臺灣大學計資中心網路組

北區學術資訊安全維運中心

資訊安全分析報告

重要資訊服務作業系統注意事項：

Windows Server 2003 終止支援後升級與資安防護之道

臺灣大學計資中心網路組

北區學術資訊安全維運中心

目錄

摘要

Windows Server 2003即將於2015年7月14日終止支援(End of Support,EOS)。依據以往經驗，伺服器升級評估與移轉需要費時至少六個月至一年不等，如不盡快升級作業系統，屆時使伺服器管理者將面臨下列三個問題：

1. 資訊安全的風險增高
2. 管理成本提高。
3. 法規(ISO27001)風險及通過認證難度增加。

本報告說明使用 Windows Server 2003 為重要資訊服務之作業系統時，當 Windows Server 2003 終止支援因應之道及升級策略，以確保應有之資安防護。

Windows Server 2003 如何升級

微軟官方提供 Windows Server 2003 升級建議步驟，依序為：

1. 資產確認與盤點：

   想確認組織內部 Windows Server 2003 的伺服器數量，微軟提供工具協助盤點軟硬體資產， MAP（Microsoft Assessment and Planning Toolkit），可由組織內部網路盤點 Windows Server。

2. 升級先後順序評估：

   企業可依據各種類型軟體，判斷程式的重要性，優先升級重要性高者。

3. 選擇升級作業系統：

   Windows Server 2003 可直接本機升級至 Windows Server 2008。若要從 Windows Server 2003 升級至 Windows Server 2012，需先將 Windows Server 2003 升級至 Windows Server 2008，再升級至 Windows Server 2012。

   Windows Server 2003和Windows Server 2012兩個版本推出時間相隔近10年，若直接升級至 Windows Server 2012 R2，需重新安裝系統。

4. 應用程式相容測試：

   為確保原使用之軟體可於新版作業系統使用，需進行軟體相容性測試以確認應用程式之相容性。

   Microsoft 提供相容性檢測工具（Microsoft Platform Ready Test Tool，MPR Test Tool），可檢測應用程式相容性。也可以建立一個 Windows Server 2012 或 Windows Server 2008 相容性測試環境，確認應用程式相容性都沒問題後，即可完成應用程式的移轉。

如何查看 Windows Server 版本與 Patch 更新

查看伺服器運作之 Windows Server 版本可以依下列方式操作：
開啟開始選單列→搜尋”cmd”開啟命令提示字元→輸入”winver”指令，即可查看，流程可參考下圖 1（參考範例圖 1，為 Windows Server 2008 Standard SP2）。

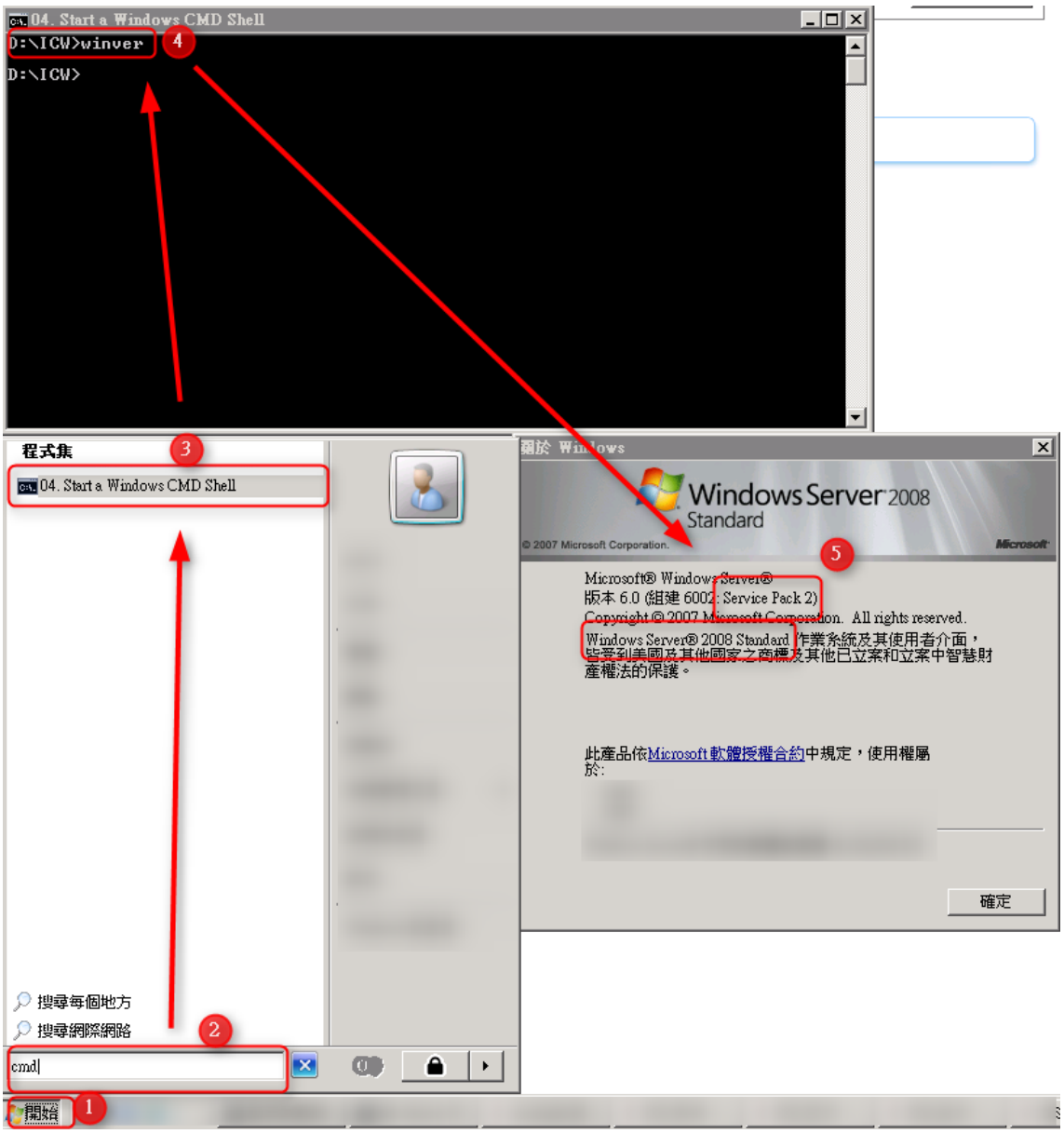


圖 1

查看主機本身是否仍有微軟最新的更新檔案釋出，手動的方式可以按下列方式進行操作：開啟開始選單列→選取”Windows Update”→點選”檢查更新”→選取”安

裝更新”，可參考圖 2 範例，圖 2 藍色框框內文字可以查看更新的內容。

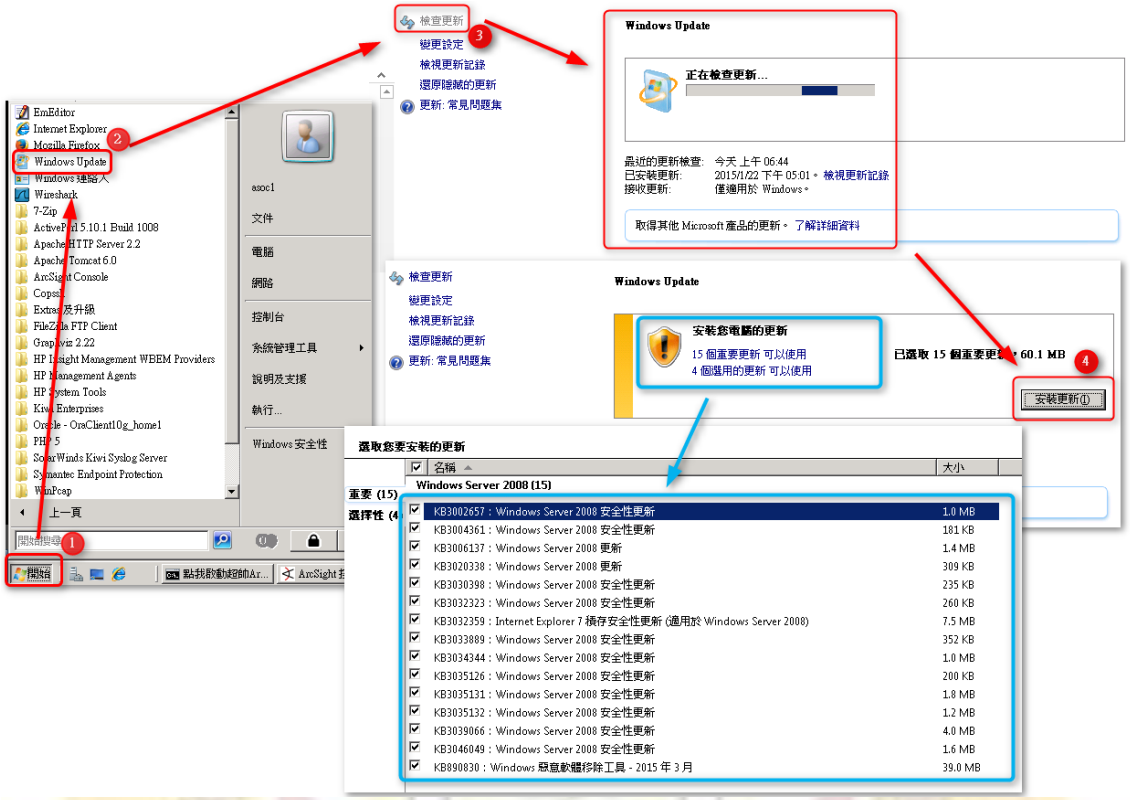


圖 2

在更新的設定上，建議採取系統自身建議的”自動安裝更新”，流程上請在 Windows Update 的介面選取”變更設定”→自動安裝更新即可。可參考下圖 3。

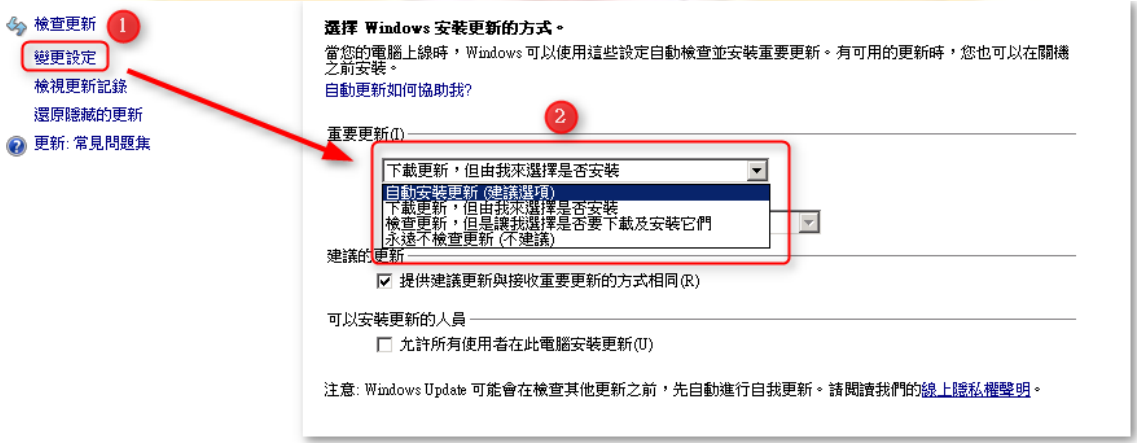


圖 3

如果想確定自己本身的主機已經安裝了哪些的更新，或確保主機的更新狀態成功與否，可點選選單上的”檢視更新紀錄”，在這裡可以查看到更新是否成功，另外

可以點選藍色框框部分進行日期的排序以得知目前最新的更新日期。相關範例請參考下圖 4。

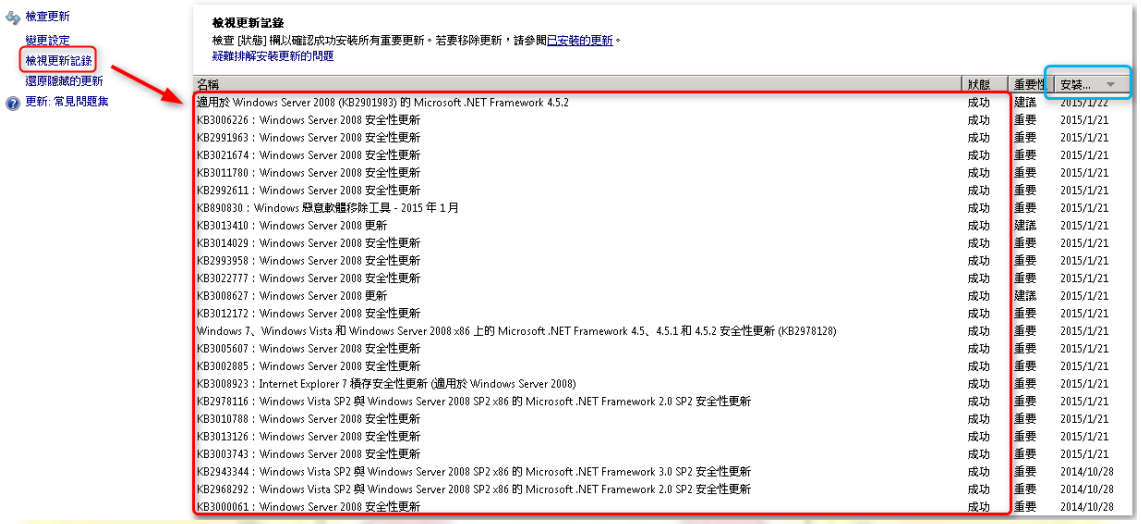


圖 4

如果對於安全性更新的漏洞有相關疑問或更多了解，可以參考網站資訊: https://technet.microsoft.com/zh-TW/library/security/ 查找相關的修補漏洞訊息，內容包含了相對應的更新檔案編碼（參見圖 5 編號 1）與此更新仍支援的作業系統清單，不受此風險影響的作業軟體不會出現在清單列上，如果已經 EOS 終止支援的作業系統也不會出現在名單列上（請見圖 5 編號 2）。

圖 5

Windows Server 2003 升級前的防禦措施

若於停止支援後繼續使用 Windows Server 2003 作業系統，將有諸多資安相關風險，未能如期在終止支援前完成伺服器的移轉與升級，則建議此期間採取防範方式如下，唯下列方法僅能降低資安風險，仍建議系統管理者儘快完成轉移：

1. 安裝防毒軟體：
   於作業系統安裝適當的防毒軟體，並定期更新病毒碼，管理者需定期掃描伺服器，圖 6、圖 7 為 Microsoft 所提供的免費防毒軟體 Security Essentials 示意圖。

圖 6

圖 7

2. 設定 Windows 防火牆，關閉不需要或不使用的通訊埠：

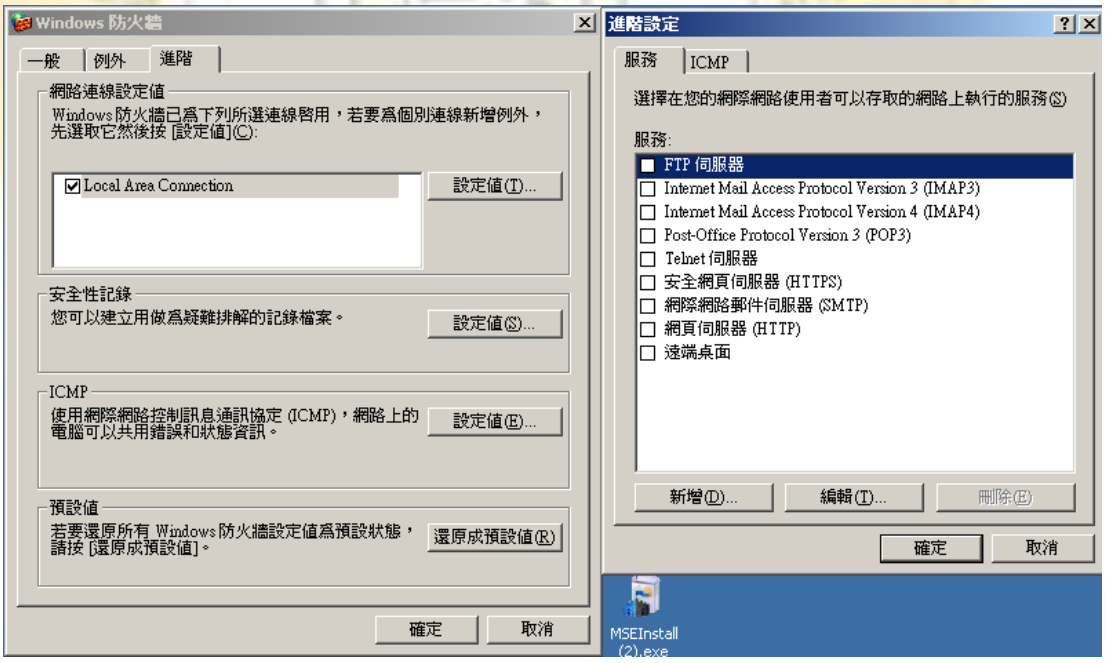


圖 8

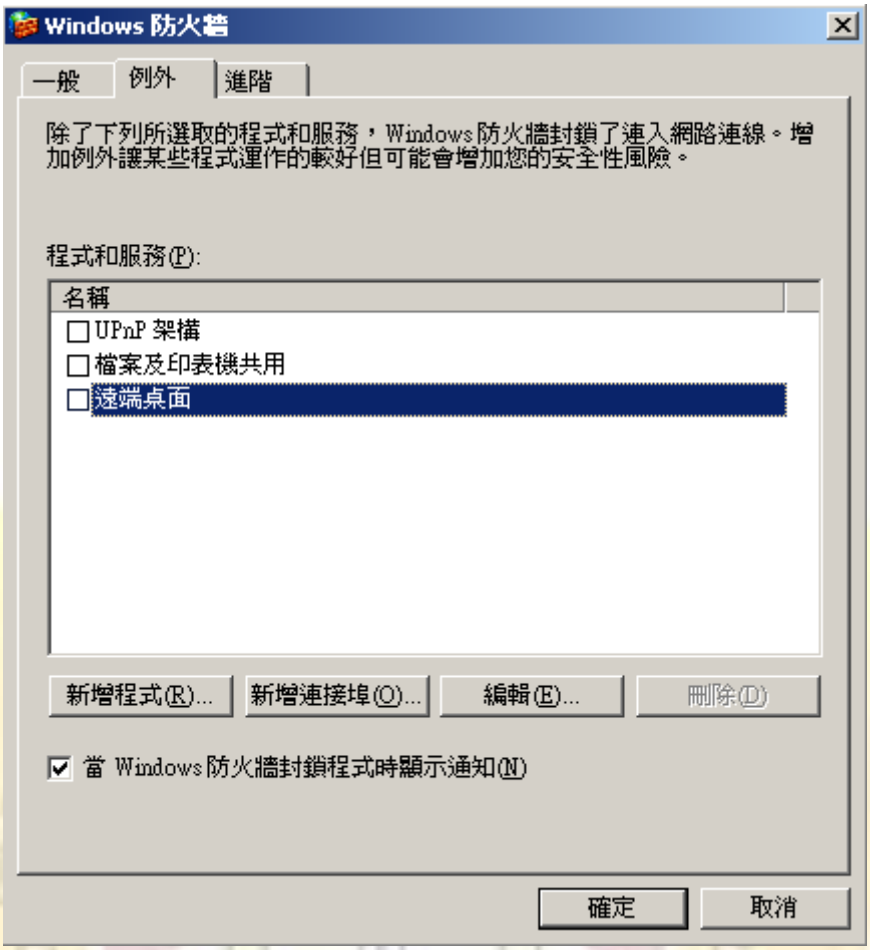
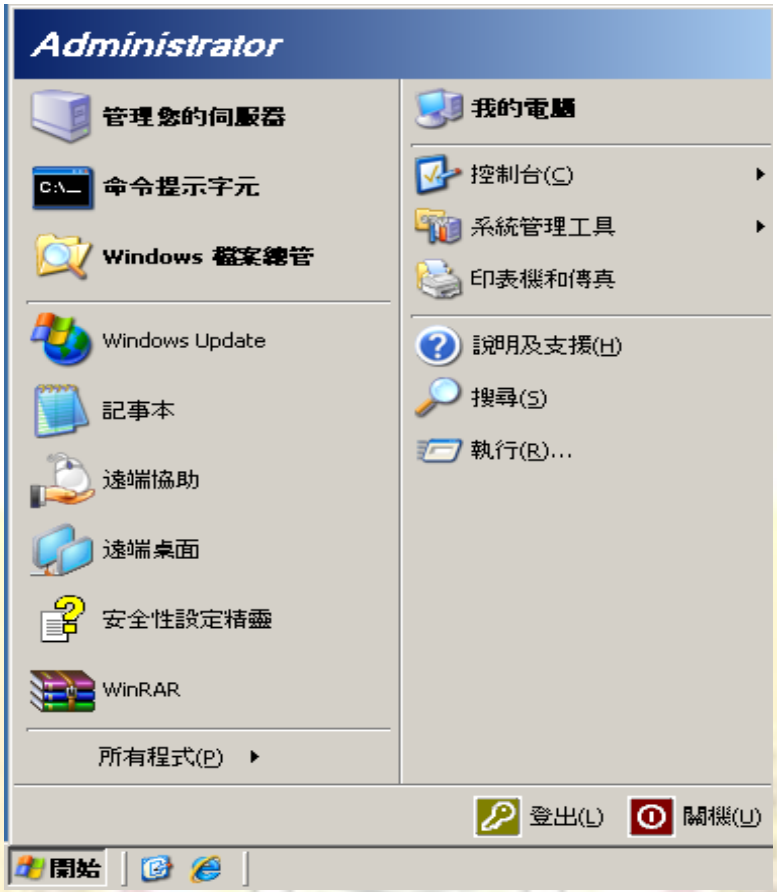


圖 9

3. 密碼強度：
   使用者在密碼設定的部份，可以加強密碼的強度設定以提高身份驗證的門檻，請到「控制台」中的「使用者帳號」中設定密碼。
4. 惡意程式移除工具：
   掃描惡意程式，可使用作業系統提供之掃描惡意程式工具，操作方式由開始選單列的執行功能中輸入 mrt（見圖 10 至圖 12），也可下載 Process Explorer(http://technet.microsoft.com/enus/sysinternals/bb896653)進行檢測，如電腦裡有經過打包加工的惡意程式則該程式會呈現紫色(非淡紫)需特別注


Administrator
管理您的伺服器
命令提示字元
Windows 檔案總管
Windows Update
記事本
遠端協助
遠端桌面
安全性設定精靈
WinRAR
所有程式(P)
我的電腦
控制台(C)
系統管理工具
印表機和傳真
說明及支援(H)
搜尋(S)
執行(R)...
登出(L)
關機(U)
開始

意。

圖 10

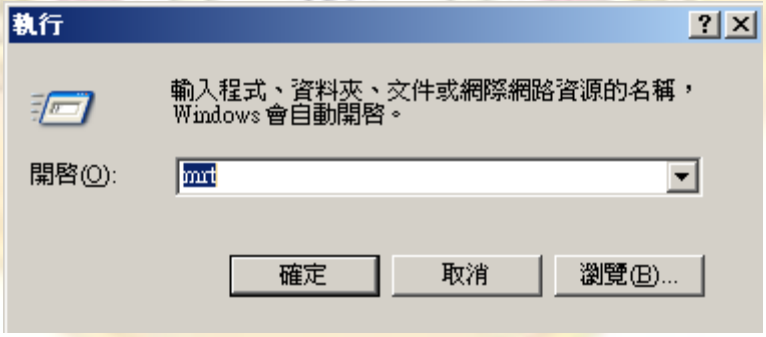

執行
輸入程式、資料夾、文件或網際網路資源的名稱，
Windows 會自動開啓。
開啓(O):
mrt
確定
取消
瀏覽(B)...

圖 11

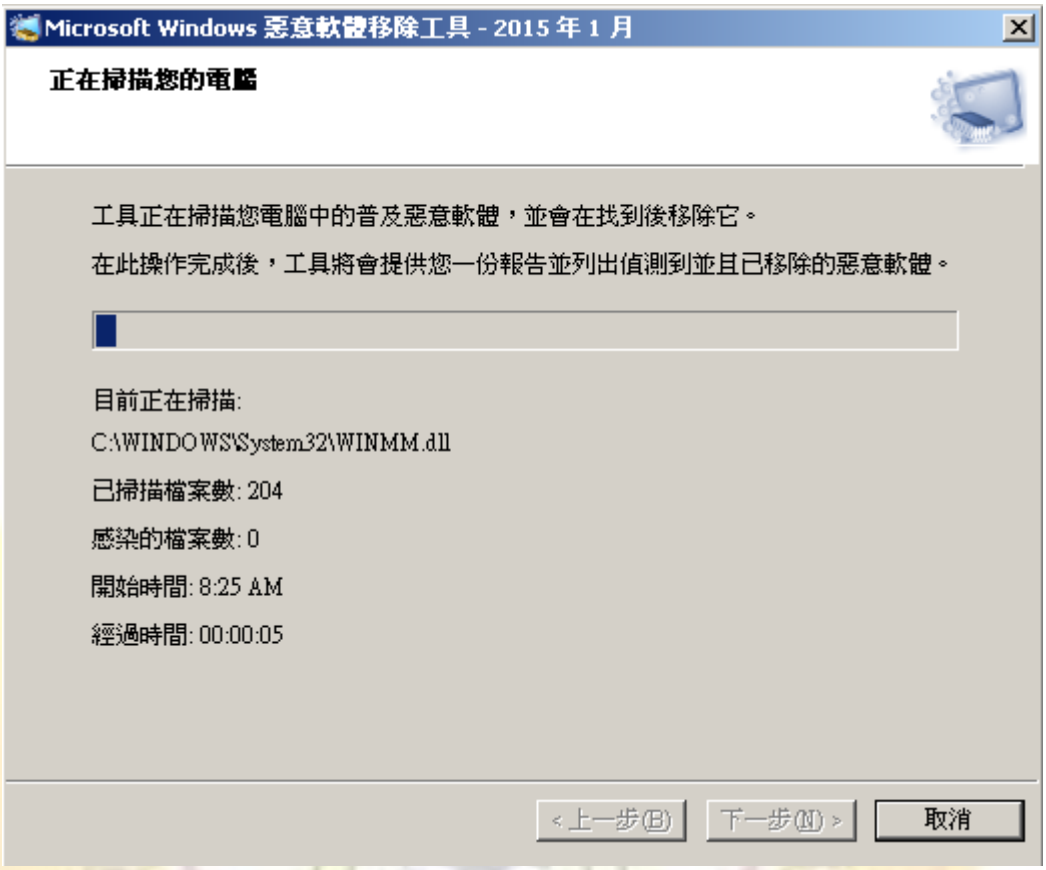


圖 12

參考資料

1. Microsoft Taiwan 台灣微軟部落格，http://blogs.technet.com/b/microsoft_taiwan/archive/2014/07/17/windows-server-2003-end-of-support.aspx
2. http://www.ithome.com.tw/news/92982
3. http://www.ithome.com.tw/node/83249
4. http://news.networkmagazine.com.tw/news/2013/04/15/49056/
5. http://www.im.taichung.gov.tw/public/data/115020/451615502771.pdf
6. https://www.google.com.tw/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CCoQFjAC&url=http%3A%2F%2F4c5i6s.ydu.edu.tw%2Ffront%2Fbin%2Fdownload.phtml%3FPart%3D09120028%26Nbr%3D30%26Category%3D53&ei=ITIIVd_IPNbc8AWo_4HADw&usg=AFQjCNF4V1wTAed2V3YacYZNkc4_POEUog
7. http://www.im.taichung.gov.tw/public/data/115020/451615502771.pdf