe
TCP MSTask.exe	660	0.0.0.0	1025			LISTEN	TCP	C:\WINNT\system32\MSTask.exe
TCP tmlisten.exe	740	0.0.0.0	12345			LISTEN	TCP	C:\OfficeScan NT\tmlisten.exe
UDP msn.msgr.exe	1512	0.0.0.0	1047			LISTEN	UDP	C:\Program Files\MSN Messenger\msn.msgr
UDP msn.msgr.exe	1512	140.116.19.144	9			LISTEN	UDP	C:\Program Files\MSN Messenger\msn.msgr
UDP msn.msgr.exe	1512	127.0.0.1	1042			LISTEN	UDP	C:\Program Files\MSN Messenger\msn.msgr
TCP msn.msgr.exe	1512	0.0.0.0	1044			LISTEN	TCP	C:\Program Files\MSN Messenger\msn.msgr
TCP msn.msgr.exe	1512	140.116.19.144	1041	207.46.106.195	1863	ESTABLIS...	TCP	C:\Program Files\MSN Messenger\msn.msgr
TCP WCESCOMM.EXE	1540	0.0.0.0	5679			LISTEN	TCP	C:\Program Files\Microsoft ActiveSync\WC
UDP CMAVA.EXE	1600	0.0.0.0	1029			LISTEN	UDP	C:\Program Files\Avaya_Wireless\Cliat Ma

At the bottom of the window, there are buttons for 'Terminate Process', 'Query Names', and 'Exit'.

# Process(工作管理員)

影像名稱	PID	CPU	CPU 時間	記憶體...
System Idle Process	0	92	2:00:44	16 K
System	8	01	0:00:20	272 K
SMSS.EXE	148	00	0:00:01	360 K
CSRSS.EXE	172	00	0:00:13	548 K
WINLOGON.EXE	192	00	0:00:01	620 K
SERVICES.EXE	220	00	0:00:04	6,472 K
LSASS.EXE	240	00	0:00:01	980 K
svchost.exe	428	00	0:00:00	5,320 K
spoolsv.exe	460	00	0:00:00	5,408 K
blackd.exe	532	00	0:00:24	9,728 K
svchost.exe	552	00	0:00:02	17,924 K
ntrtscan.exe	588	00	0:00:00	2,592 K
mstask.exe	704	00	0:00:00	3,236 K
tmlisten.exe	748	00	0:00:00	3,840 K
WinMgmt.exe	844	00	0:00:06	732 K
svchost.exe	848	00	0:00:00	5,024 K
explorer.exe	972	02	0:00:31	2,880 K
OfcDog.exe	1052	00	0:00:00	1,416 K
promon.exe	1056	00	0:00:00	1,264 K
internet.exe	1188	00	0:00:00	1,672 K

結束處理程序(E)

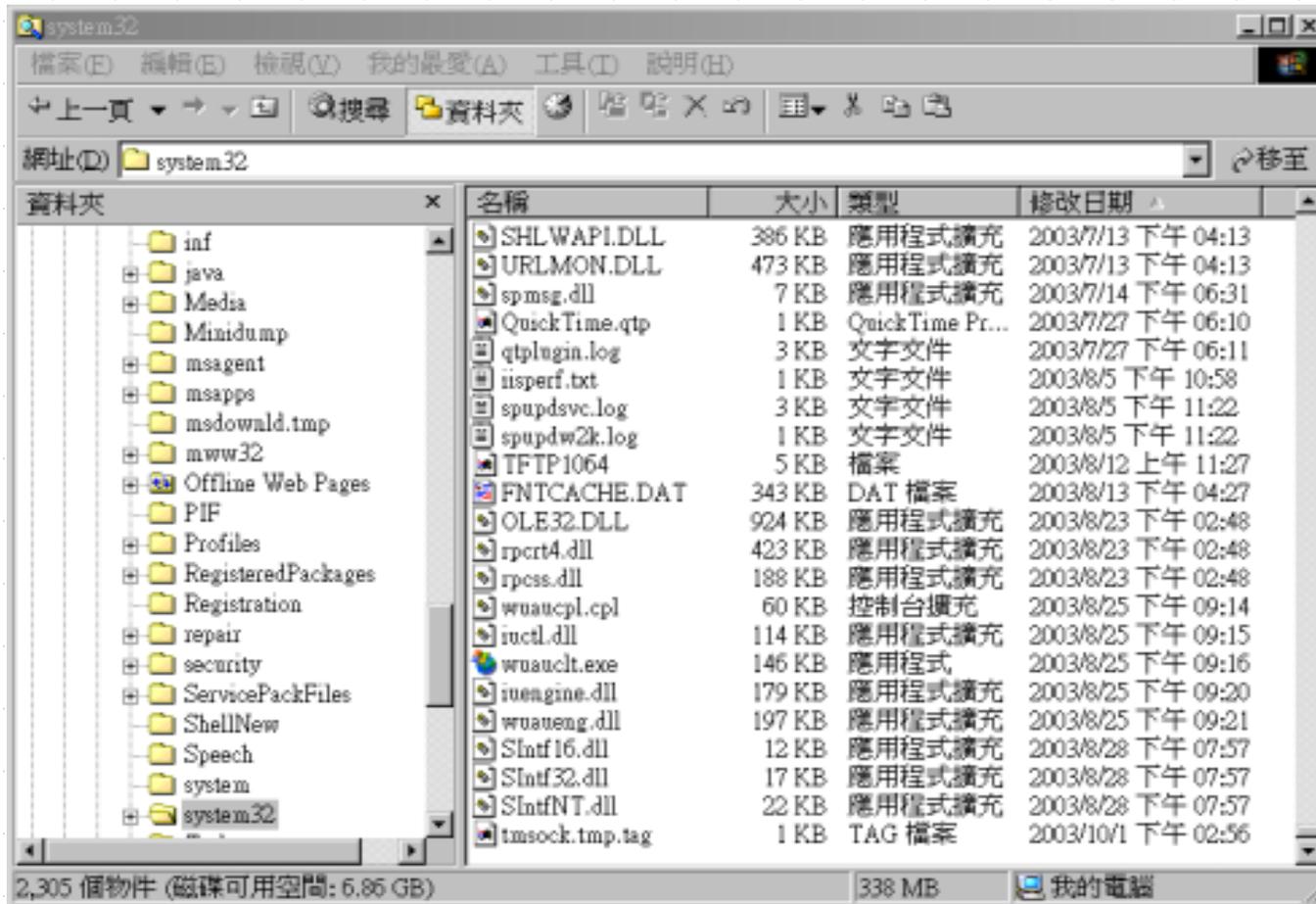
程序: 42    CPU 使用: 8%    MEM 使用: 165728K / 433684K

開啟工作管理員（按 Ctrl+Alt+Del 鍵，點選工作管理員），按下處理程序頁

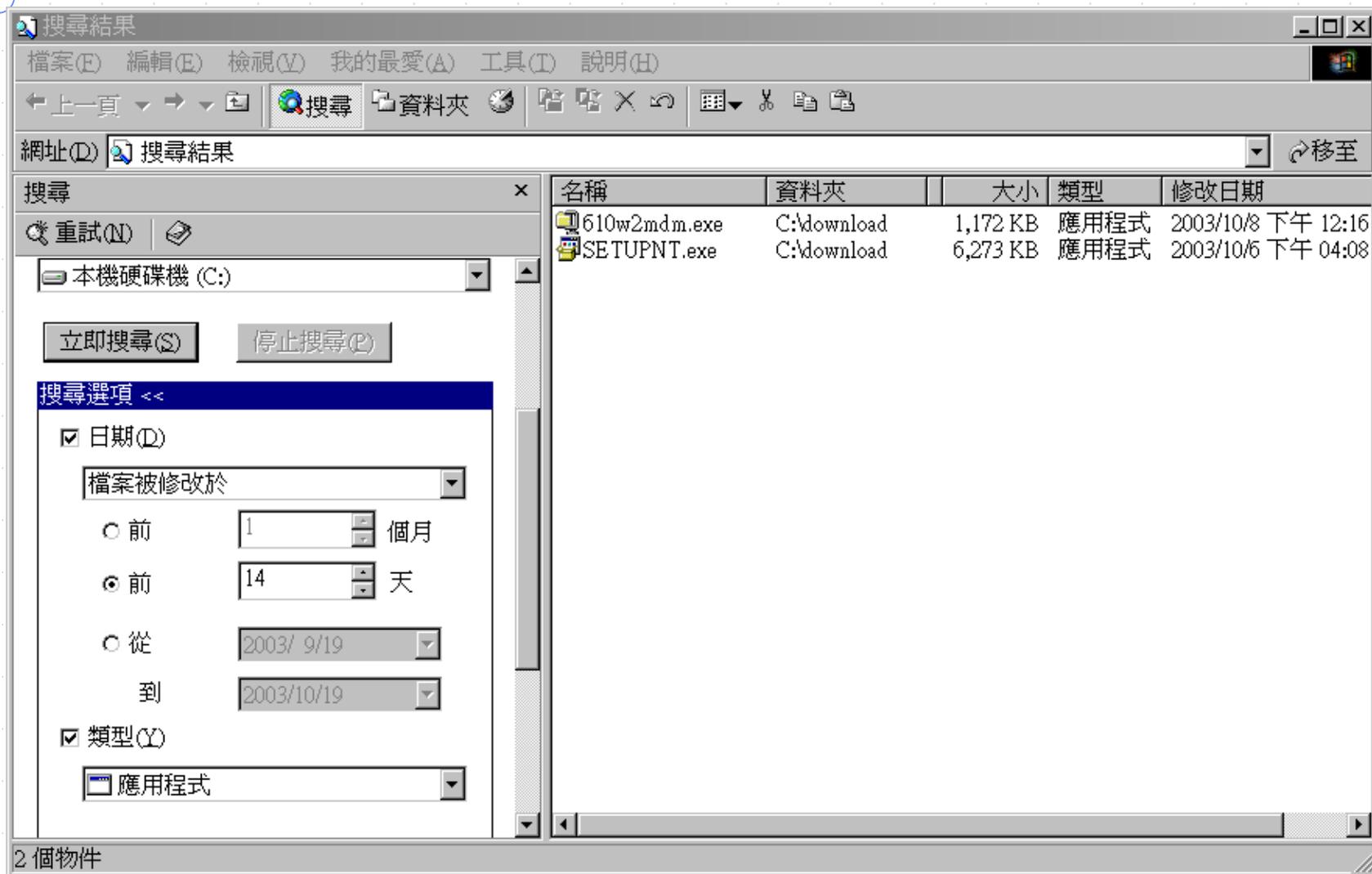
- 檢查是否有在耗用 CPU 但卻非自己所欲執行之程式。
- 是否有佔用大量 CPU 或記憶體之程式

# 由檔案總管檢查檔案異動日期

以「詳細資料」及「排列圖示 / 依日期」看最近異動之執行檔。  
預設Win2000為/WINNT/system32, WinXP為/Windows/system32



# 利用搜尋選項檢查檔案異動日期



The screenshot shows a Windows Explorer window titled "搜尋結果" (Search Results). The address bar shows the search path. The search options pane on the left is expanded, showing the following settings:

- 日期(D) (Date)
- 檔案被修改於 (Files modified on):
  - 前 (Before) 1 個月 (1 month)
  - 前 (Before) 14 天 (14 days)
  - 從 (From) 2003/ 9/19 (2003/ 9/19) 到 (to) 2003/10/19 (2003/10/19)
- 類型(Y) (Type)
- 應用程式 (Application)

The main pane displays a table of search results:

名稱	資料夾	大小	類型	修改日期
610w2mdm.exe	C:\download	1,172 KB	應用程式	2003/10/8 下午 12:16
SETUPNT.exe	C:\download	6,273 KB	應用程式	2003/10/6 下午 04:08

At the bottom left of the window, it indicates "2 個物件" (2 items).

# 登錄表 (registry)

由 開始/執行 輸入 regedit

The screenshot shows the Windows Registry Editor window titled "登錄編輯程式". The left pane displays a tree view of the registry, with "Run" selected under "HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion". The right pane shows a list of registry values with columns for "名稱" (Name), "類型" (Type), and "資料" (Data).

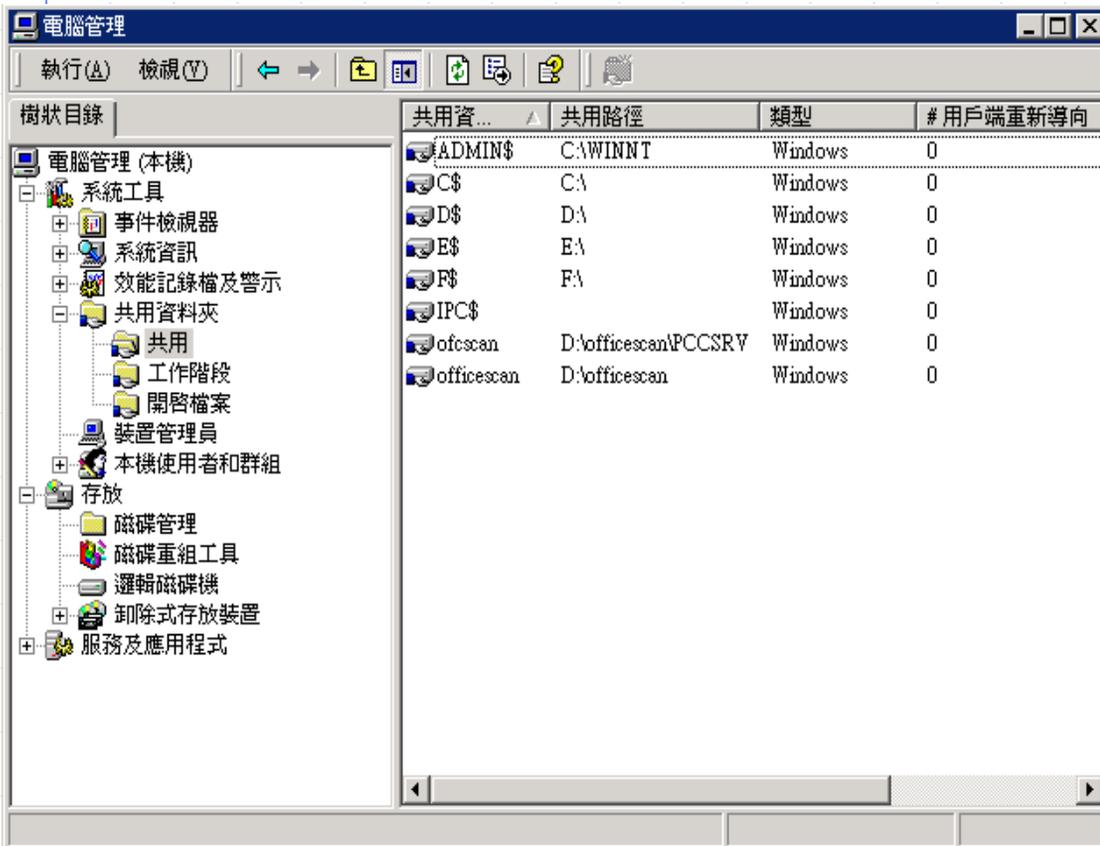
名稱	類型	資料
(預設值)	REG_SZ	(數值未設定)
ALDaemon	REG_SZ	ALDAEMON.EXE
CtrlVol	REG_SZ	"C:\Program Files\Acer\Launch Man
HotkeyApp	REG_SZ	"C:\Program Files\Acer\Launch Man
HotKeysCmds	REG_SZ	C:\WINNT\System32\hkcmd.exe /De
IgfxTray	REG_SZ	C:\WINNT\System32\igfxtray.exe
KeyHook	REG_SZ	"C:\Program Files\Acer\Launch Man
Launch App	REG_SZ	c:\DMSINFO\launapp.exe
LaunchAp	REG_SZ	"C:\Program Files\Acer\Launch Man
LTSMMMSG	REG_SZ	LTSMMMSG.exe
OfficeScanNT 監...	REG_SZ	"C:\OfficeScan NT\pcntmon.exe"
Powerkey	REG_SZ	"C:\Program Files\Acer\Powerkey\pc
Promon.exe	REG_SZ	Promon.exe
PRPCMonitor	REG_SZ	PRPCUI.exe
Real Tray	REG_SZ	C:\Program Files\Real\RealPlayer\Re
Synchronization ...	REG_SZ	mobsync.exe /logon
Wbutton	REG_SZ	"C:\Program Files\Acer\Launch Man
Winupdate	REG_SZ	regedit /s C:\Winnt\Discover.reg

我的電腦\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

# 登錄表檢查項目

- ◆ \HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion下之Run、RunOnce、RunServices是否不尋常的程式被啟動
- ◆ \HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows 之 AppInit\_DLLs其資料欄應為空白
- ◆ \HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogin之GinaDLL應該不存在  
Shell資料欄應為無路徑之Explorer.exe  
Userinit資料欄應為C:\WINNT\system32\userinit.exe (win2000) or C:\Windows\System32\userinit.exe (XP)

# 資源分享



開啟 開始 / 設定 / 控制台，點選 系統管理工具 / 電腦管理，於左邊之樹狀目錄，點選「共用資料夾」左邊之+符號，會展開「共用資料夾」下之子項目。

其中「共用」為share出去之目錄，請檢查是否有不必要之檔案分享。

「工作階段」為目前連上分享的來源。

「開啟檔案」為目前連上分享所開啟的檔案。

# 限制共享設定 \*

- ◆ 關閉Windows2000/XP/2003系統預設並享  
\\HKEY\_LOCAL\_MACHINE\CurrentControlSet\Services\Lanmanserver\parameters  
新增AutoShareWks:REG\_DWORD:0  
(說明:以新增DWORD值,值的名稱為AutoShareWks,值為0)  
新增AutoShareServer:REG\_DWORD:0
- ◆ 限制IPC\$匿名存取的權限(預防匿名列舉帳號及密碼暴力破解)  
\\HKEY\_LOCAL\_MACHINE\CurrentControlSet\Control\Lsa  
新增RestrictAnonymous:REG\_DWORD:1  
新增RestrictAnonymousSAM:REG\_DWORD:1  
新增EveryoneIncludesAnonymous:REG\_DWORD:0

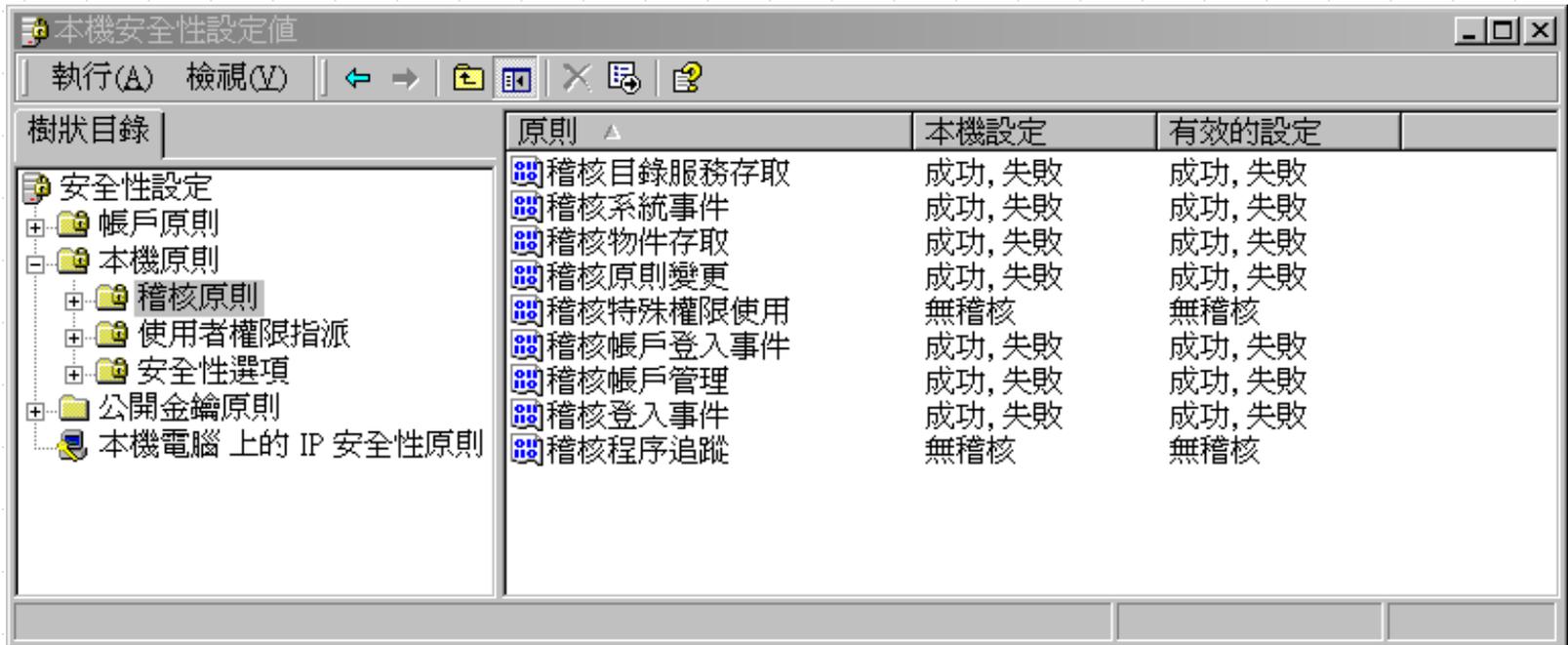
# 事件檢視

開啟 開始 / 設定 / 控制台，點選 系統管理工具 / 事件檢視器，  
檢視是否有不正常事件

類型	日期	時間	來源	類
警告	2003/10/4	上午 08...	RMSPPPOE	無
警告	2003/10/4	上午 08...	RMSPPPOE	無
警告	2003/10/4	上午 08...	RemoteAccess	無
警告	2003/10/4	上午 08...	RemoteAccess	無
錯誤	2003/10/4	上午 08...	RemoteAccess	無
錯誤	2003/10/4	上午 08...	RemoteAccess	無
錯誤	2003/10/4	上午 08...	RemoteAccess	無
錯誤	2003/10/4	上午 08...	RemoteAccess	無
資訊	2003/10/4	上午 08...	eventlog	無
資訊	2003/10/4	上午 08...	eventlog	無
警告	2003/10/4	上午 08...	Dhcp	無
資訊	2003/10/3	下午 10...	eventlog	無
錯誤	2003/10/3	下午 10...	NetBT	無
錯誤	2003/10/3	下午 10...	NetBT	無
錯誤	2003/10/3	下午 10...	NetBT	無
錯誤	2003/10/3	下午 09...	NetBT	無
錯誤	2003/10/3	下午 09...	NetBT	無
錯誤	2003/10/3	下午 09...	NetBT	無
錯誤	2003/10/3	下午 09...	NetBT	無

# 事件檢視之安全性記錄檔 \*

開啟 開始 / 設定 / 控制台 / 系統管理工具 / 本機安全性原則，於其樹狀目錄欄之本機原則下之稽核原則，設定如下項目之設定值



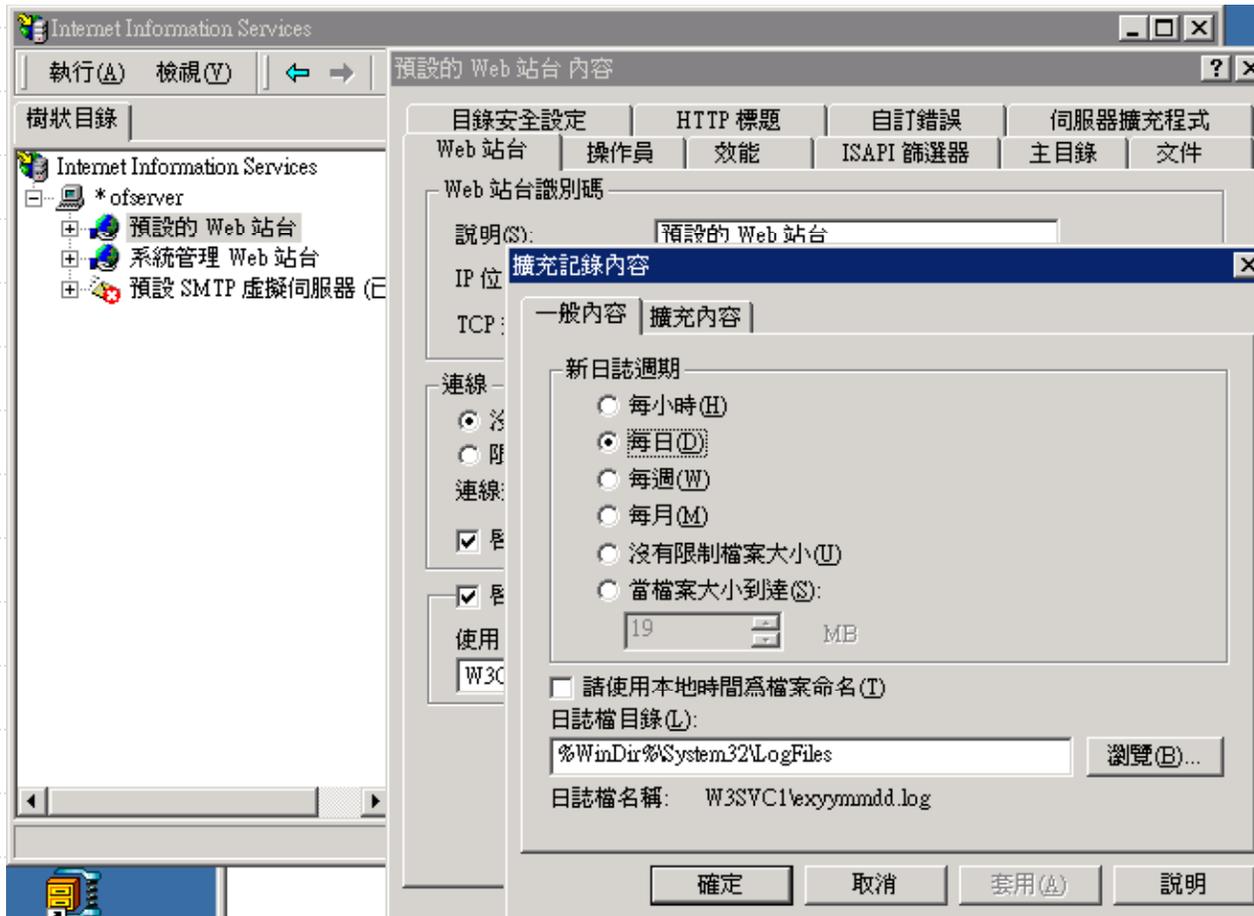
The screenshot shows the 'Local Security Policy' window in Windows. The left pane shows a tree view with 'Local Policies' expanded to 'Audit Policies'. The right pane displays a table of audit policies with their current and effective settings.

原則	本機設定	有效的設定
稽核目錄服務存取	成功, 失敗	成功, 失敗
稽核系統事件	成功, 失敗	成功, 失敗
稽核物件存取	成功, 失敗	成功, 失敗
稽核原則變更	成功, 失敗	成功, 失敗
稽核特殊權限使用	無稽核	無稽核
稽核帳戶登入事件	成功, 失敗	成功, 失敗
稽核帳戶管理	成功, 失敗	成功, 失敗
稽核登入事件	成功, 失敗	成功, 失敗
稽核程序追蹤	無稽核	無稽核

即可在事件檢視之安全性記錄檔檢查如上項目之事件

# Internet Services Logs \*

假如有開啟 Internet ( www、 ftp 、 smtp ) Services , Log一般放置在 /WINNT/system32/logFiles



# Internet Services Logs



```
ex020825.log - 記事本
檔案(F) 編輯(E) 格式(O) 說明(H)
2002-08-25 08:12:40 61.221.32.109 - 140.116.6.10 80 GET
/OfficeScan/download/server.ini - 200 TMhtload/1.31.00.1708
2002-08-25 08:12:49 140.116.142.19 - 140.116.6.10 80 GET
/officescan/cgi/cgiOnClose.exe
UID=1d80e23a-ee48-4ae1-978a-cd865a11b4f8&DATE=20020825&TIME=161306&RELEASE=5.02 200 TMhtload/1.31.00.1708
2002-08-25 08:12:49 61.221.32.109 - 140.116.6.10 80 GET
/OfficeScan/download/pattern/v_335.337 - 200 TMhtload/1.31.00.1708
2002-08-25 08:12:50 61.221.32.109 - 140.116.6.10 80 GET
/OfficeScan/download/Product/AUOfcCln.zip - 200 TMhtload/1.31.00.1708
2002-08-25 08:13:05 61.221.32.109 - 140.116.6.10 80 GET
/officescan/hotfix_ADMIN/Instreg.exe - 200 TMhtload/1.31.00.1708
2002-08-25 08:13:07 61.221.32.109 - 140.116.6.10 80 GET
/officescan/cgi/cgiRqCfg.exe
UID=ddd3fcab-ab8a-4368-b1d7-20d2d8edc10d&EVENT=0&RELEASE=5.02 200
TMhtload/1.31.00.1708
2002-08-25 08:13:10 61.221.32.109 - 140.116.6.10 80 GET
/officescan/cgi/cgiRqAlertMsg.exe RELEASE=5.02 200
TMhtload/1.31.00.1708
2002-08-25 08:13:10 140.116.142.19 - 140.116.6.10 80 GET
/officescan/cgi/cgiOnStart.exe
UID=1d80e23a-ee48-4ae1-978a-cd865a11b4f8&DATE=20020825&TIME=161328&COMP
```

# 服務 (Service)

至控制台 / 系統管理工具 / 服務，無描述，啟動類型為「自動」，狀態為「啟動」，顯示其內容之執行程式路徑，是否為遭植入的檔案

The screenshot shows the Windows Service console with the 'Remote Administrator Service' selected. The service is currently 'Stopped' (停止) and has an 'Automatic' (自動) start type. The path to the executable is shown as 'C:\WINNT\system32\rundll16.exe /service'.

名稱	描述	狀...	啟動類型
OfficeScan Master Se...		啟動	自動
OfficeScan_Master_...		啟動	自動
pcAnywhere Host Se...	"Allows Re...	啟動	自動
Performance Logs an...	設定效能記...		手動
Plug and Play	管理裝置安...	啟動	自動
Print Spooler	將檔案載入...	啟動	自動
Protected Storage	提供受保護...	啟動	自動
QoS RSVP	提供網路訊...		手動
Remote Access Auto ...	當程式參照...		手動
Remote Access Conn...	建立網路連...	啟動	手動
Remote Administrato...			停用
Remote Procedure C...	提供結束點...	啟動	自動
Remote Procedure C...	管理 RPC ...		手動
Remote Registry Ser...	允許遠端登...	啟動	自動
Removable Storage	管理卸除式...	啟動	自動
Routing and Remote...	提供連到區...		停用
RunAs Service	啓用在不同...	啟動	自動
Security Accounts E...			自動
Security Accounts M...	儲存本機帳...	啟動	自動
Server	提供 RPC ...	啟動	自動
Simple Mail Transpo...	跨網路之電...	啟動	自動

Remote Administrator Service 內容 (本機電腦)

一般 | 登入 | 修復 | 依存關係

服務名稱: r\_server

顯示名稱(N): Remote Administrator Service

描述(D):

執行程式路徑(H): "C:\WINNT\system32\rundll16.exe" /service

啟動類型(E): 停用

服務狀態: 停止

啟動(S) | 停止(T) | 暫停(P) | 繼續(R)

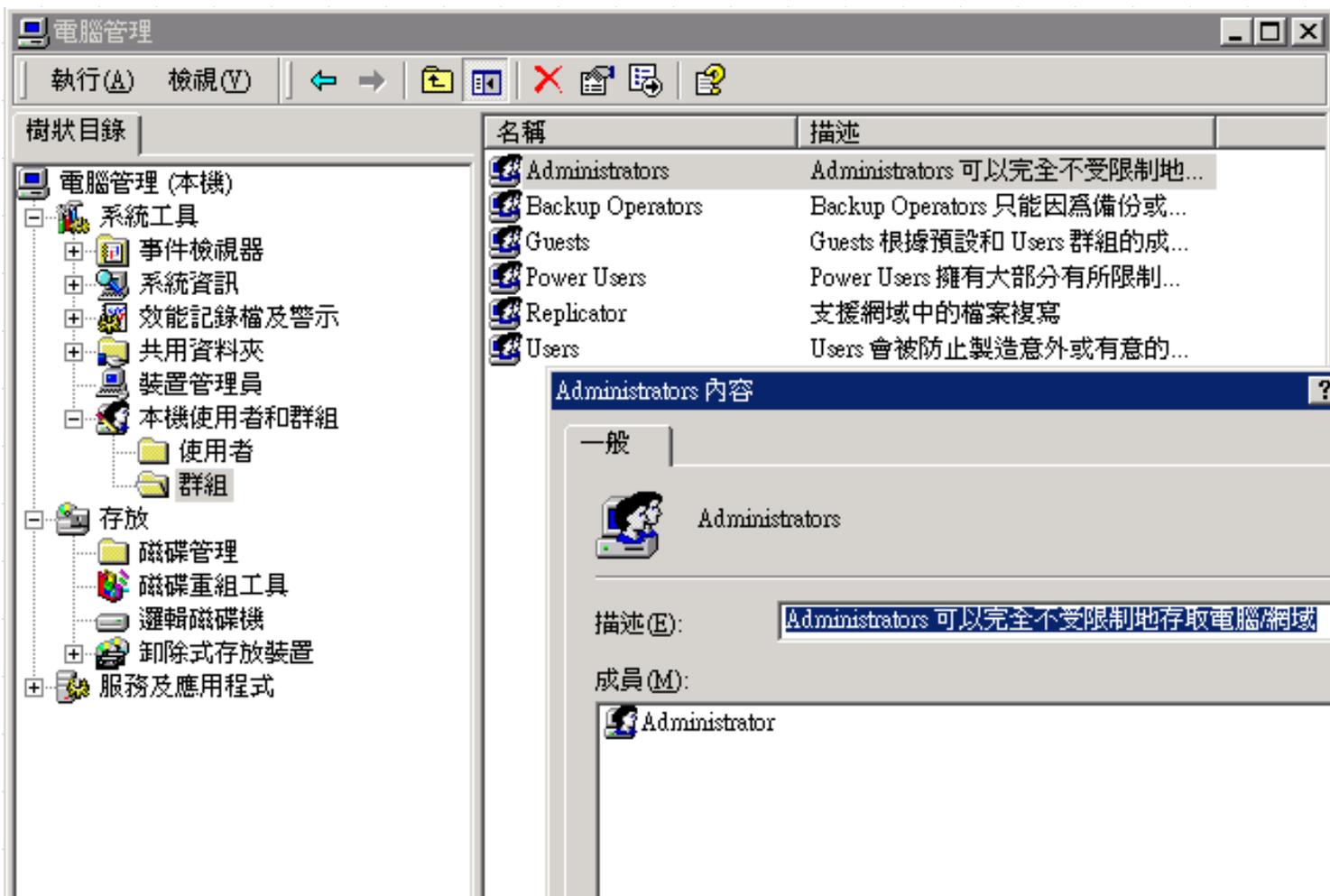
您可以指定啟動參數，當您從這裡啟動服務時，這些指定的參數將會被套用。

啟動參數(M):

確定 | 取消 | 套用(A)

# 使用者帳號及其權限

是否有不明之使用者，一般使用者是否有administrator權限或群組



The screenshot shows the Windows Computer Management console. The left pane displays a tree view with '本機使用者和群組' (Local Users and Groups) expanded to show '使用者' (Users) and '群組' (Groups). The right pane shows a list of groups with their descriptions:

名稱	描述
Administrators	Administrators 可以完全不受限制地...
Backup Operators	Backup Operators 只能因為備份或...
Guests	Guests 根據預設和 Users 群組的成...
Power Users	Power Users 擁有大部分有所限制...
Replicator	支援網域中的檔案複寫
Users	Users 會被防止製造意外或有意的...

Below the list, the 'Administrators 內容' (Administrators Content) pane is visible, showing the '一般' (General) tab. It displays the group name 'Administrators' and its description: 'Administrators 可以完全不受限制地存取電腦/網域' (Administrators can access the computer/network without restrictions). The '成員 (M):' (Members) section lists 'Administrator'.

# 關於帳號

- ◆ Windows 登入必須設定密碼
- ◆ 移除guest帳號
- ◆ 注意不明帳號及Administrator群組之帳號
- ◆ 密碼設定不要過於簡單及英文單子，最好是大小寫數字及特殊符號混合設定

# 網頁綁架 \*

- ◆ 先取消IE之proxy，及點選 工具/網際網路選項/一般之Temporary Internet file之[刪除Cookie]及[刪除檔案]之按鍵
- ◆ 首頁被更改：  
HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main及  
HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main 內名稱為“ Start Page ” 更改為首頁之網址  
進入  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 刪除值為“ internat.exe ”  
用regedit之搜尋原本被置放之網頁，並刪除
- ◆ 自動開啟到不知名的網站：  
以 Regedit找尋該網站的網址，若找到internat.exe 的機碼有該網址，刪除該網址，然後重新開機即可!!!

# 其他

- ◆ Autoexec.bat , Config.sys
- ◆ %windir%/win.ini 之 load= run =
- ◆ %windir%/system.ini 之 shall=
- ◆ 程式集 / 附屬應用程式 / 系統工具 / 排定的工作
- ◆ 程式集 / 啟動
- ◆ 硬碟是否被不正常使用