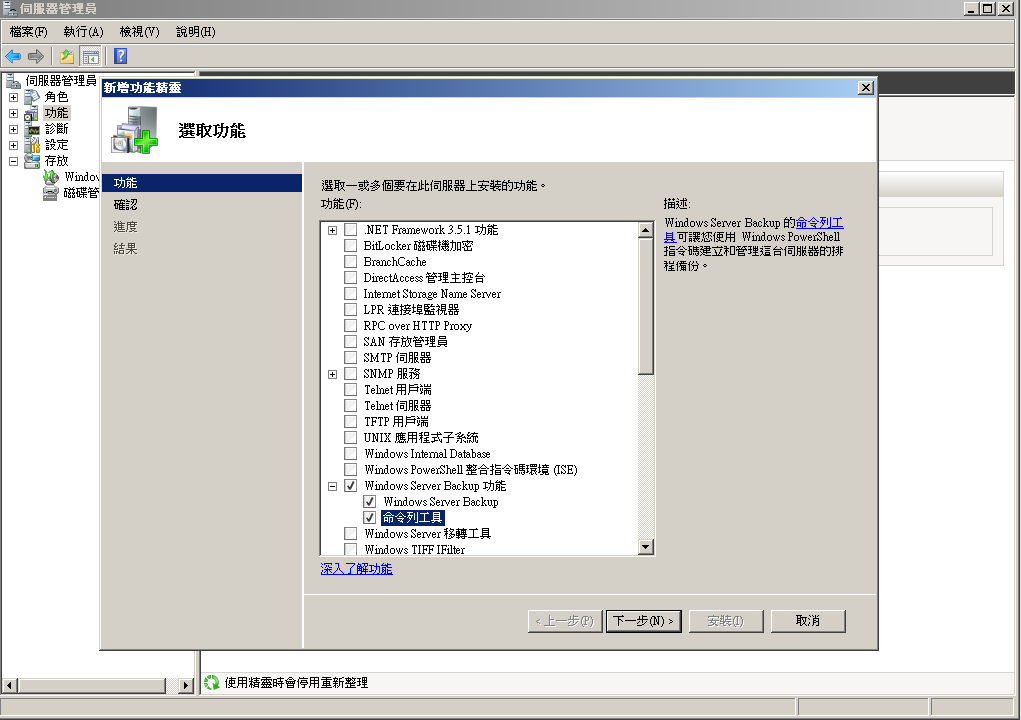
**iDPBG AD災難恢復**

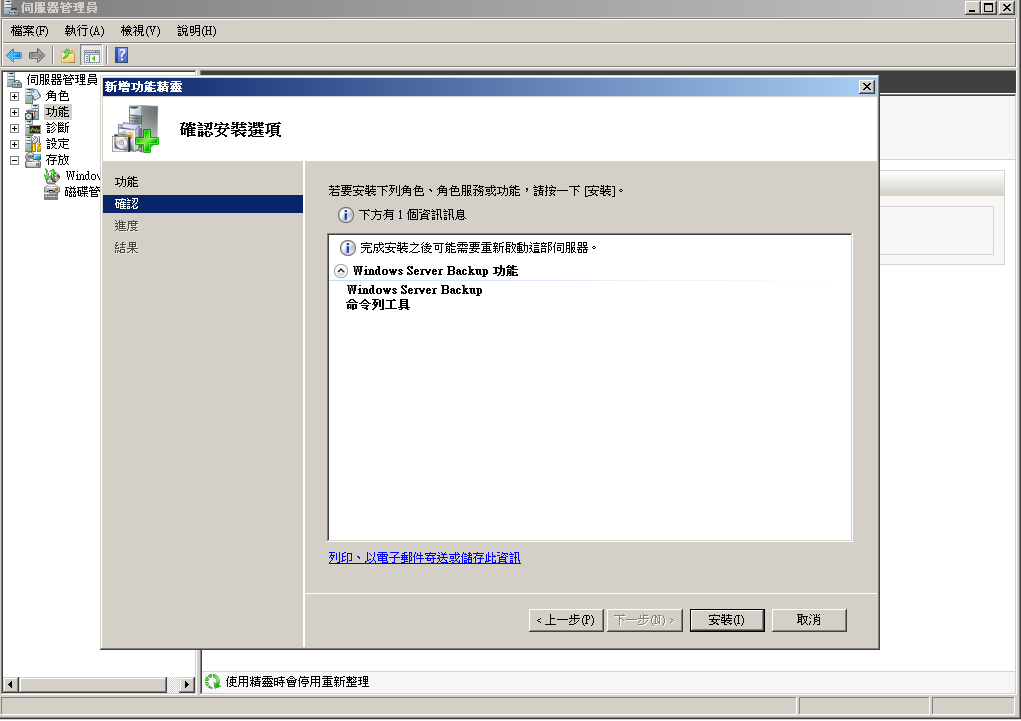
|  |  |  |  |
| --- | --- | --- | --- |
| 恢復日期 | 2020/07/21 | 負責人 | 蒲曈宇 |
| 數據&資料 | 完全備份 | 恢復工具 | Windows Server Backup |
| 恢復介質 | 磁碟備份 | 備份時間 | 2020/07/21 |
| 恢復開始時間 | 2020/07/21 13:30 | 恢復完成時間 | 2020/07/21 19:30 |
| **恢復環境**：Windows Server 2008 R2  **目的**：驗證備份數據正確性和可恢復性  **災難恢復方式一般有以下兩種：**  1、系統狀態恢復（此種恢復前提，恢復電腦能正常進入活動目錄還原安全模式，該方式主要針對AD服務器做恢復）  2、裸機恢復（此種恢復主要是針對服務器無法正常啟動，需要注意的是，恢復電腦硬件配置必須與之前備份的電腦配置基本相同，否則恢復後會出現藍屏或無法正常啟動）  配置要求：（此處是指實體機的配置）  1、實體機可以實現虛擬化  2、硬件：Intel8核處理器+8G內存  **本次所涉及到的災難恢復大概步驟：**  1、使用Windows Server Backup進行一次完全備份，包含系統狀態、活動目錄資料庫、卷等相關資訊，將備份傳輸至移動硬盤。  2、使用U盤內的PE工具將移動硬盤內備份文件複製到需要恢復的電腦硬盤中。  3、使用Windows Server 2008 R2系統光盤對需要恢復的電腦做裸機恢復。  **做演練前必須理解以下幾個名詞含義：**  裸機恢復：一個進行裸機恢復的一個備份接口  系統狀態：包含Boot Files、COM+ Class Registration Database、Redistry等，  如果是域控制器，還會包含sysvol、AD資料庫等。  系統保留：就是我們在安裝系統的時候提示我們要保留的100M空間  本機磁碟C：即C分區裏面所有的數據文件 | | | |

**災難恢復演示（演示系統為Windows 2008 R2）**  
 1、Windows Server Backup工具安裝

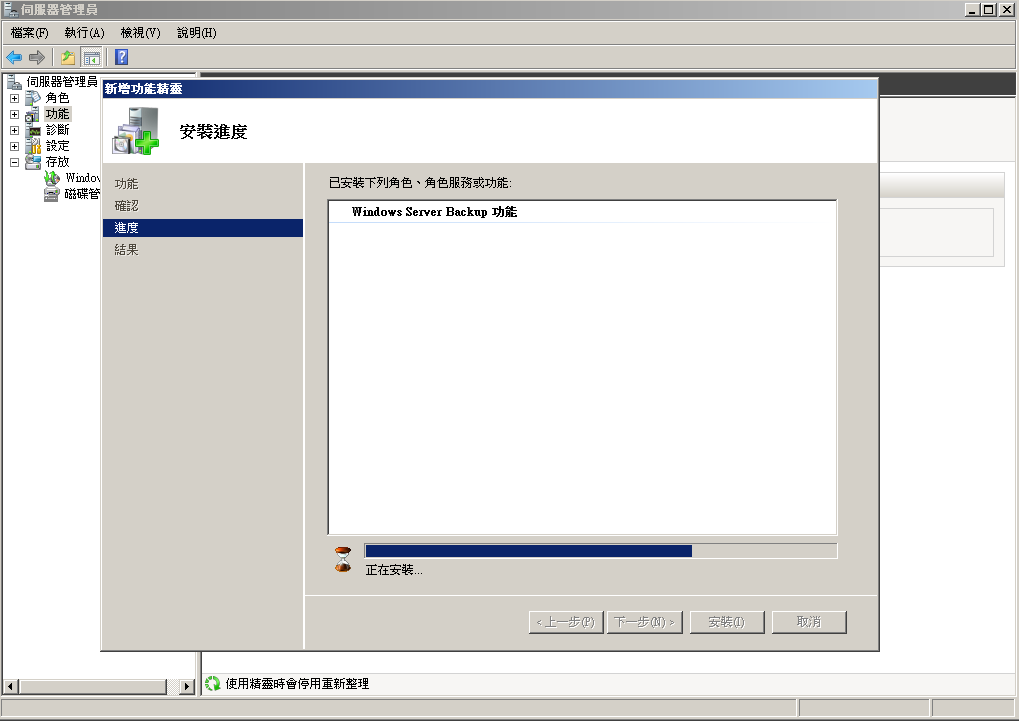
伺服器管理員-->功能-->新增功能，如圖勾選後點擊“下一步”



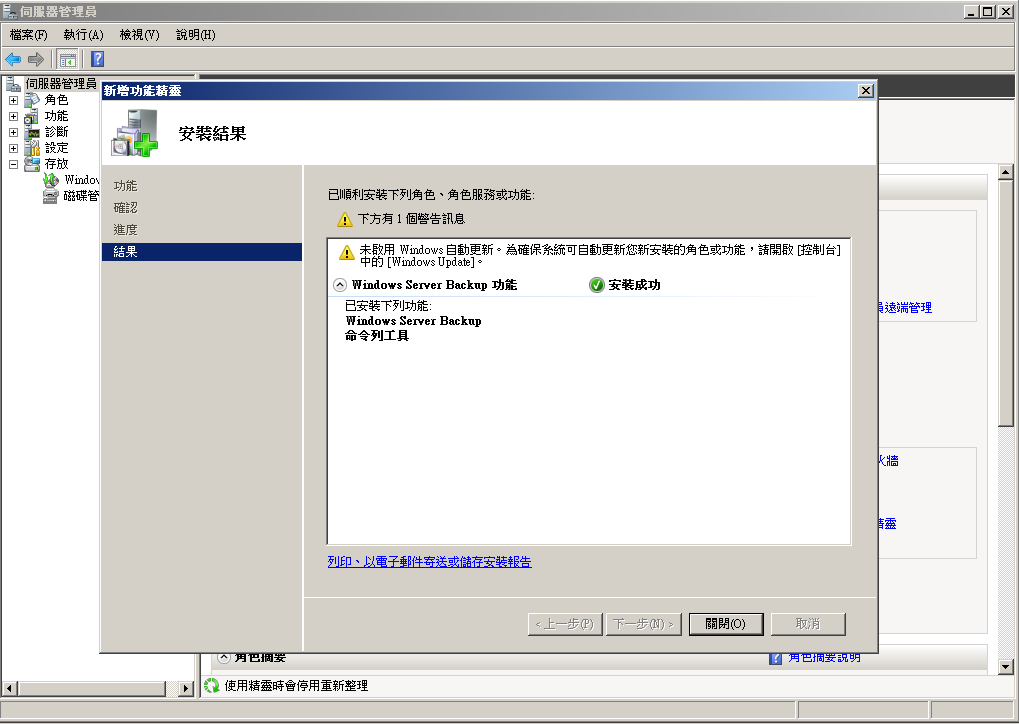
點擊“安裝”



下圖為安裝狀態

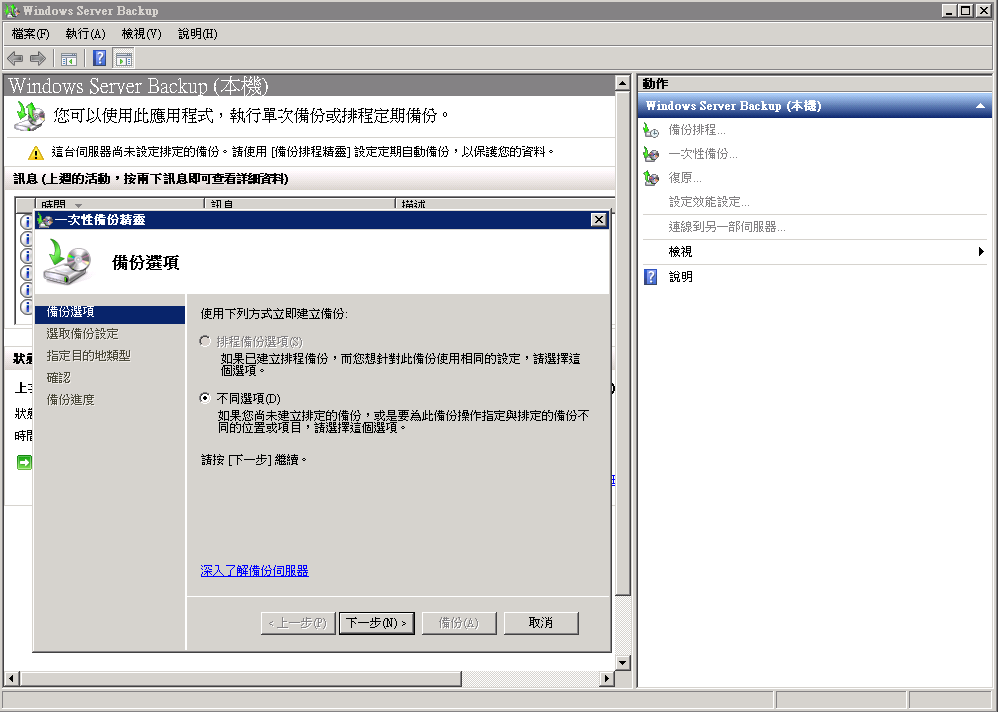


安裝成功後，點擊“關閉”

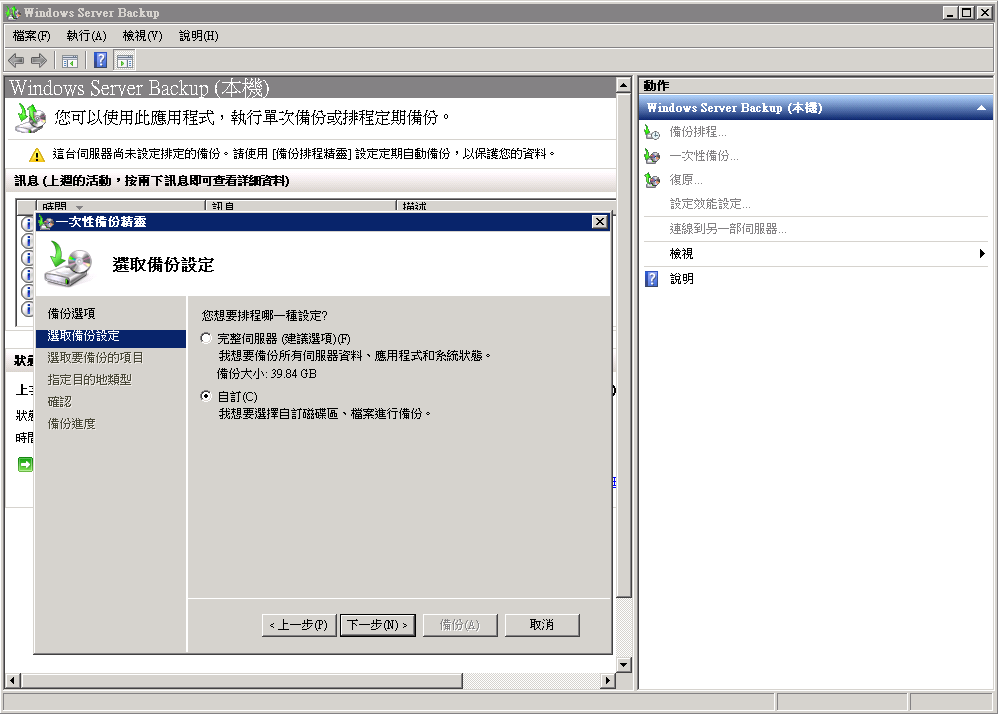


2、活動目錄備份

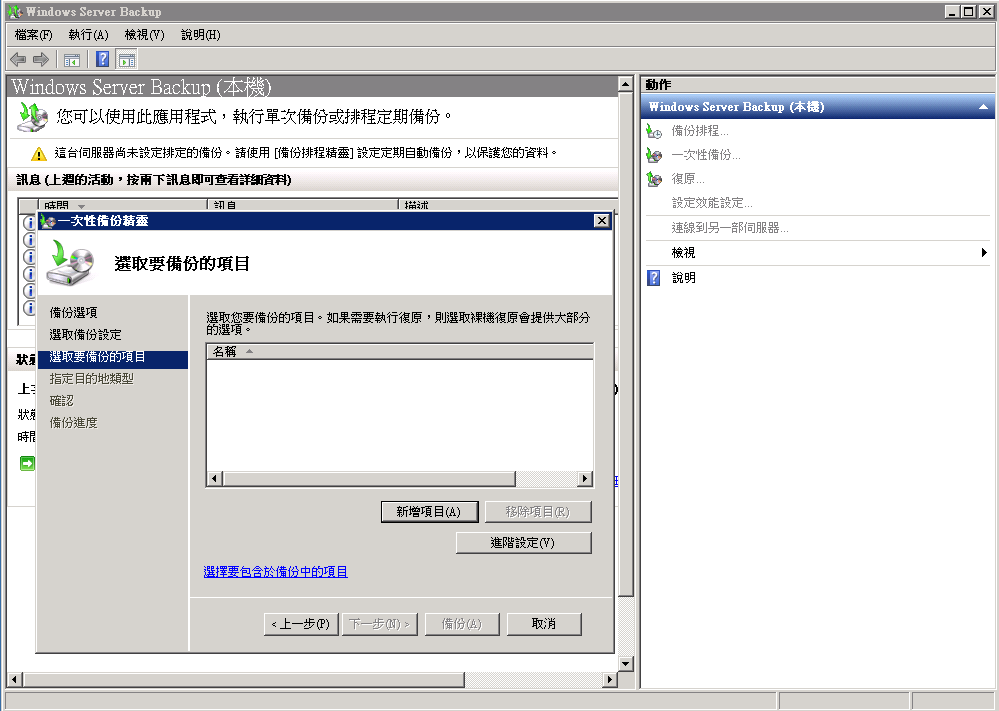
開始-->所有程式-->系統管理工具-->Windows Server Backup，點擊“一次性備份”，再如圖點擊“下一步”



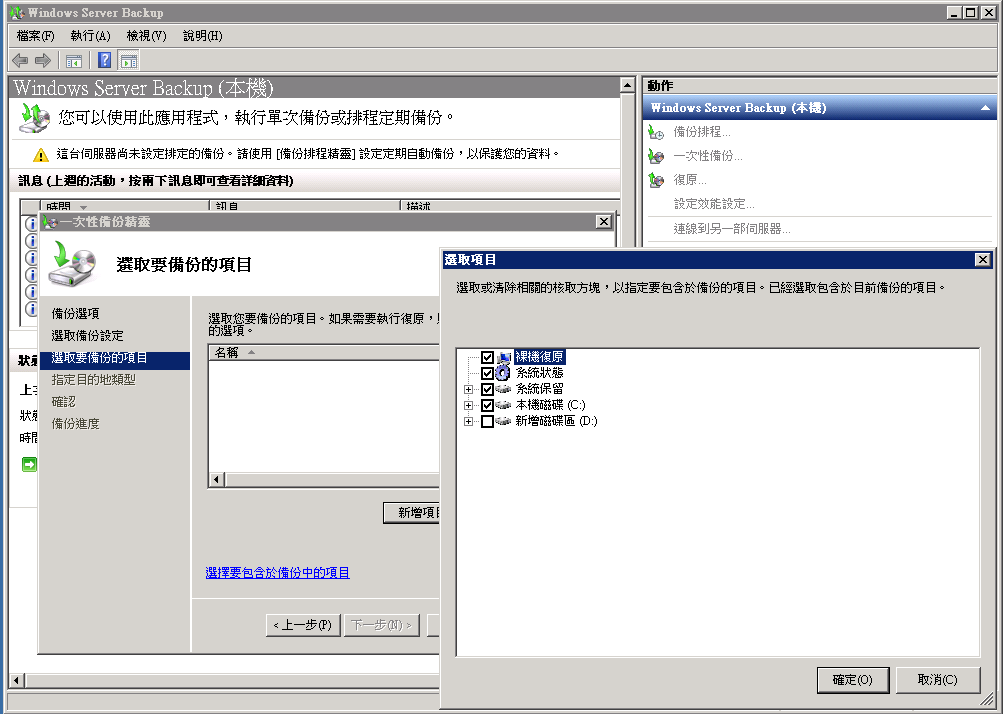
如圖選擇“自訂”，點擊“下一步”



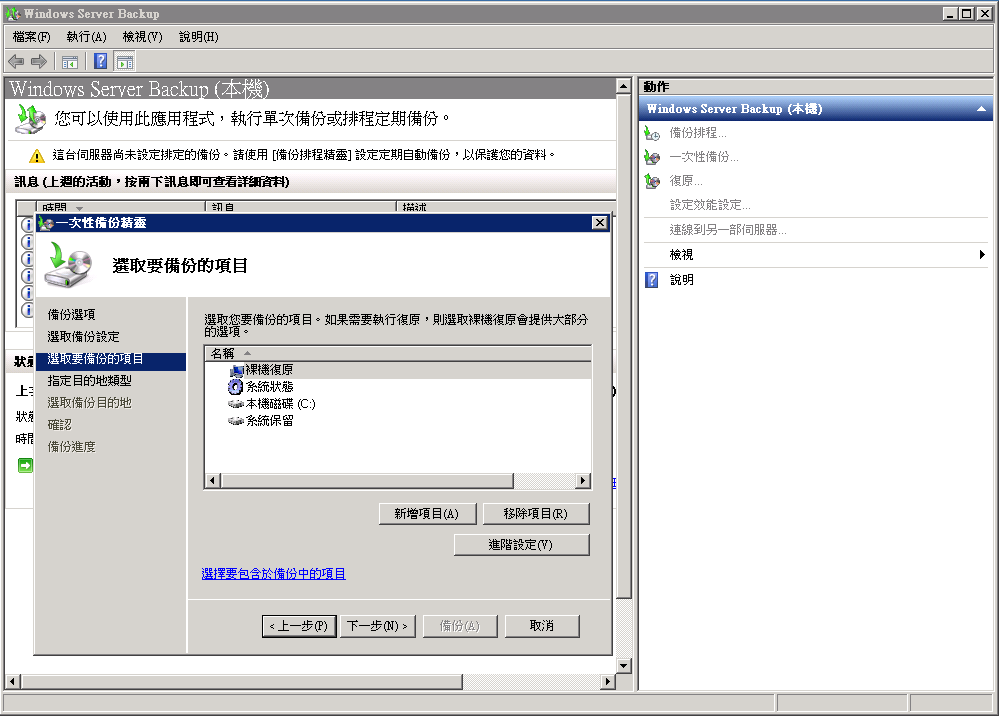
點擊“新增項目”



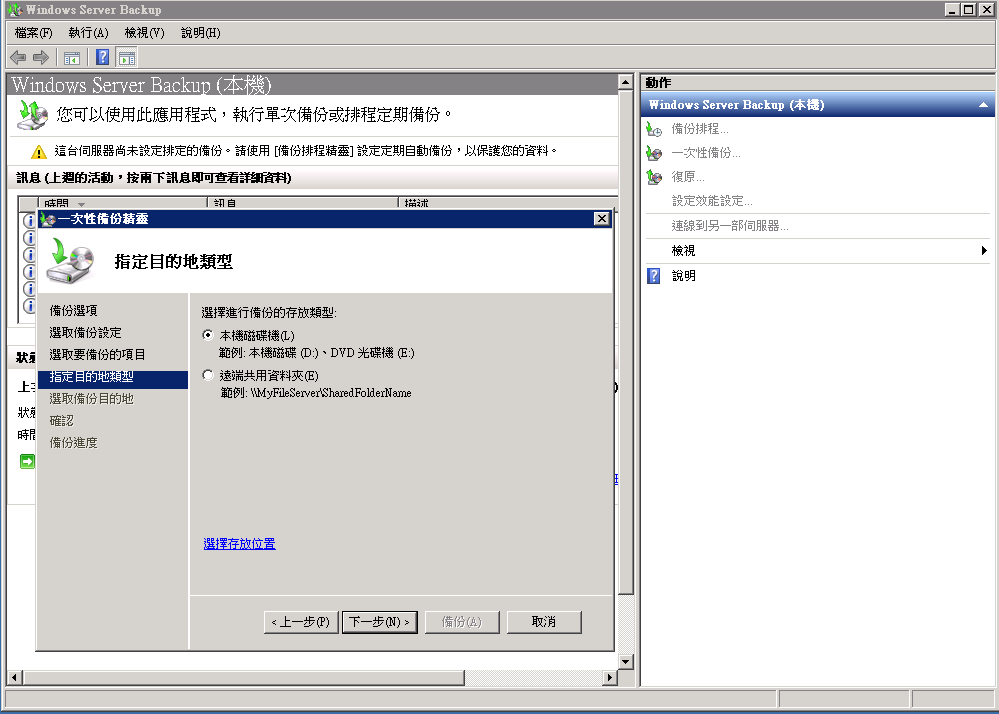
如圖勾選相關選項點擊“確定”



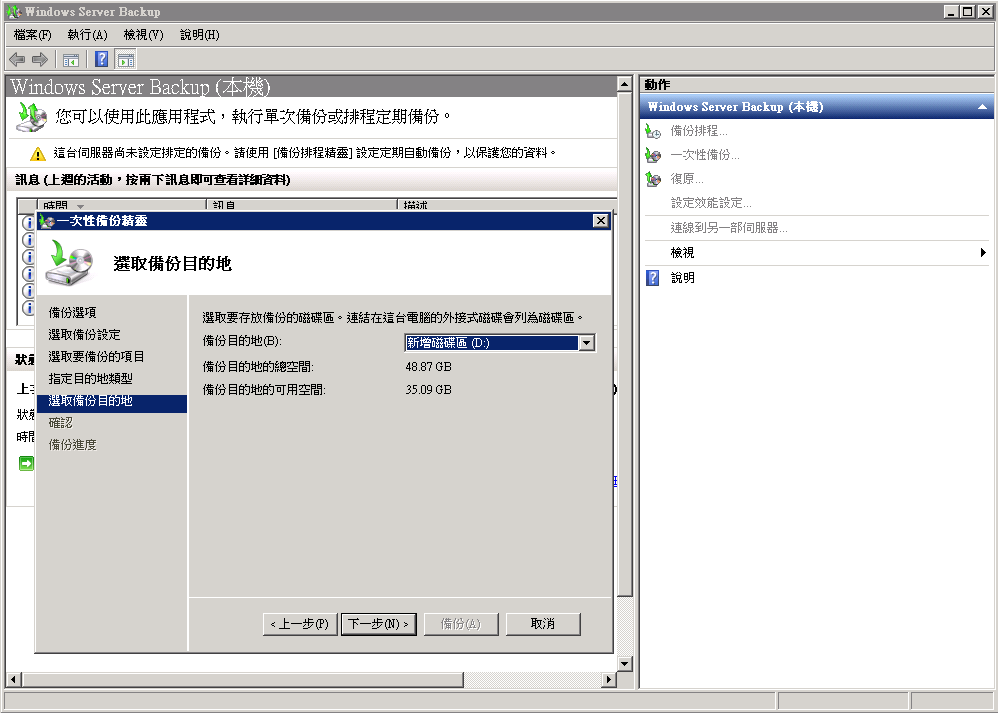
點擊“下一步”



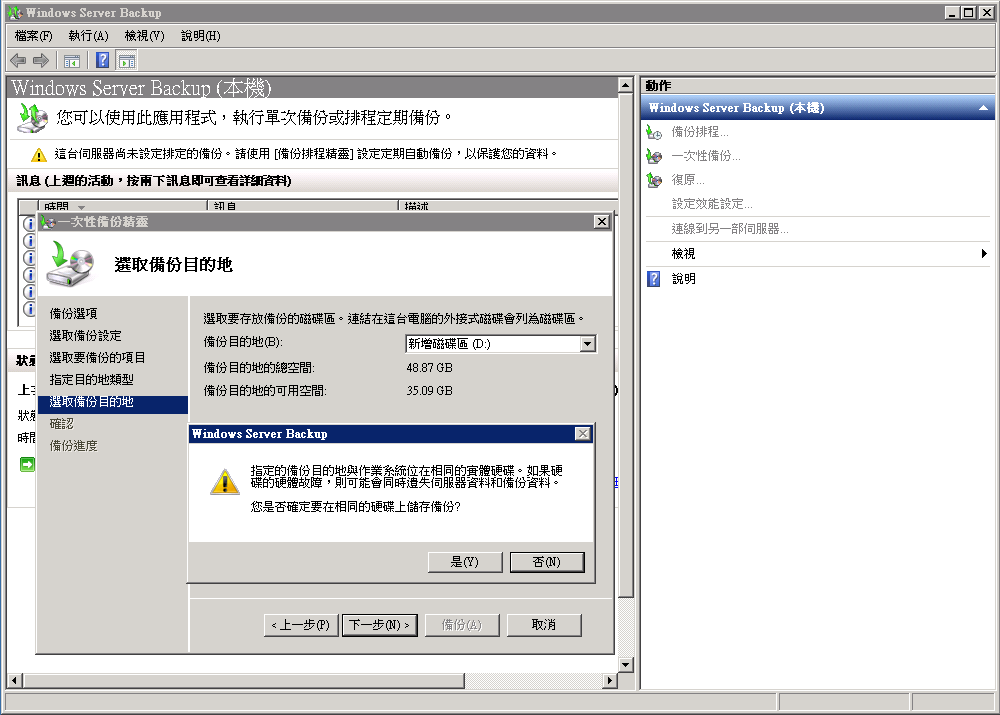
如圖勾選點擊“下一步”（注意：由於本次是災難恢復演練實驗，故此為了加快備份速度，選擇存放在本地磁盤。如果是正式備份，為了數據安全則必須備份在異地）



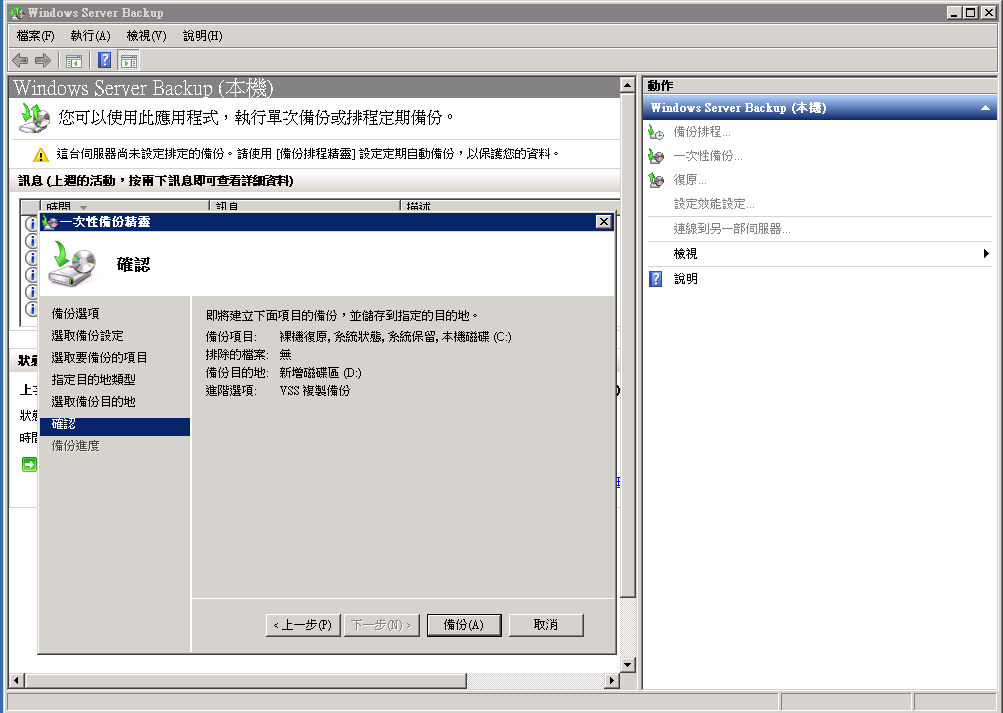
選擇好備份目的分區，點擊“下一步”

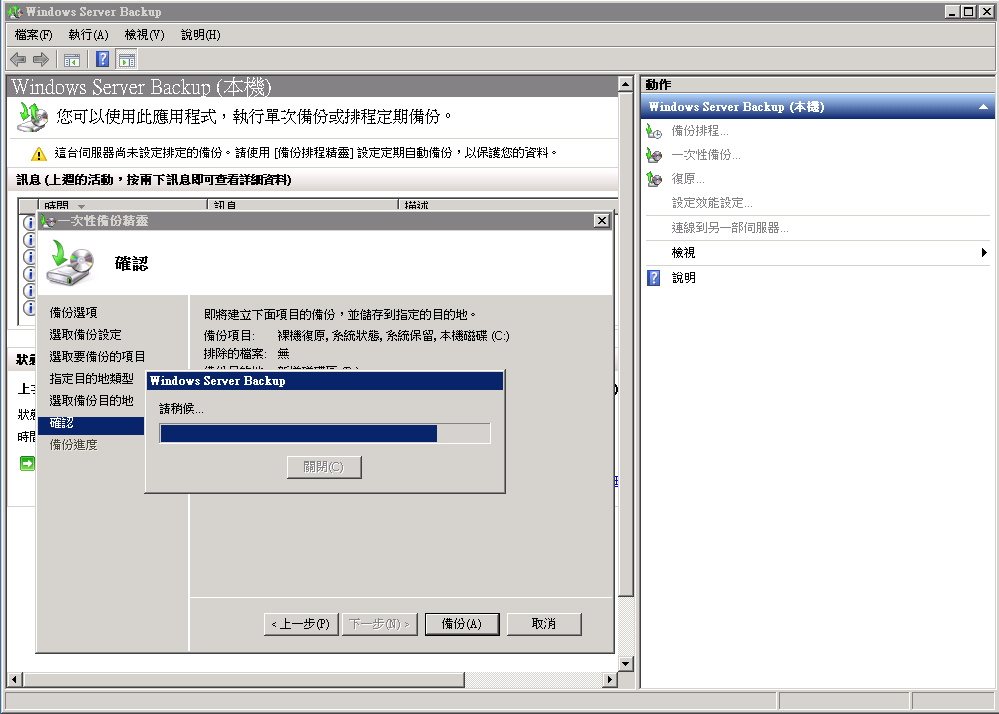


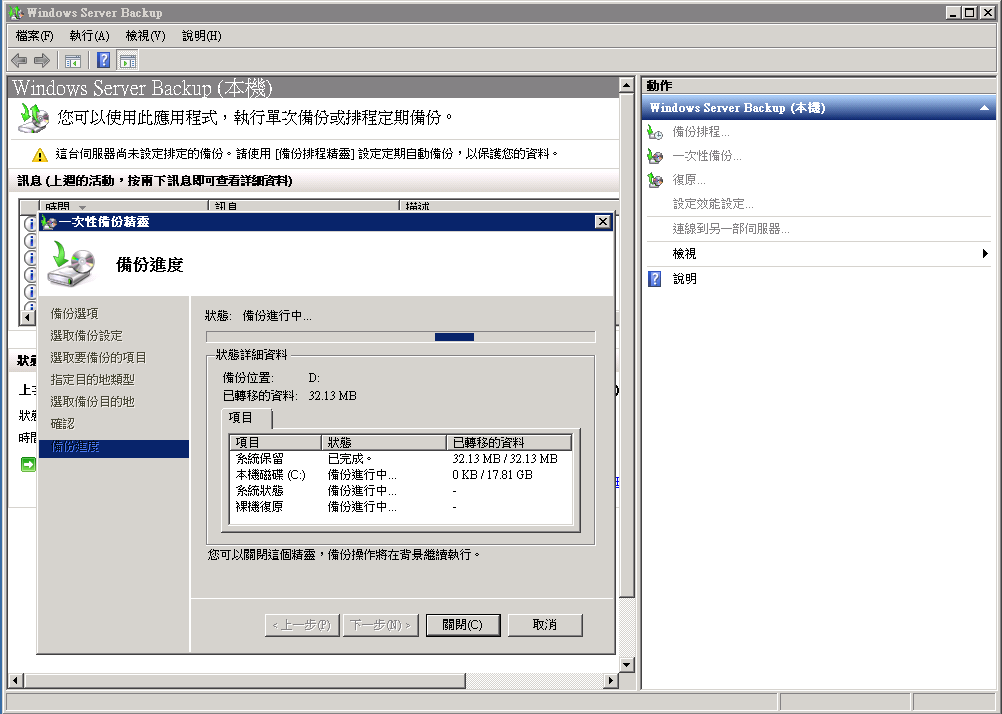
點擊“是”



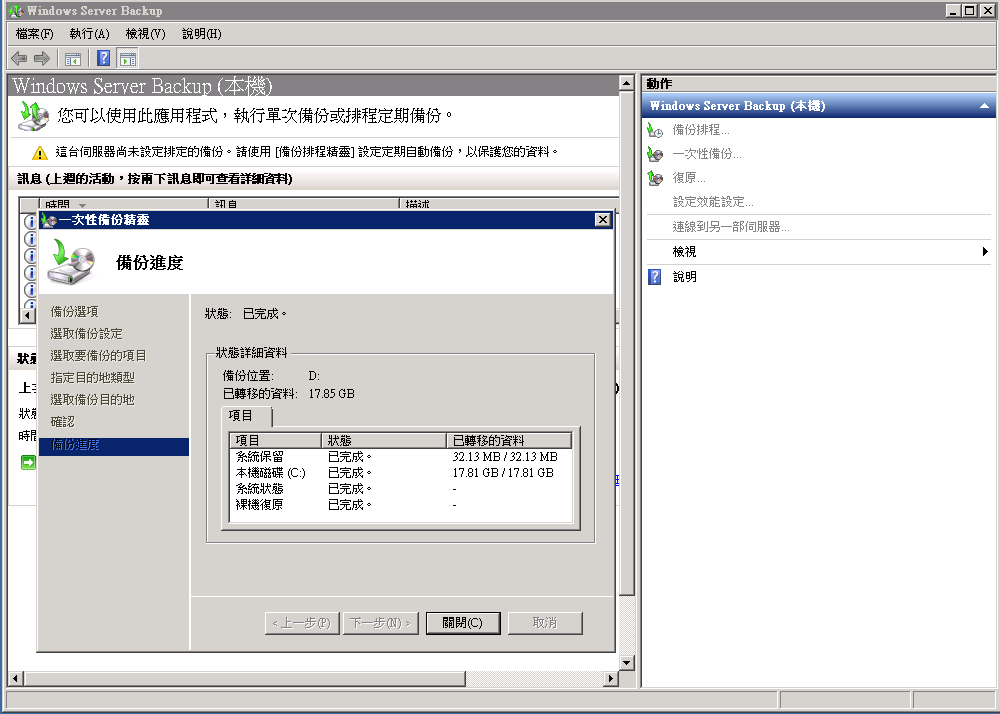
點擊“備份”







出現如圖介面，表示備份完成，點擊“關閉”結束活動目錄備份



**此刻，去備份目的分區查看，會發現該分區下有一個名稱為WindowsImageBackup的文件夾，該文件夾中的數據即為備份文件，大概18GB**

**如下圖（由於下圖在測試虛擬機內，時間上跟實際備份文件有出入）**



將WindowsImageBackup傳輸至移動硬盤（備份時間約為50MIN，拷貝至移動硬盤時間約為10MIN，共1H）

3、活動目錄恢復（注意：做災難恢復時，一定要斷開網絡）

**將移動硬盤內的WindowsImageBackup數據通過U盤PE工具恢復到需要恢復活動目錄的電腦硬盤當中（即下面的虛擬機當中）**

（加載PE系統及傳輸數據，時間為1H）

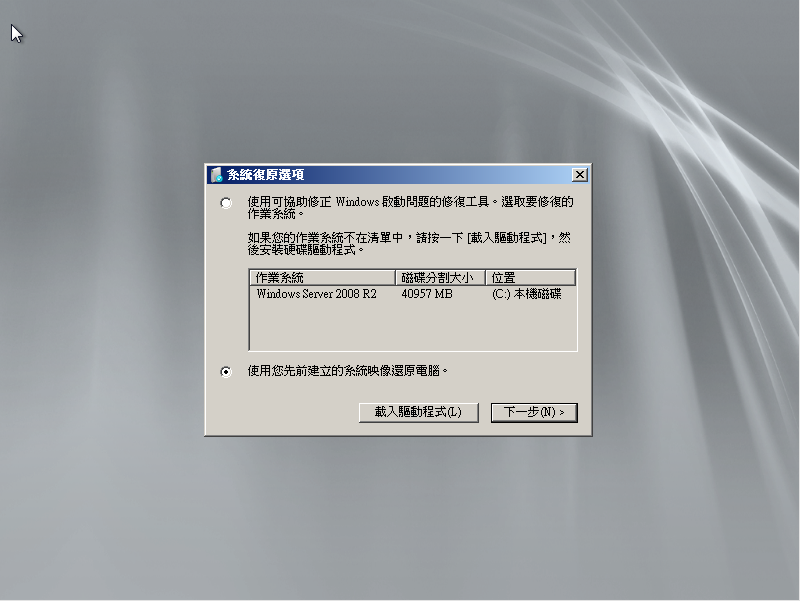
在虛擬機當中掛在Windows Server 2008 R2系統光盤，並從光盤



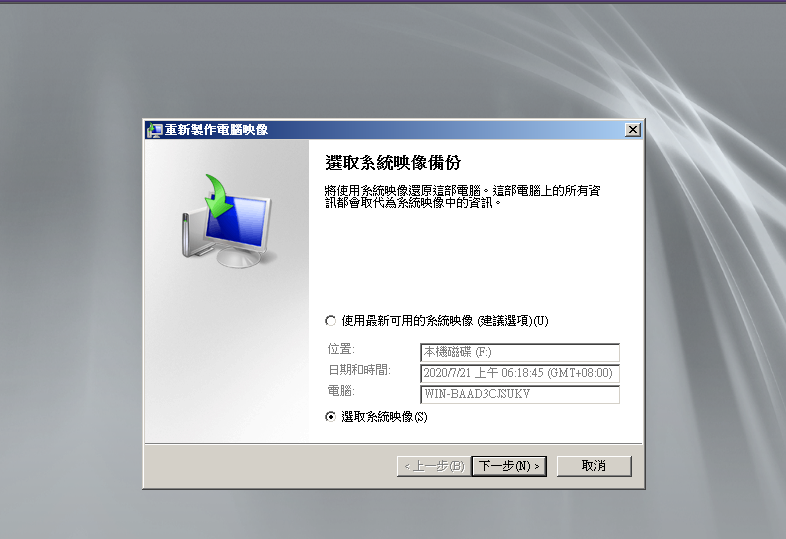
點擊左下角“恢復您的電腦”



如圖所選，點擊“下一步”

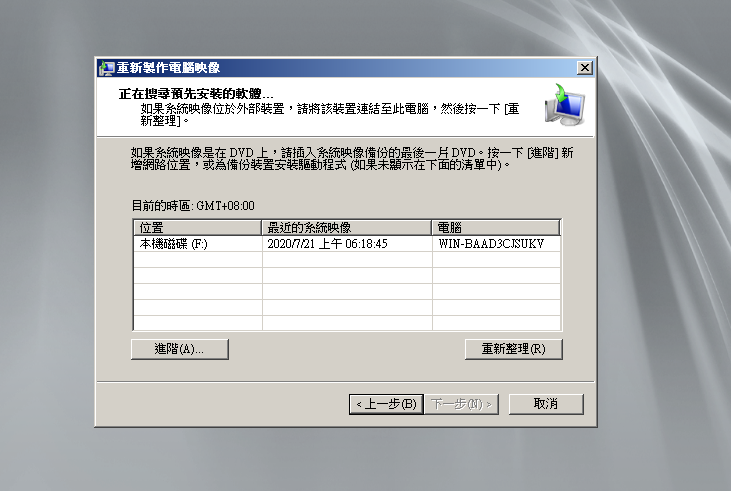


如圖所選，點擊“下一步”

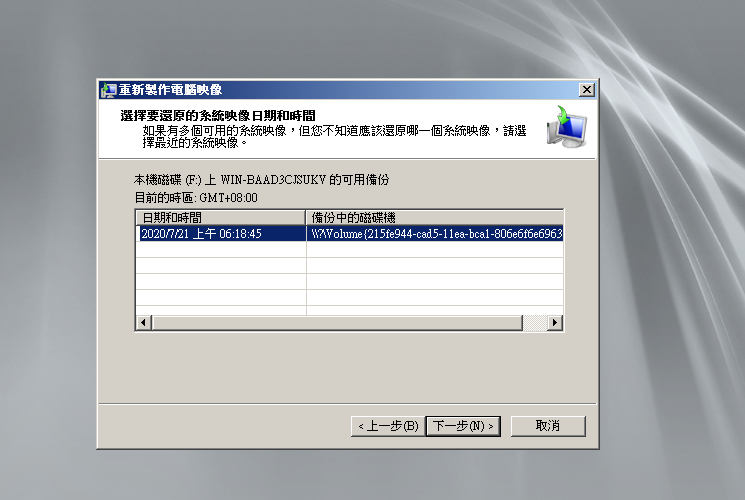


如圖選中需要還原的系統映像，點擊“下一步”

Kvm在此处安装硬盘驱动程式

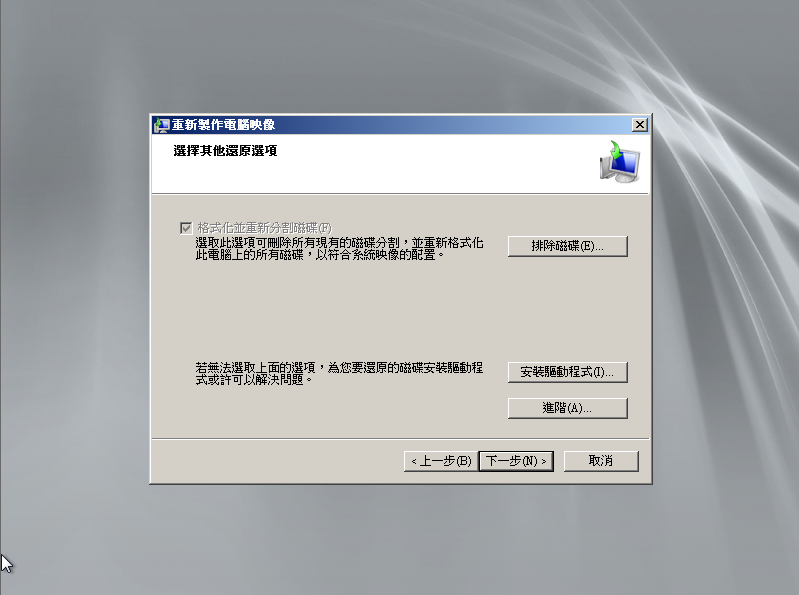


如圖選中需要還原的系統映像時間及備份位置，點擊“下一步”



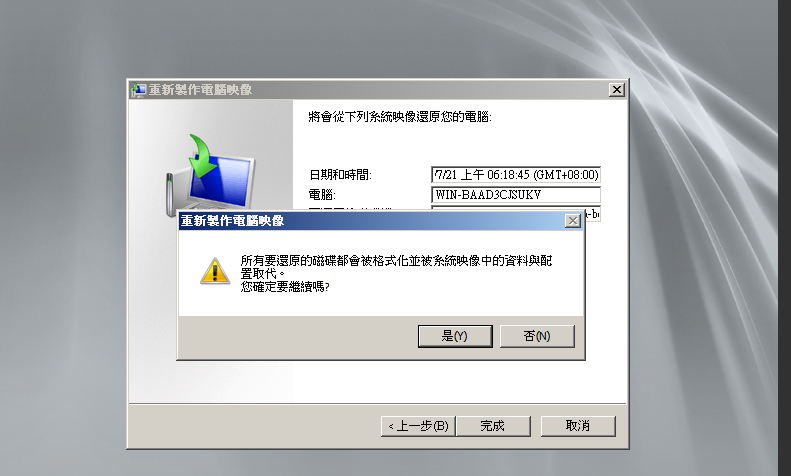
點擊“下一步” ，

Kvm 虚拟机在此处安装驱动会提示0x80070103，这个提示是系统中已安装对应版本的磁盘驱动，所以返回之前的步骤“使用最新可用的系统镜像”，之后再下一步下一步下一步，等待还原

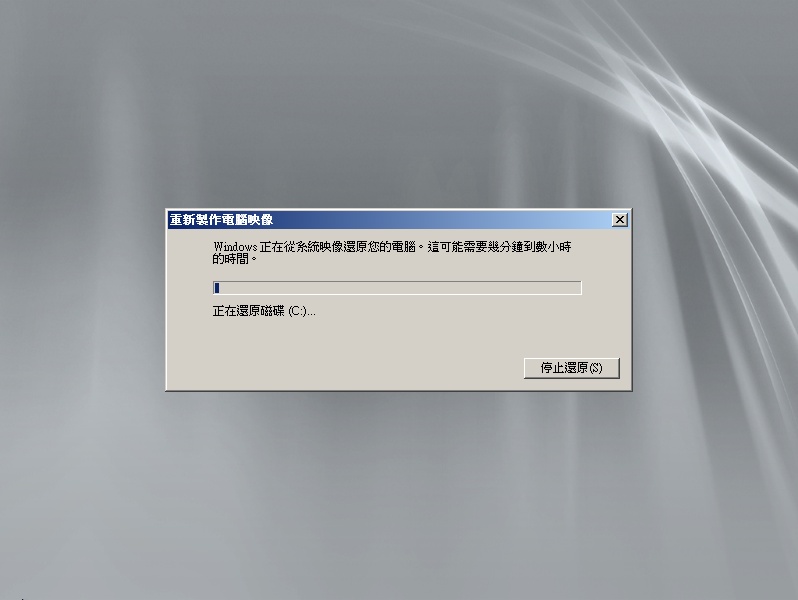


點擊 “完成”

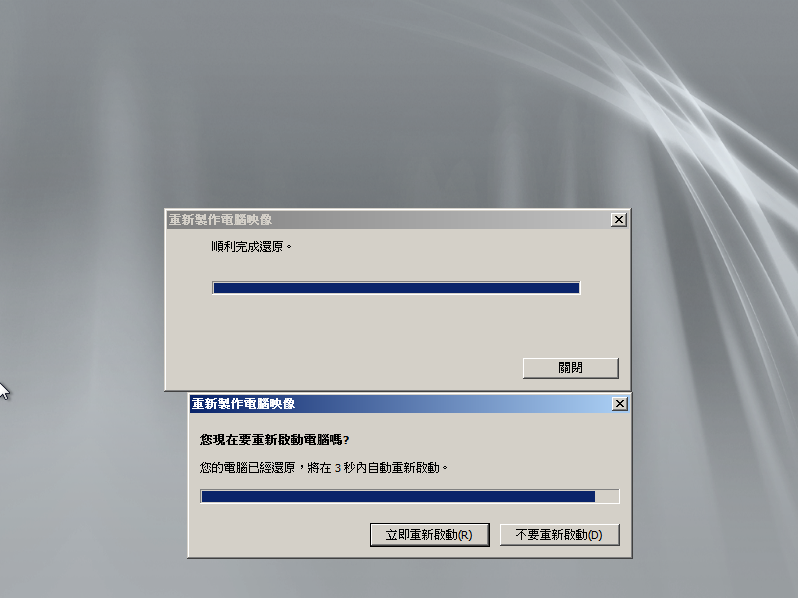
.點擊 “是”



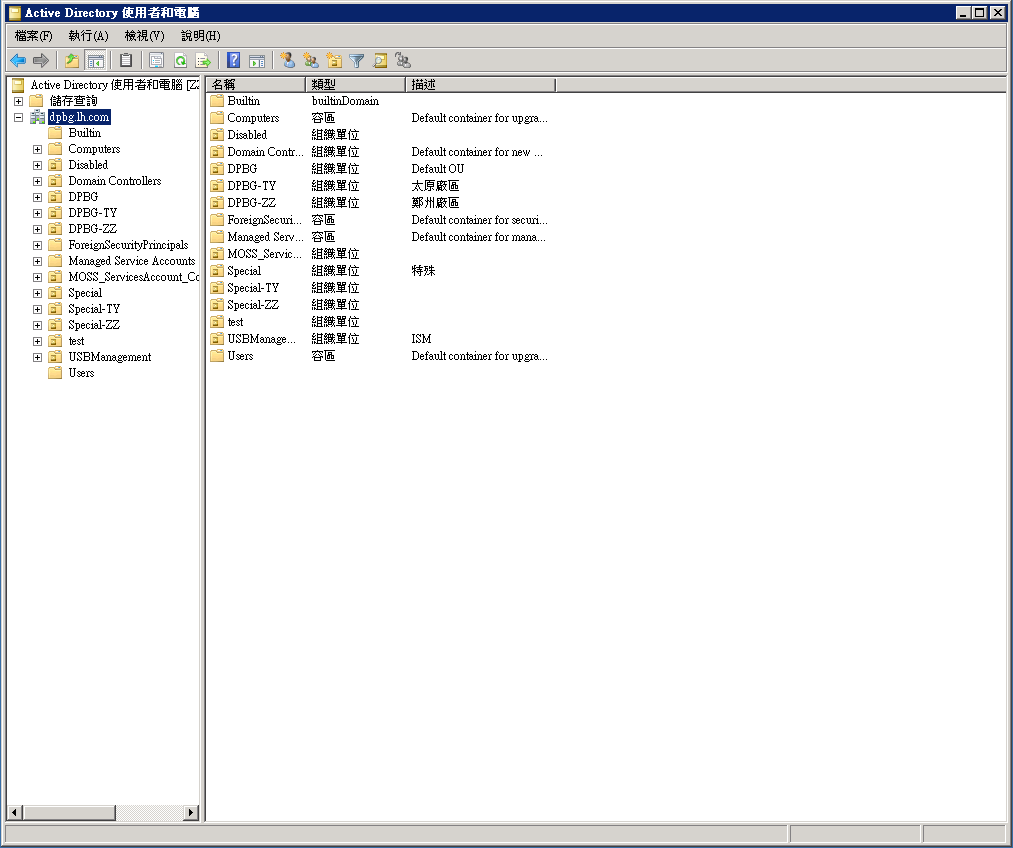
下圖為恢復狀態，請耐心等待，該段恢復時間有點長。



下圖為恢復成功後的圖片，電腦將會在1分鐘後自動重啟。



正常重啟電腦後，登錄到桌面並打開Active Directory 使用者和電腦，如圖



AD活動目錄恢復及同步、校驗共需3H

**恢復時間大概統計：**

Windows Server Backup工具安裝5MIN

活動目錄備份及傳輸至移動硬盤1H

將備份文件恢復到恢復主機1H

活動目錄恢復2H

總共恢復時間約4H

資安事件通報30MIN

恢復后的同步、校驗1H

完成過程需5.5H

**備註：1.裸機恢復一定要注意硬件配置問題，如果硬件配置相差太大，恢復後會藍屏或者無法正常啟動。**

**2.由於受資源限制，找不到相關配置的HP服務器，本次實驗藉助的是VMware Workstation虛擬軟件來模擬的實際環境。**

**災難恢復要點：**

1. **恢復的電腦硬件配置必須與之前的當機電腦硬件配置完全相同；（說必須完全相同是為了數據穩定及安全考慮，實際上硬件配置基本相同即可。）**
2. **使用裸機恢復必須要有完整的備份文件，即包含：裸機恢復、系統狀態、系統保留及本地磁碟C。（其中C分區為系統分區）**
3. **為了AD災難恢復節約時間，將備份文件刻錄到光盤等外置存儲設備當中，方便節約恢復備份文件的時間，從而節約AD災難恢復時間。**
4. **恢復過程當中，恢復電腦必須斷開網絡。**
5. **恢復完成後，在將IP地址與DNS配置與之前的相同，接通網絡，手動同步DC間的複製。**