

Partner

如何使用 WMI 設定

Windows AD 事件記錄和使用者資料

V008

2021/05/18



版權聲明

N-Partner Technologies Co.版權所有。未經 N-Partner Technologies Co.書面許可，不得以任何形式仿製、拷貝、謄抄或轉譯本手冊的任何內容。由於產品一直在更新中， N-Partner Technologies Co. 保留不告知變動的權利。

商標

本手冊內所提到的任何的公司產品、名稱及註冊商標，均屬其合法註冊公司所有。

目錄

前言	2	4.3.3.2 設定讀取使用者資料權限	132
1. Windows 2000	3	4.3.4 設定 Event log 讀取權限	137
1.1 組織單位設定	3	4.3.5 重啟 WMI 服務	143
1.2 群組原則設定	7	4.4 設定防火牆	144
1.3 新增非管理帳號	13	5. Windows 2016	145
1.3.1 新增使用者	13	5.1 組織單位設定	145
1.3.2 設定 DCOM 權限	16	5.2 群組原則設定	149
1.3.3 設定 WMI 權限	20	5.3 新增非管理帳號	156
1.3.3.1 設定事件日誌權限	20	5.3.1 新增使用者	156
1.3.3.2 設定讀取使用者資料權限	25	5.3.2 設定 DCOM 權限	157
1.3.4 設定 Event log 讀取權限	30	5.3.3 設定 WMI 權限	162
1.3.5 重啟 WMI 服務	36	5.3.3.1 設定事件日誌權限	162
2. Windows 2003	37	5.3.3.2 設定讀取使用者資料權限	167
2.1 組織單位設定	37	5.3.4 設定 Event log 讀取權限	172
2.2 群組原則設定	41	5.3.5 重啟 WMI 服務	178
2.3 新增非管理帳號	49	5.4 設定防火牆	179
2.3.1 新增使用者	49	6. Windows 2019	180
2.3.2 設定 DCOM 權限	50	6.1 組織單位設定	180
2.3.3 設定 WMI 權限	54	6.2 群組原則設定	184
2.3.3.1 設定事件日誌權限	54	6.3 新增非管理帳號	191
2.3.3.2 設定讀取使用者資料權限	59	6.3.1 新增使用者	191
2.3.4 設定 Event log 讀取權限	64	6.3.2 設定 DCOM 權限	192
2.3.5 重啟 WMI 服務	71	6.3.3 設定 WMI 權限	197
2.4 設定防火牆	73	6.3.3.1 設定事件日誌權限	197
3. Windows 2008	75	6.3.3.2 設定讀取使用者資料權限	202
3.1 組織單位設定	75	6.3.4 設定 Event log 讀取權限	207
3.2 群組原則設定	79	6.3.5 重啟 WMI 服務	213
3.3 新增非管理帳號	86	6.4 設定防火牆	214
3.3.1 新增使用者	86	7. N-Reporter	215
3.3.2 設定 DCOM 權限	87	7.1 Windows 2003 或之前版本作業系統	216
3.3.3 設定 WMI 權限	92	7.2 Windows 2008 或之後版本作業系統	217
3.3.3.1 設定事件日誌權限	92	8. 問題排除	218
3.3.3.2 設定讀取使用者資料權限	97	8.1 WMI Query Language 檢查	218
3.3.4 設定 Event log 讀取權限	102		
3.3.5 重啟 WMI 服務	107		
3.4 設定防火牆	108		
4. Windows 2012	110		
4.1 組織單位設定	110		
4.2 群組原則設定	114		
4.3 新增非管理帳號	121		
4.3.1 新增使用者	121		
4.3.2 設定 DCOM 權限	122		
4.3.3 設定 WMI 權限	127		
4.3.3.1 設定事件日誌權限	127		

前言

本文件描述 N-Reporter 使用者如何使用 WMI 設定 Windows AD 日誌和使用者資料。

稽核原則建議：<https://docs.microsoft.com/zh-tw/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations>

註：本文件僅做為如何用 WMI 抓取日誌設定參考，建議您仍應聯繫設備或是軟體原廠尋求日誌 WMI 方式之協助。

1. Windows 2000

Windows 稽核原則設定 [詳細說明請參考前言的稽核原則建議連結](#)

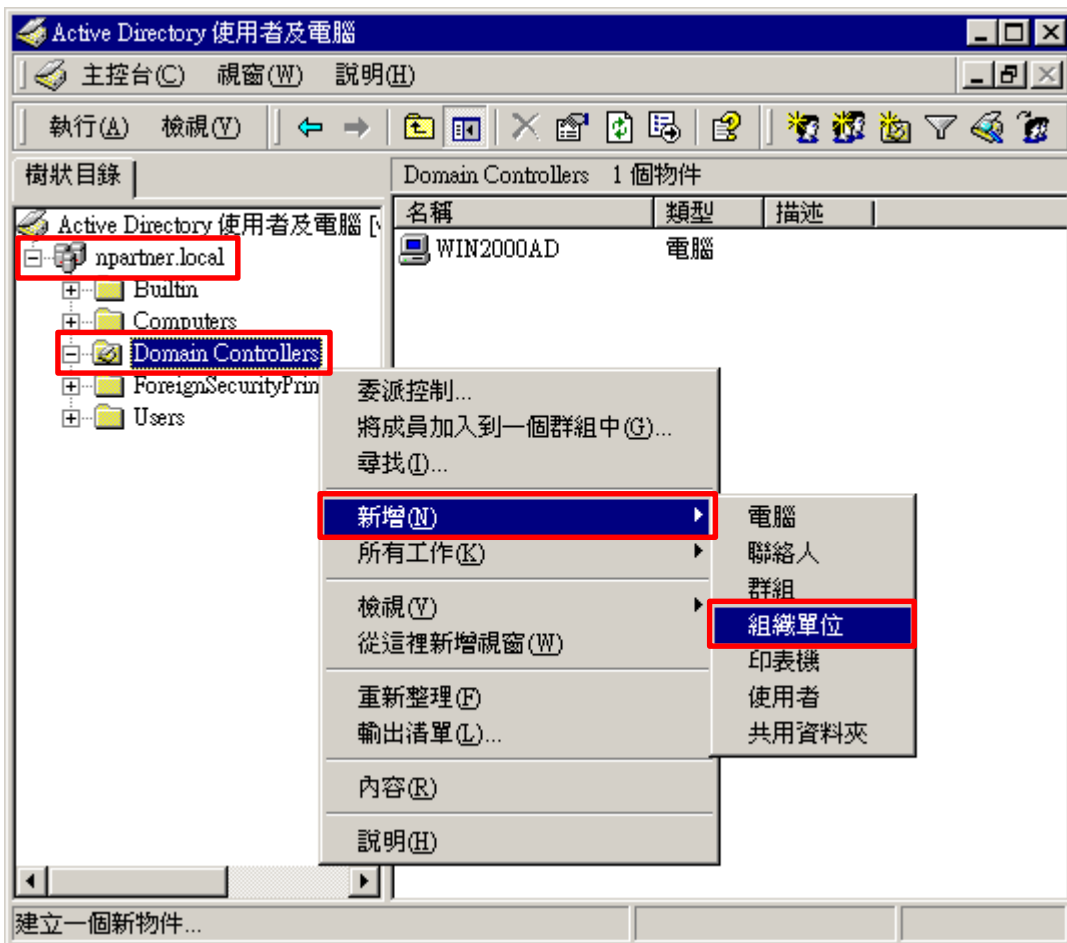
1.1 組織單位設定

(1) 開啟 [Active Directory 使用者和電腦]



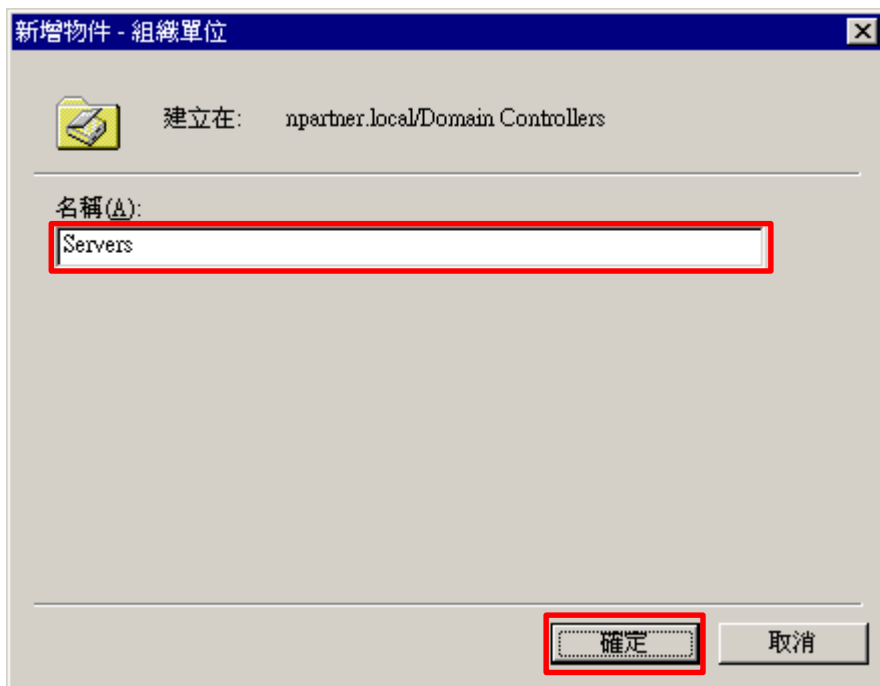
(2) 新增組織單位

[網域名稱] 的 [Domain Controllers] 組織單位，按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]



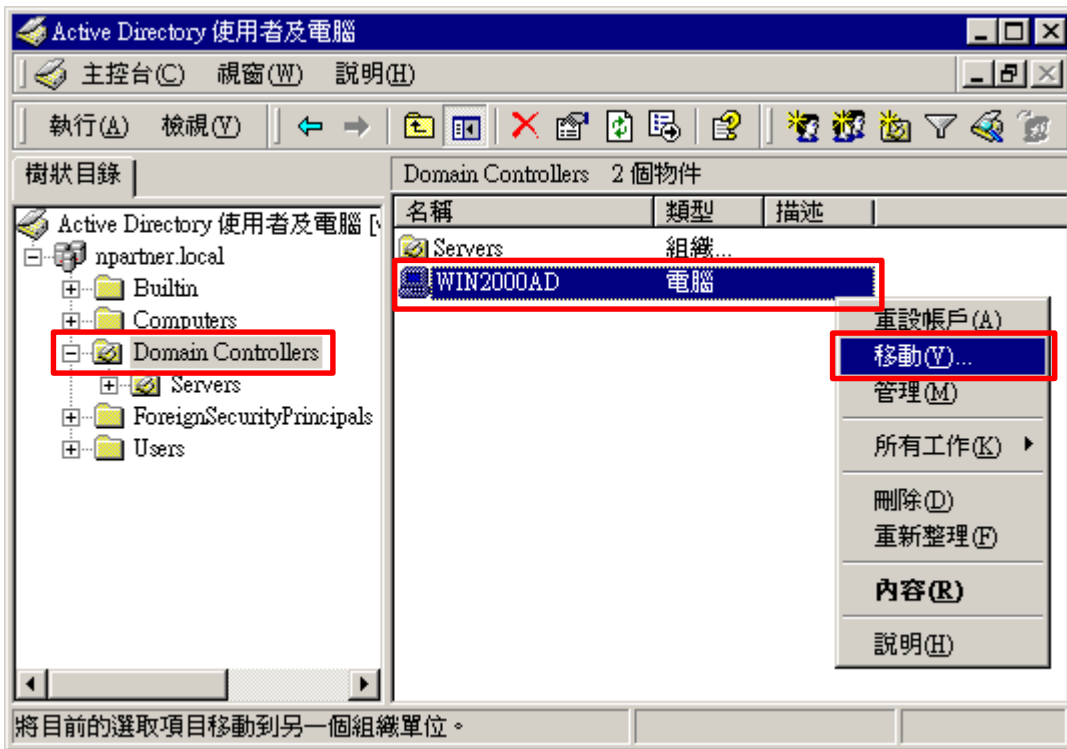
(3) 輸入組織單位名稱

輸入組織單位名稱: Servers 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



(4) 移動伺服器至新的組織單位

選擇 [Domain Controllers] 組織單位 -> 在 [Win2000AD] 伺服器，按滑鼠右鍵 註：請依客戶環境選擇 Windows AD 主機 -> 點選 [移動]



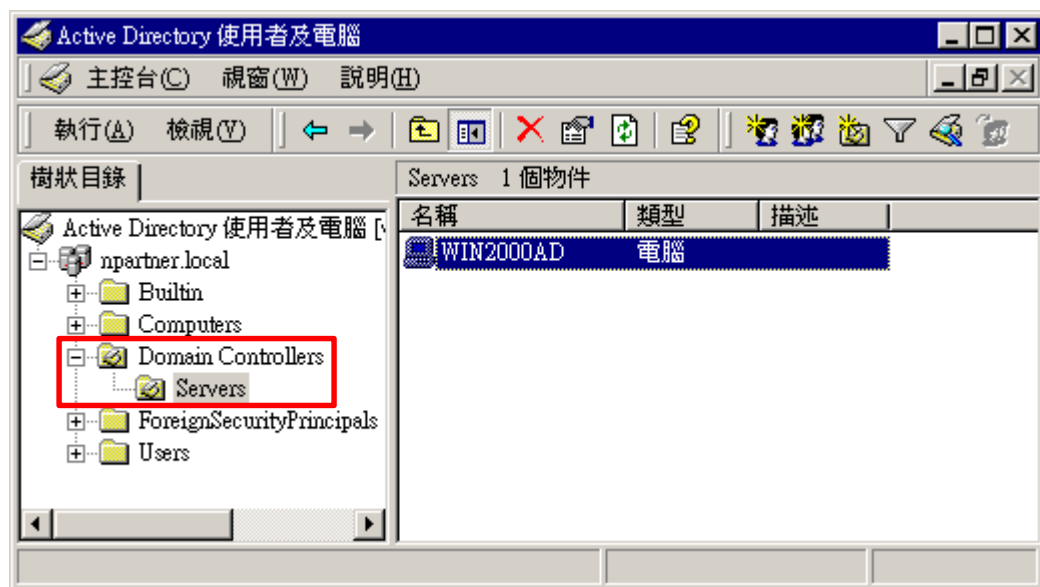
(5) 選擇組織單位

選擇 [Domain Controllers] 的 [Servers] 組織單位 -> 按 [確定]



(6) 確認伺服器已移動至新的組織單位

展開 [Domain Controllers] 的 [Servers] 組織單位，確認 [Win2003] 伺服器已移動。



1.2 群組原則設定

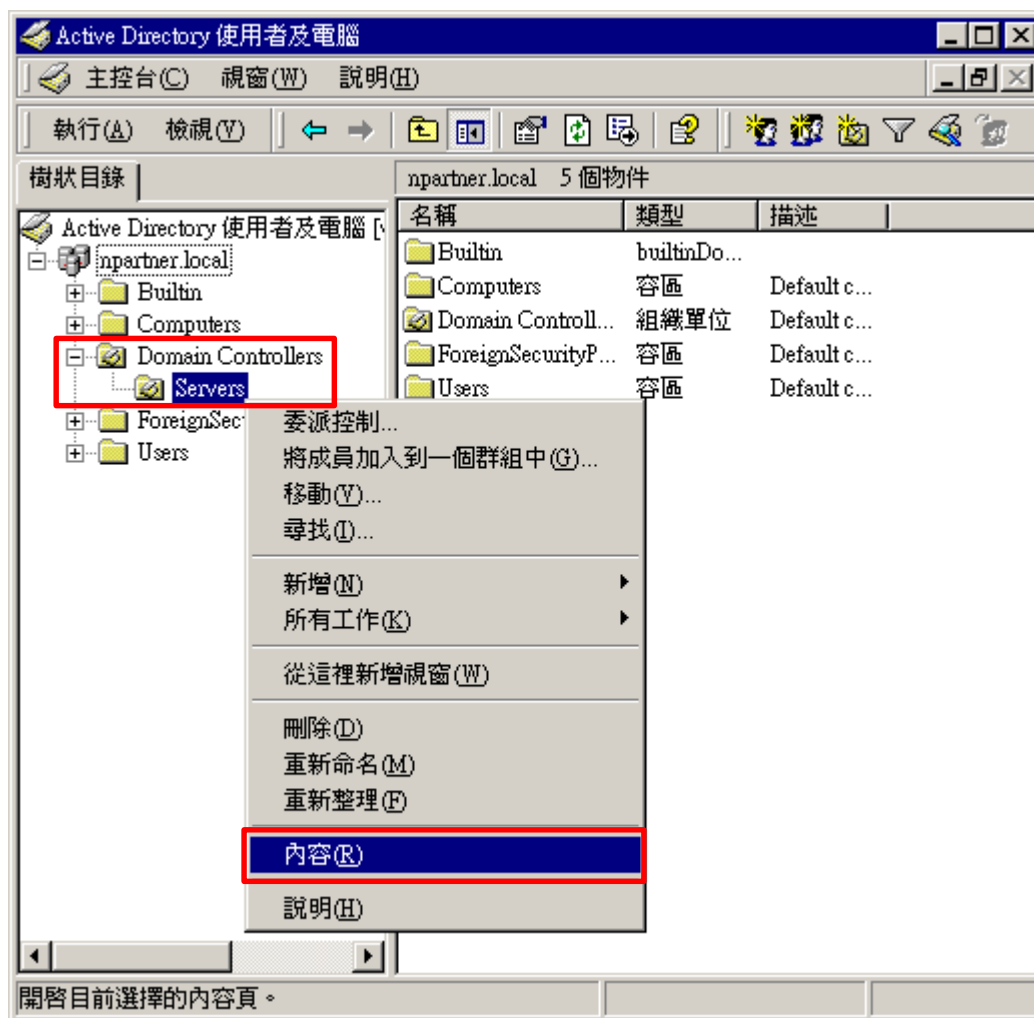
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



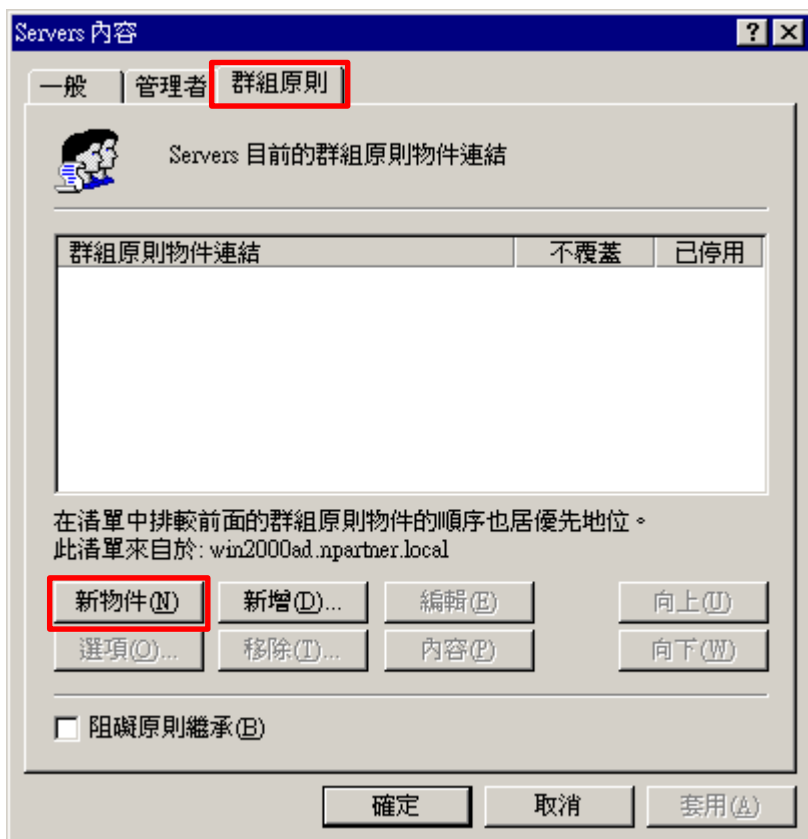
(2) Domain Controllers 的 Servers 組織單位，點選內容

選擇 [Domain Controllers] 的 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [內容]



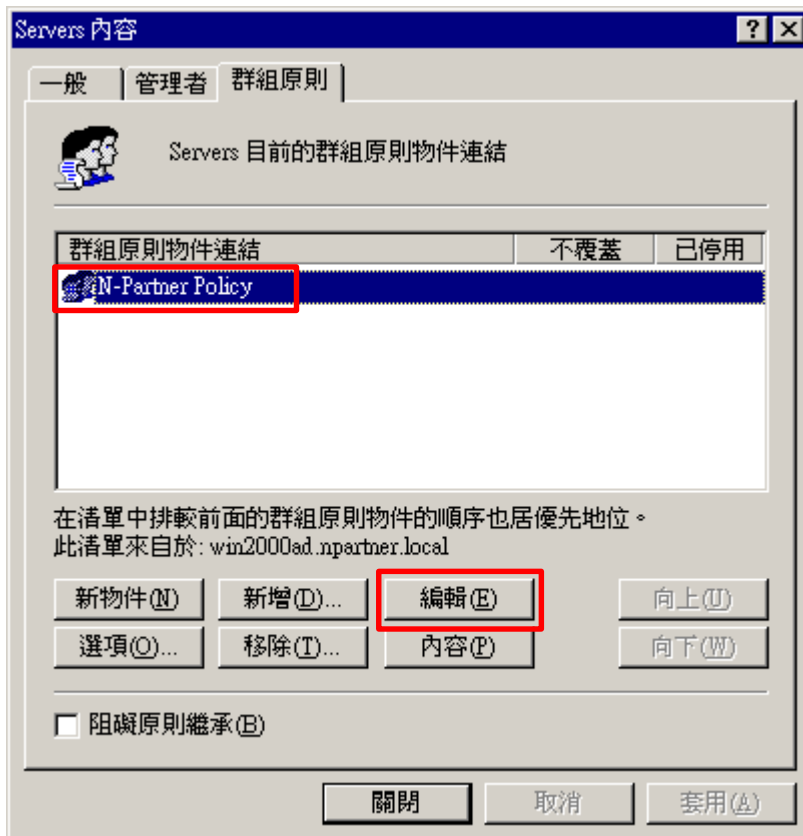
(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按 [新物件]



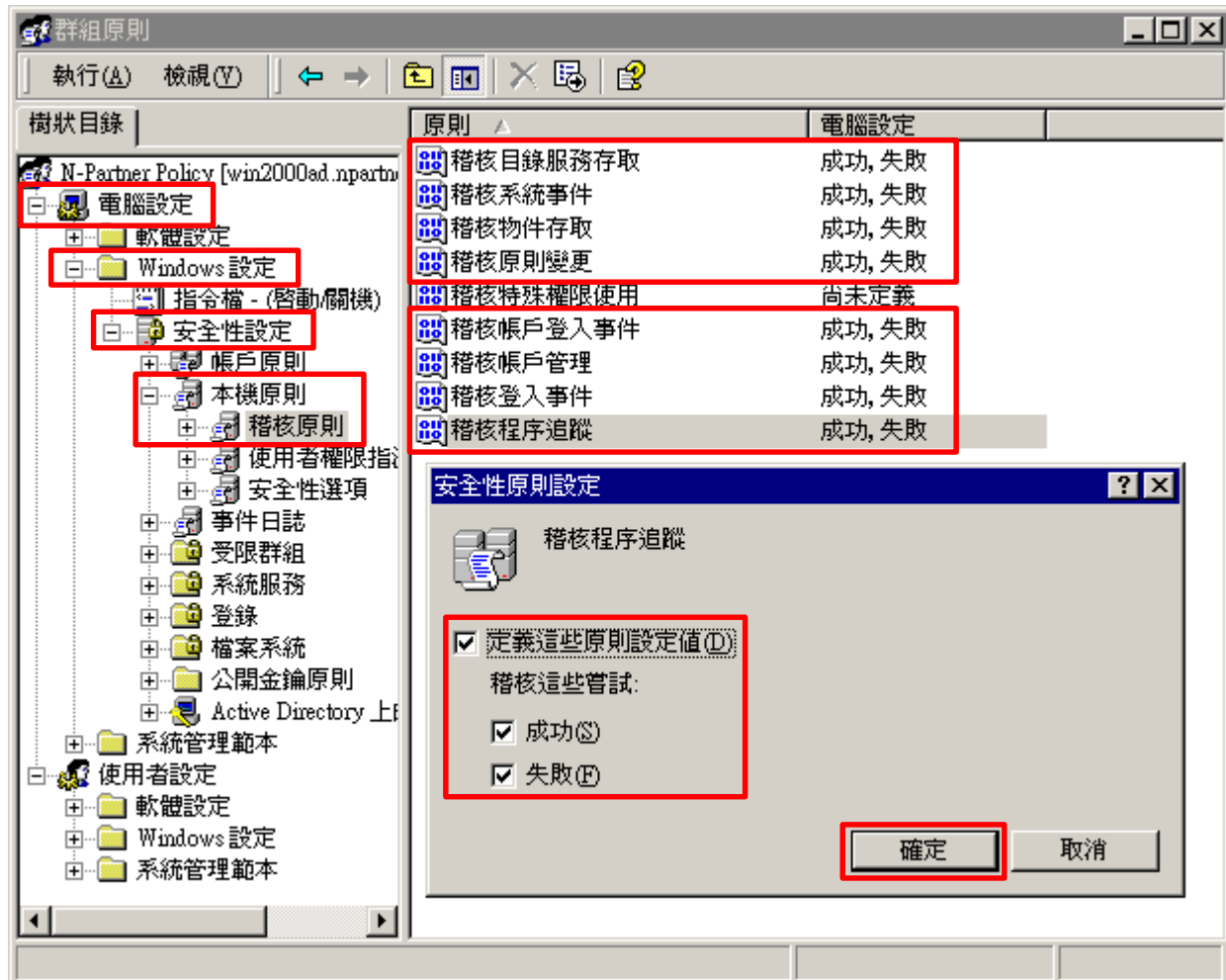
(4) 編輯群組原則物件

輸入群組原則物件名稱 **N-Partner Policy** 註：請依客戶環境建立群組物件名稱 -> 按 [編輯]



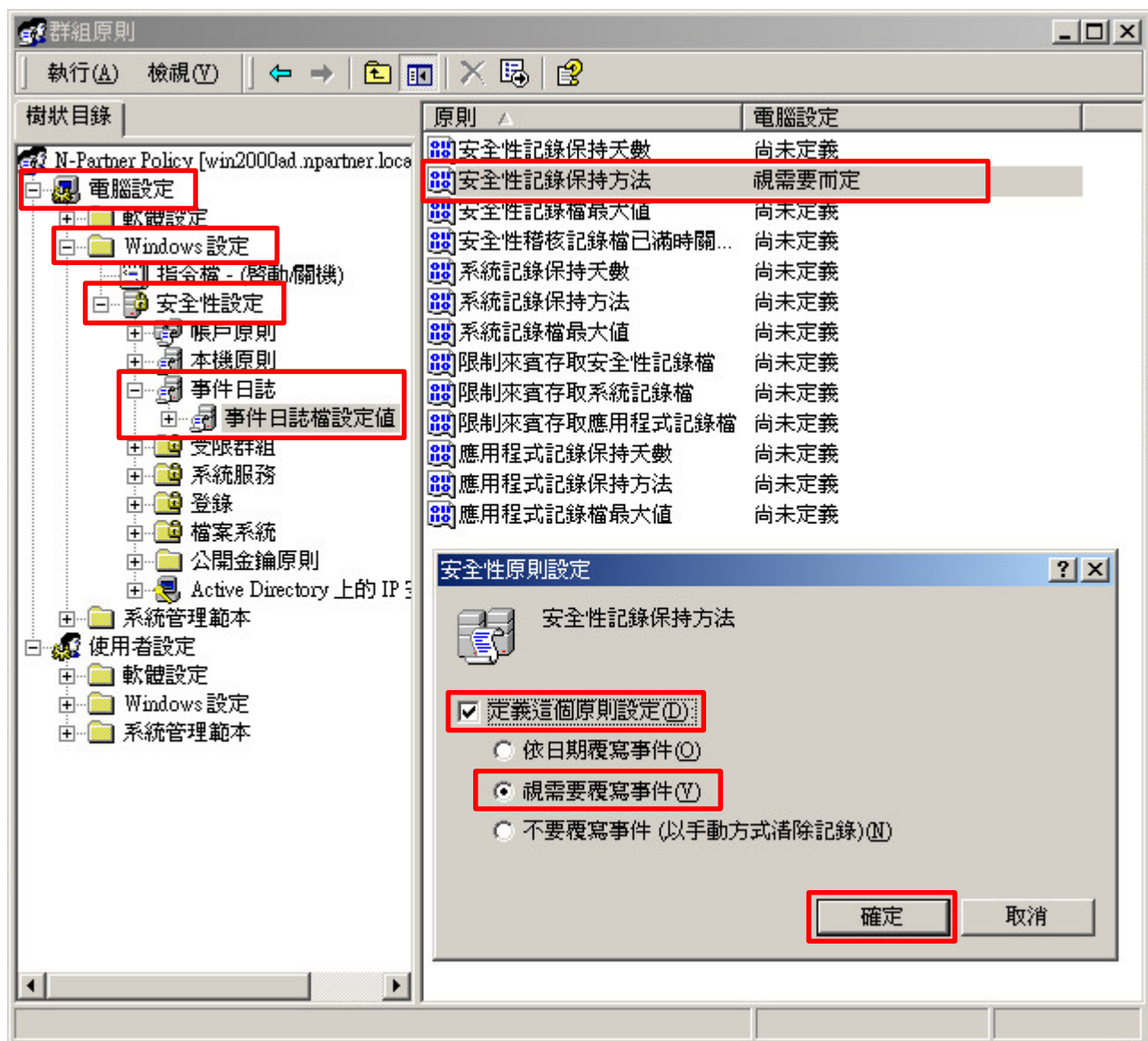
(5) 本機原則：稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核目錄服務存取], [稽核系統事件], [稽核物件存取], [稽核原則變更], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件], [稽核程序追蹤] 項目
-> 勾選 [定義這些原則設定:] & [成功] & [失敗] -> 按 [確定]



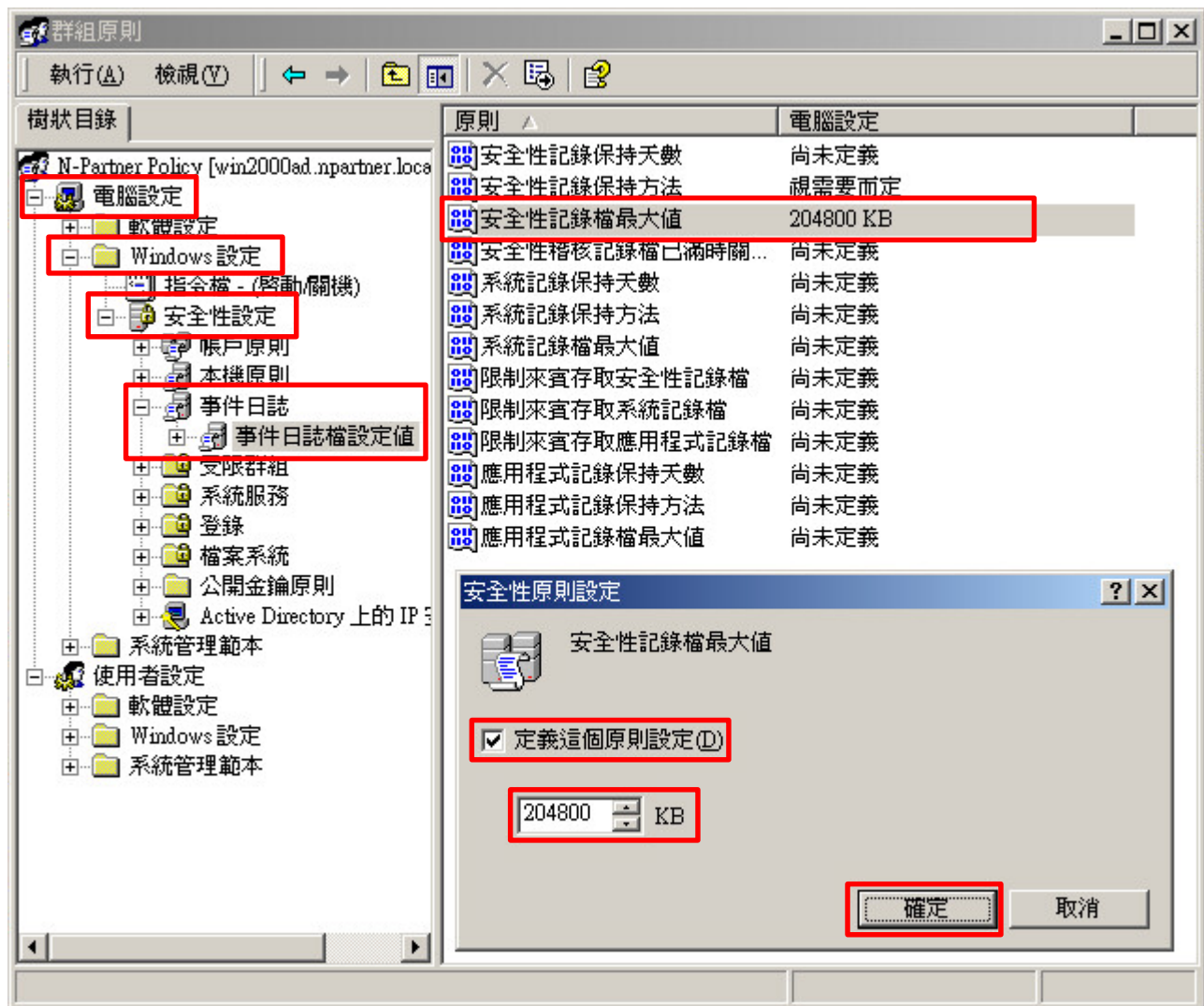
(6) 事件日誌：安全性記錄保持方法

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [事件日誌] -> [事件日誌檔設定值] -> 點選 [安全性記錄保持方法] 項目 -> 勾選 [定義這個原則設定]: -> 點選 [視需要覆寫事件] -> 按 [確定]



(7) 事件日誌：安全性記錄檔最大值

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [事件日誌] -> [事件日誌檔設定值] -> 點選 [安全性記錄檔最大值] 項目 -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]



(8) 在 Windows Server 伺服器，開啟 [命令提示字元]



(9) 更新群組原則。

```
C:\> secdit /refreshpolicy machine_policy /enforce
```




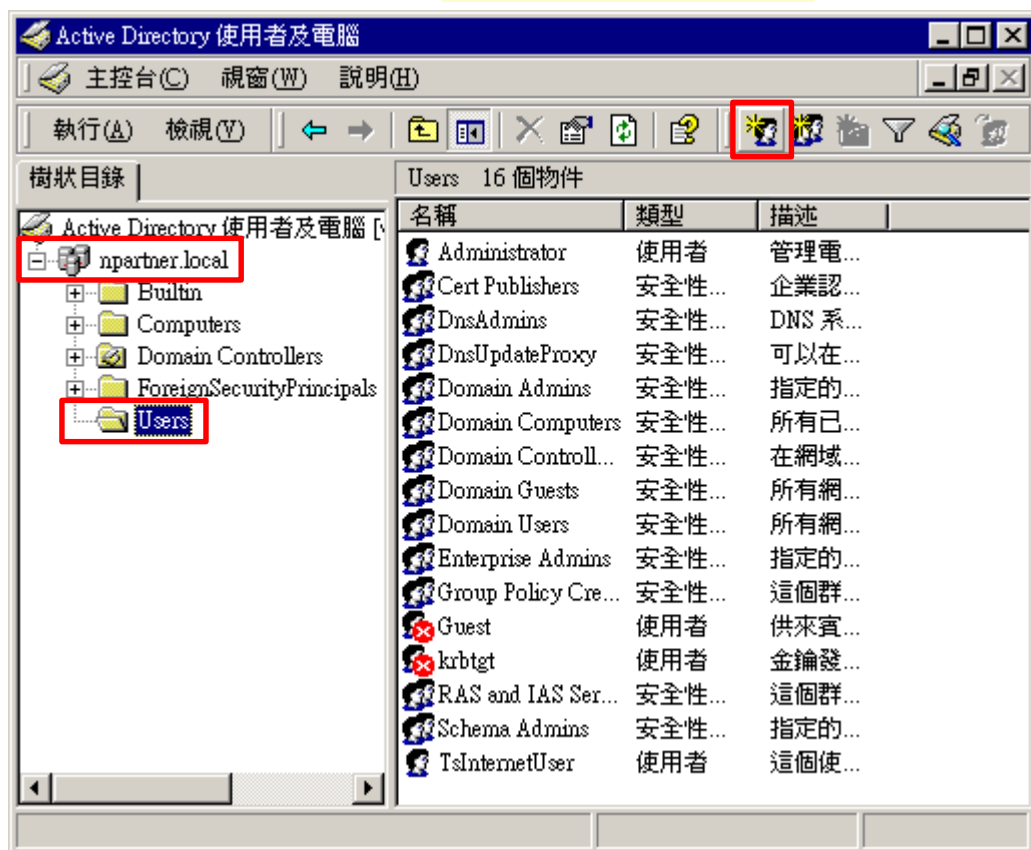
1.3 新增非管理帳號

1.3.1 新增使用者

(1) 開啟 [Active Directory 使用者及電腦]



(2) [網域名稱] 的 [Users] 組織單位 註：請依客戶環境選擇組織單位 -> 按  [建立新使用者]



(3) 輸入 全名, 使用者登入名稱 -> 按 [下一步]



新增物件 - 使用者

建立在: npartner.local/Users

姓氏(L):

名字(F): 英文縮寫(I):

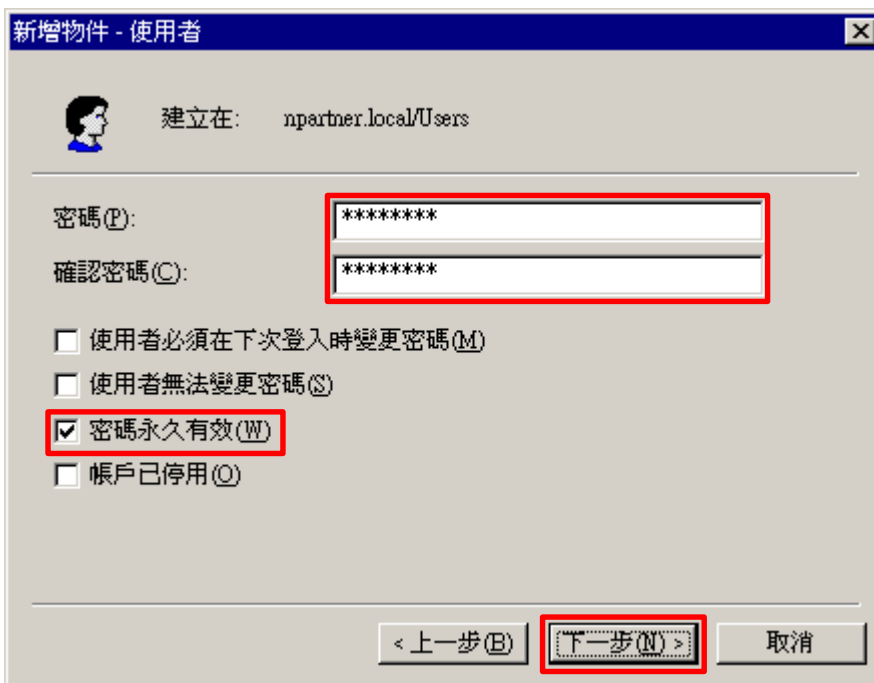
全名(A): npartner

使用者登入名稱(U): npartner @npartner.local

使用者登入名稱 (Windows 2000 前版)(W): NPARTNER\ npartner

< 上一步(B) 下一步(N) > 取消

(4) 輸入 密碼, 確認密碼 -> 勾選 [密碼永久有效] -> 按 [下一步]



新增物件 - 使用者

建立在: npartner.local/Users

密碼(P): *****

確認密碼(C): *****

使用者必須在下次登入時變更密碼(M)

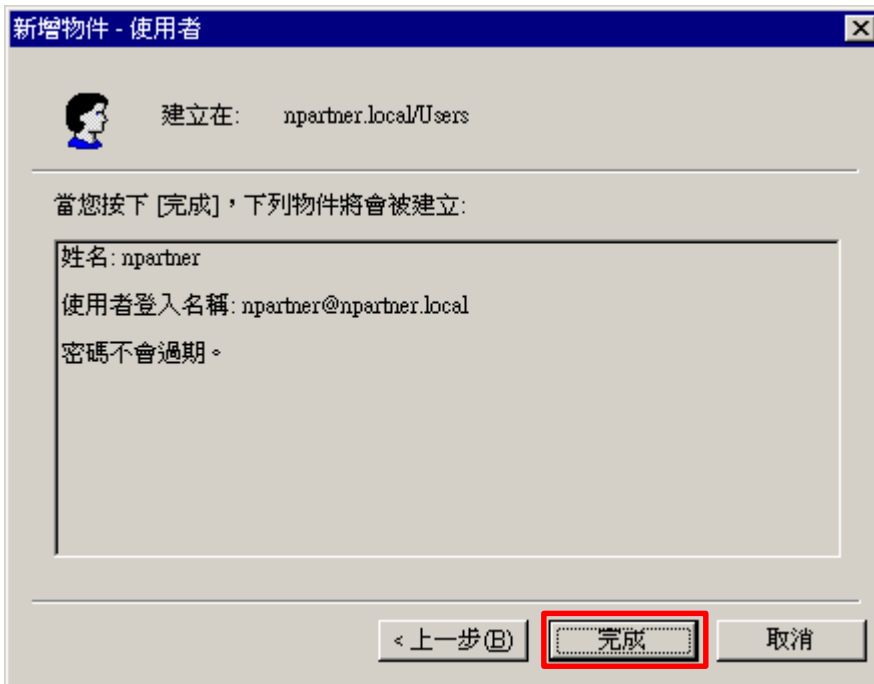
使用者無法變更密碼(S)

密碼永久有效(W)

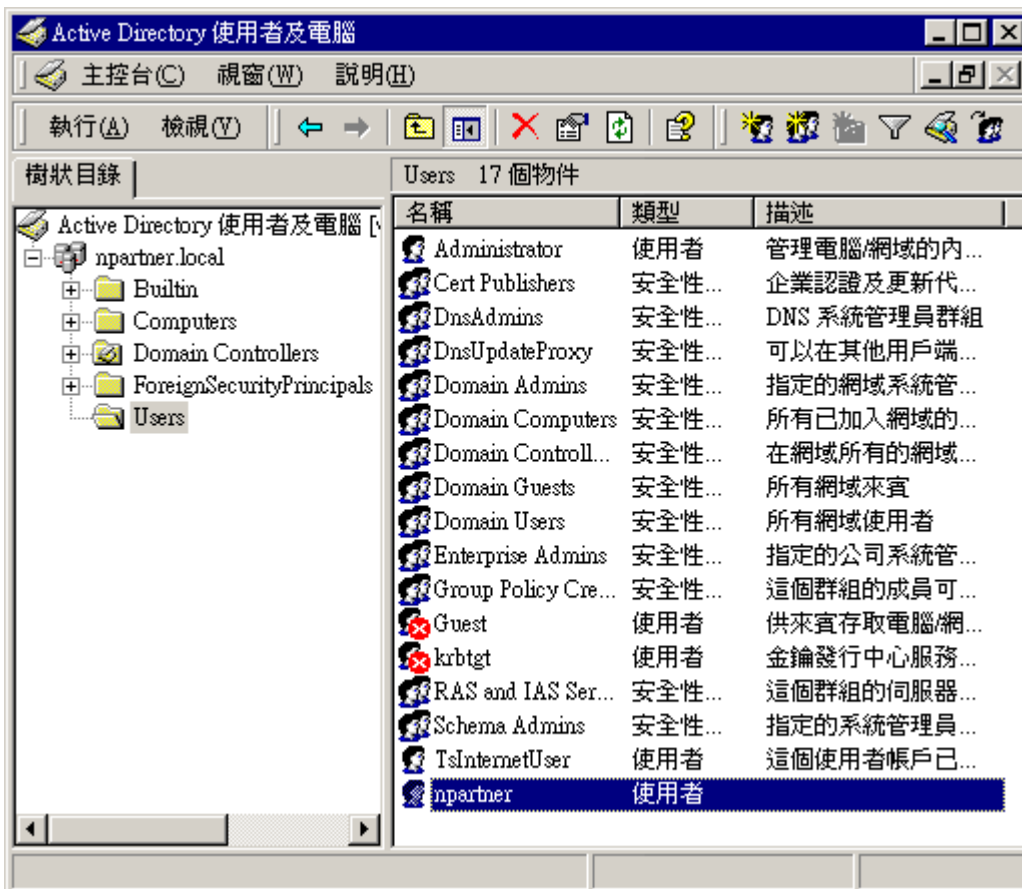
帳戶已停用(O)

< 上一步(B) 下一步(N) > 取消

(5) 按 [完成]

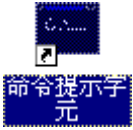


(6) 顯示帳號情形



1.3.2 設定 DCOM 權限

(1) 開啟 [命令提示字元]



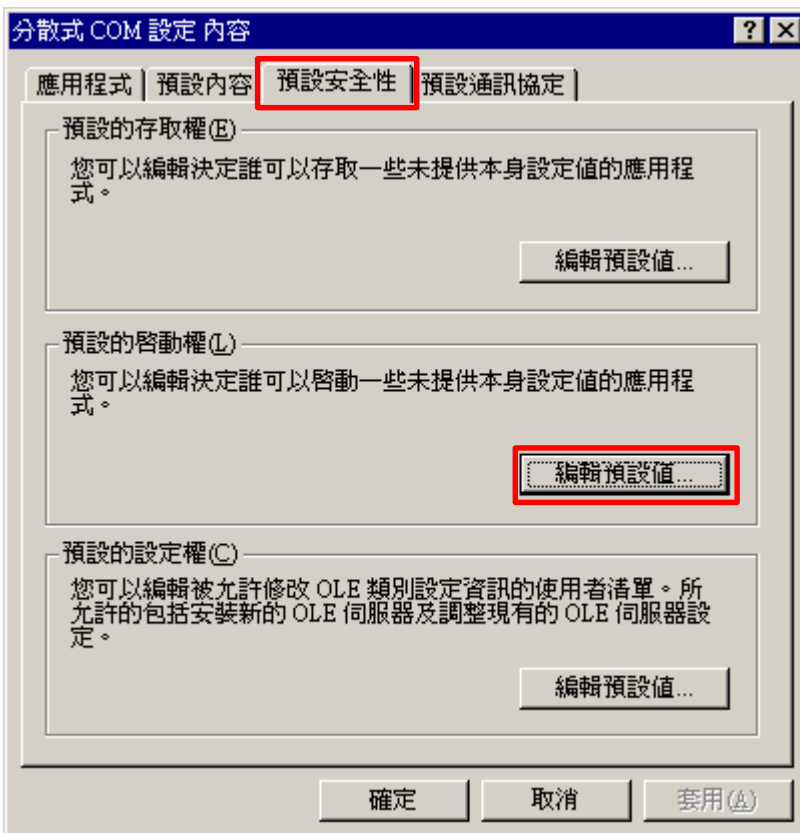
(2) 開啟元件服務

C:\> dcomcnfg.exe



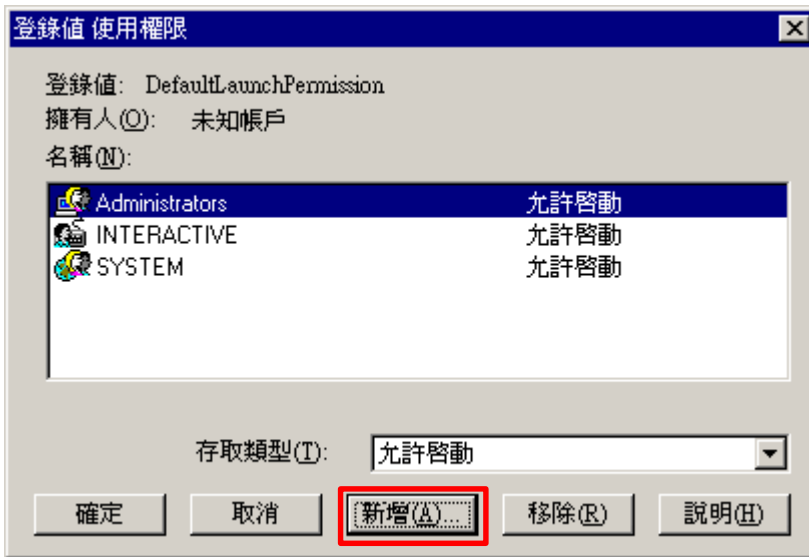
(3) 啟用權限

點選 [預設安全性] 頁面 -> 預設的啟動權 · 按 [編輯預設值]



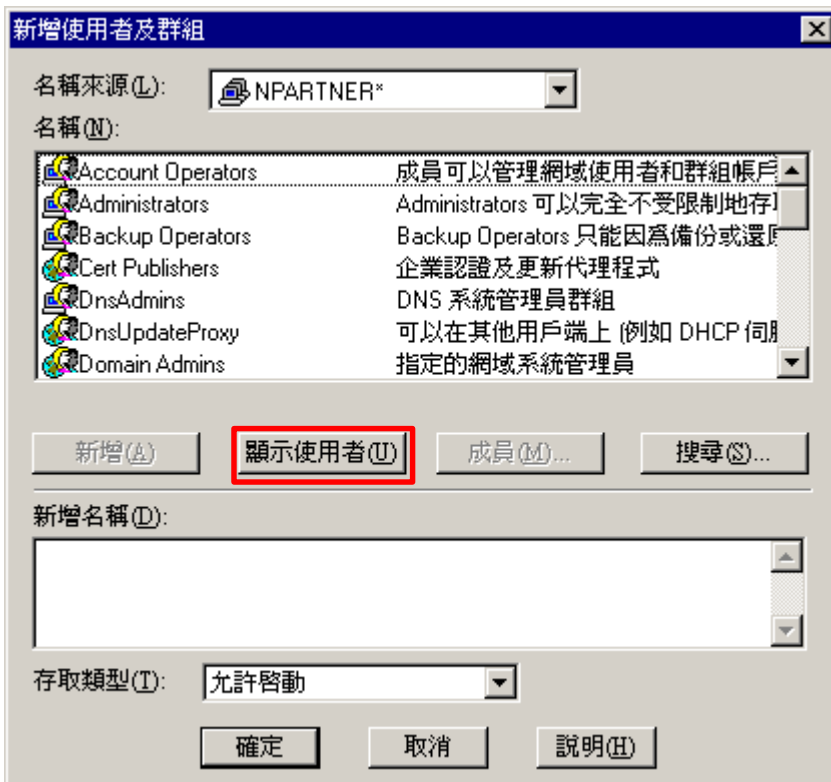
(4) 新增使用者權限

點選 [新增...]



(5) 顯示使用者

按 [顯示使用者]

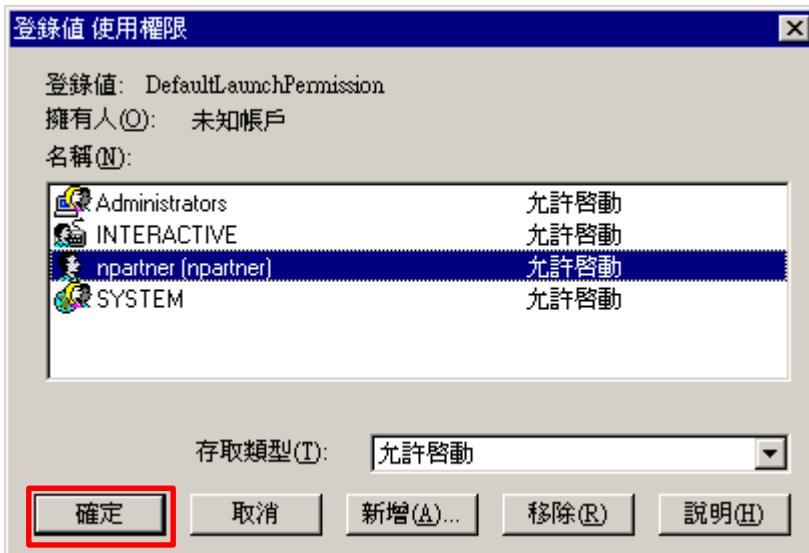


(6) 輸入使用者

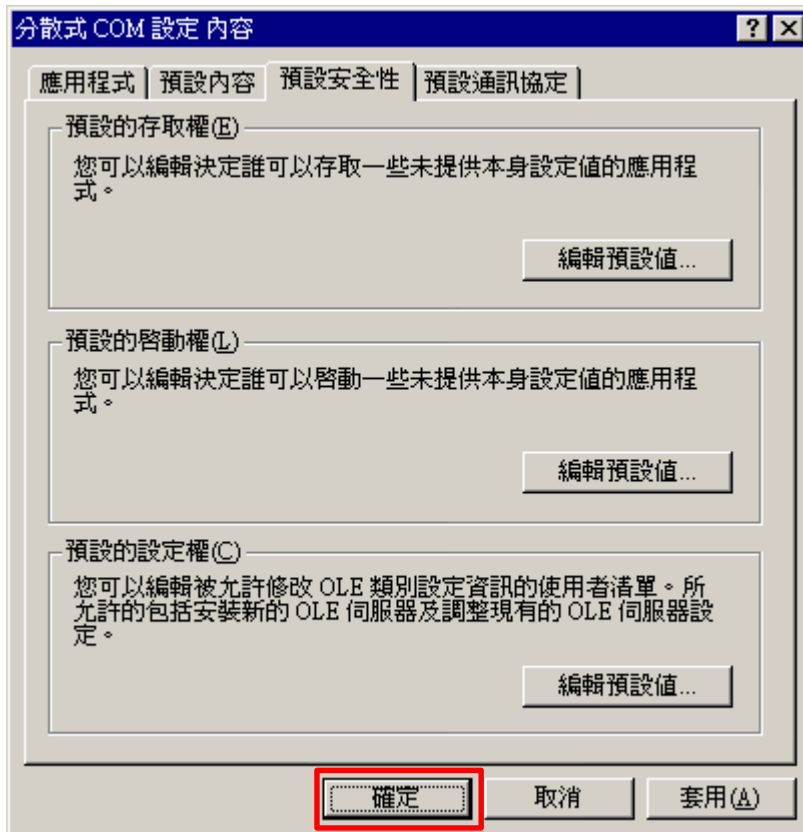
點選使用者帳號 本例 npartner -> 按 [新增] -> 存取類型: 點選 [允許啟動] -> 按 [確定]



(7) 按 [確定]



(8) 按 [確定]



1.3.3 設定 WMI 權限

1.3.3.1 設定事件日誌權限

(1) 開啟 [命令提示字元]



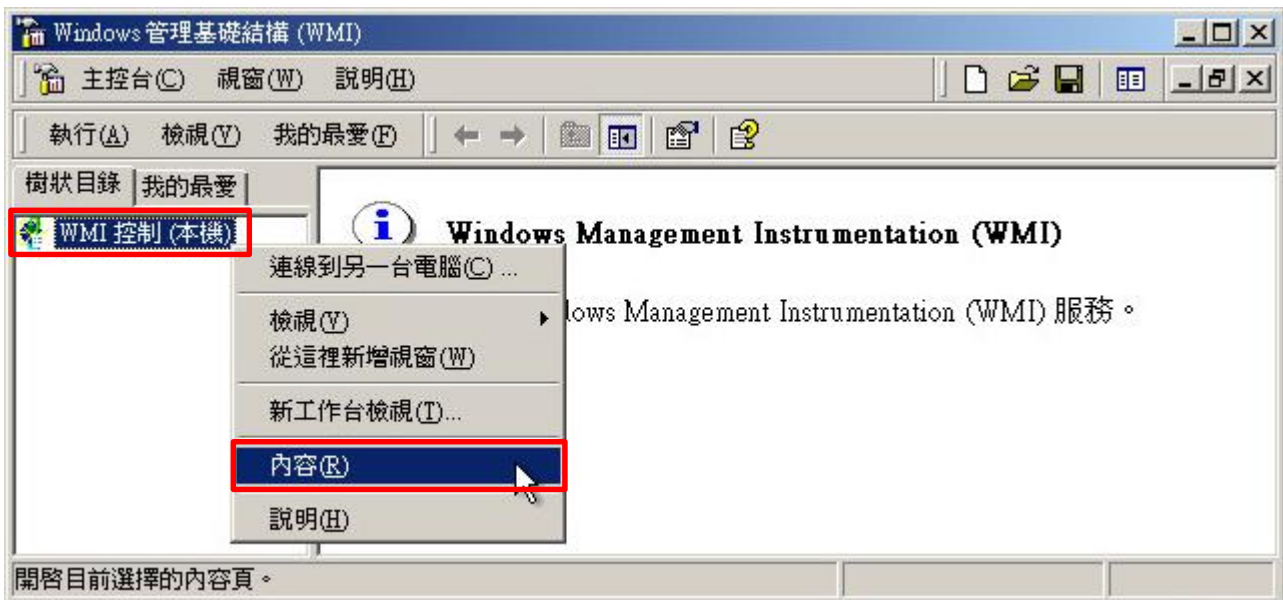
(2) 開啟 WMI 控制

C:\> wimgmt.msc



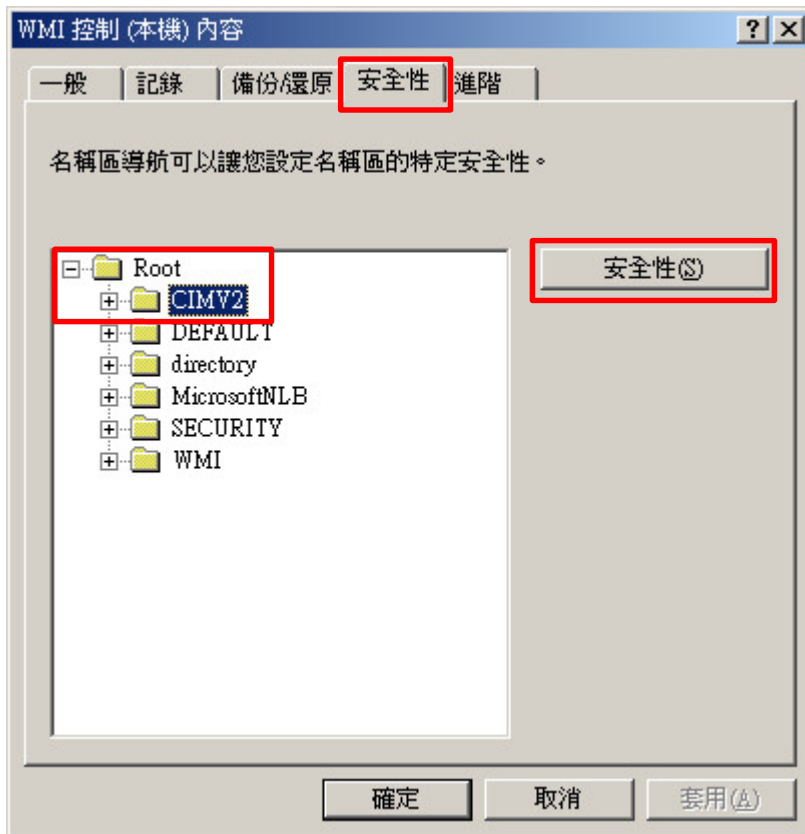
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



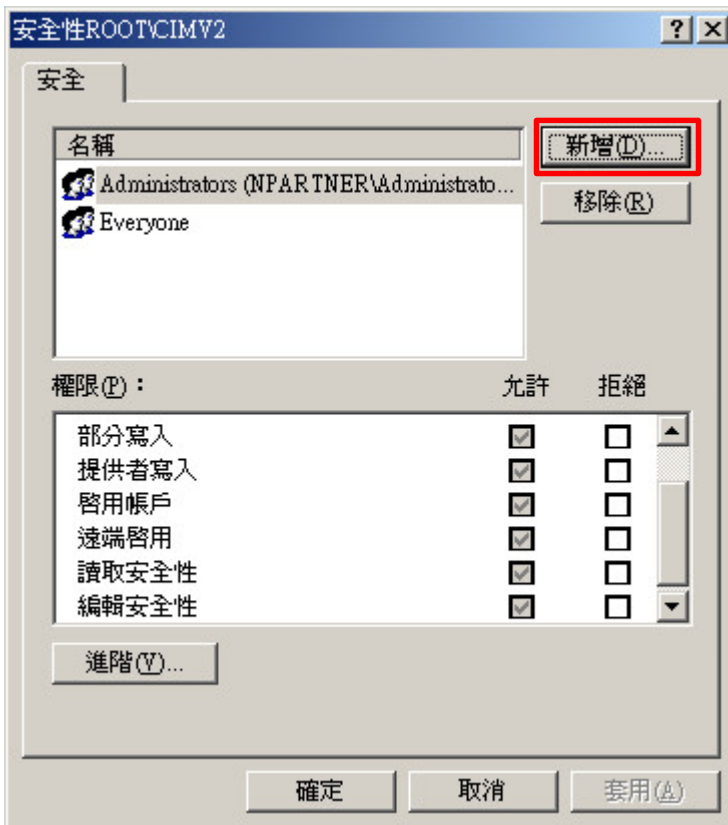
(4) 編輯 CIMV2 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [CIMV2] -> 按 [安全性]



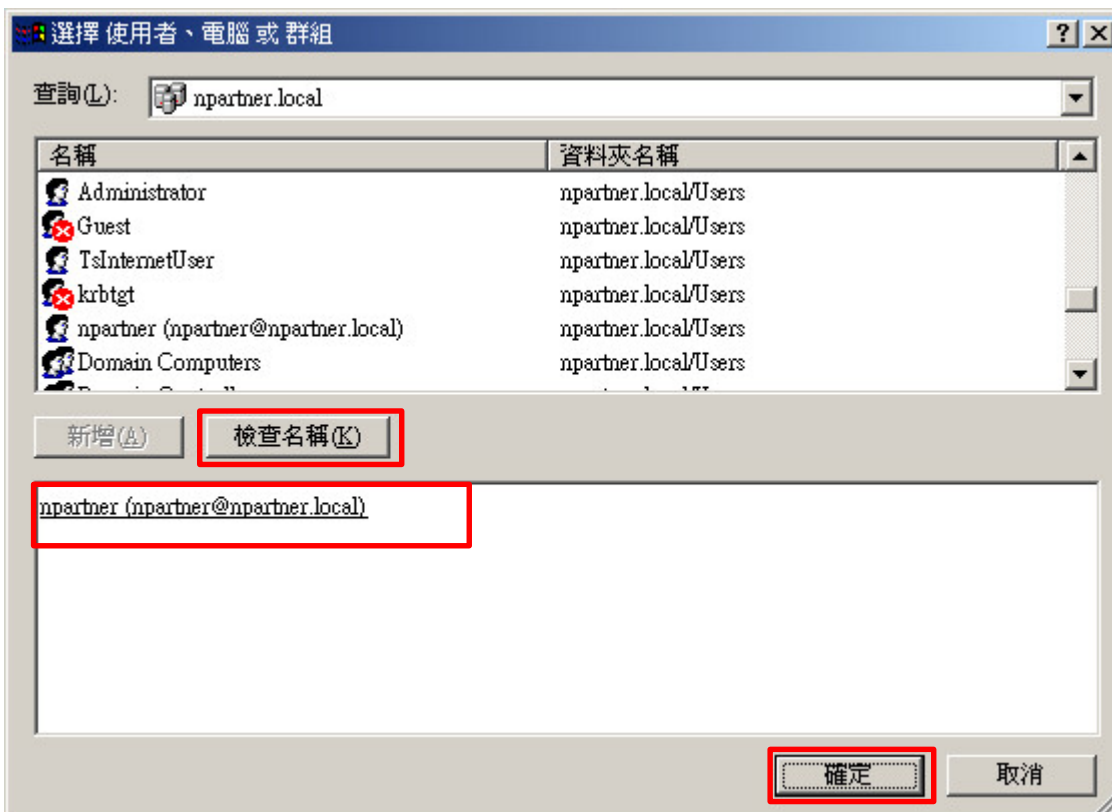
(5) 新增 WMI 使用者權限

按 [新增]



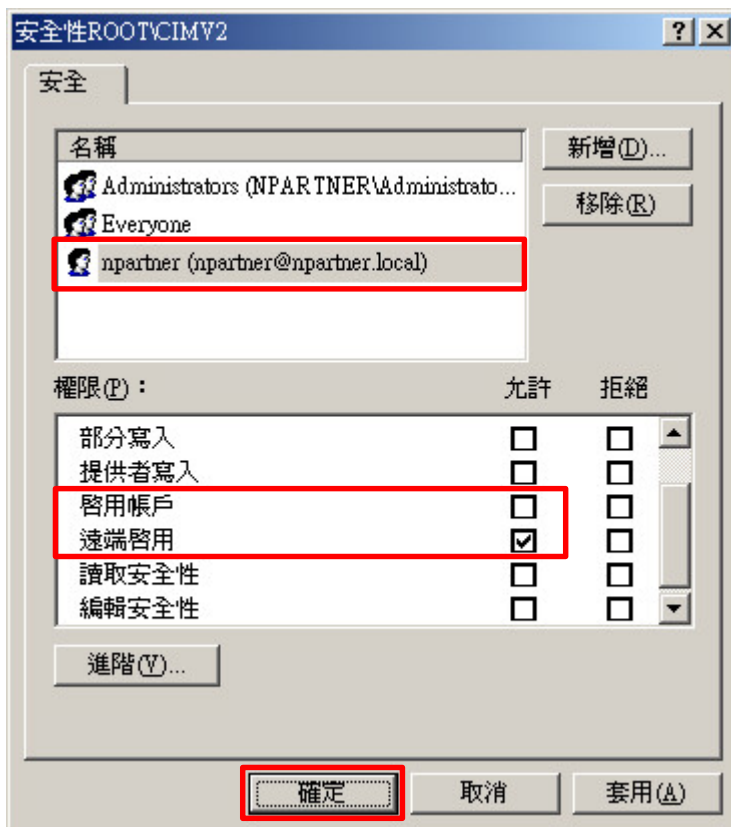
(6) 輸入使用者

輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

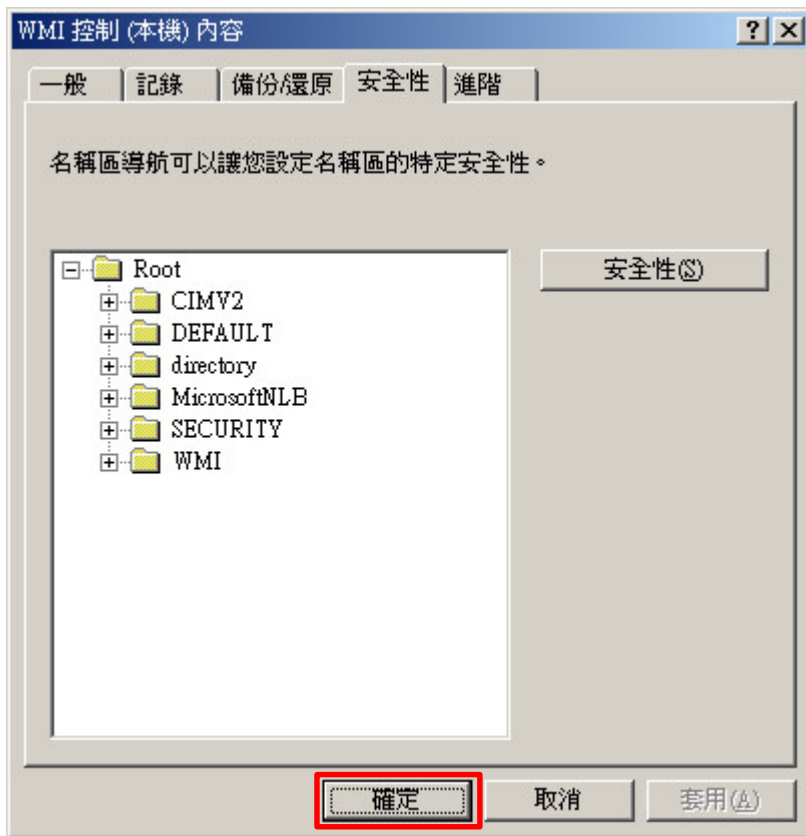


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



1.3.3.2 設定讀取使用者資料權限

(1) 開啟 [命令提示字元]



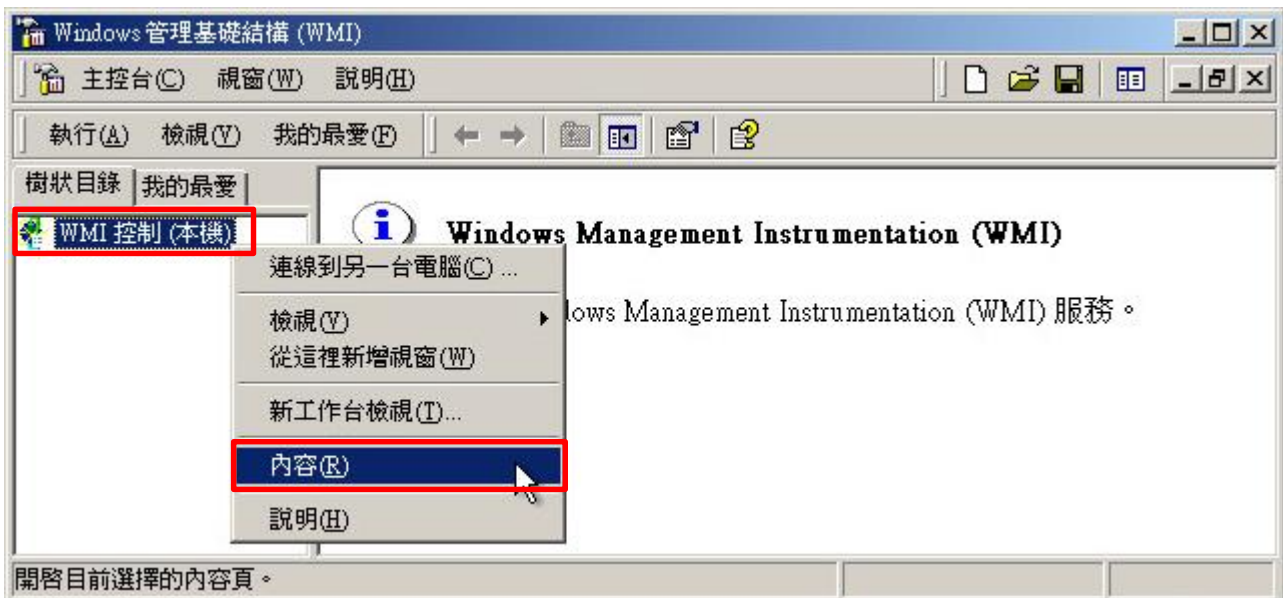
(2) 開啟 WMI 控制

C:\> wimgmt.msc



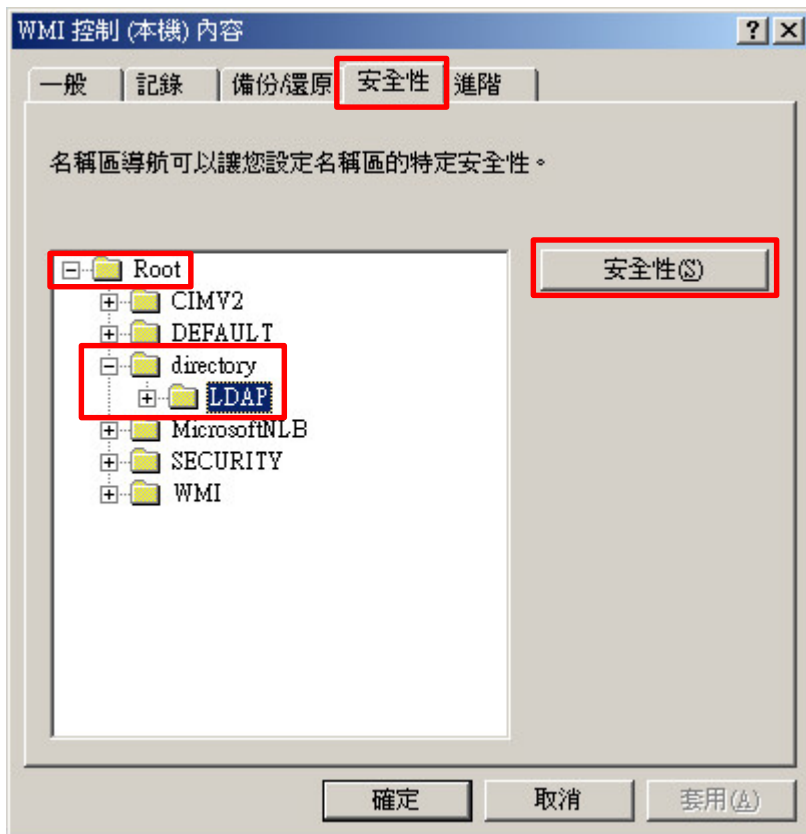
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



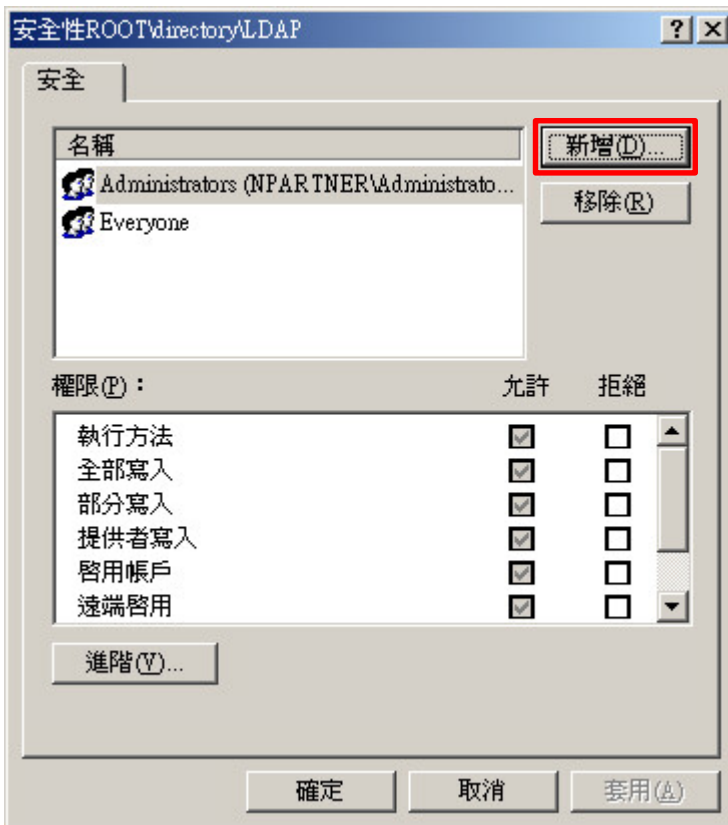
(4) 編輯 LDAP 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [directory] -> [LDAP] -> 按 [安全性]



(5) 新增 WMI 使用者權限

按 [新增]



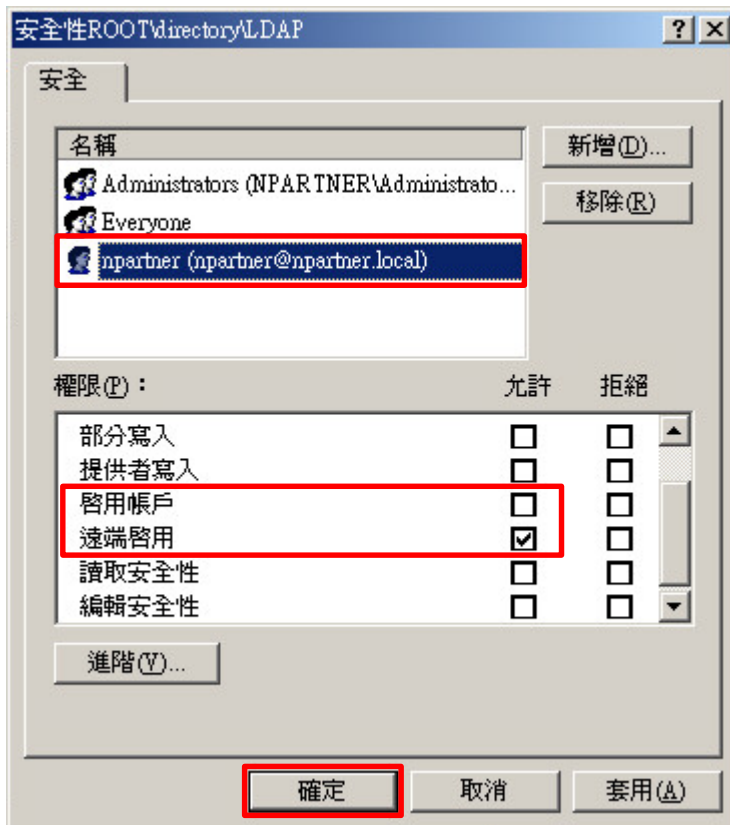
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

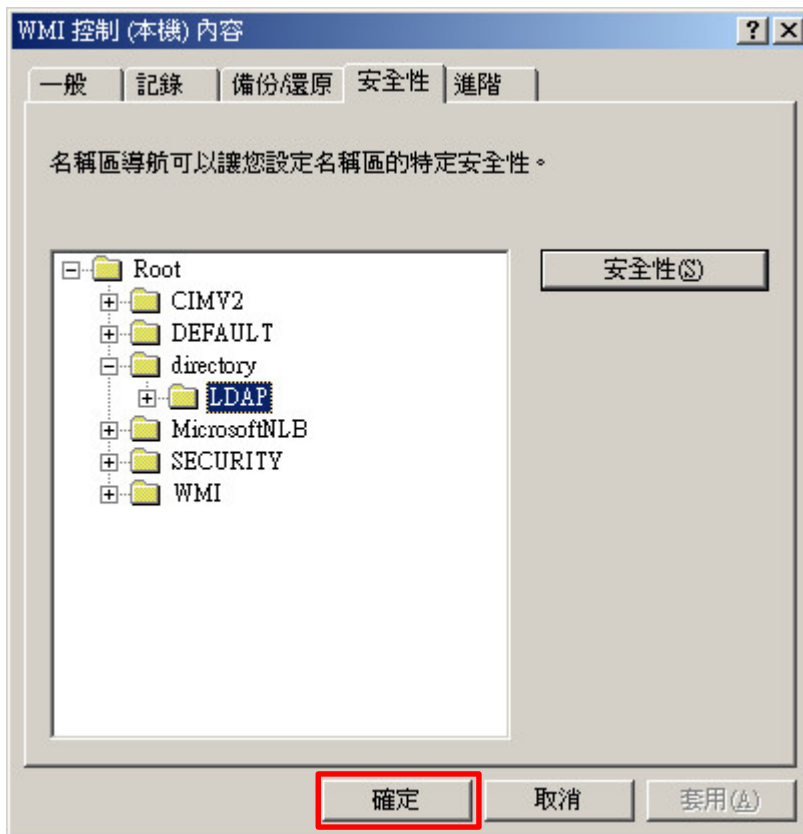


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



1.3.4 設定 Event log 讀取權限

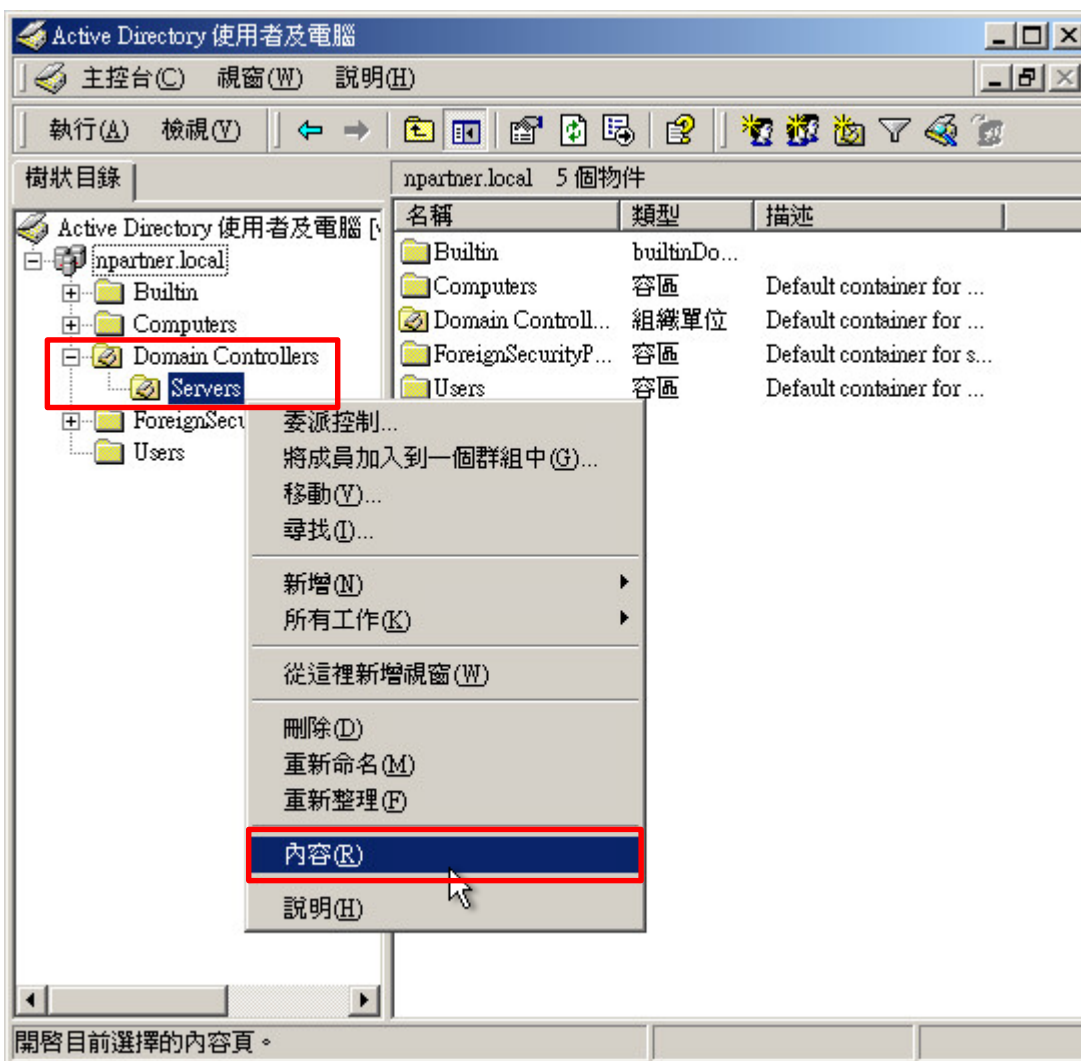
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



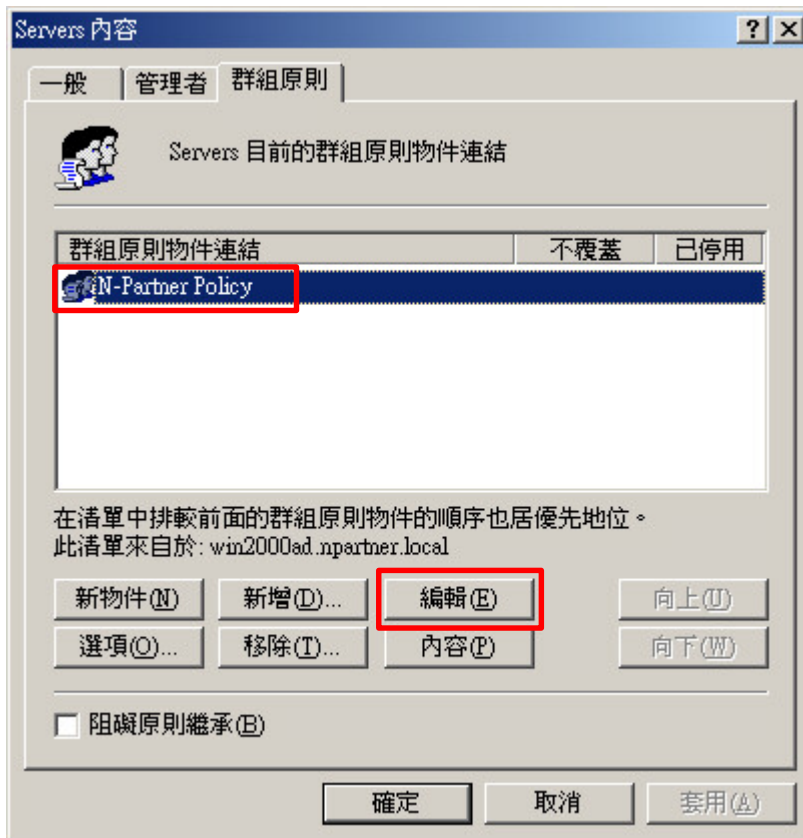
(2) Domain Controllers 的 Servers 組織單位，點選內容

選擇 [Domain Controllers] 的 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [內容]



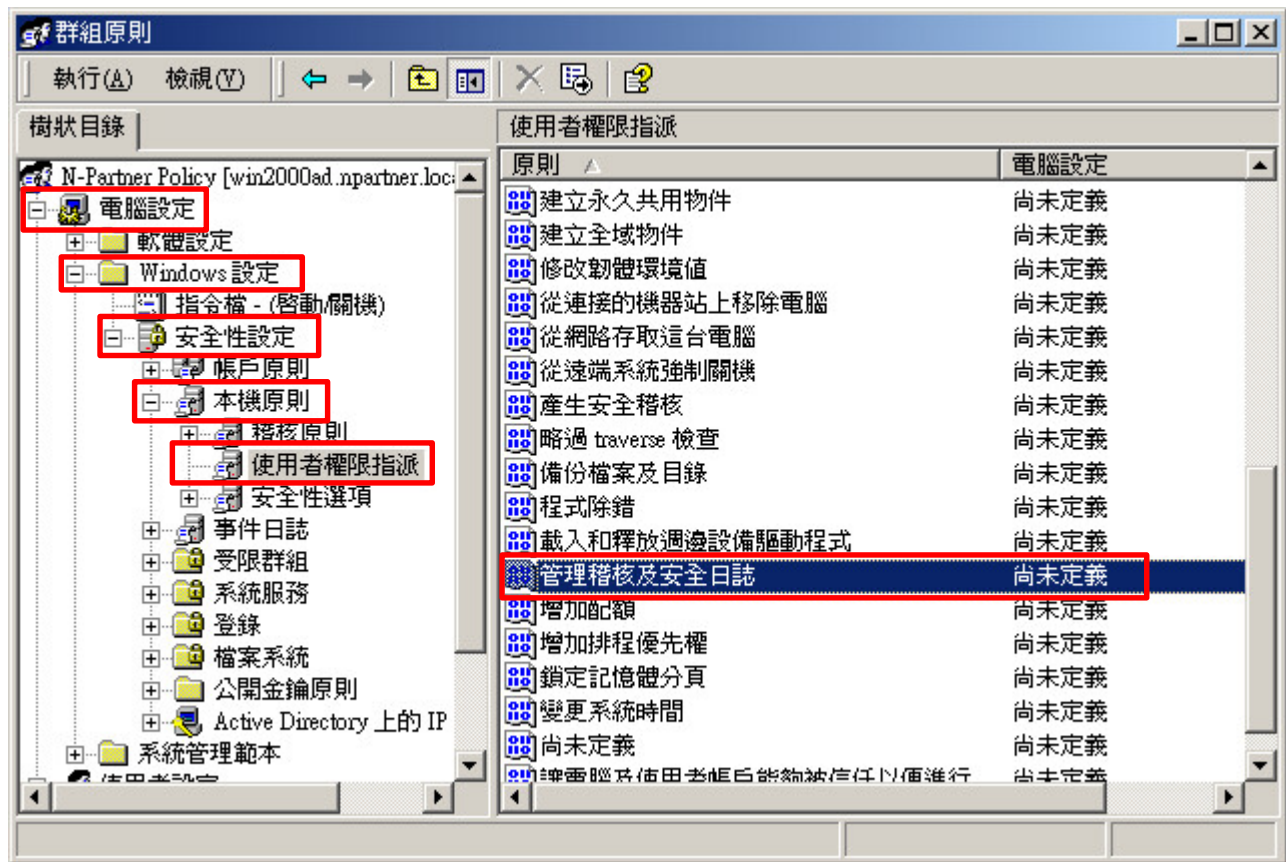
(3) 編輯群組原則物件

點選群組原則物件名稱 [N-Partner Policy] -> 按 [編輯]



(4) 設定記錄檔

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [使用者權限指派] -> 點選 [管理稽核及安全性記錄檔] 項目



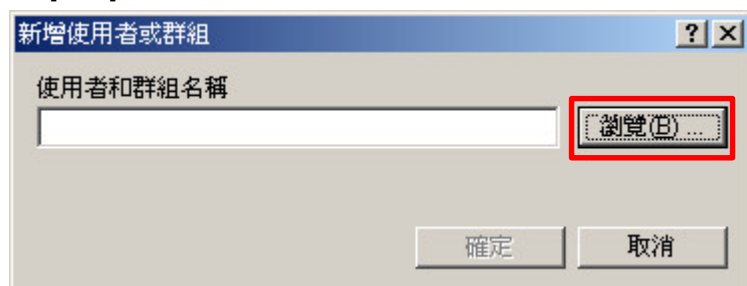
(5) 新增管理稽核使用者

勾選 [定義這些原則設定值(D)] -> 按 [新增...]



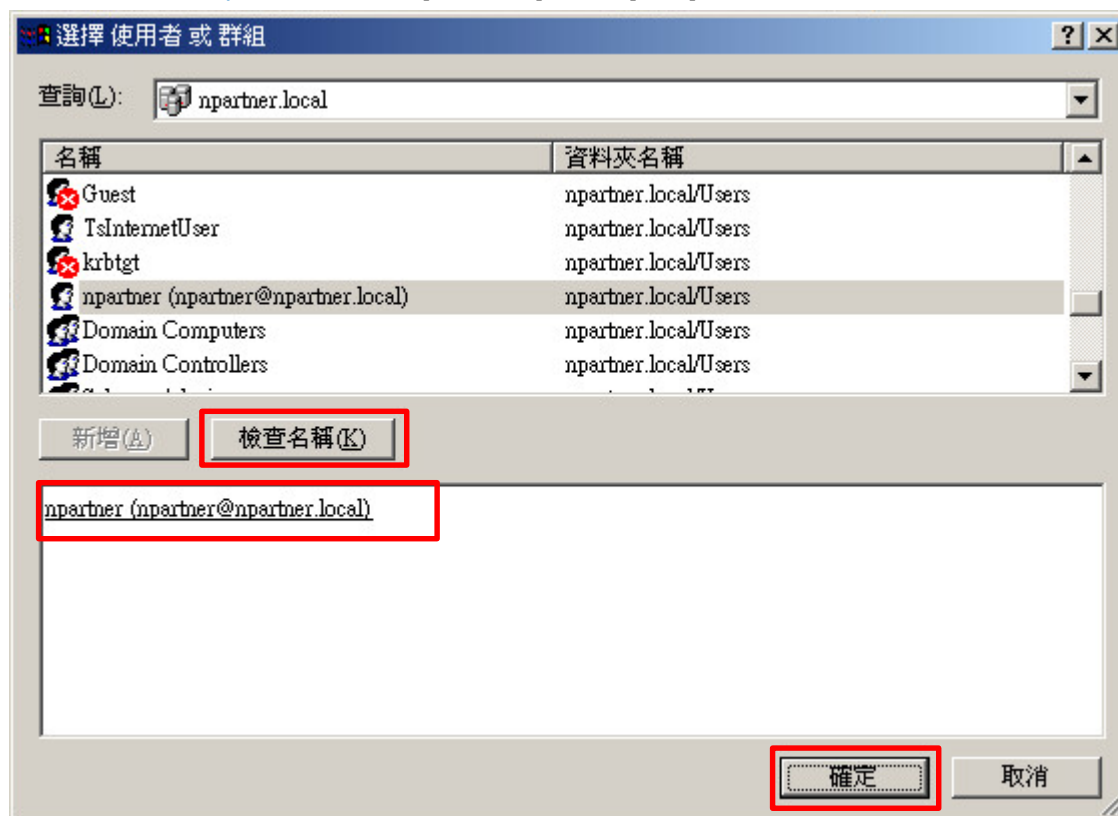
(6) 搜尋使用者

按 [瀏覽]



(7) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]



(8) 確定使用者

按 [確定]



(9) 確定設定記錄檔

按 [確定]



(10) 開啟 [命令提示字元]



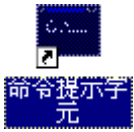
(11) 更新群組原則

C:\> secedit /refreshpolicy machine_policy /enforce



1.3.5 重啟 WMI 服務

(1) 開啟 [Windows PowerShell]



(2) 停用 WMI 服務

C:\> net stop winmgmt



(3) 啟用 WMI 服務

C:\> net start winmgmt



2. Windows 2003

Windows 稽核原則設定 [詳細說明請參考前言的稽核原則建議連結](#)

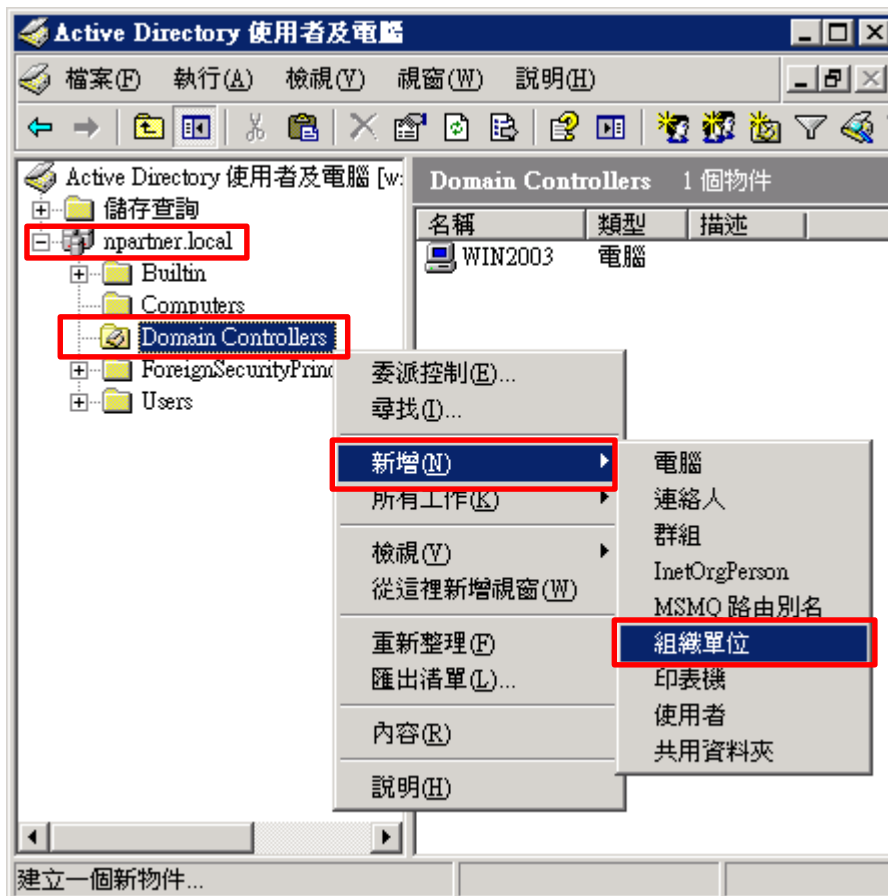
2.1 組織單位設定

(1) 開啟 [Active Directory 使用者和電腦]



(2) 新增組織單位

[網域名稱] 的 [Domain Controllers] 組織單位，按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]



(3) 輸入組織單位名稱

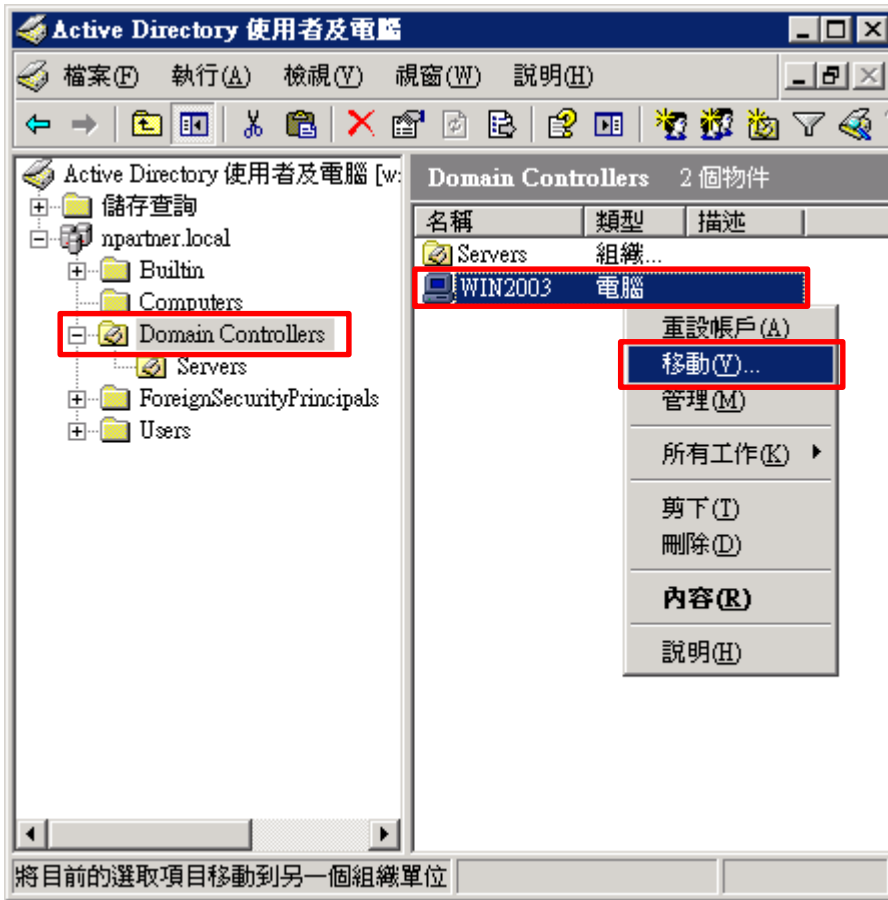
輸入組織單位名稱: Servers 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



(4) 移動伺服器至新的組織單位

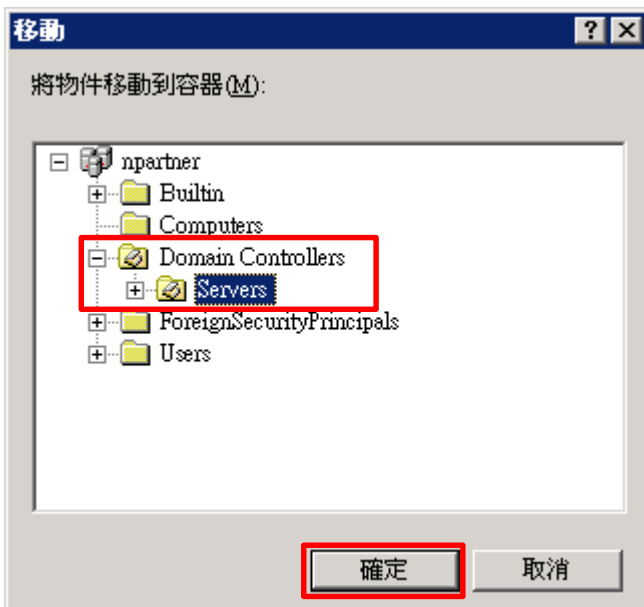
選擇 [Domain Controllers] 組織單位 -> 在 [Win2003] 伺服器，按滑鼠右鍵
主機 -> 點選 [移動]

註：請依客戶環境選擇 Windows AD



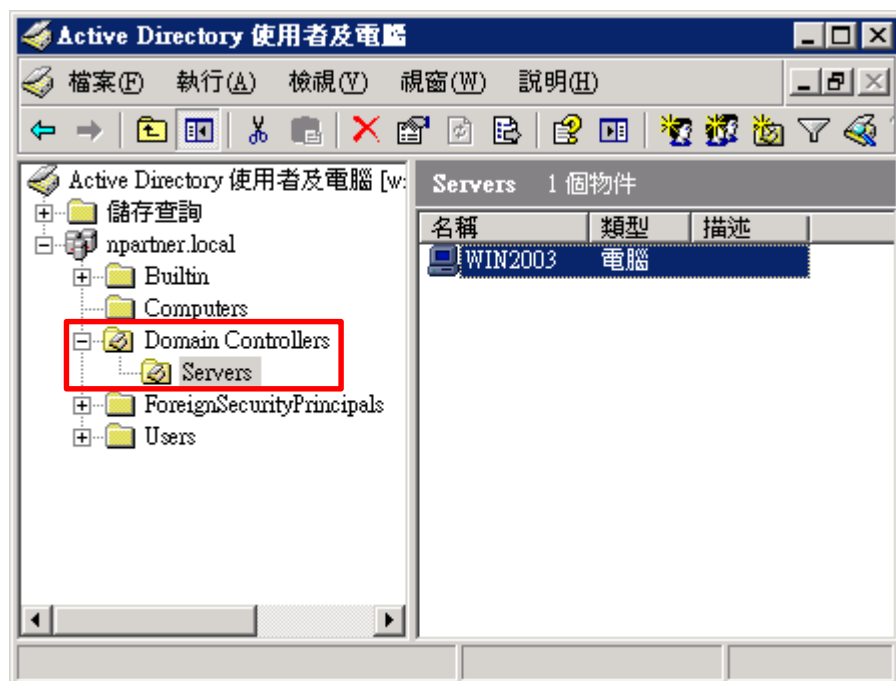
(5) 選擇組織單位

選擇 [Domain Controllers] 的 [Servers] 組織單位 -> 按 [確定]



(6) 確認伺服器已移動至新的組織單位

展開 [Domain Controllers] 的 [Servers] 組織單位，確認 [Win2003] 伺服器已移動。



2.2 群組原則設定

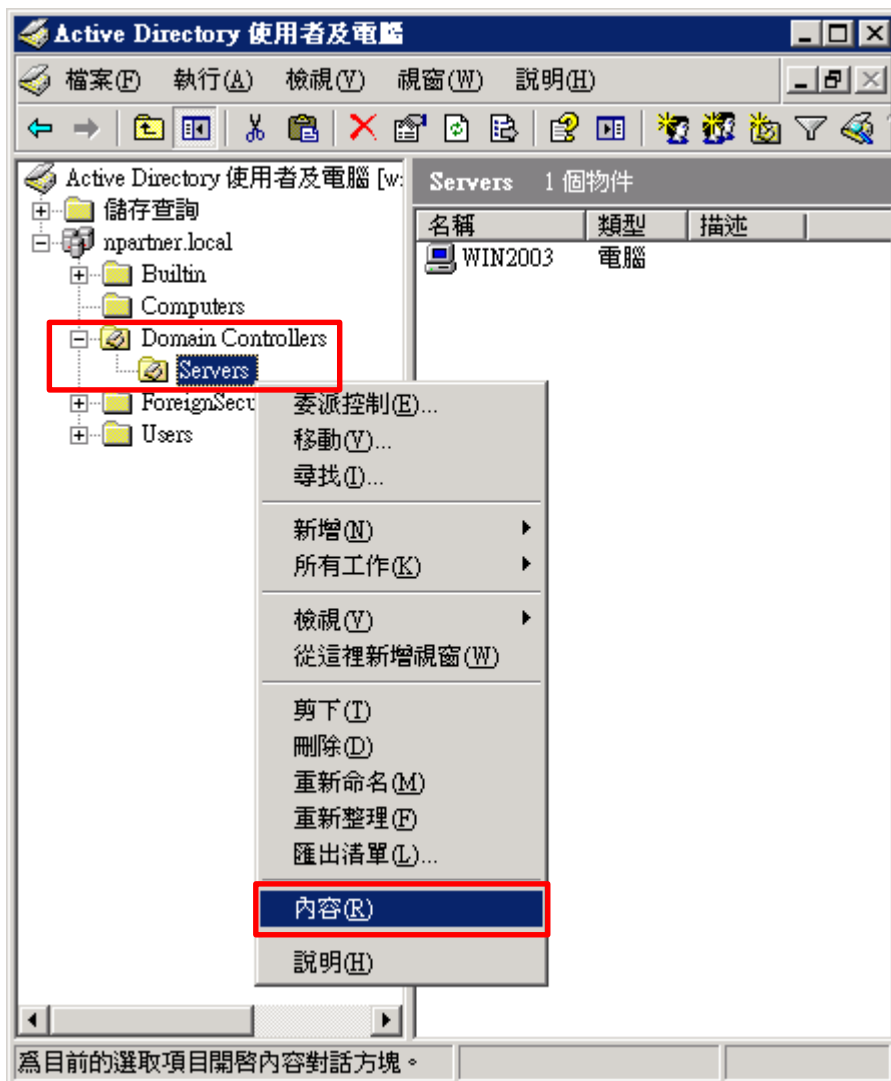
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



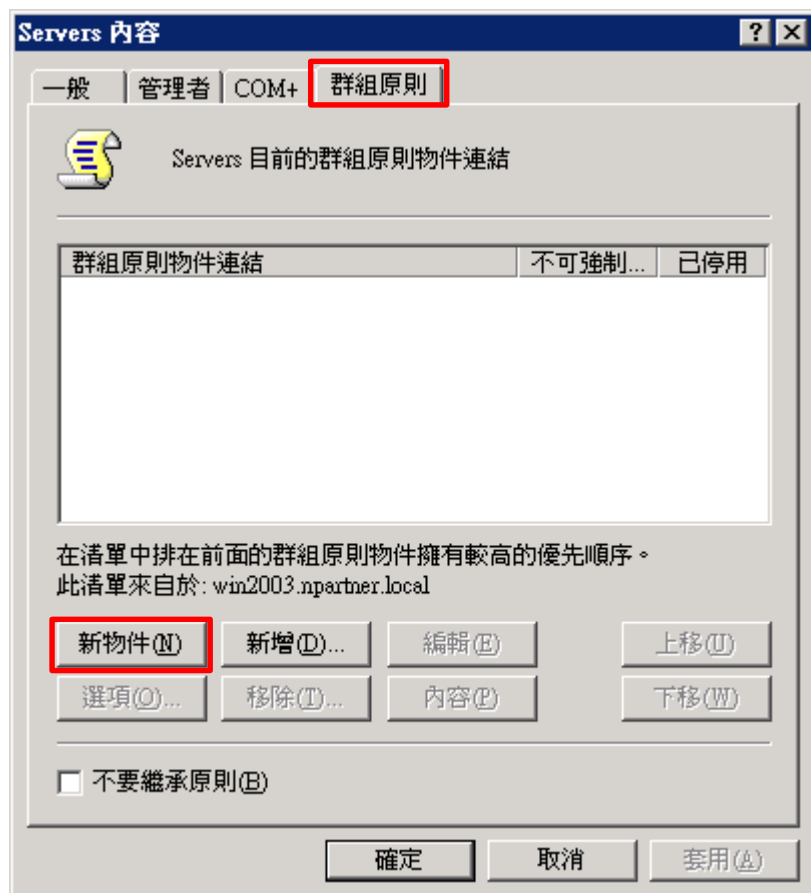
(2) Domain Controllers 的 Servers 組織單位，點選內容

選擇 [Domain Controllers] 的 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [內容]



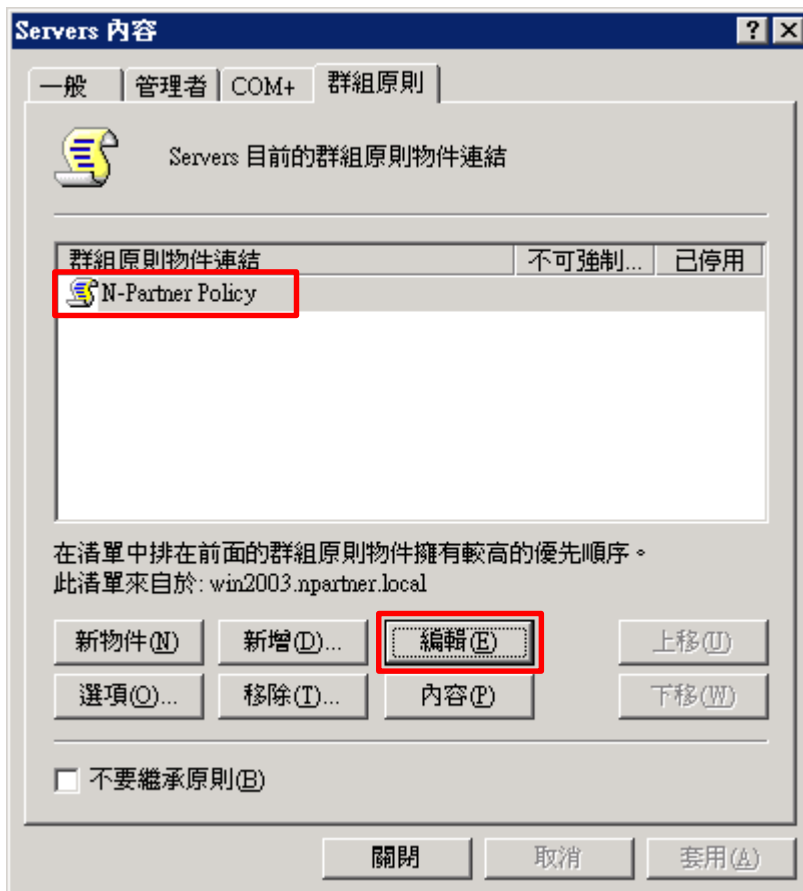
(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按 [新物件]



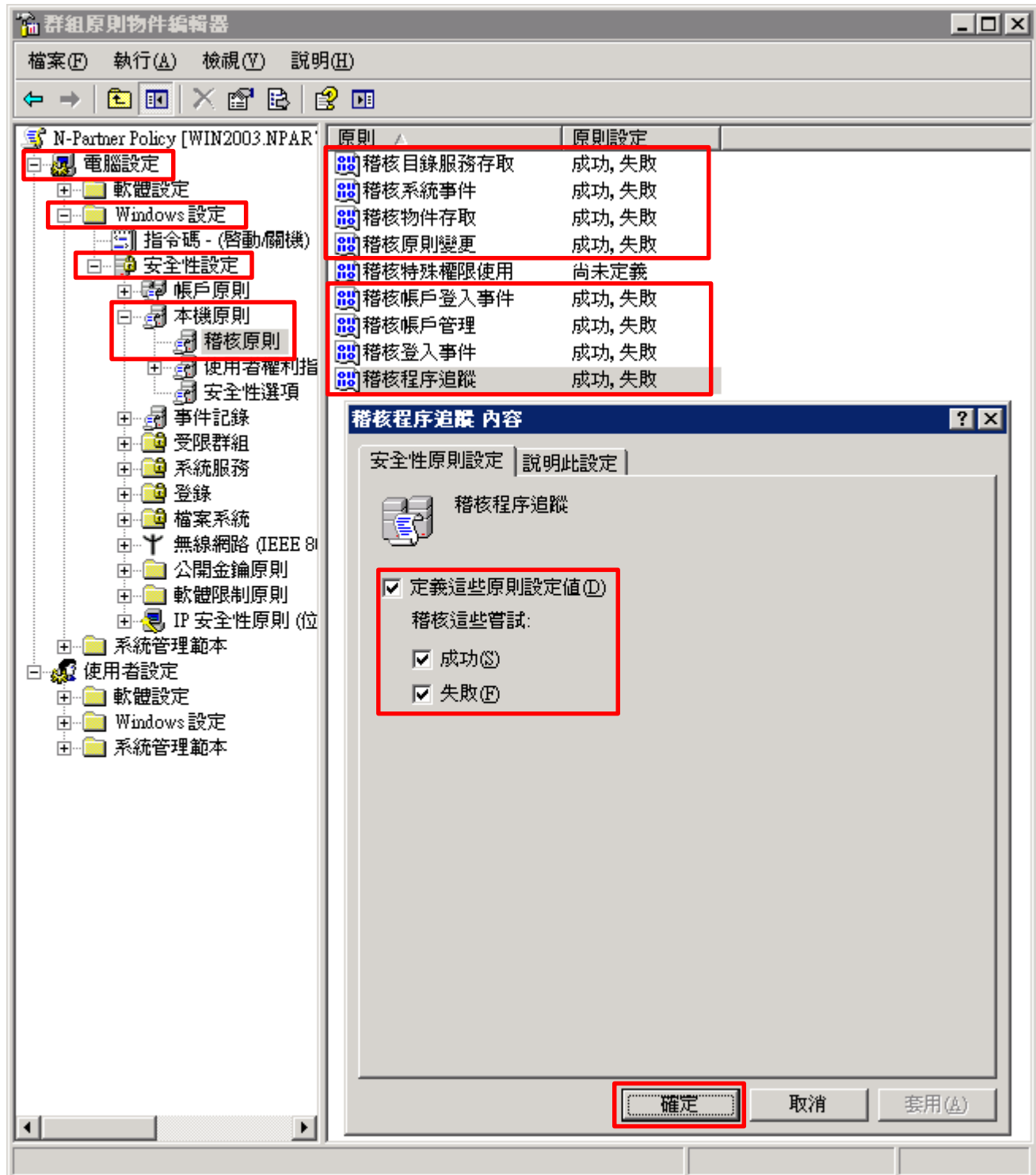
(4) 編輯群組原則物件

輸入群組原則物件名稱 **N-Partner Policy** 註：請依客戶環境建立群組物件名稱 -> 按 [編輯]



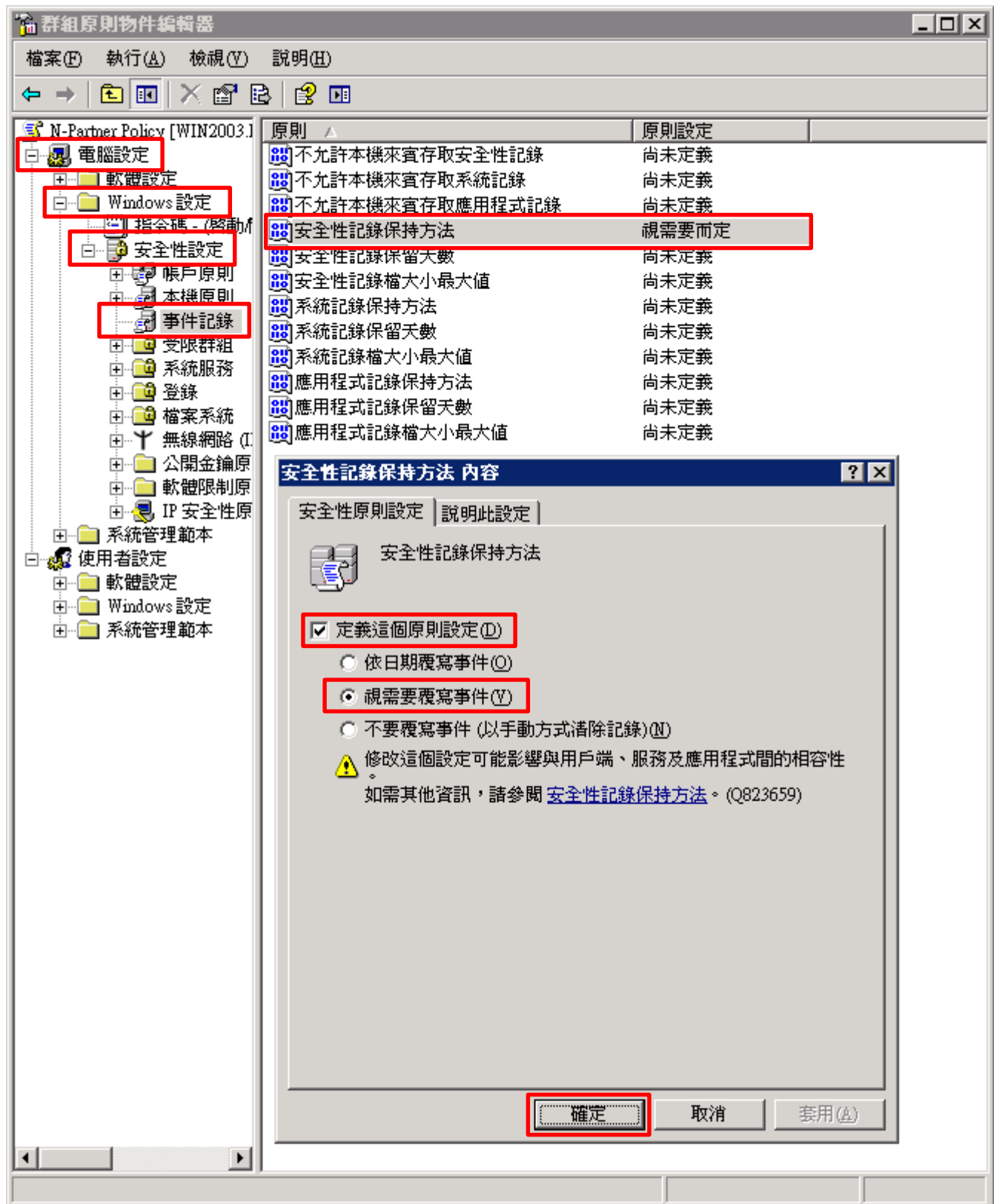
(5) 本機原則：稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核目錄服務存取], [稽核系統事件], [稽核物件存取], [稽核原則變更], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件], [稽核程序追蹤] 項目 -> 勾選 [定義這些原則設定:] & [成功] & [失敗] -> 按 [確定]



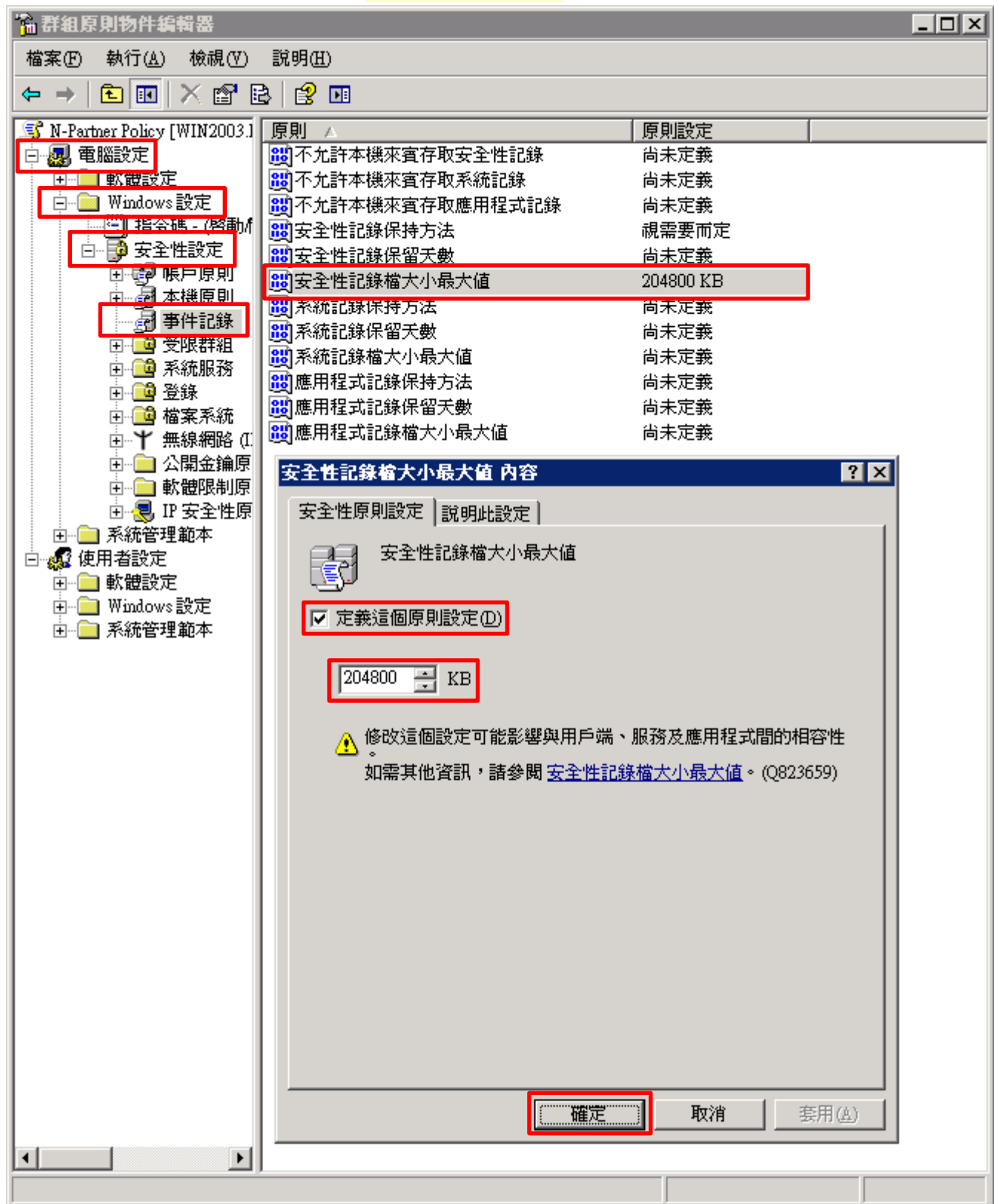
(6) 事件記錄：安全性記錄保持方法

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [事件記錄] -> 點選 [安全性記錄保持方法] 項目 -> 勾選 [定義這個原則設定]: -> 點選 [視需要覆寫事件] -> 按 [確定]



(7) 事件記錄：安全性記錄檔大小最大值

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [事件記錄] -> 點選 [安全性記錄檔大小最大值] 項目 -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]



(8) 開啟 [命令提示字元]



命令提示字元

(9) 更新群組原則

C:\> gpupdate /force

A screenshot of a Windows Command Prompt window. The title bar reads 'C:\ 命令提示字元'. The window content shows the following text:

```
Microsoft Windows [版本 5.2.3790]  
<C> 版權所有 1985-2003 Microsoft Corp.  
  
C:\Documents and Settings\Administrator>gpupdate /force  
正在重新整理原則...  
  
使用者原則重新整理已完成。  
電腦原則重新整理已完成。  
  
如果要檢查原則處理中的錯誤，請檢視事件日誌。  
  
C:\Documents and Settings\Administrator>_
```

(10) 查看群組原則套用情形

C:\> gpresult /v

```
命令提示字元
C:\Documents and Settings\Administrator>gpresult /v

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
Copyright (C) Microsoft Corp. 1981-2001

建立於 2019/6/14 上午 10:43:01

NPARTNER\Administrator 的 RSOP 資料在 WIN2003: 記錄模式
-----

OS 類型:                Microsoft(R) Windows(R) Server 2003 Enterprise x64 Edition
OS 設定:                網域主控站
OS 版本:                5.2.3790
終端機伺服器模式:      遠端系統管理
站台名稱:              Default-First-Site-Name
漫遊設定檔:
本機設定檔:            C:\Documents and Settings\Administrator
用低速連結來連線?:    否

電腦設定
-----
CN=WIN2003,OU=Servers,OU=Domain Controllers,DC=npartner,DC=local
上次套用的群組原則:    2019/6/14 於 上午 10:39:00
套用的群組原則來自:    win2003.npartner.local
群組原則低速連結閾值: 500 kbps
網域名稱:              npartner
網域類型:              Windows 2000

已套用的群組原則物件
-----
N-Partner Policy
Default Domain Controllers Policy
Default Domain Policy
```

2.3 新增非管理帳號

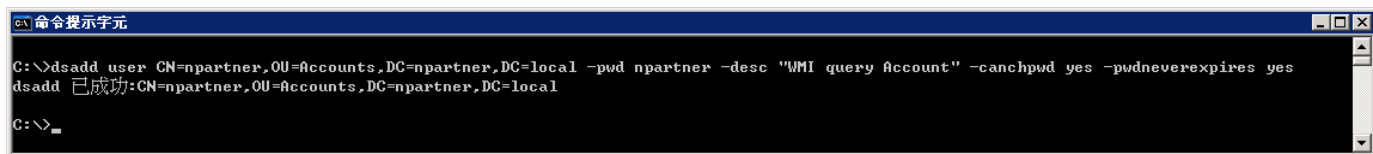
2.3.1 新增使用者

(1) 開啟 [命令提示字元]



(2) 新增帳號

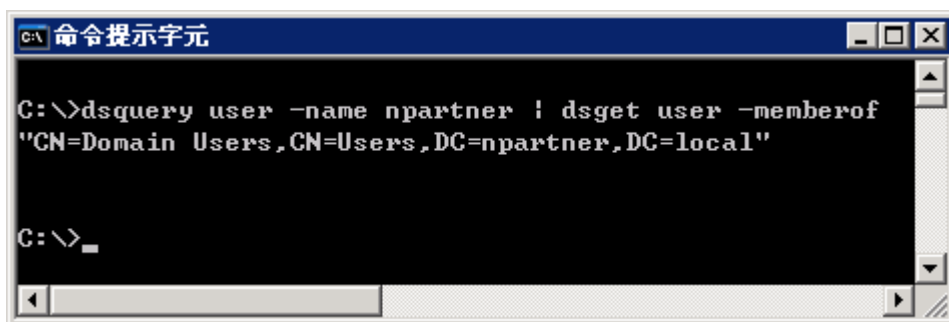
```
C:\> dsadd user CN=npartner,OU=Accounts,DC=npartner,DC=local -pwd npartner -desc "WMI query Account" -canchpwd yes -pwdneverexpires yes
```



紅色文字部位請輸入帳號密碼及網域資訊

(3) 查看帳號狀態

```
C:\> dsquery user -name npartner | dsget user -memberof
```



2.3.2 設定 DCOM 權限

(1) 開啟 [命令提示字元]



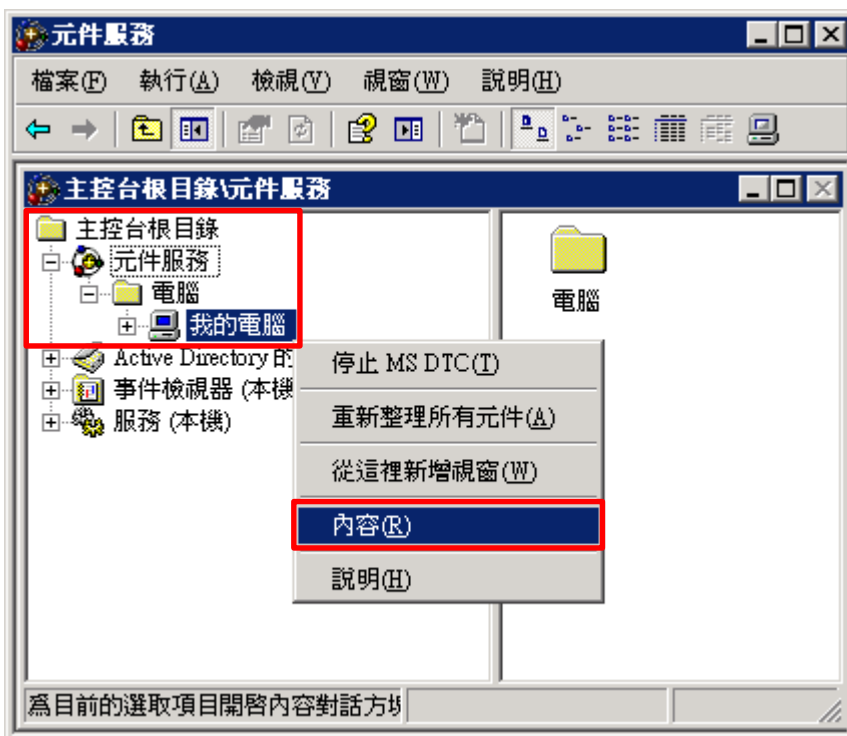
(2) 開啟元件服務

C:\> dcomcnfg.exe



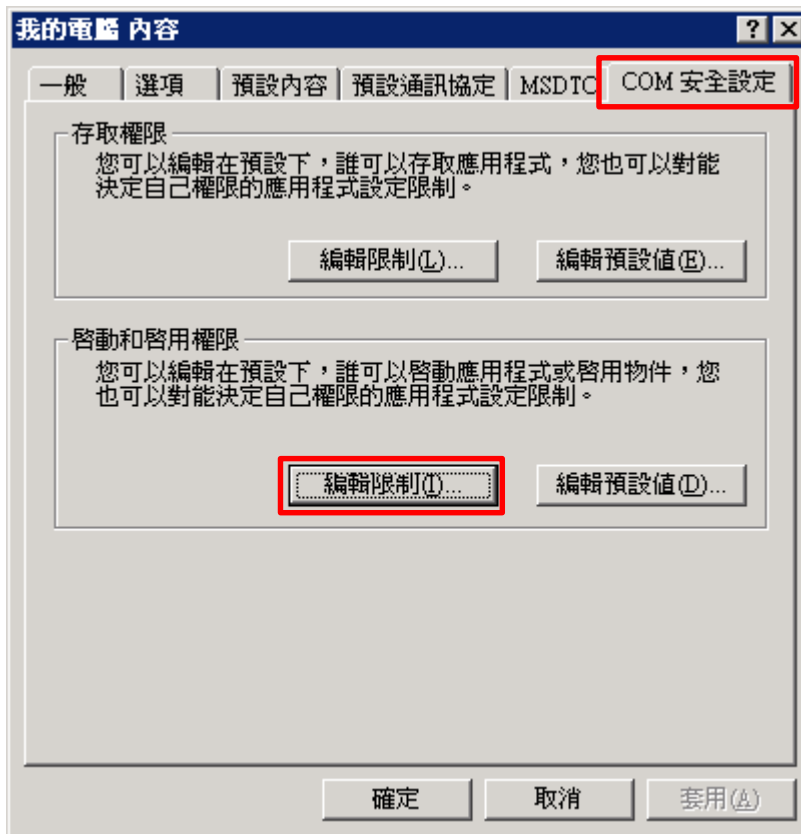
(3) 編輯電腦內容

展開 [主控台根目錄], [元件服務], [電腦] -> 在 [我的電腦] 按滑鼠右鍵 -> 點選 [內容]



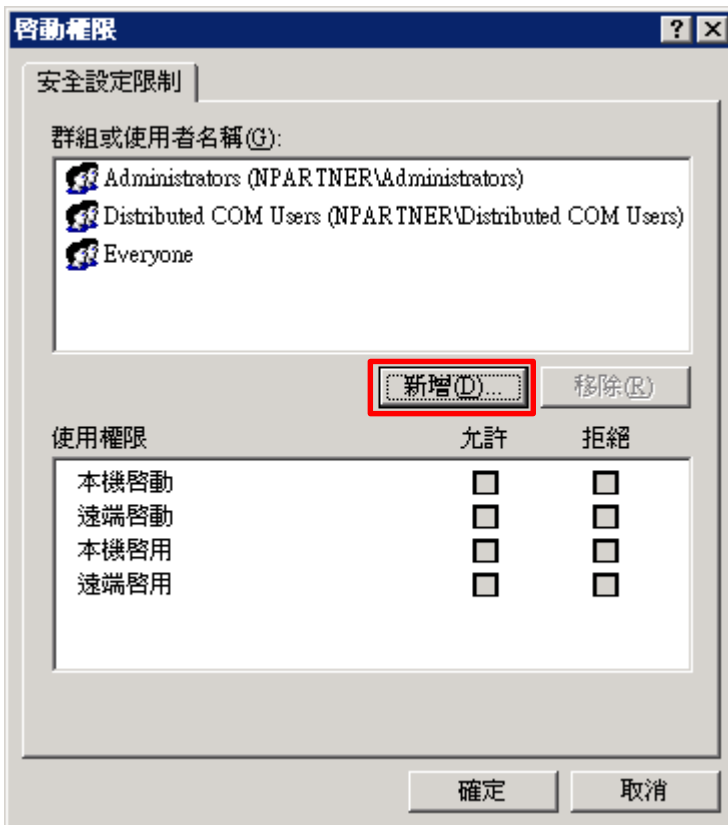
(4) 啟用權限

點選 [COM 安全性] 頁面 -> 啟動和啟用權限，按 [編輯限制]



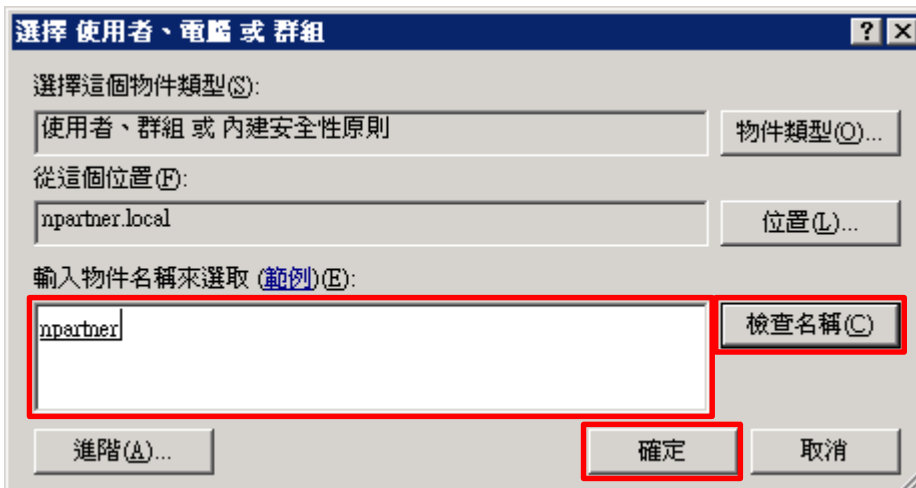
(5) 新增 DCOM 使用者權限

點選 [新增]



(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

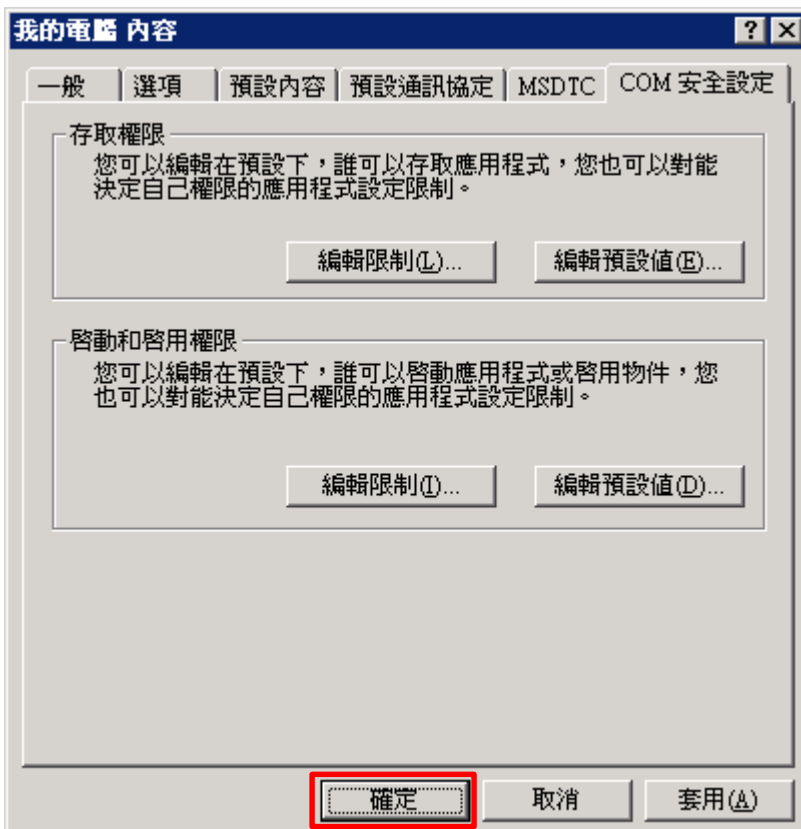


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [本機啟動:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



2.3.3 設定 WMI 權限

2.3.3.1 設定事件日誌權限

(1) 開啟 [命令提示字元]



(2) 開啟 WMI 控制

```
C:\> wmicmgmt.msc
```



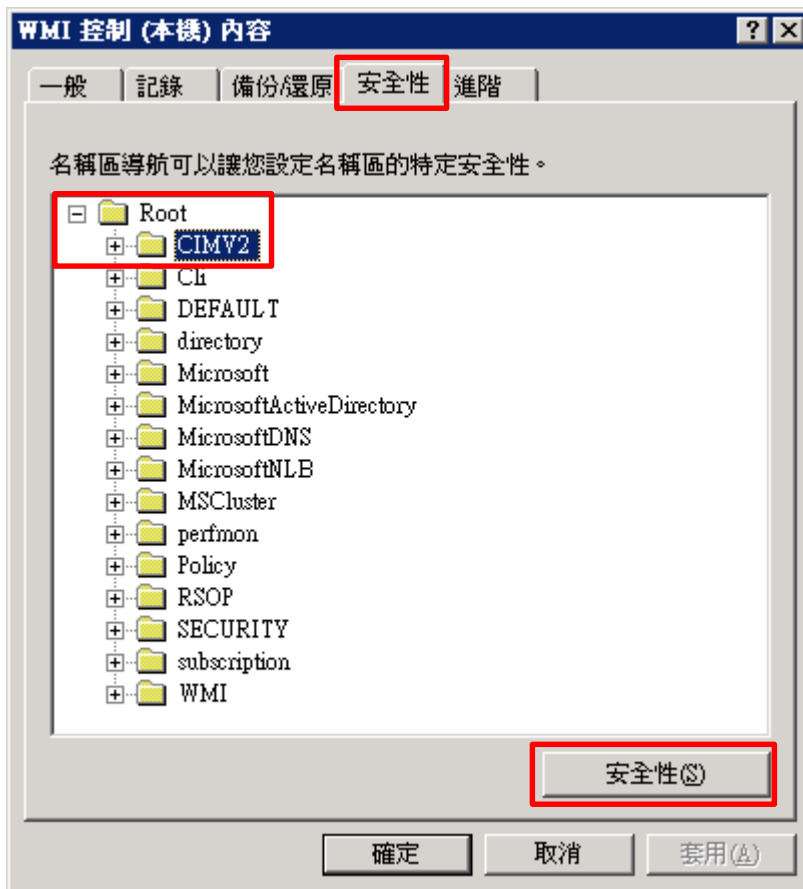
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



(4) 編輯 CIMV2 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [CIMV2] -> 按 [安全性]



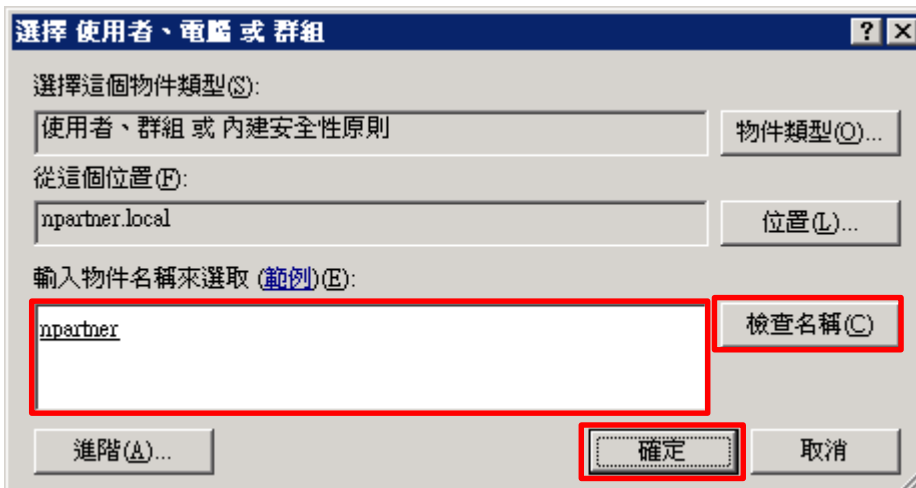
(5) 新增 WMI 使用者權限

按 [新增]



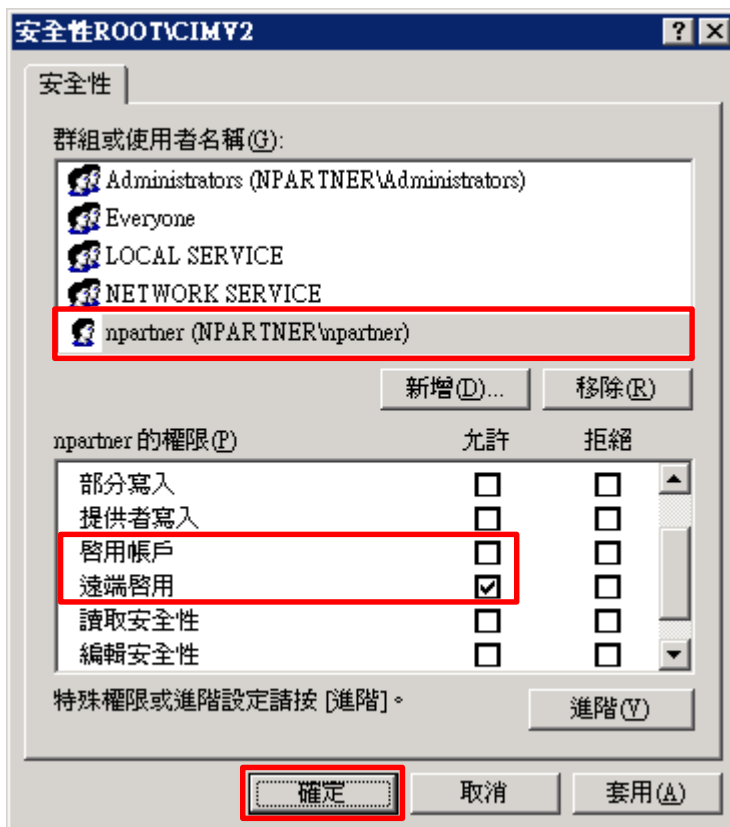
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

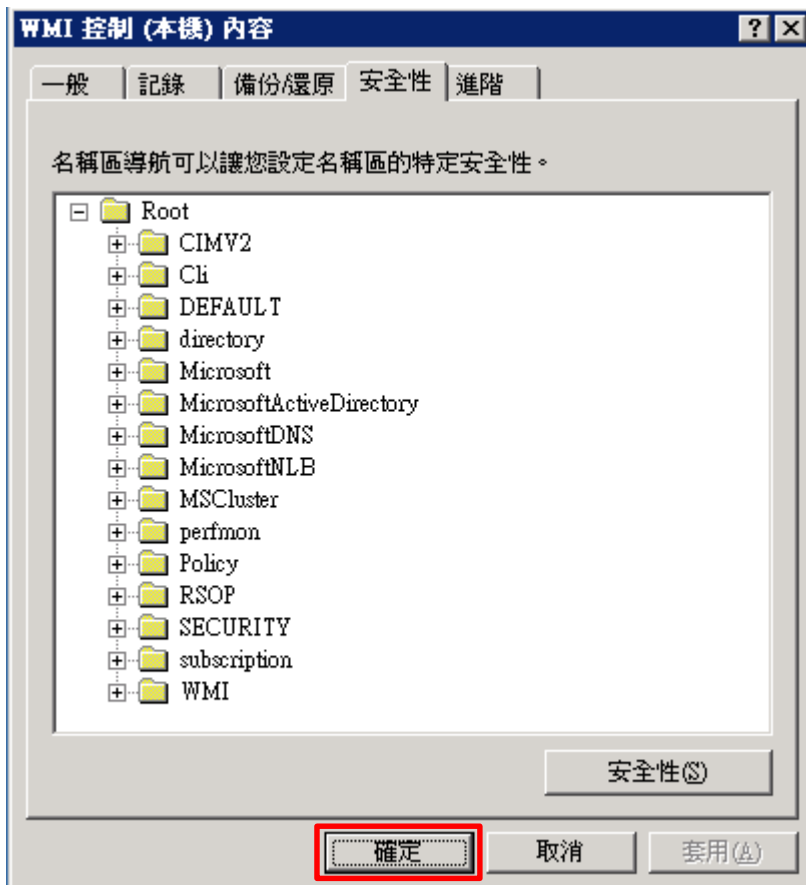


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



2.3.3.2 設定讀取使用者資料權限

(1) 開啟 [命令提示字元]



(2) 開啟 WMI 控制

```
C:\> wimgmt.msc
```



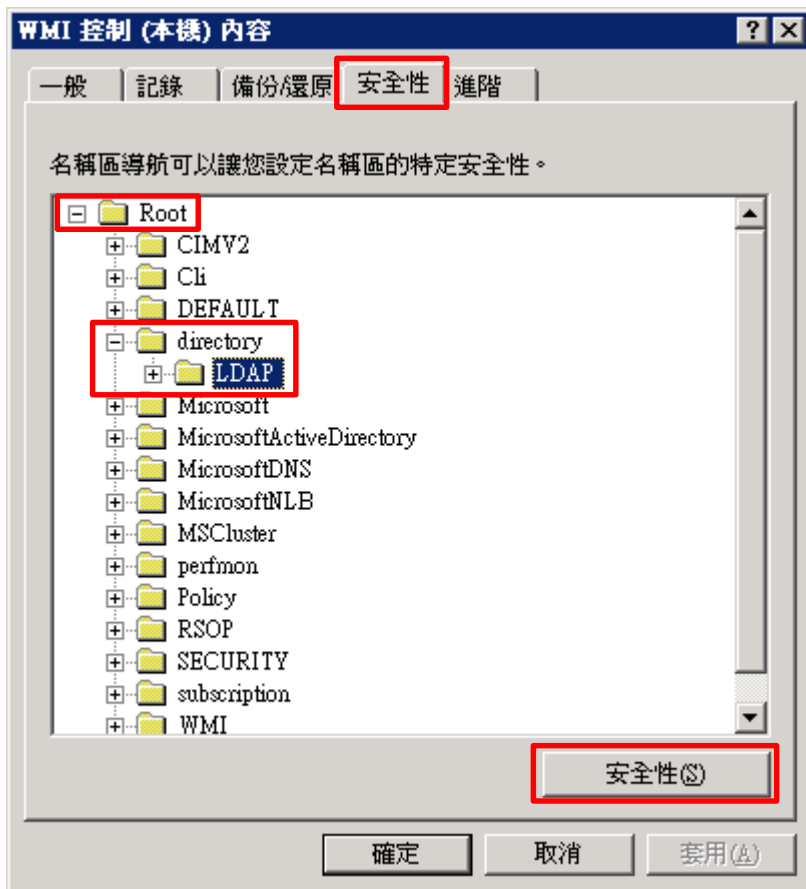
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



(4) 編輯 LDAP 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [directory] -> [LDAP] -> 按 [安全性]



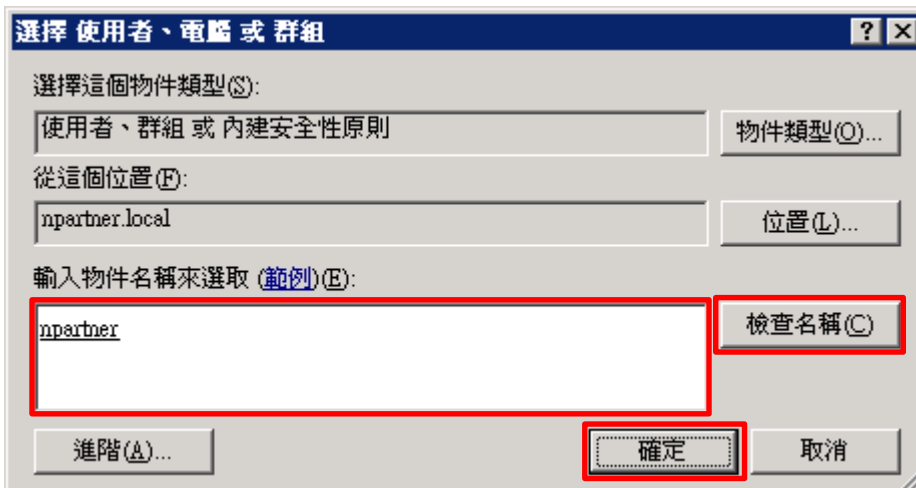
(5) 新增 WMI 使用者權限

按 [新增]



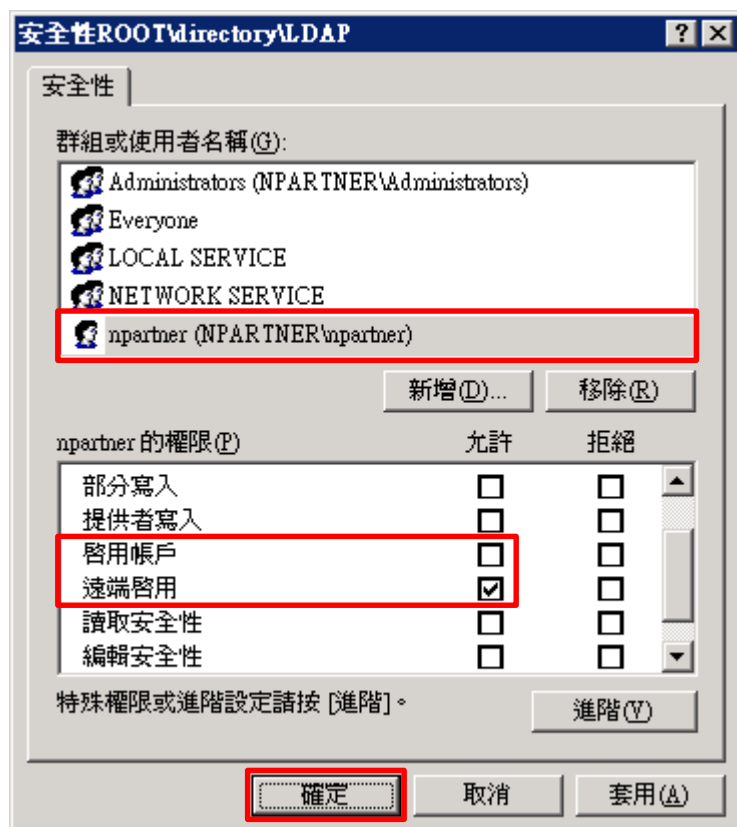
(6) 輸入使用者

輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

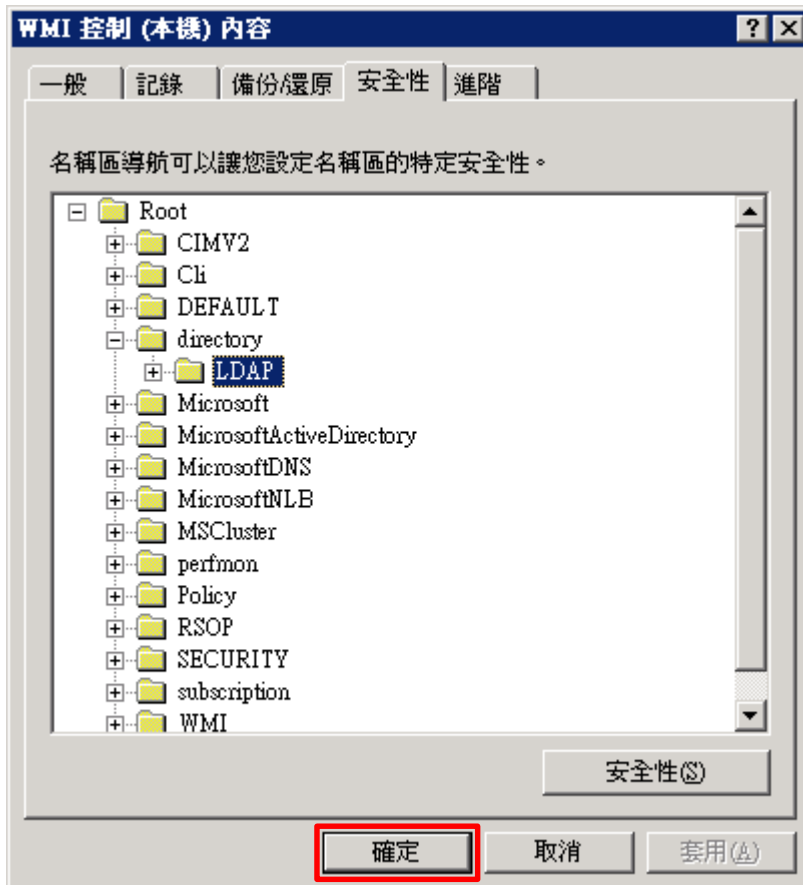


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



2.3.4 設定 Event log 讀取權限

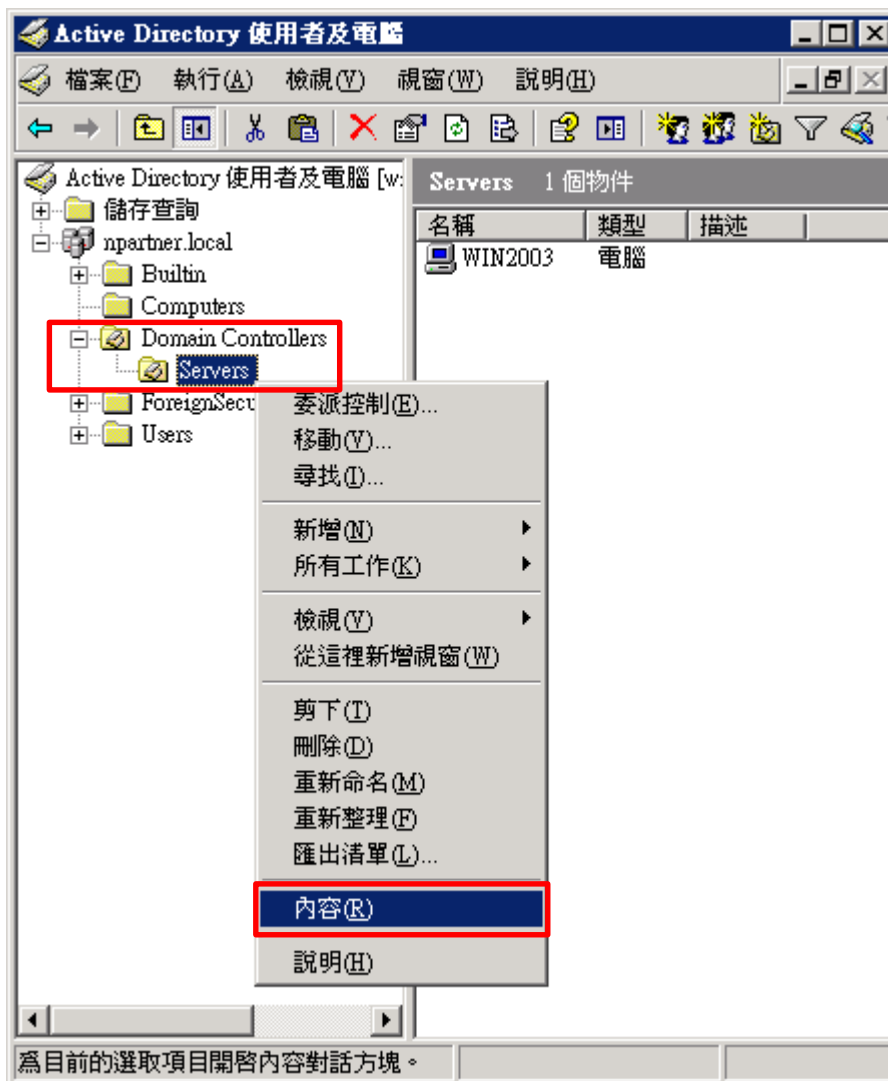
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



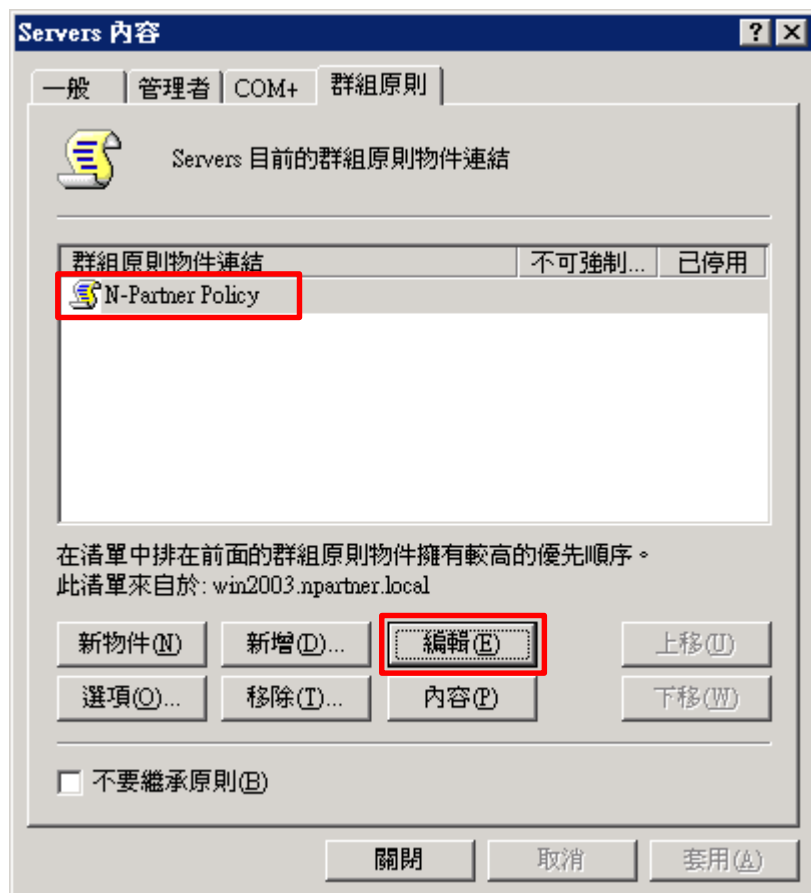
(2) Domain Controllers 的 Servers 組織單位，點選內容

選擇 [Domain Controllers] 的 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [內容]




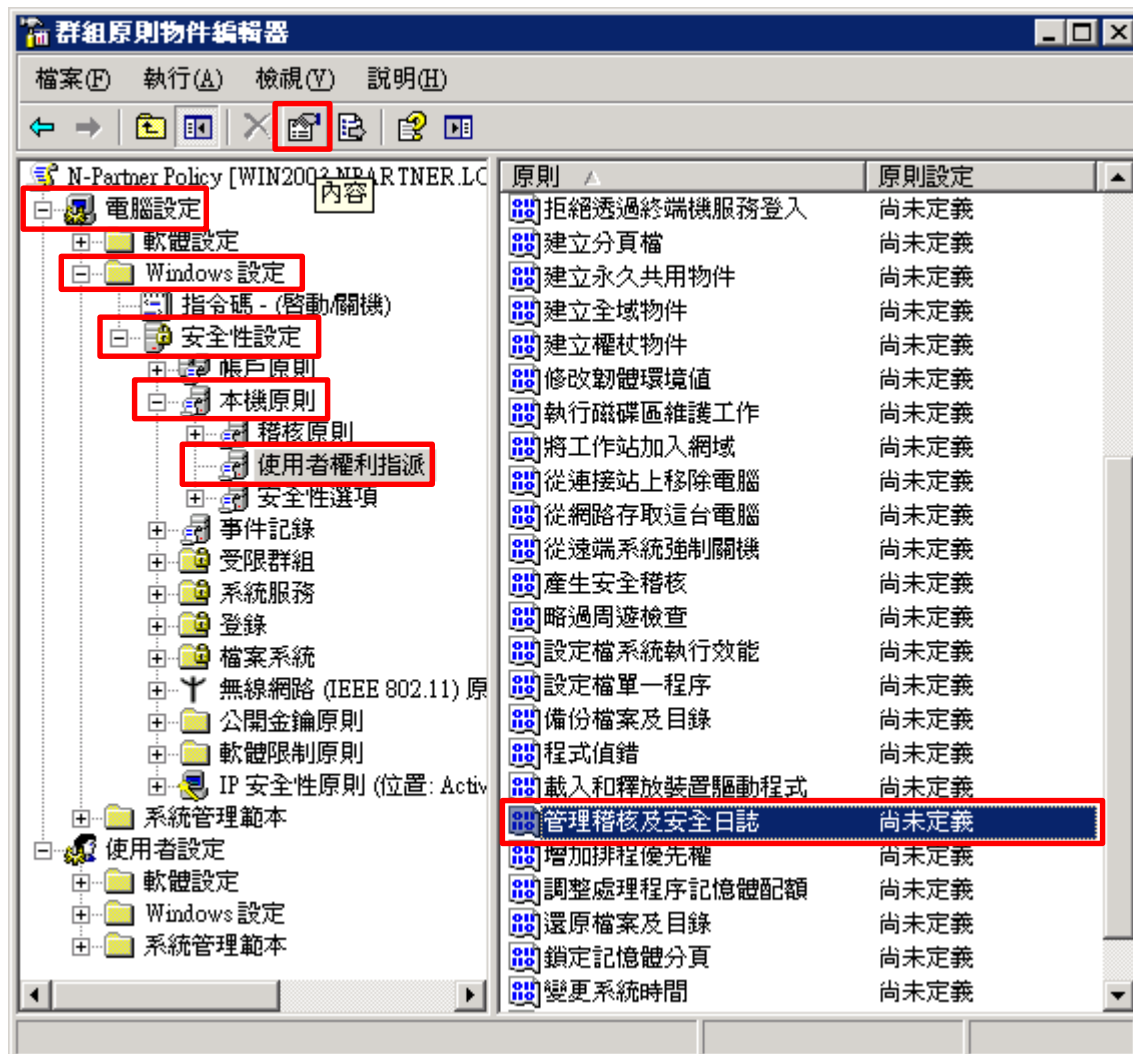
(3) 編輯群組原則物件

點選群組原則物件名稱 [N-Partner Policy] -> 按 [編輯]



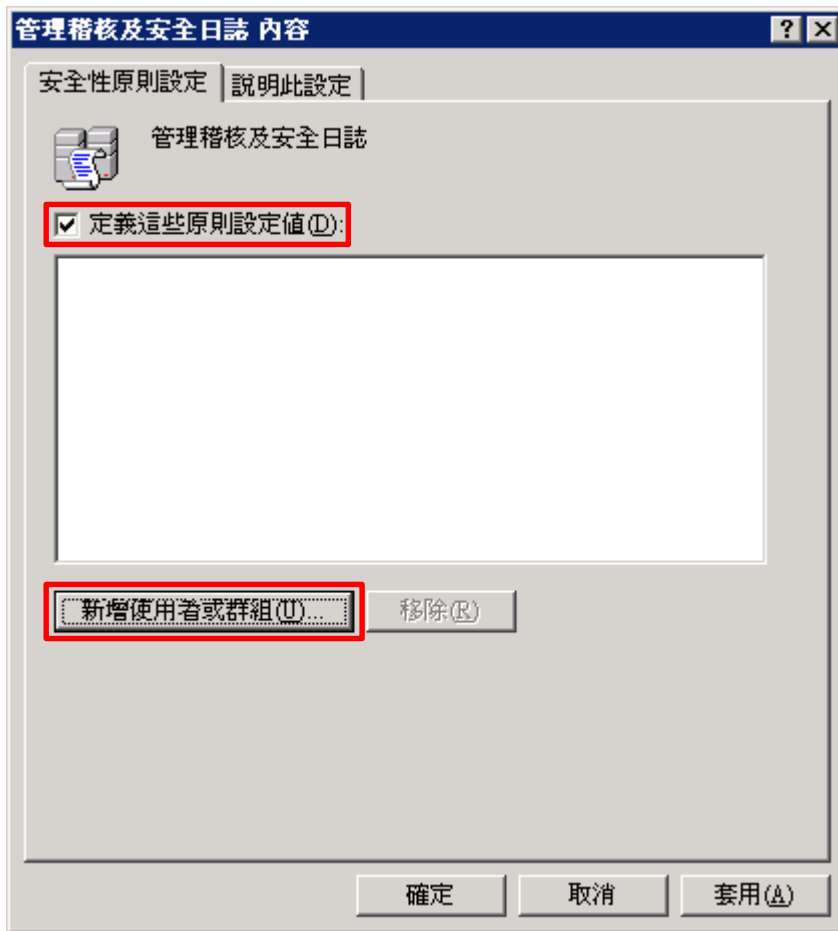
(4) 設定記錄檔

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [使用者權利指派] -> 點選 [管理稽核及安全性記錄檔] 項目 -> 按  內容



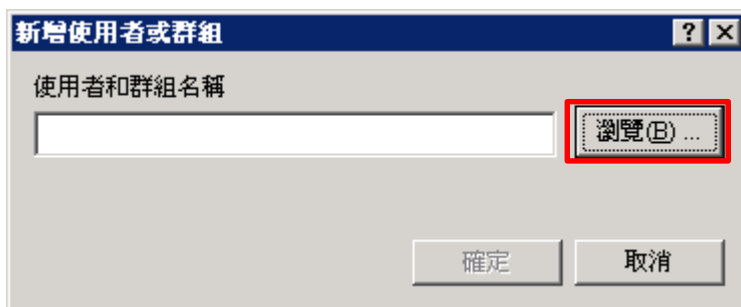
(5) 新增管理稽核使用者

勾選 [定義這些原則設定] -> 按 [新增使用者或群組...]



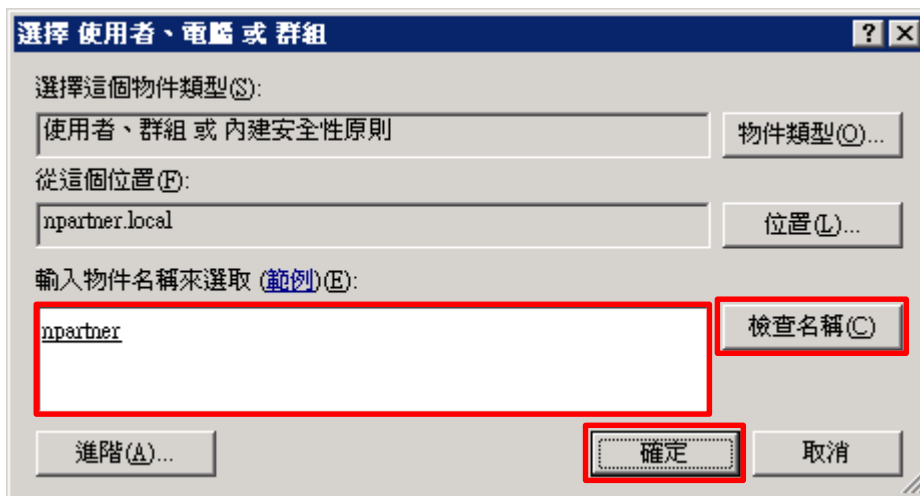
(6) 搜尋使用者

按 [瀏覽]



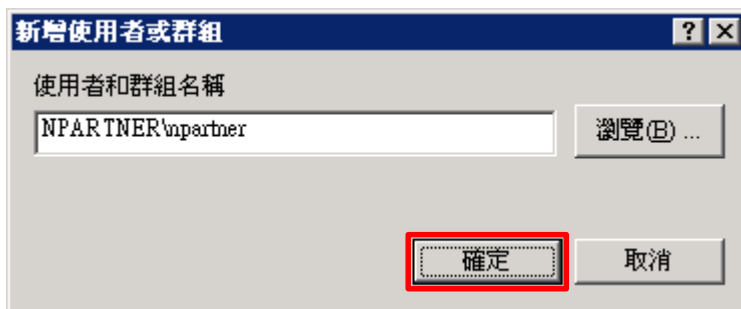
(7) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]



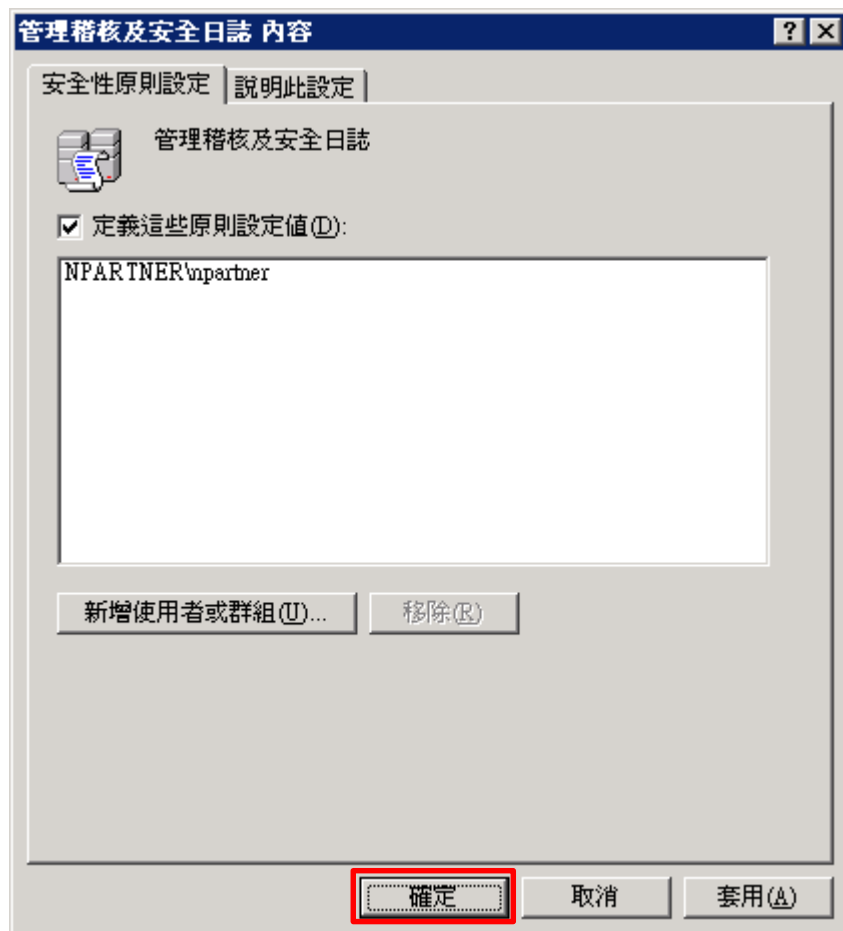
(8) 確定使用者

按 [確定]



(9) 確定設定記錄檔

按 [確定]

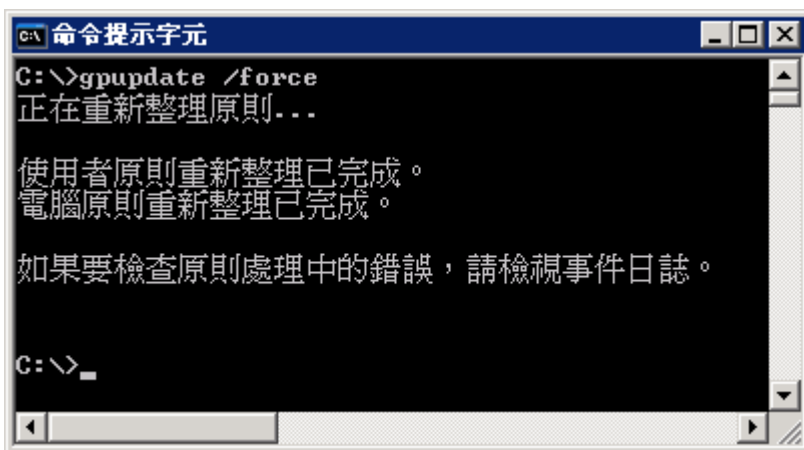


(10) 開啟 [命令提示字元]



(11) 更新群組原則

C:\> gpupdate /force



```
命令提示字元
C:\>gpupdate /force
正在重新整理原則...

使用者原則重新整理已完成。
電腦原則重新整理已完成。

如果要檢查原則處理中的錯誤，請檢視事件日誌。

C:\>_
```


2.3.5 重啟 WMI 服務

(1) 開啟 [Windows PowerShell]



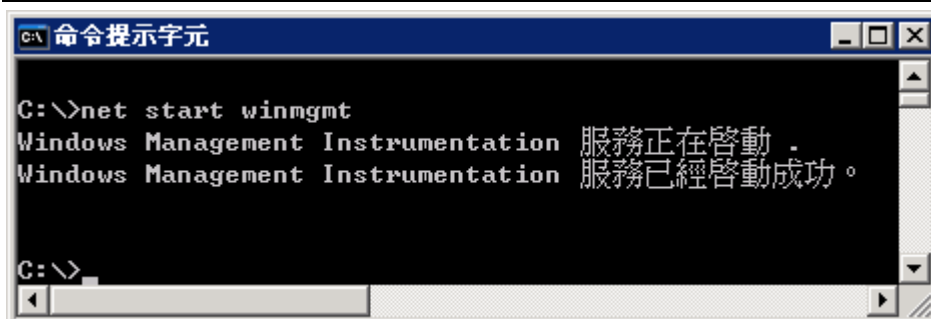
(2) 停用 WMI 服務

C:\> net stop winmgmt



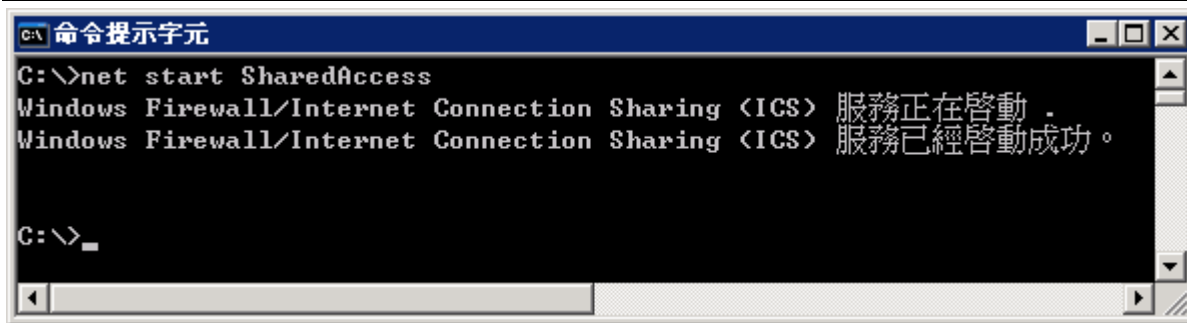
(3) 啟用 WMI 服務

C:\> net start winmgmt



(4) 啟用 Firewall 服務

C:\> net start SharedAccess



```
C:\> net start SharedAccess
Windows Firewall/Internet Connection Sharing (ICS) 服務正在啓動。
Windows Firewall/Internet Connection Sharing (ICS) 服務已經啓動成功。

C:\> _
```

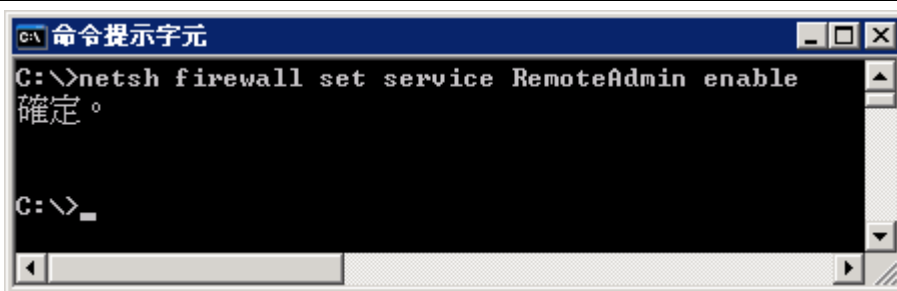
2.4 設定防火牆

(1) 開啟 [命令提示字元]



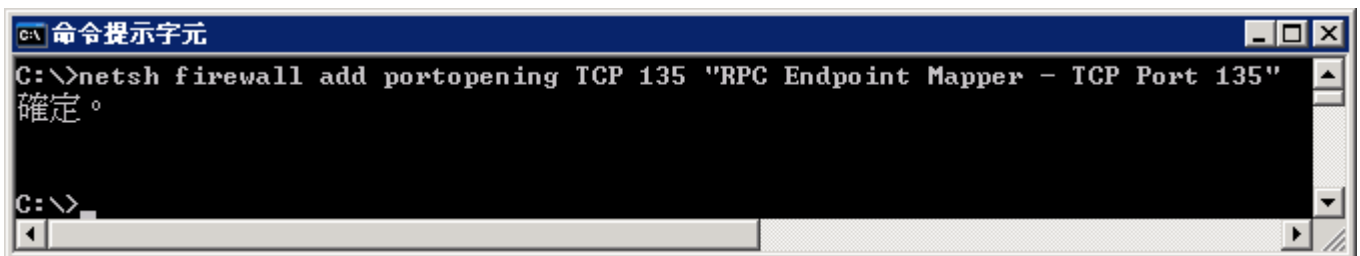
(2) 允許 WMI 通過防火牆

```
C:\> netsh firewall set service RemoteAdmin enable
```



(3) 允許 TCP 135 Port 通過防火牆

```
C:\> netsh firewall add portopening TCP 135 "RPC Endpoint Mapper - TCP Port 135"
```



(4) 查看防火牆設定

C:\> netsh firewall show config

```
命令提示字元
C:\> netsh firewall show config

網域 設定檔組態:
-----
操作模式 = 啟用
例外模式 = 啟用
多點傳送/廣播回應模式 = 啟用
通知模式 = 啟用

標準 設定檔組態 <目前的>:
-----
操作模式 = 啟用
例外模式 = 啟用
多點傳送/廣播回應模式 = 啟用
通知模式 = 啟用

標準 設定檔的服務設定:
-----
模式 自訂 名稱
-----
啟用 否 遠端桌面
啟用 否 遠端系統管理

標準 設定檔的連接埠設定:
-----
連接埠 通訊協定 模式 名稱
-----
135 TCP 啟用 RPC Endpoint Mapper - TCP Port 135
3389 TCP 啟用 遠端桌面

記錄設定:
-----
檔案位置 = C:\tmp\pf firewall.log
最大檔案大小 = 4096 KB
丟棄的封包 = 停用
連線 = 啟用

區域連線 防火牆設定:
-----
操作模式 = 啟用

C:\>
```

3. Windows 2008

Windows 稽核原則設定 [詳細說明請參考前言的稽核原則建議連結](#)

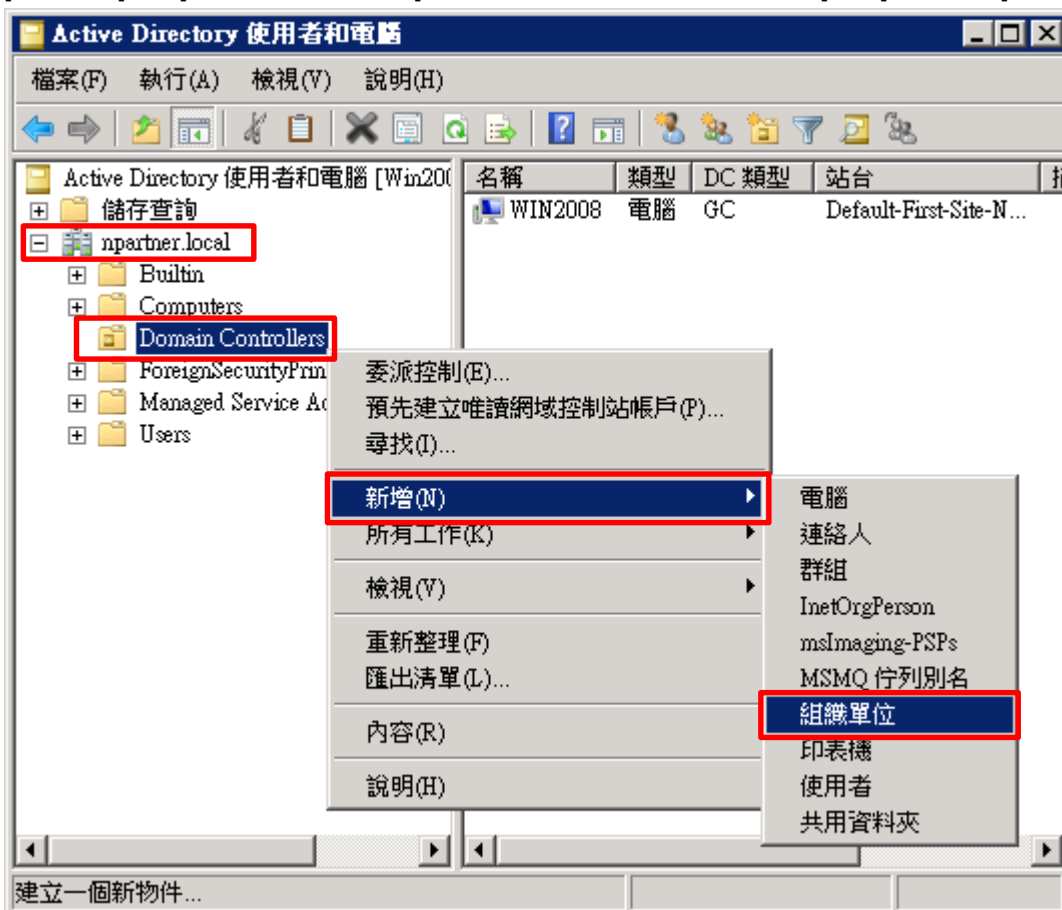
3.1 組織單位設定

(1) 開啟 [Active Directory 使用者和電腦]



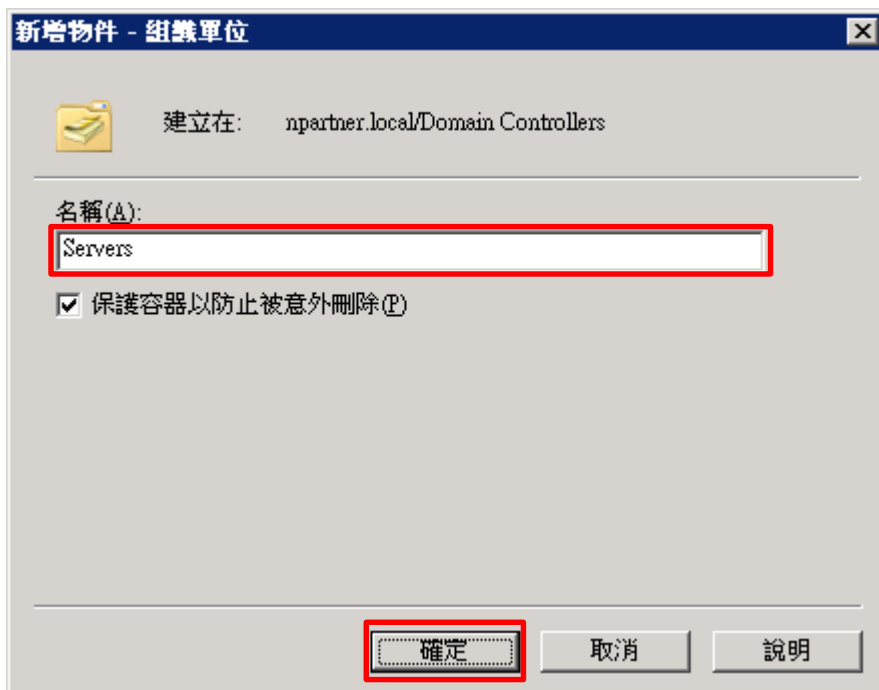
(2) 新增組織單位

[網域名稱] 的 [Domain Controllers] 組織單位，按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]



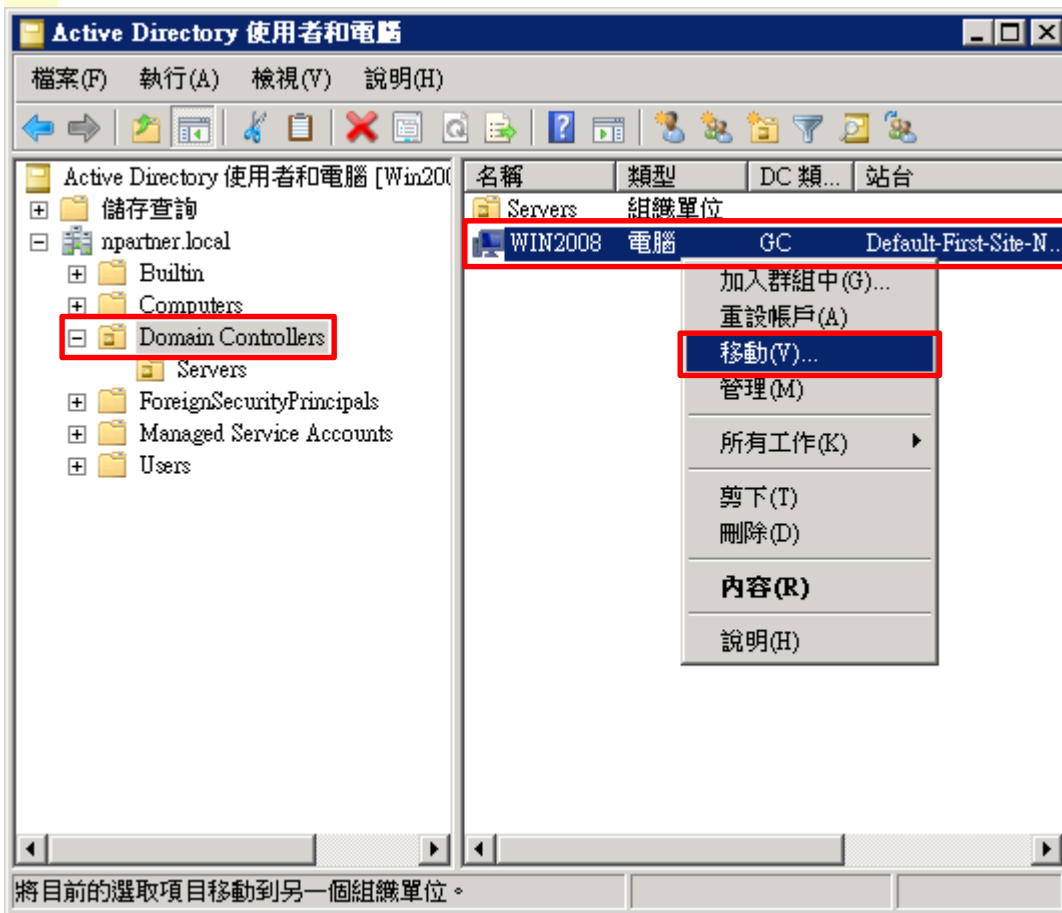
(3) 輸入組織單位名稱

輸入組織單位名稱: Servers 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



(4) 移動伺服器至新的組織單位

選擇 [Domain Controllers] 組織單位 -> 在 [Win2008] 伺服器，按滑鼠右鍵，註：請依客戶環境選擇 Windows AD 主機 -> 點選 [移動]



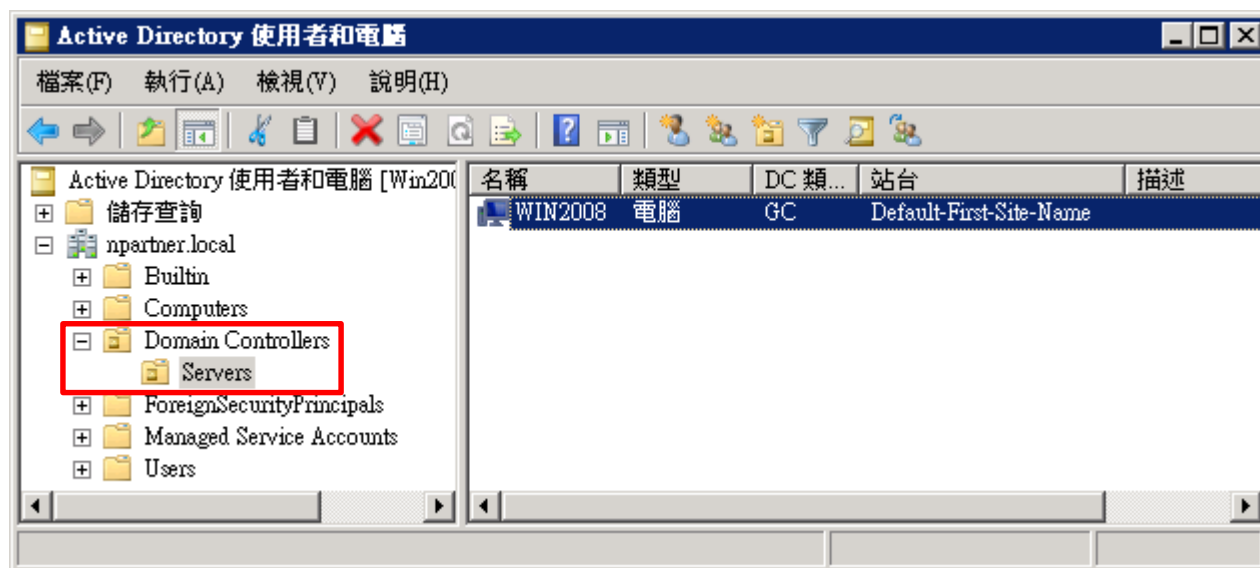
(5) 選擇組織單位

選擇 [Domain Controllers] 的 [Servers] 組織單位 -> 按 [確定]



(6) 確認伺服器已移動至新的組織單位

展開 [Domain Controllers] 的 [Servers] 組織單位，確認 [Win2008] 伺服器已移動



3.2 群組原則設定

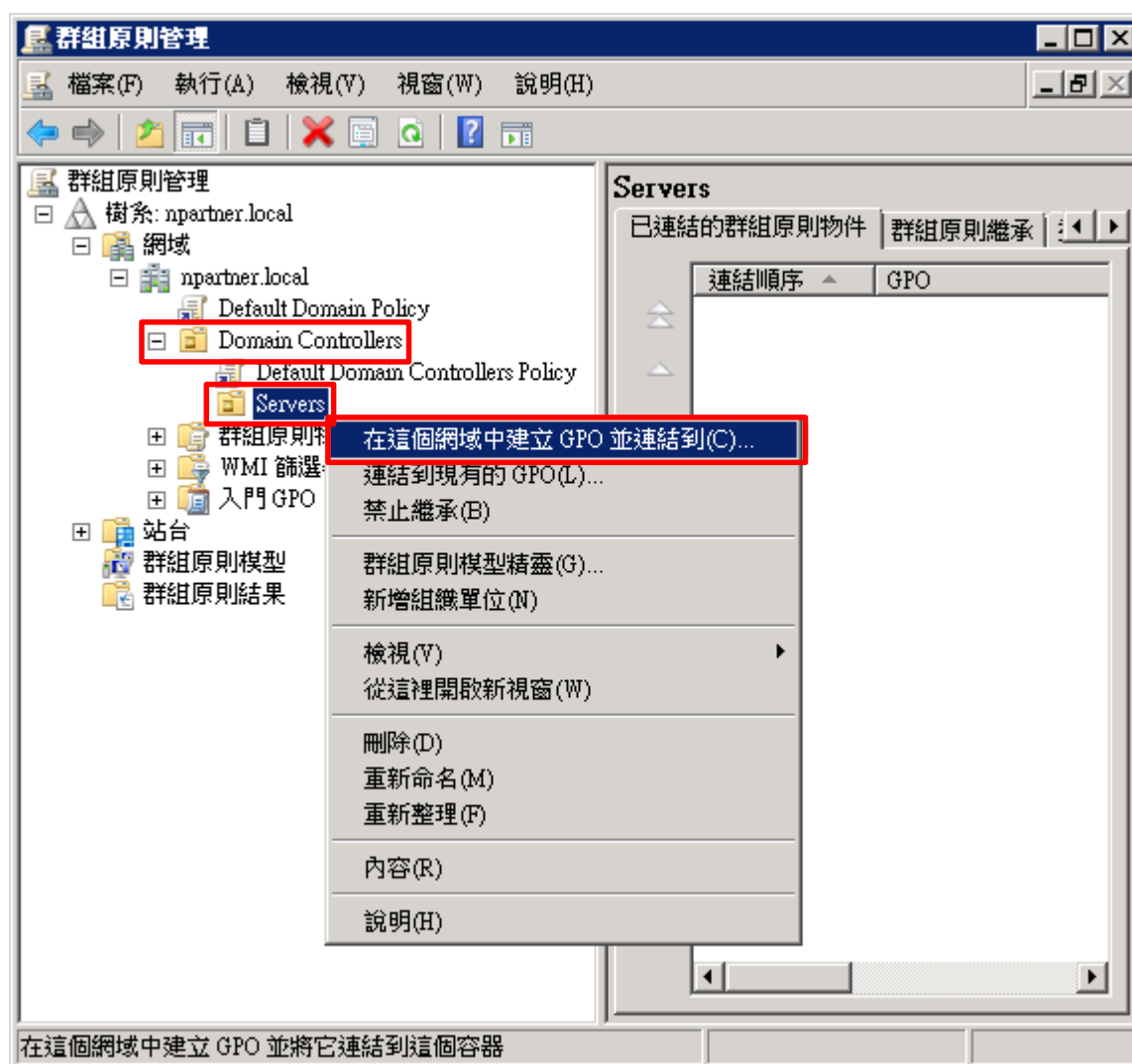
(1) 開啟群組原則管理

開啟 [群組原則管理]



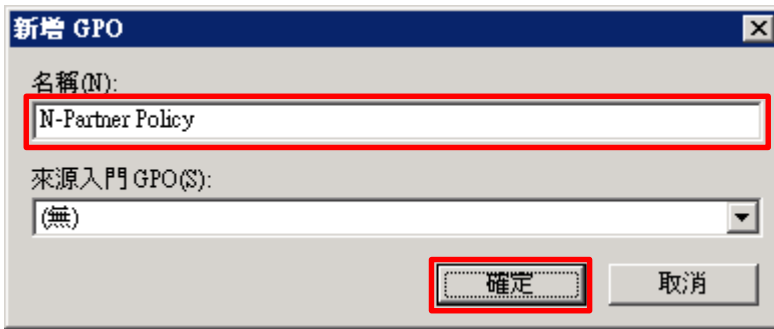
(2) 在 Servers 組織單位，新增群組原則物件

在 [Domain Controllers] 的 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到...]



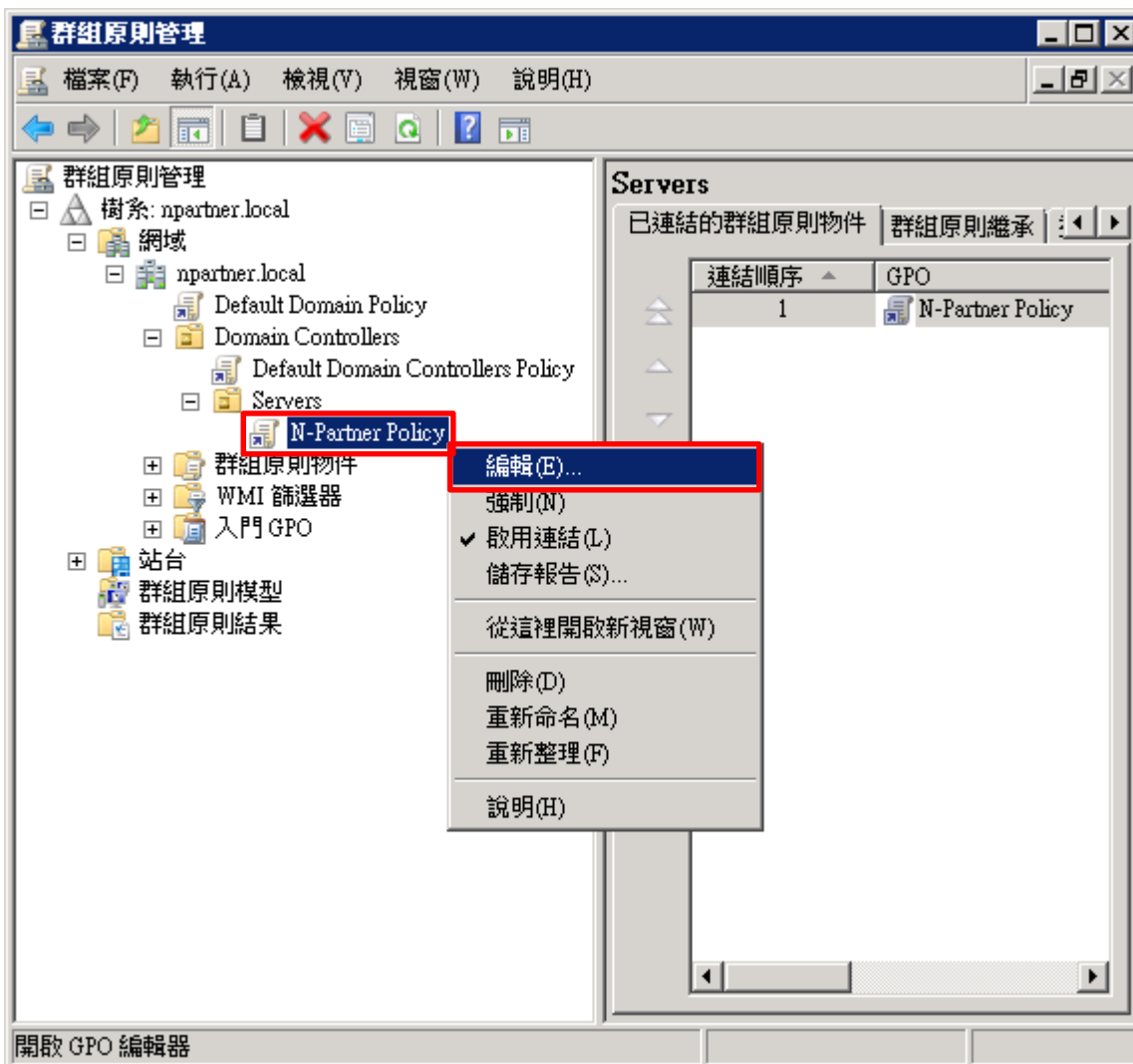
(3) 輸入群組原則物件名稱

輸入群組原則物件名稱: **N-Partner Policy** 註：請依客戶環境建立群組物件名稱 -> 按 [確定]



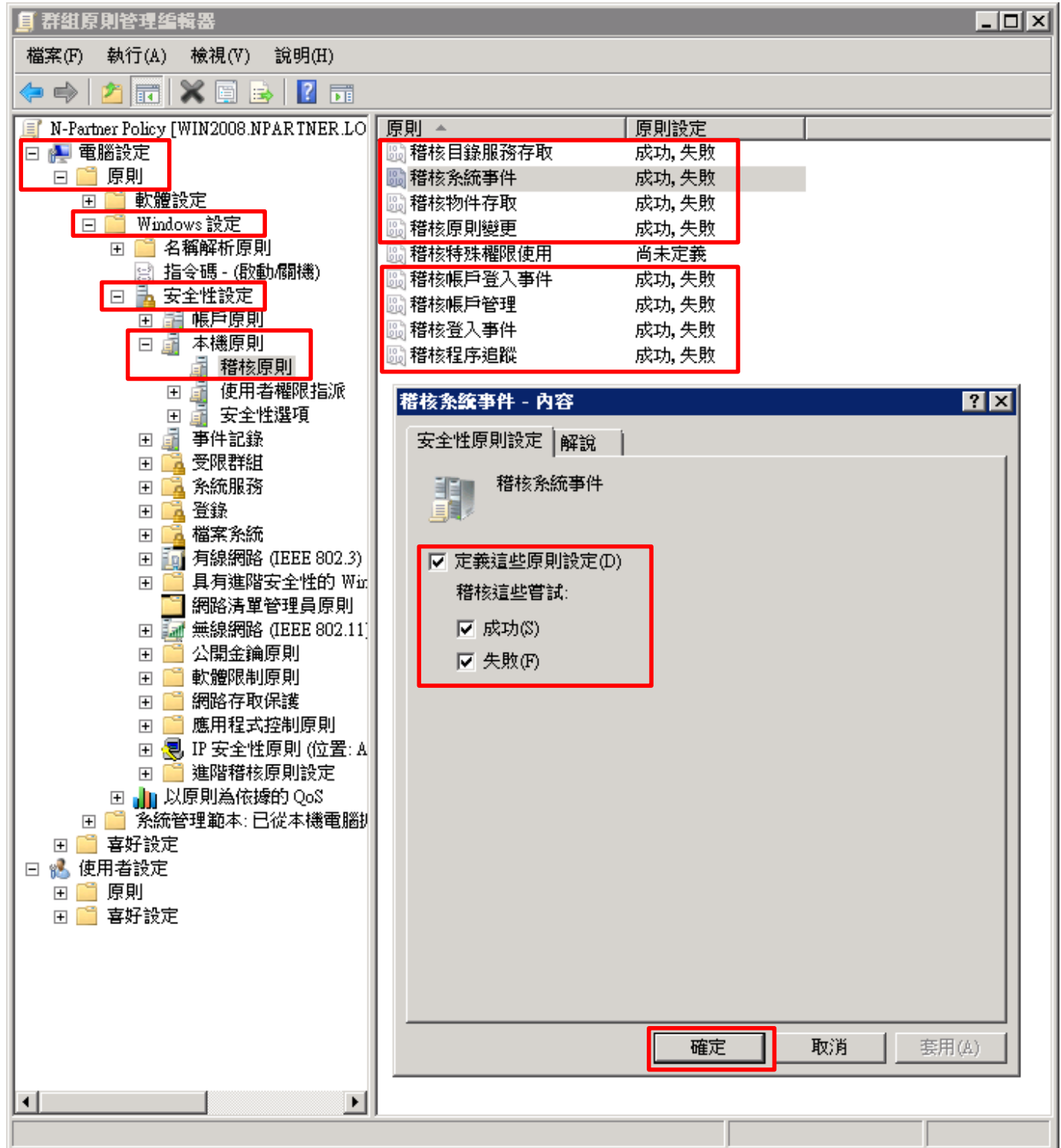
(4) 編輯群組原則物件

在 [N-Partner Policy] 群組原則物件，按滑鼠右鍵 -> 點選 [編輯]



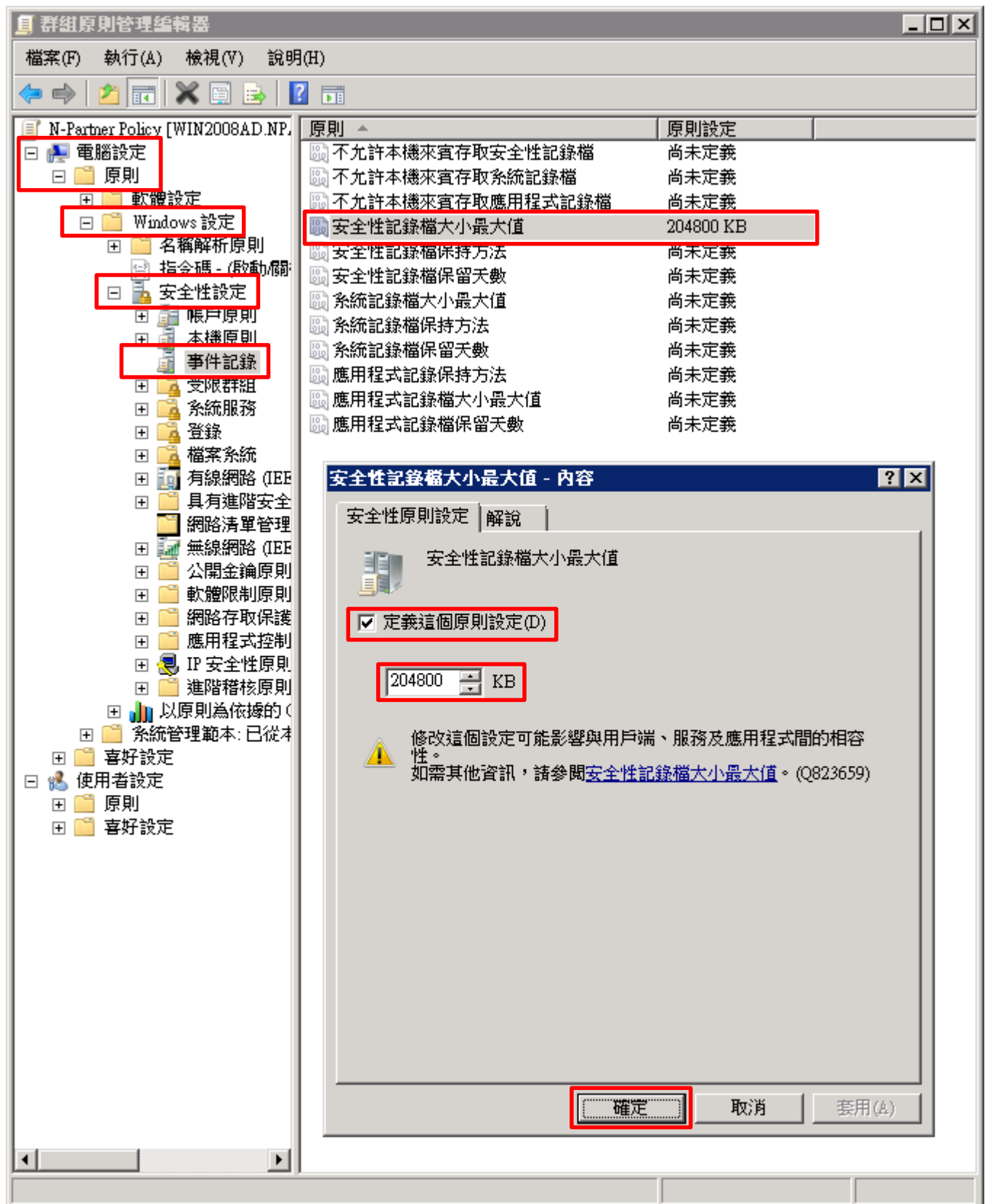
(5) 本機原則：稽核原則

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核目錄服務存取], [稽核系統事件], [稽核物件存取], [稽核原則變更], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件], [稽核程序追蹤] 項目 -> 勾選 [定義這些原則設定:] & [成功] & [失敗] -> 按 [確定]



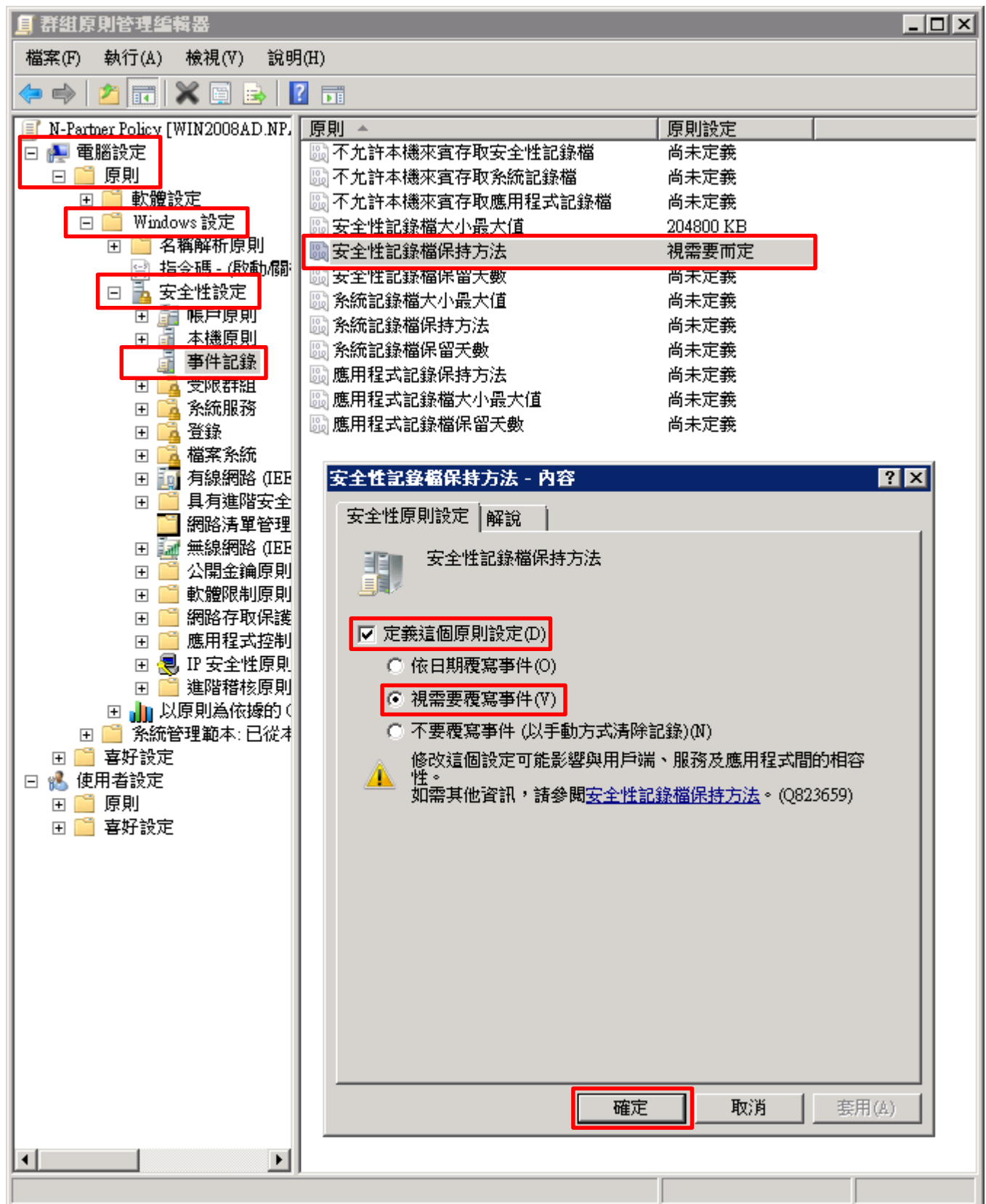
(6) 事件記錄：安全性記錄檔大小最大值

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄] -> 點選 [安全性記錄檔大小最大值] 項目 -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]



(7) 事件記錄：安全性記錄檔大小最大值

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄] -> 點選 [安全性記錄檔保持方法] 項目 -> 勾選 [定義這個原則設定] -> 點選 [視需要覆寫事件] -> 按 [確定]



(8) 開啟 Windows PowerShell



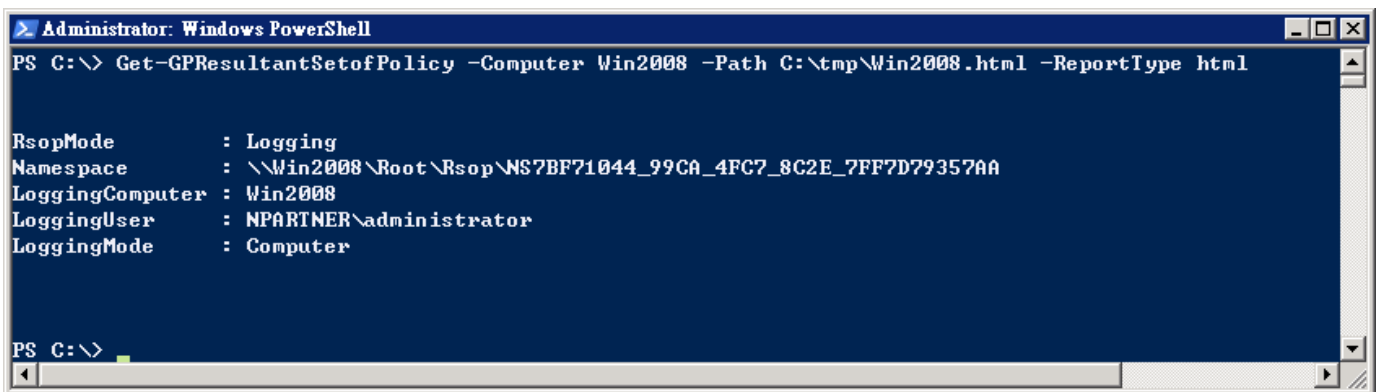
(9) 更新群組原則

```
PS C:\> gpupdate /force
```



(10) 產生伺服器群組原則報表

```
PS C:\> Get-GPResultantSetofPolicy -Computer Win2008 -Path C:\tmp\Win2008.html -ReportType html
```



紅色文字部位請輸入 Windows AD 伺服器名稱和資料夾路徑檔案名稱

(11) 開啟報表，確認 Windows AD 伺服器，套用 N-Partner Policy 群組原則

群組原則結果

NPARTNER\WIN2008
資料收集: 2021/5/14 下午 04:29:33

摘要 顯示全部

電腦設定 隱藏

原則 隱藏

Windows 設定 隱藏

安全性設定 隱藏

帳戶原則/密碼規則 顯示

帳戶原則/帳戶鎖定原則 顯示

帳戶原則/Kerberos 原則 顯示

本機原則/稽核原則 隱藏

原則	設定	優勢 GPO
稽核目錄服務存取	成功, 失敗	N-Partner Policy
稽核系統事件	成功, 失敗	N-Partner Policy
稽核物件存取	成功, 失敗	N-Partner Policy
稽核原則變更	成功, 失敗	N-Partner Policy
稽核帳戶登入事件	成功, 失敗	N-Partner Policy
稽核帳戶管理	成功, 失敗	N-Partner Policy
稽核登入事件	成功, 失敗	N-Partner Policy
稽核程序追蹤	成功, 失敗	N-Partner Policy

本機原則/使用者權限指派 顯示

本機原則/安全性選項 顯示

事件記錄檔 隱藏

原則	設定	優勢 GPO
安全性記錄檔保持方法	視需要而定	N-Partner Policy
安全性記錄檔容量最大值	204800 KB	N-Partner Policy

公開金鑰原則/憑證服務用戶端 - 自動註冊設定 顯示

公開金鑰原則/加密檔案系統 顯示

公開金鑰原則/被信任的根憑證授權單位 顯示

使用者設定 顯示

3.3 新增非管理帳號

3.3.1 新增使用者

(1) 開啟 [Windows PowerShell PowerShell Snap-In]



(2) 新增帳號

```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" `
>> -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -
AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True
```

A screenshot of a Windows PowerShell console window titled "Administrator: Windows PowerShell 的 Active Directory 模組". The console shows the execution of the command to create a new user. The output is empty, indicating successful execution.

```
Administrator: Windows PowerShell 的 Active Directory 模組
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" `
>> -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True
PS C:\> _
```

紅色文字部位請輸入帳號密碼及網域資訊

(3) 查看帳號狀態

```
PS C:\> Get-ADUser npartner -Properties MemberOf,PasswordNeverExpires,Enabled
```

A screenshot of a Windows PowerShell console window titled "Administrator: Windows PowerShell 的 Active Directory 模組". The console shows the output of the command to retrieve user properties for 'npartner'. The output lists various attributes such as DistinguishedName, Enabled, GivenName, MemberOf, Name, ObjectClass, ObjectGUID, PasswordNeverExpires, SamAccountName, SID, Surname, and UserPrincipalName.

```
Administrator: Windows PowerShell 的 Active Directory 模組
PS C:\> Get-ADUser npartner -Properties MemberOf,PasswordNeverExpires,Enabled

DistinguishedName      : CN=npartner,CN=Users,DC=npartner,DC=local
Enabled                : True
GivenName              :
MemberOf               : {}
Name                   : npartner
ObjectClass            : user
ObjectGUID             : 72bcb9e-46db-42e4-aae6-597e8c33cd73
PasswordNeverExpires  : True
SamAccountName         : npartner
SID                    : S-1-5-21-2487502702-2233515932-3288244281-1106
Surname                :
UserPrincipalName      : npartner@npartner.local

PS C:\> _
```

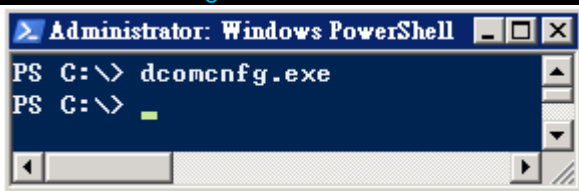

3.3.2 設定 DCOM 權限

(1) 開啟 [Windows PowerShell]



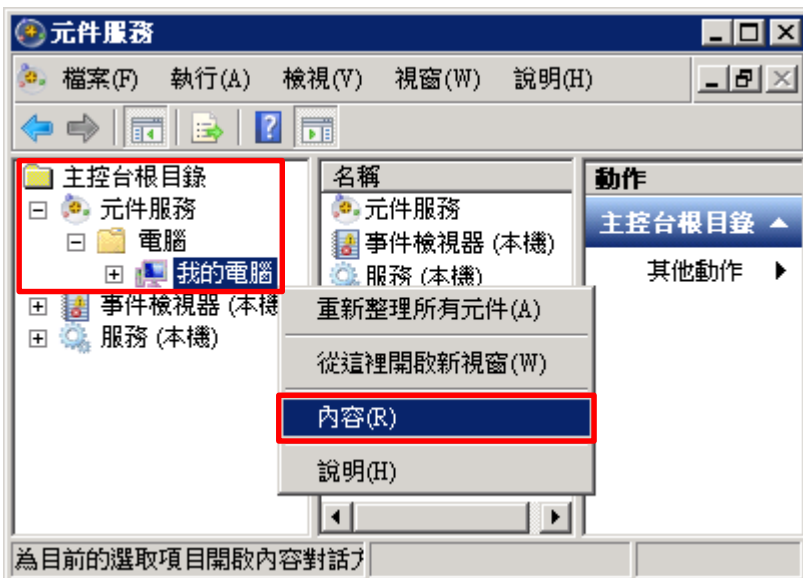
(2) 開啟元件服務

```
PS C:\> dcomcnfg.exe
```



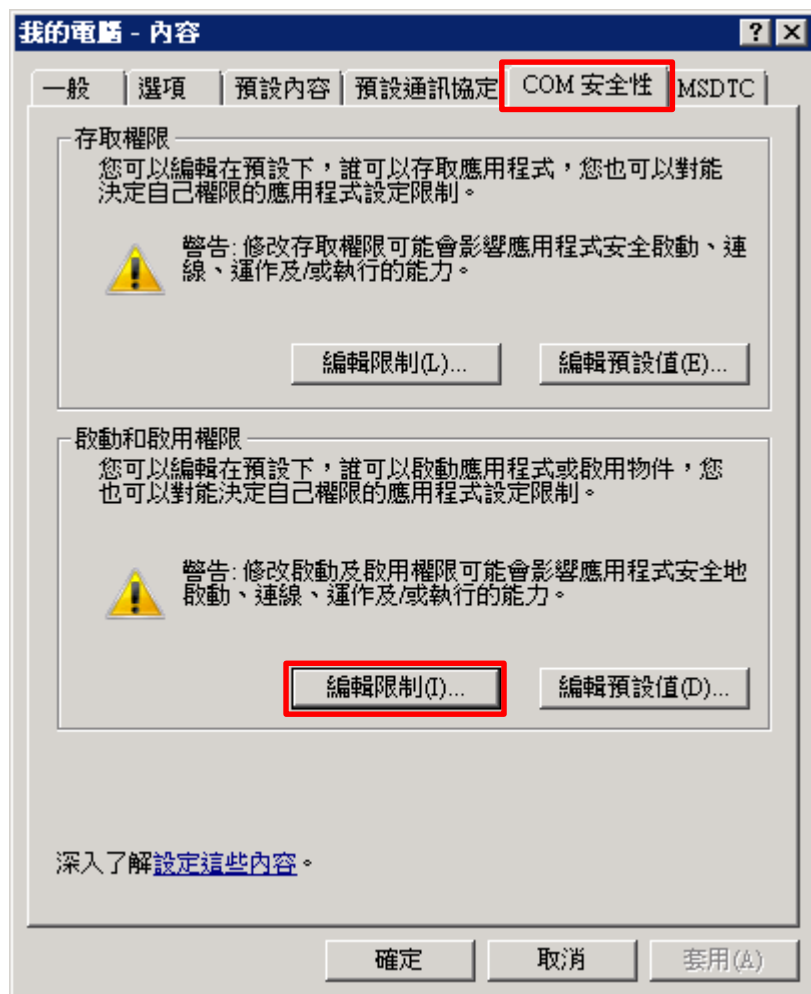
(3) 編輯電腦內容

展開 [主控台根目錄] -> [元件服務] -> [電腦] -> 在 [我的電腦] 按滑鼠右鍵 -> 點選 [內容]



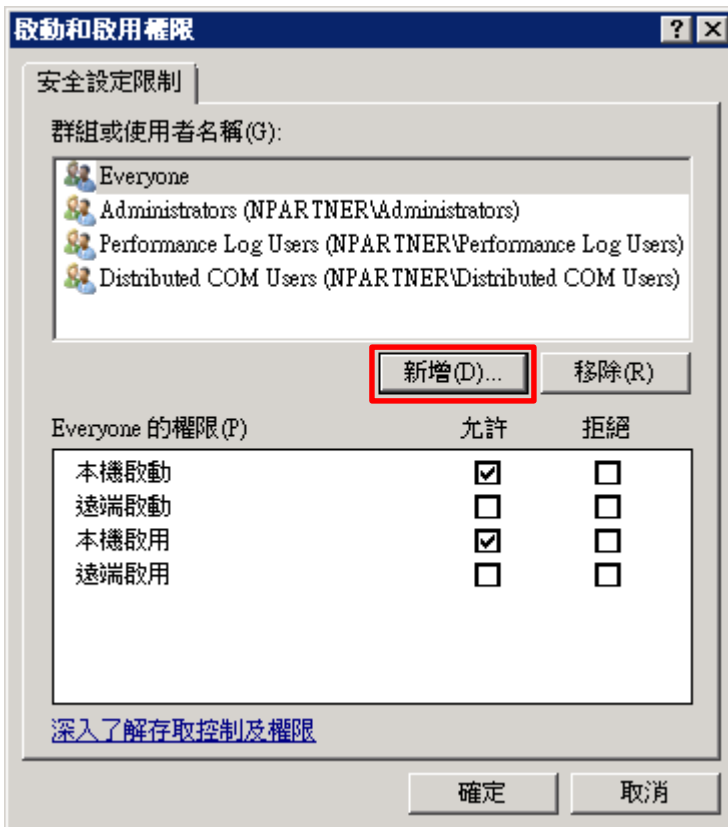
(4) 啟用權限

點選 [COM 安全性] 頁面 -> 啟動和啟用權限，按 [編輯限制]



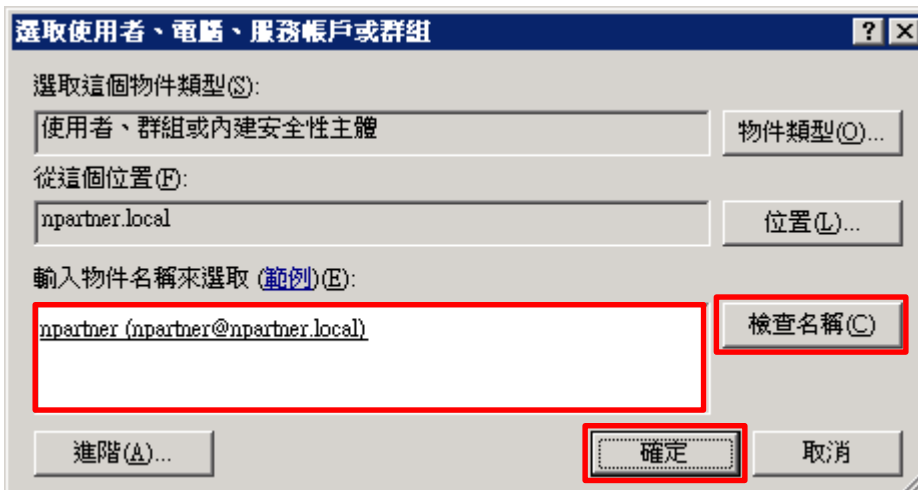
(5) 新增 DCOM 使用者權限

點選 [新增]



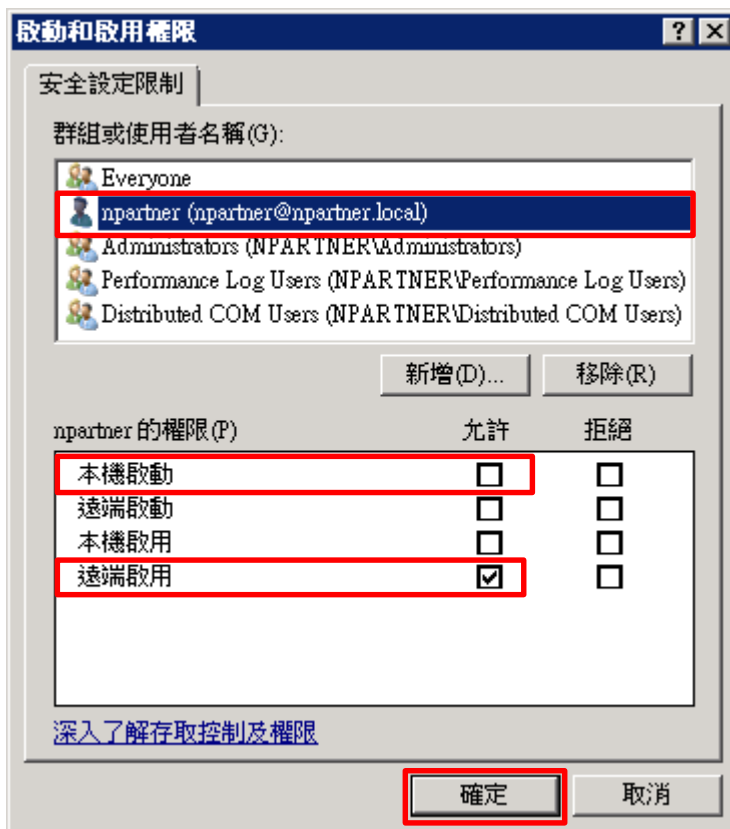
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

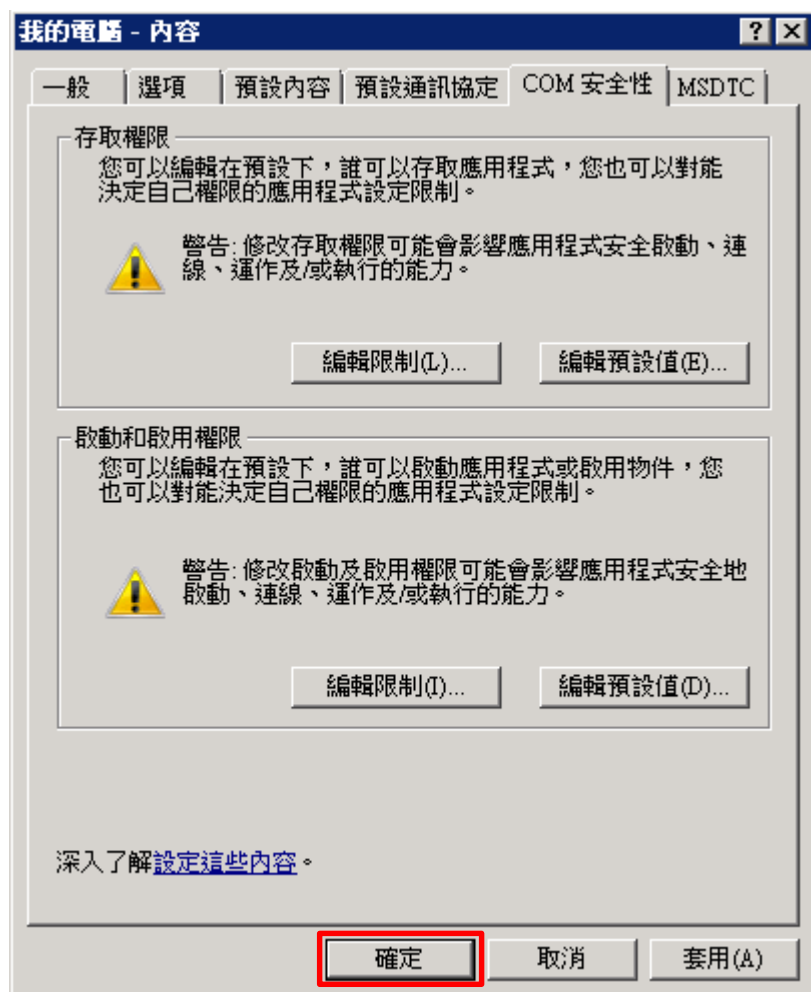


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [本機啟動:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



3.3.3 設定 WMI 權限

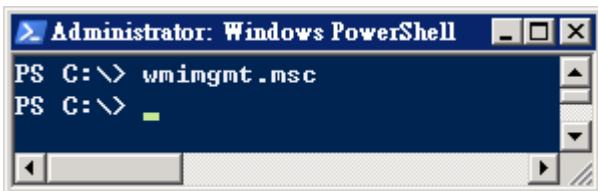
3.3.3.1 設定事件日誌權限

(1) 開啟 [Windows PowerShell]




(2) 開啟 WMI 控制

PS C:\> wimgmt.msc



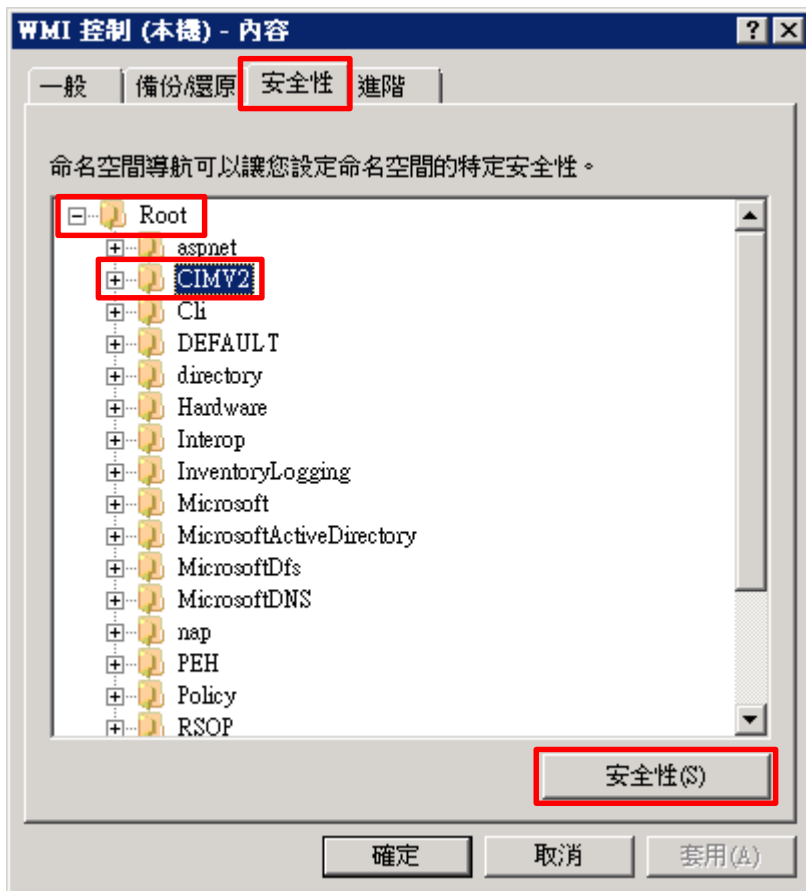
(3) 編輯 WMI 控制

點選 [WMI 控制 (本機)] -> 按  [內容]



(4) 編輯 CIMV2 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [CIMV2] -> 按 [安全性]



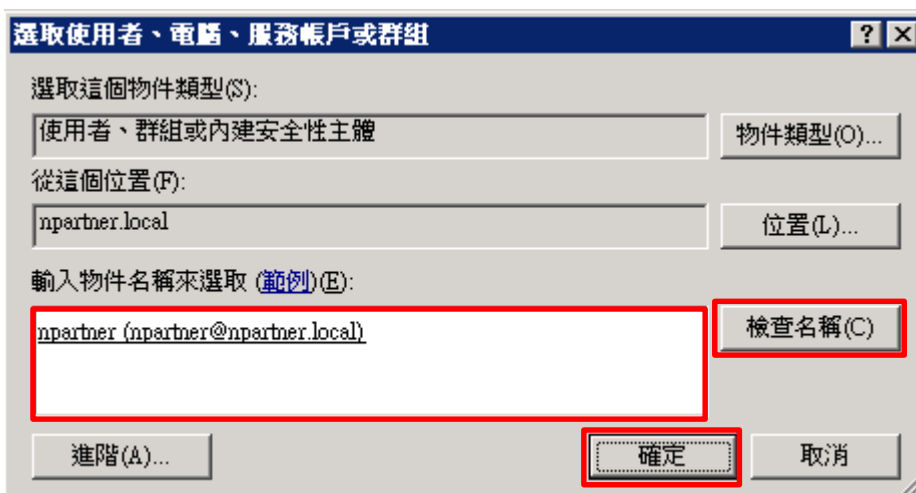
(5) 新增 WMI 使用者權限

按 [新增]



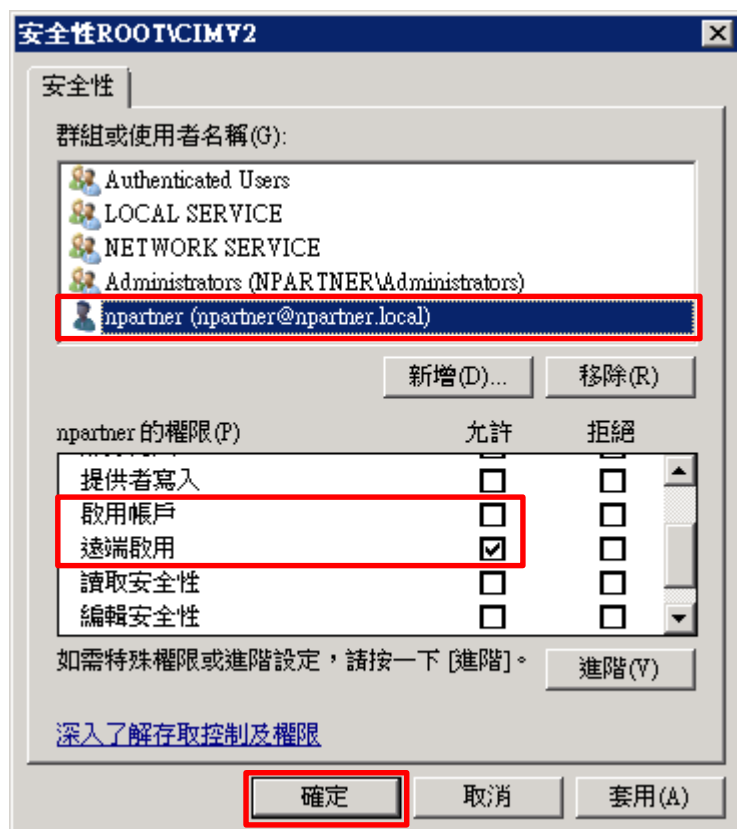
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

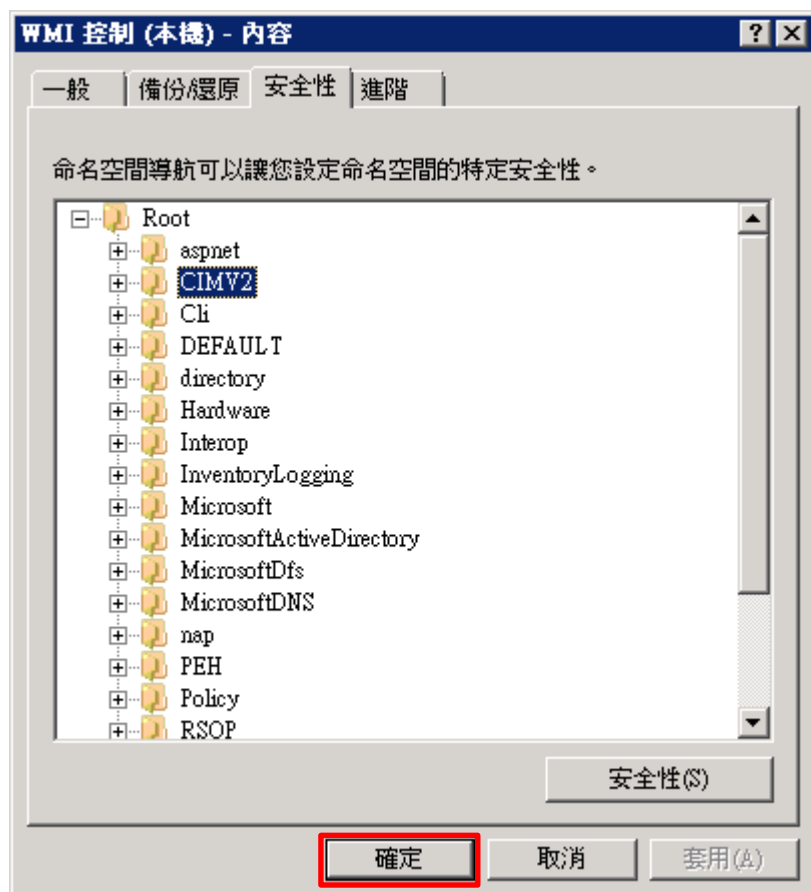


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



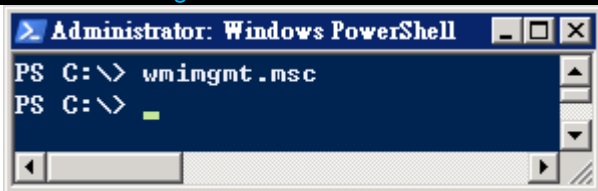
3.3.3.2 設定讀取使用者資料權限

(1) 開啟 [Windows PowerShell]



(2) 開啟元件服務

PS C:\> wimgmt.msc



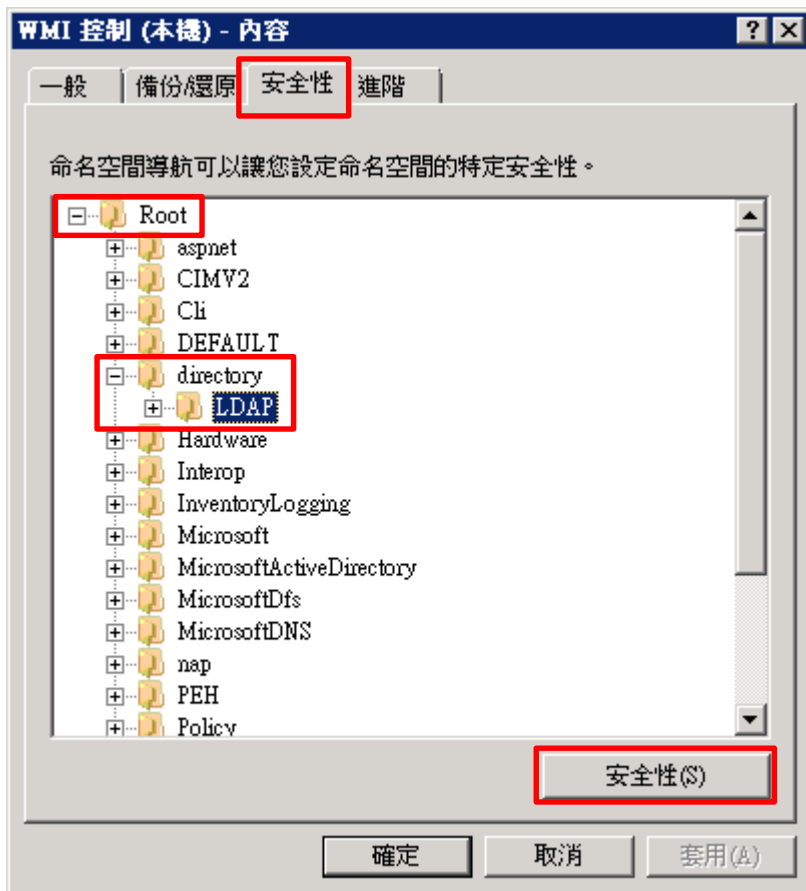
(3) 編輯 WMI 控制

點選 [WMI 控制 (本機)] -> 按 [內容]



(4) 編輯 LDAP 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [directory] -> [LDAP] -> 按 [安全性]



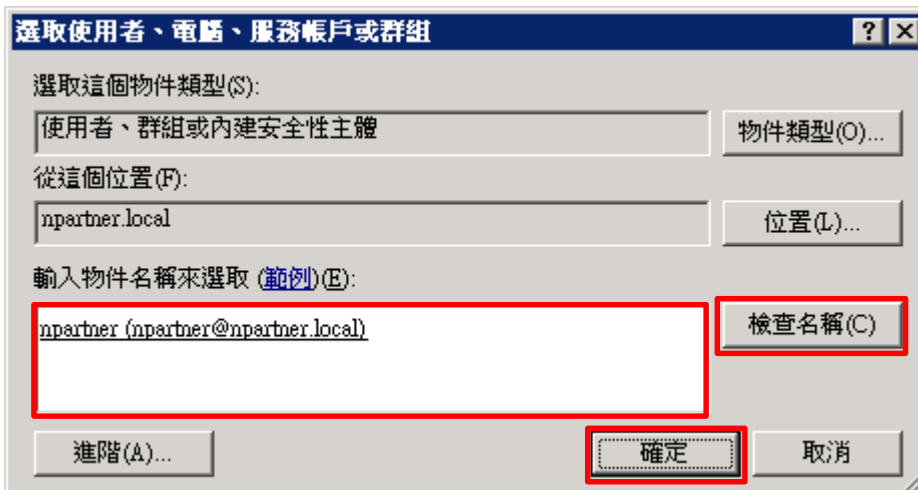
(5) 新增 WMI 使用者權限

按 [新增]



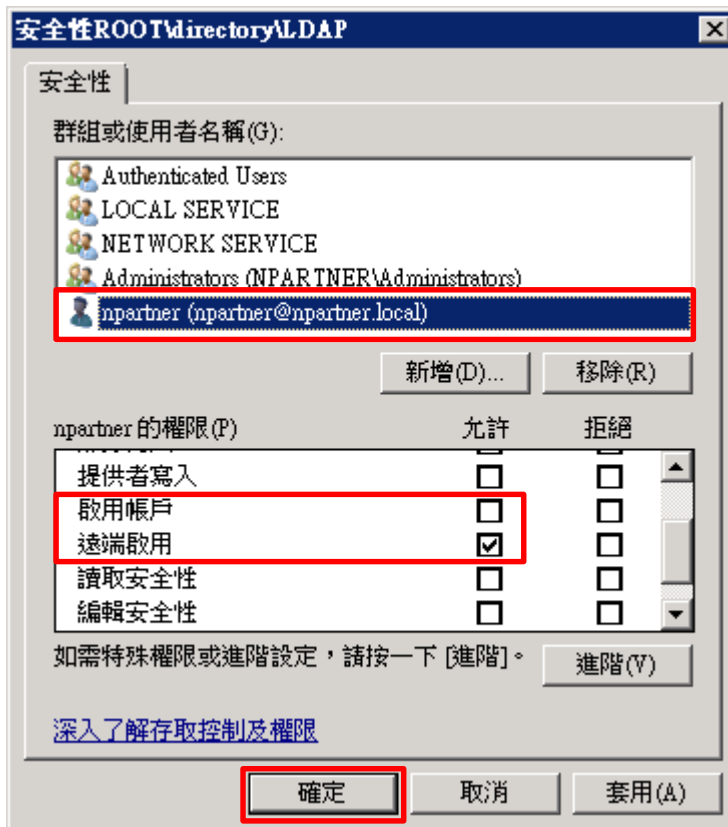
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

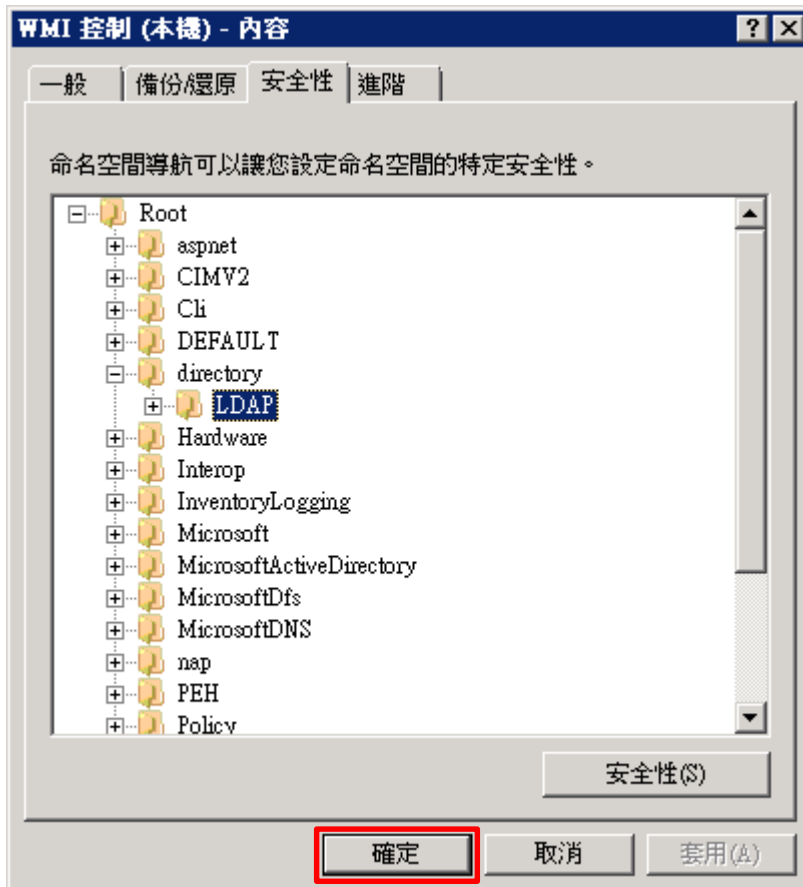


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



3.3.4 設定 Event log 讀取權限

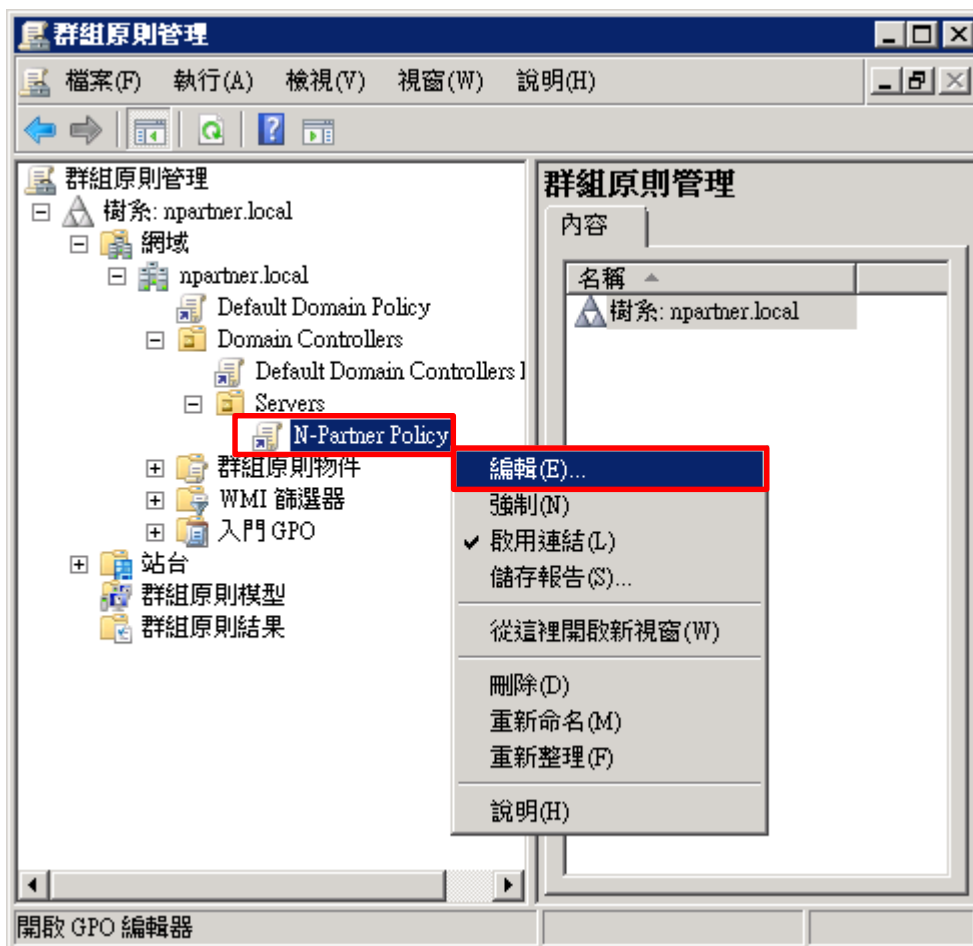
(1) 開啟群組原則管理

開啟 [群組原則管理]




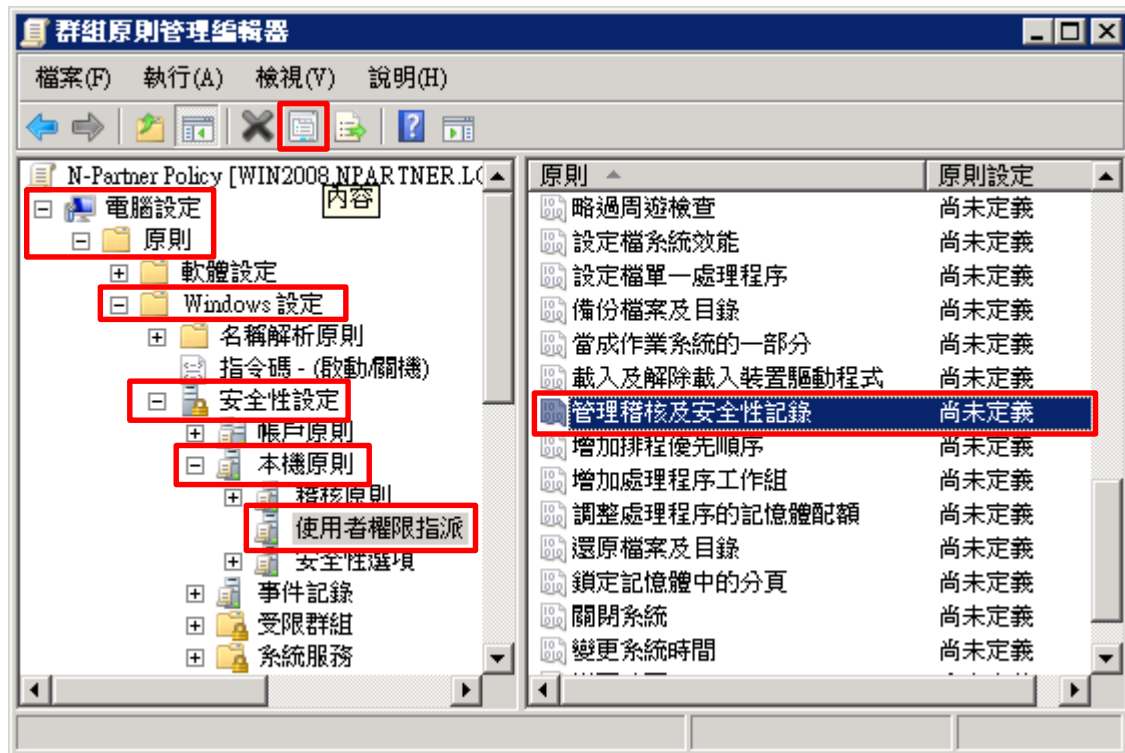
(2) 編輯群組原則物件

在 [N-Partner Policy] 群組原則物件，按滑鼠右鍵 -> 點選 [編輯]



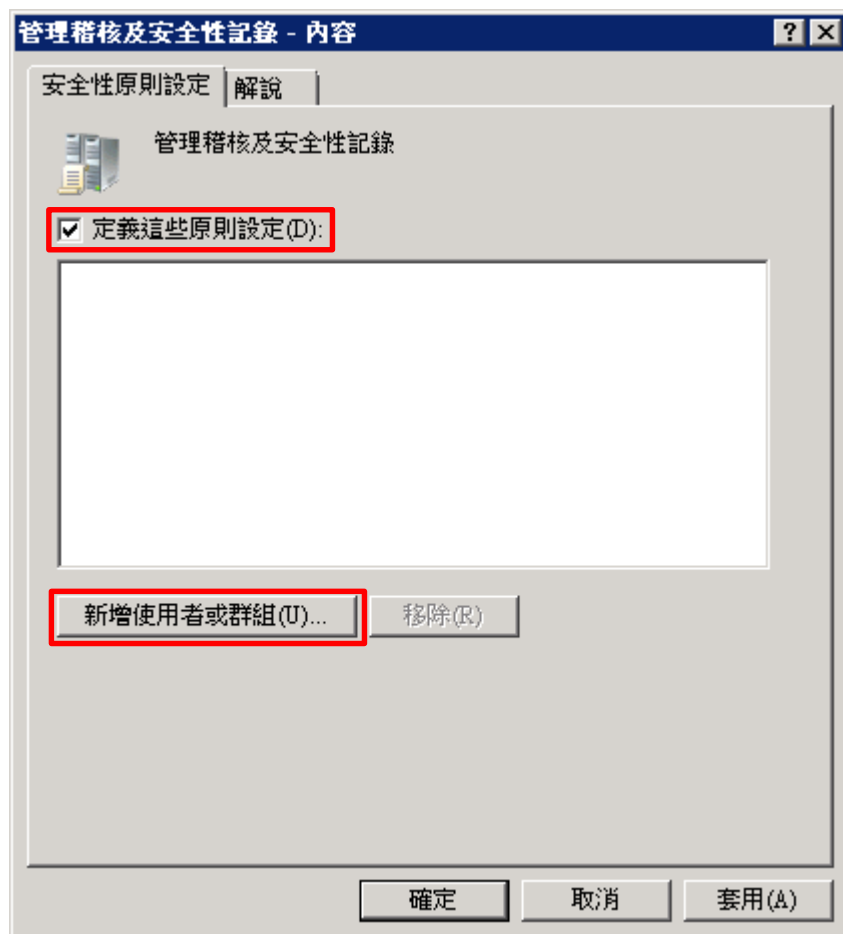
(3) 設定記錄檔

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [使用者權限指派] -> 選擇 [管理稽核及安全性記錄] 項目 -> 點選  內容



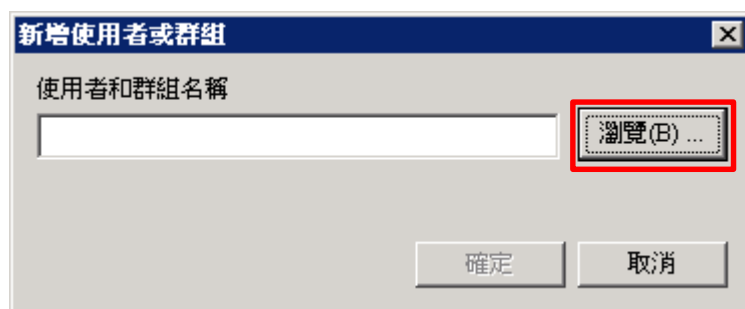
(4) 新增管理稽核使用者

勾選 [定義這些原則設定] -> 按 [新增使用者或群組...]



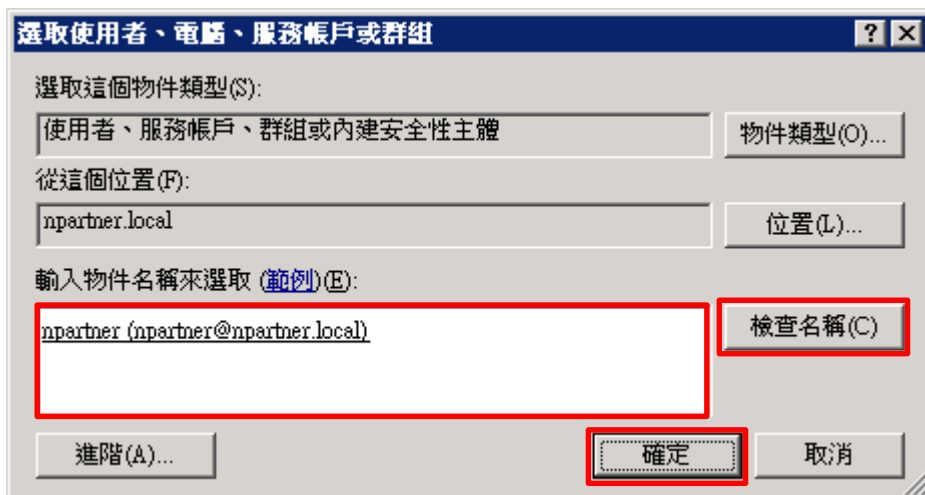
(5) 搜尋使用者

按 [瀏覽]



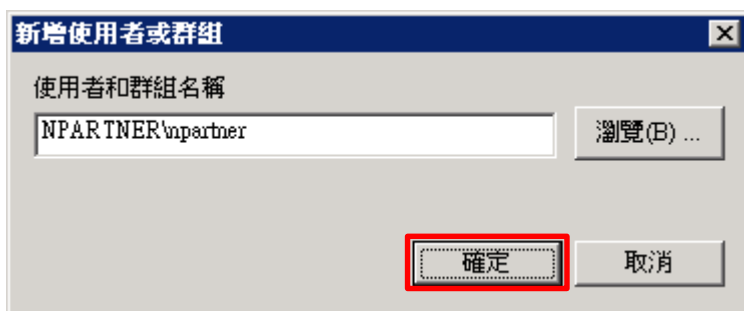
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]



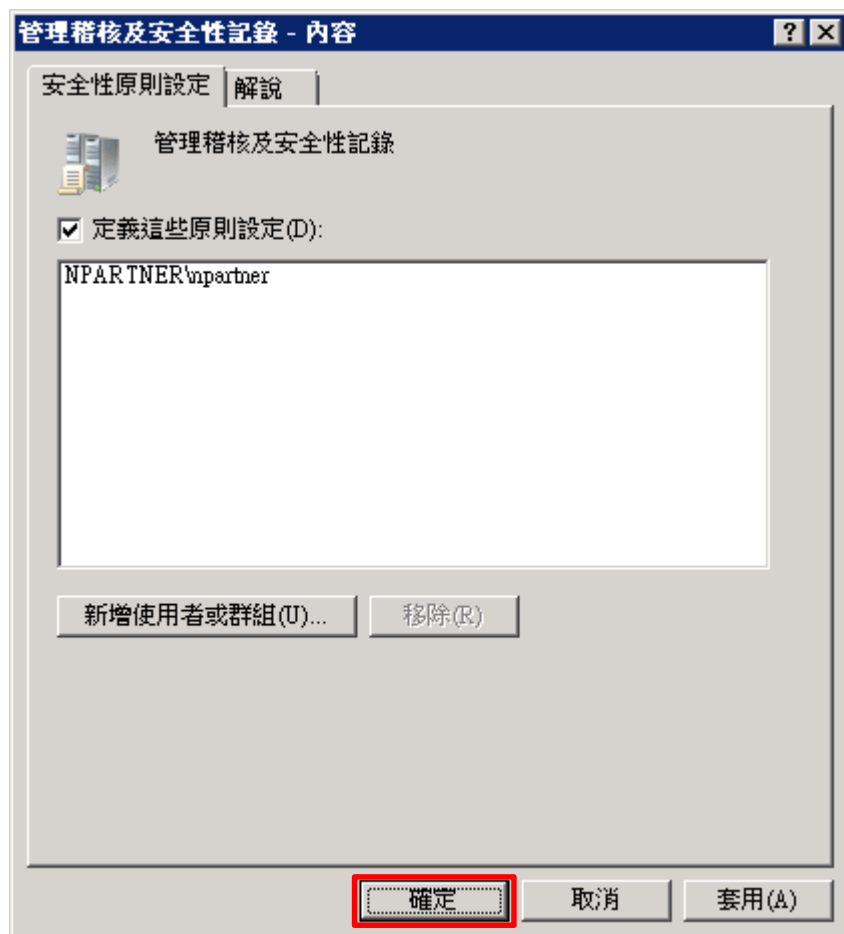
(7) 確定使用者

按 [確定]



(8) 確定設定記錄檔

按 [確定]

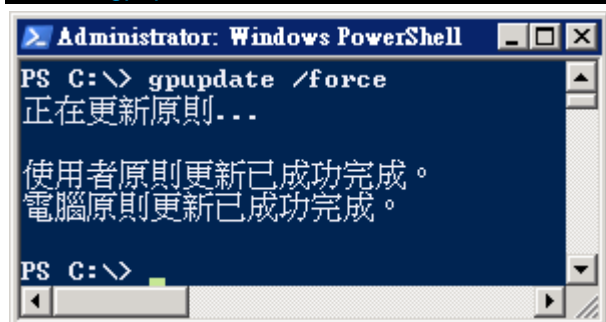


(9) 開啟 [Windows PowerShell]



(10) 更新群組原則

```
PS C:\> gpupdate /force
```



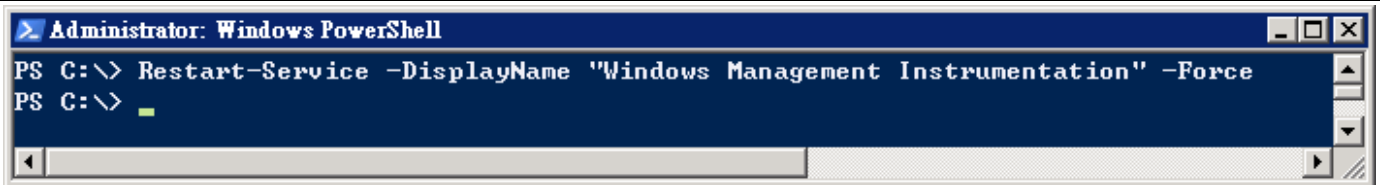
3.3.5 重啟 WMI 服務

(1) 開啟 [Windows PowerShell]



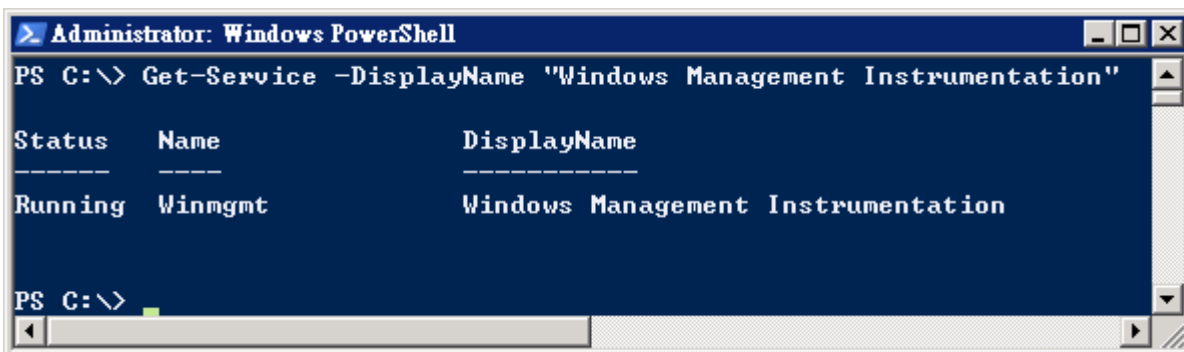
(2) 重啟 WMI 服務

```
PS C:\> Restart-Service -DisplayName "Windows Management Instrumentation" -Force
```



(3) 查看 WMI 服務

```
PS C:\> Get-Service -DisplayName "Windows Management Instrumentation"
```



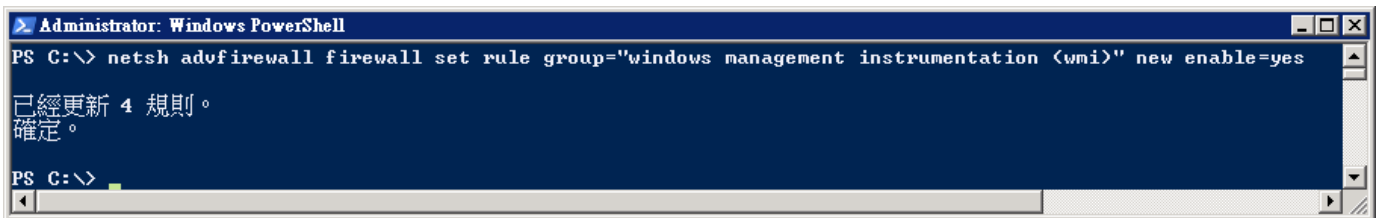
3.4 設定防火牆

(1) 開啟 [Windows PowerShell]



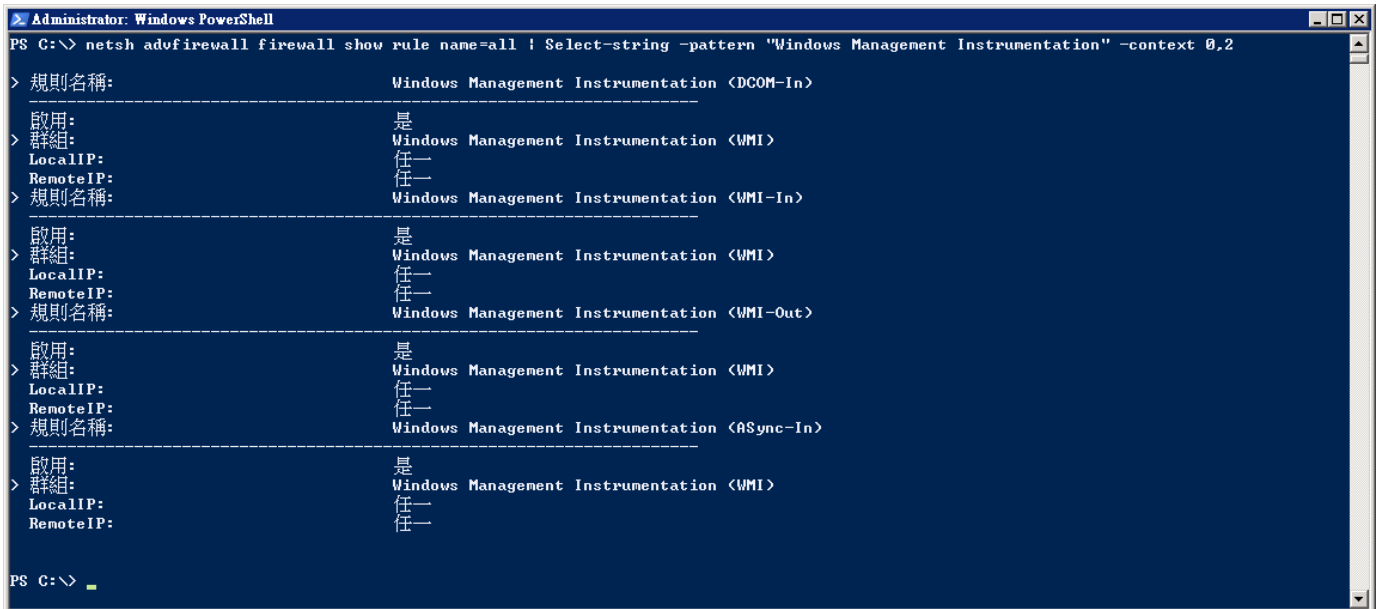
(2) 允許 WMI 通過防火牆

```
PS C:\> netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
```



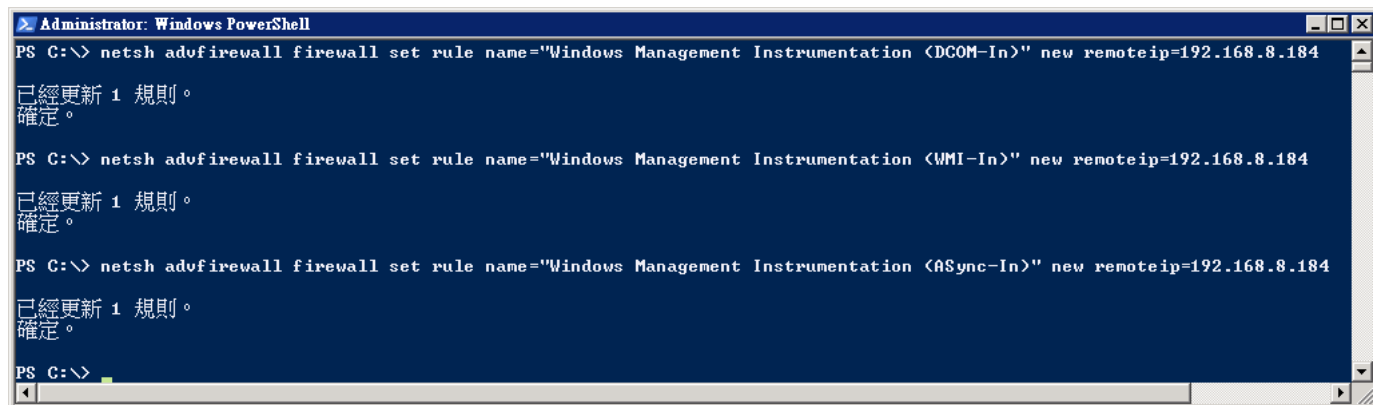
(3) 查看防火牆 WMI 啟用狀態

```
PS C:\> netsh advfirewall firewall show rule name=all | Select-string -pattern "Windows Management Instrumentation" -context 0,2
```



(4) 設定防火牆 · 只允許 N-Reporter IP query WMI

```
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (DCOM-In)" new remoteip=192.168.8.184
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (WMI-In)" new remoteip=192.168.8.184
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (ASync-In)" new remoteip=192.168.8.184
```



```
Administrator: Windows PowerShell
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (DCOM-In)" new remoteip=192.168.8.184
已經更新 1 規則。
確定。

PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (WMI-In)" new remoteip=192.168.8.184
已經更新 1 規則。
確定。

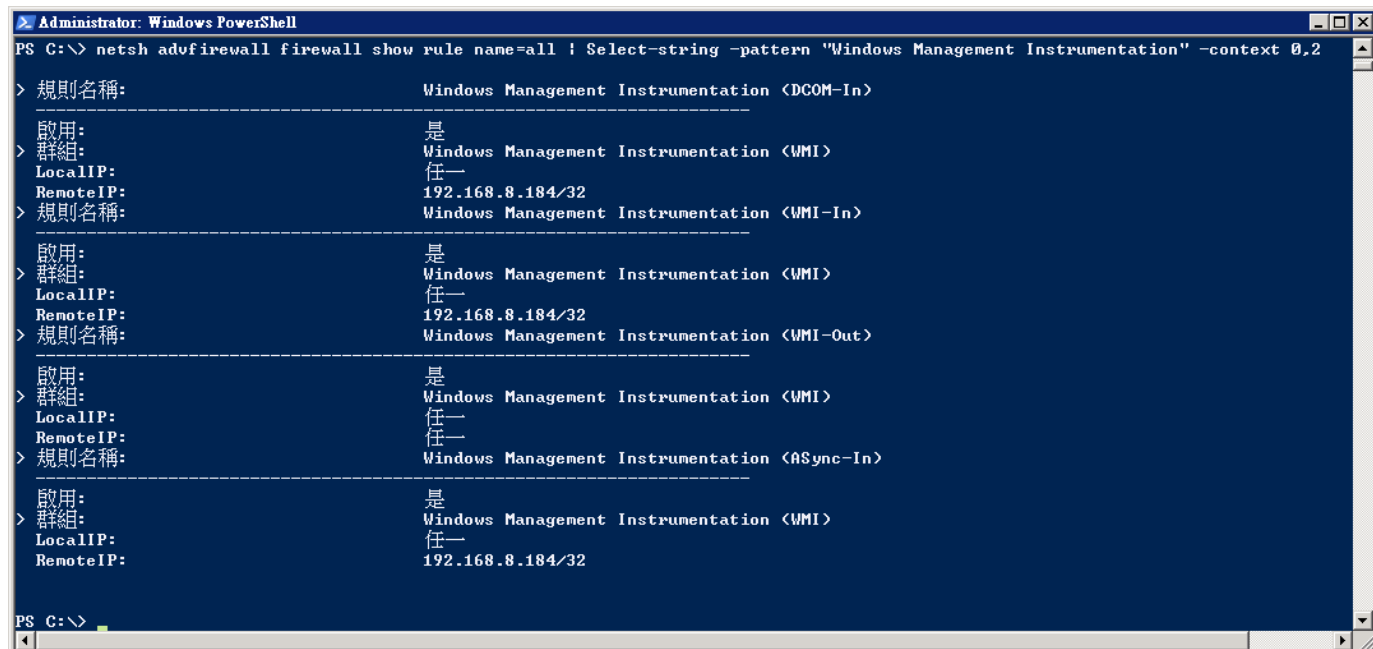
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (ASync-In)" new remoteip=192.168.8.184
已經更新 1 規則。
確定。

PS C:\>
```

紅色文字部位請輸入 N-Reporter IP address

(5) 查看防火牆 WMI 設定狀態

```
PS C:\> netsh advfirewall firewall show rule name=all | Select-string -pattern "Windows Management Instrumentation" -context 0,2
```



```
Administrator: Windows PowerShell
PS C:\> netsh advfirewall firewall show rule name=all | Select-string -pattern "Windows Management Instrumentation" -context 0,2
> 規則名稱: Windows Management Instrumentation (DCOM-In)
-----
  啟用: 是
  群組: Windows Management Instrumentation (WMI)
  LocalIP: 任一
  RemoteIP: 192.168.8.184/32
> 規則名稱: Windows Management Instrumentation (WMI-In)
-----
  啟用: 是
  群組: Windows Management Instrumentation (WMI)
  LocalIP: 任一
  RemoteIP: 192.168.8.184/32
> 規則名稱: Windows Management Instrumentation (WMI-Out)
-----
  啟用: 是
  群組: Windows Management Instrumentation (WMI)
  LocalIP: 任一
  RemoteIP: 任一
> 規則名稱: Windows Management Instrumentation (ASync-In)
-----
  啟用: 是
  群組: Windows Management Instrumentation (WMI)
  LocalIP: 任一
  RemoteIP: 192.168.8.184/32

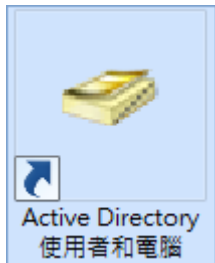
PS C:\>
```

4. Windows 2012

Windows 稽核原則設定 [詳細說明請參考前言的稽核原則建議連結](#)

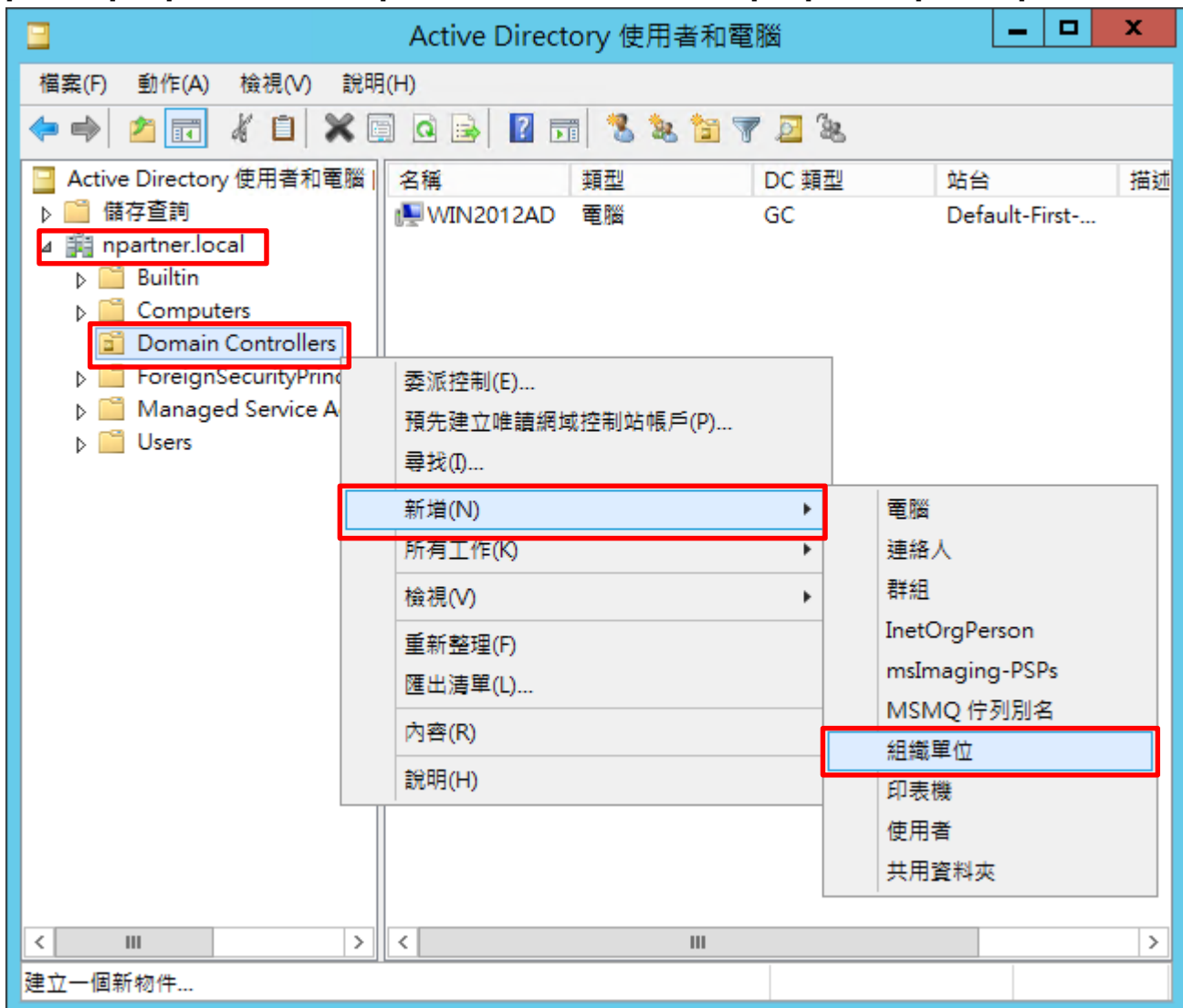
4.1 組織單位設定

(1) 開啟 [Active Directory 使用者和電腦]



(2) 新增組織單位

[網域名稱] 的 [Domain Controllers] 組織單位，按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]



(3) 輸入組織單位名稱

輸入組織單位名稱: Servers 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



新增物件 - 組織單位

建立在: npartner.local/Domain Controllers

名稱(A):
Servers

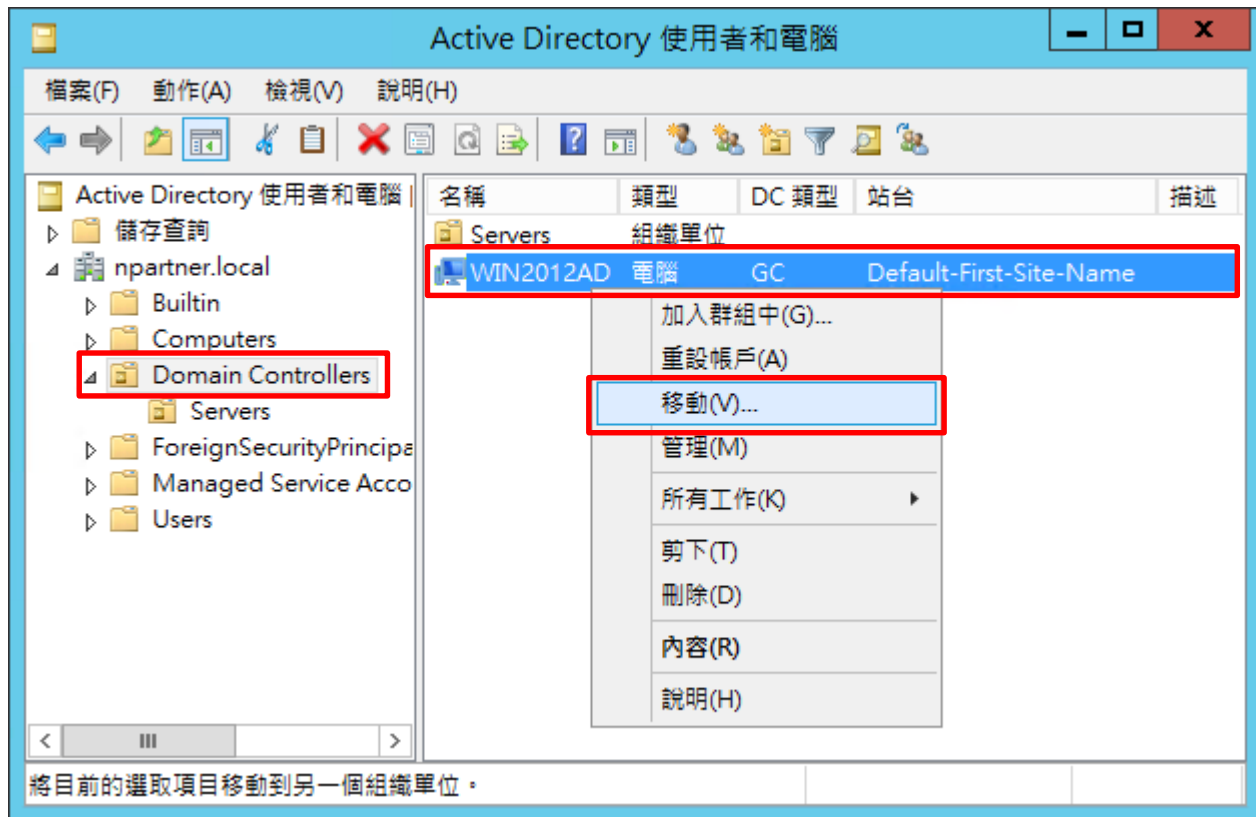
保護容器以防止被意外刪除(P)

確定 取消 說明

(4) 移動伺服器至新的組織單位

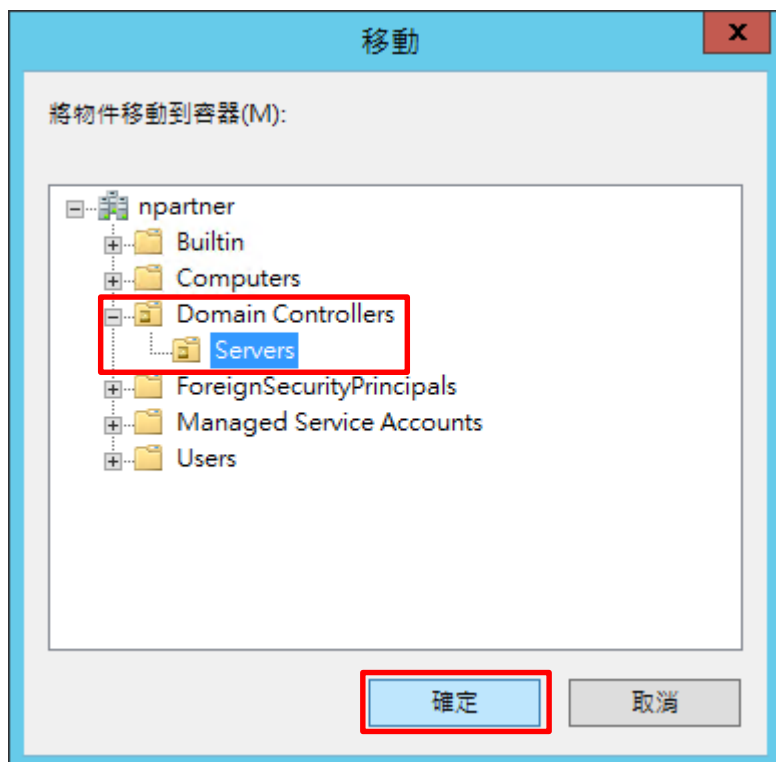
選擇 [Domain Controllers] 組織單位 -> 在 [Win2012AD] 按滑鼠右鍵 · 註：請依客戶環境選擇 Windows AD 主機

-> 點選 [移動]



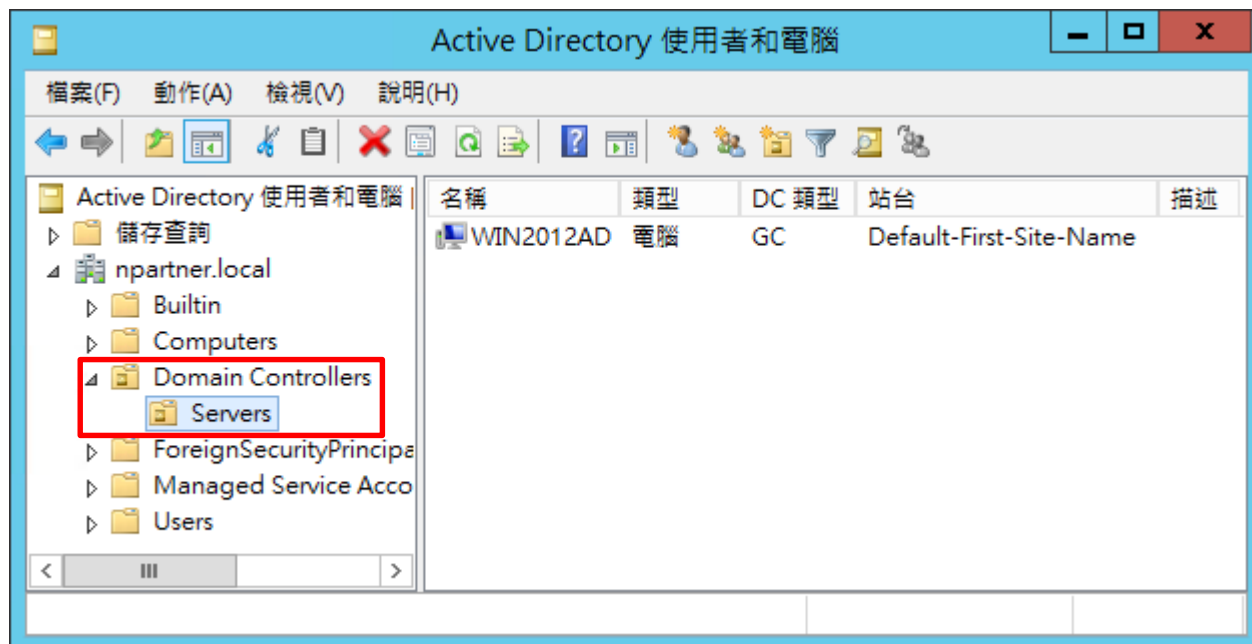
(5) 選擇組織單位

選擇 [Domain Controllers] 的 [Servers] 組織單位 -> 按 [確定]



(6) 確認伺服器已移動至新的組織單位

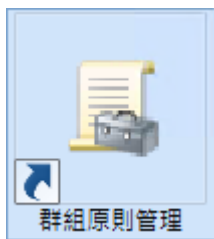
展開 [Domain Controllers] 的 [Servers] 組織單位，確認 [Win2012AD] 伺服器已移動



4.2 群組原則設定

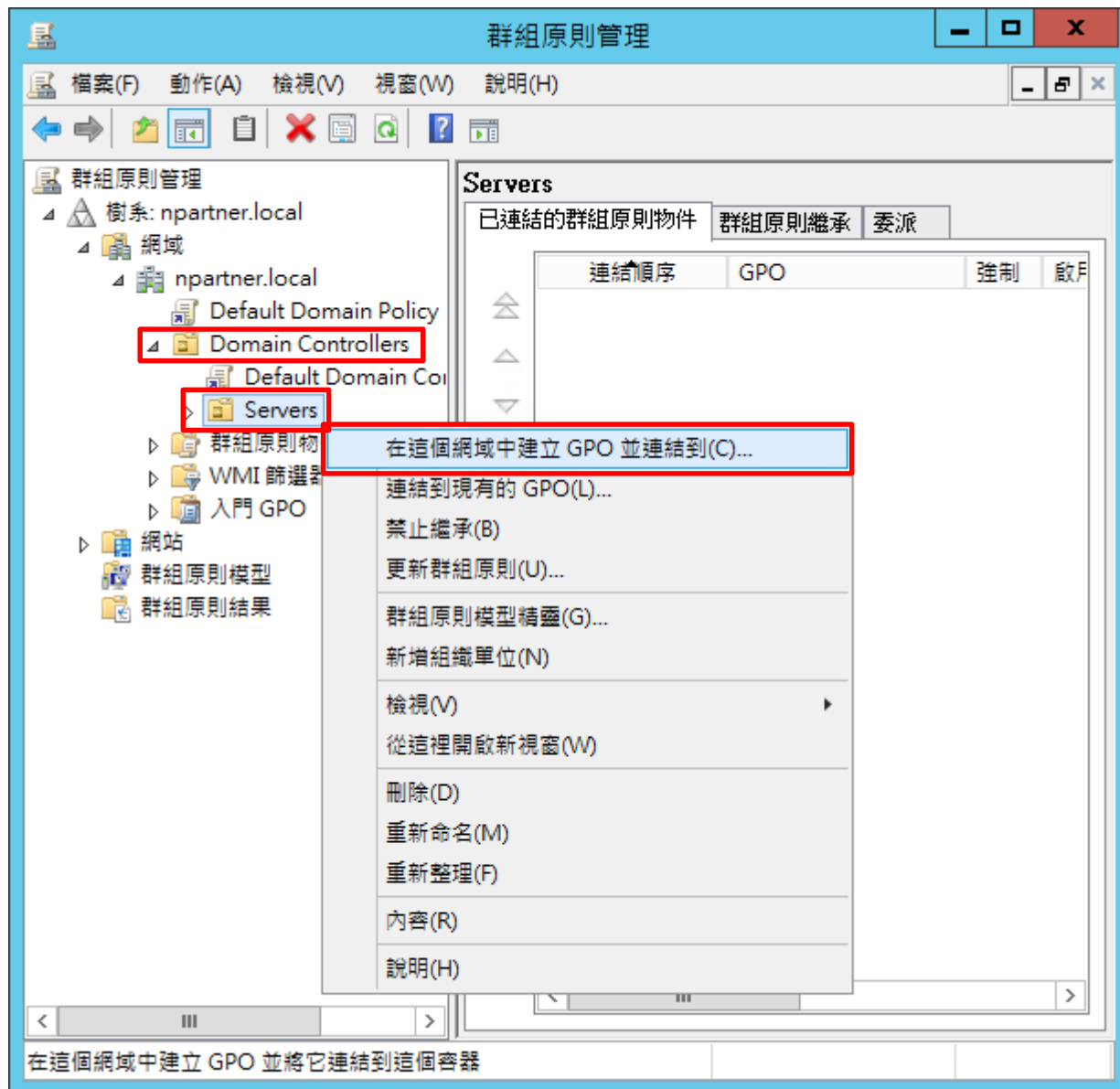
(1) 開啟群組原則管理

開啟 [群組原則管理]



(2) 在 Servers 組織單位，新增群組原則物件

在 [Domain Controllers] 的 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到...]



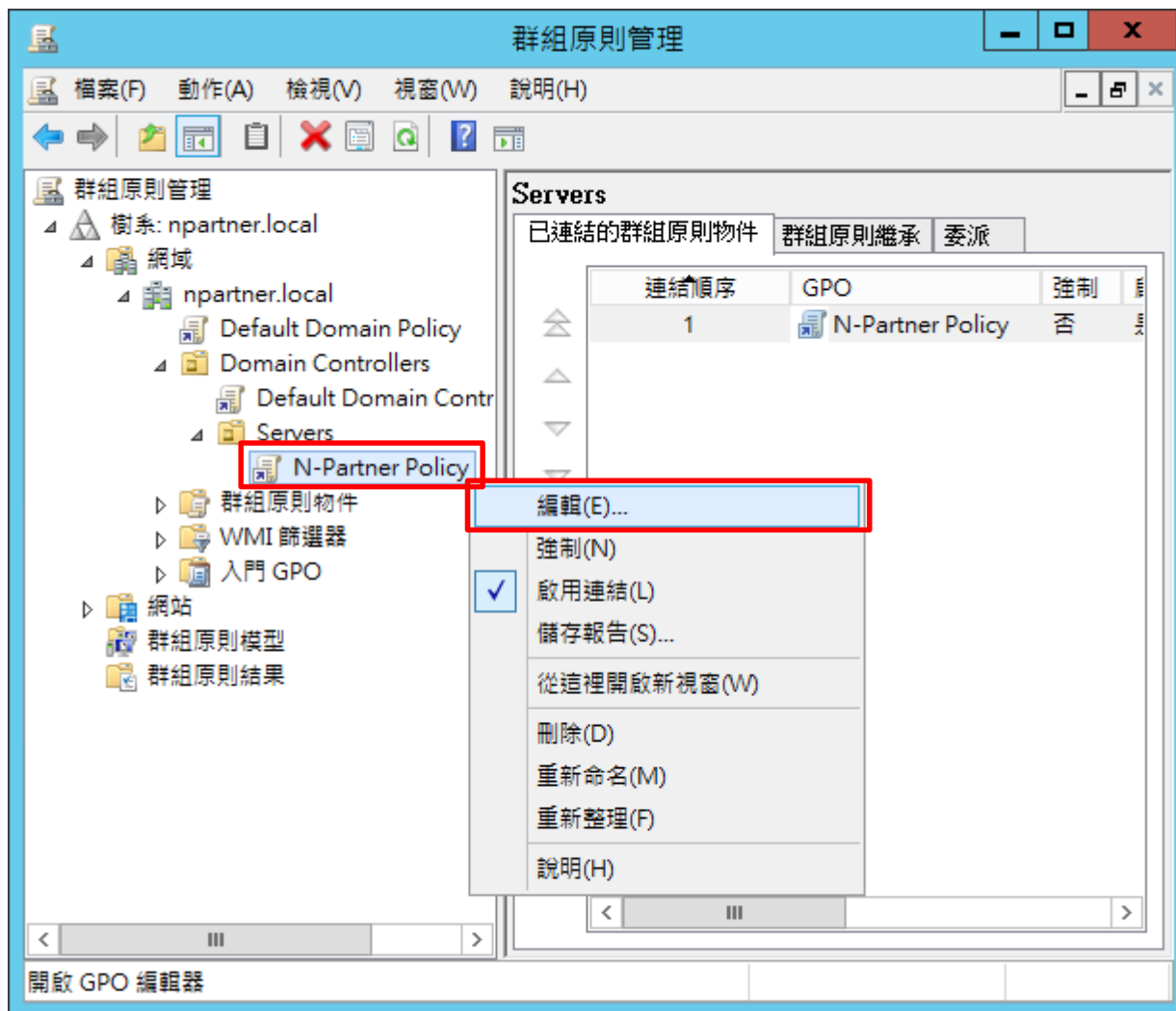
(3) 輸入群組原則物件名稱

輸入群組原則物件名稱: N-Partner Policy 註：請依客戶環境建立群組物件名稱 -> 按 [確定]



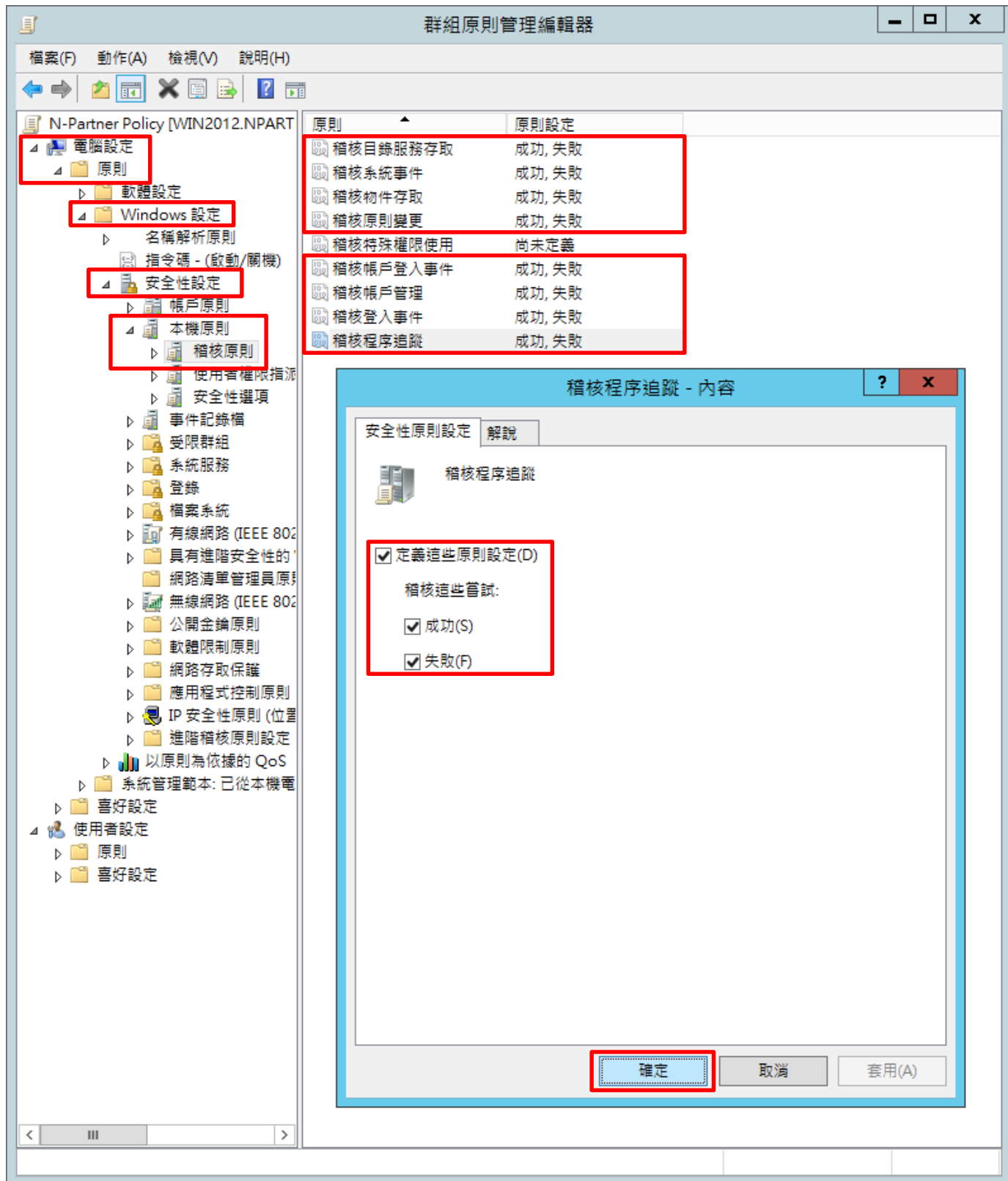
(4) 編輯群組原則物件

在 [N-Partner Policy] 群組原則物件 · 按滑鼠右鍵 -> 點選 [編輯]



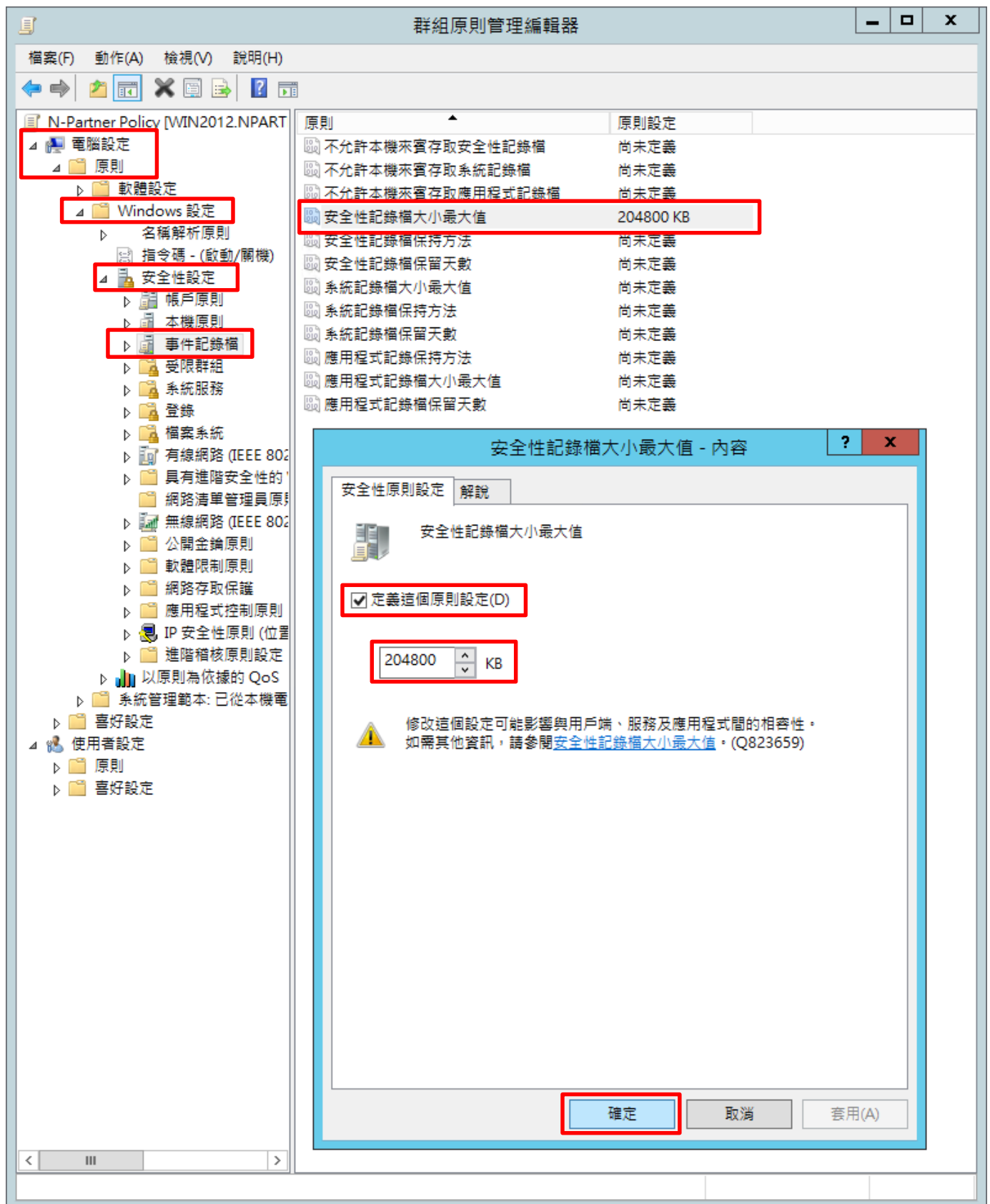
(5) 本機原則：稽核原則

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核目錄服務存取], [稽核系統事件], [稽核物件存取], [稽核原則變更], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件], [稽核程序追蹤] 項目 -> 勾選 [定義這些原則設定:] & [成功] & [失敗] -> 按 [確定]



(6) 事件記錄：安全性記錄檔大小最大值

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔大小最大值] 項目 -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]

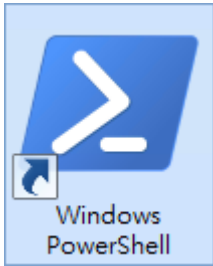


(7) 事件記錄：安全性記錄檔大小最大值

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔保持方法] 項目 -> 勾選 [定義這個原則設定] -> 點選 [視需要覆寫事件] -> 按 [確定]

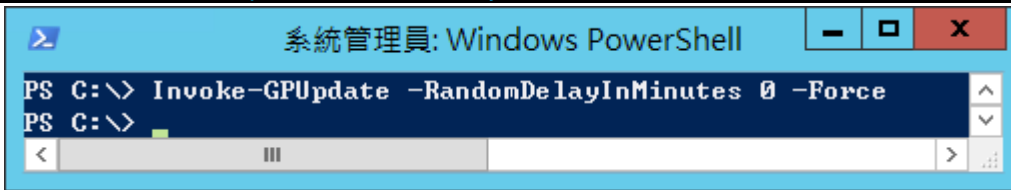


(8) 開啟 [Windows PowerShell]



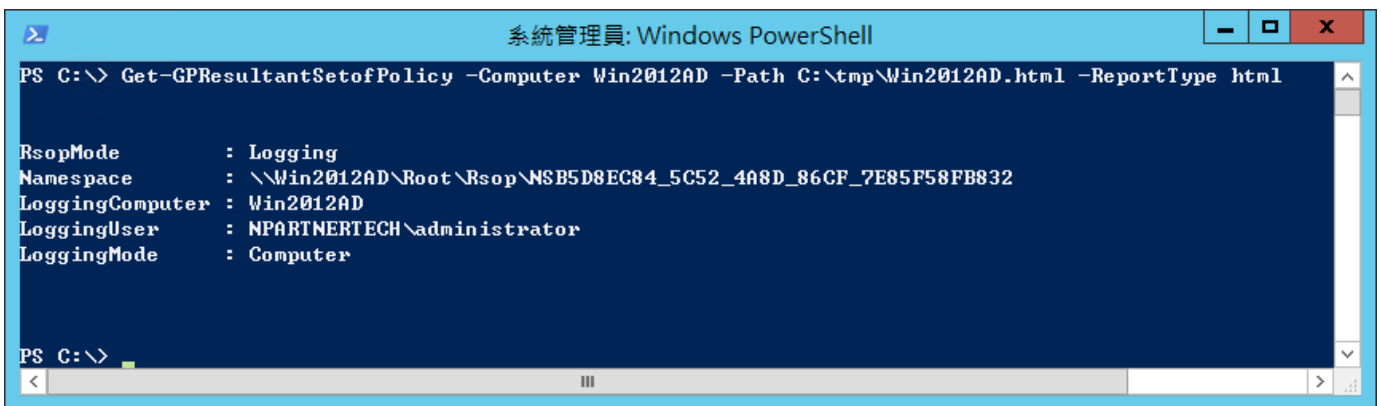
(9) 更新群組原則

PS C:\> `Invoke-GPUdate -RandomDelayInMinutes 0 -Force`



(10) 產生伺服器群組原則報表

PS C:\> `Get-GPResultantSetofPolicy -Computer Win2012AD -Path C:\tmp\Win2012AD.html -ReportType html`



紅色文字部位請輸入 Windows AD 伺服器名稱和資料夾路徑檔案名稱

(11) 開啟報表 · 確認 Windows 2012 AD 伺服器 · 套用 N-Partner Policy 群組原則

群組原則結果

NPARTNER\WIN2012AD
資料收集: 2021/5/14 下午 05:04:43

顯示全部

摘要 顯示

電腦詳細資料 隱藏

一般 顯示

元件狀態 顯示

設定 隱藏

原則 隱藏

Windows 設定 隱藏

安全性設定 隱藏

帳戶原則/密碼規則 顯示

帳戶原則/帳戶鎖定原則 顯示

帳戶原則/Kerberos 原則 顯示

本機原則/稽核原則 隱藏

原則	設定	優勢 GPO
稽核目錄服務存取	成功, 失敗	N-Partner Policy
稽核系統事件	成功, 失敗	N-Partner Policy
稽核物件存取	成功, 失敗	N-Partner Policy
稽核原則變更	成功, 失敗	N-Partner Policy
稽核帳戶登入事件	成功, 失敗	N-Partner Policy
稽核帳戶管理	成功, 失敗	N-Partner Policy
稽核登入事件	成功, 失敗	N-Partner Policy
稽核程序追蹤	成功, 失敗	N-Partner Policy

本機原則/使用者權限指派 顯示

本機原則/安全性選項 顯示

事件記錄檔 隱藏

原則	設定	優勢 GPO
安全性記錄檔保持方法	視需要而定	N-Partner Policy
安全性記錄檔容量最大值	204800 KB	N-Partner Policy

公開金鑰原則/憑證服務用戶端 - 自動註冊設定 顯示

公開金鑰原則/加密檔案系統 顯示

群組原則物件 顯示

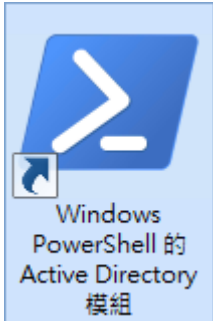
WMI 篩選器 顯示

使用者詳細資料 顯示

4.3 新增非管理帳號

4.3.1 新增使用者

(1) 開啟 [Windows PowerShell 的 Active Directory 模組]



(2) 新增帳號

```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" `
>> -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -
AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True
```

```
系統管理員: Windows PowerShell 的 Active Directory 模組
PS C:\Users\Administrator> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" `
>> -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True
PS C:\Users\Administrator>
```

紅色文字部位請輸入帳號密碼及網域資訊

(3) 查看帳號狀態

```
PS C:\> Get-ADUser npartner -Properties MemberOf,PasswordNeverExpires,Enabled
```

```
系統管理員: Windows PowerShell 的 Active Directory 模組
PS C:\Users\Administrator> Get-ADUser npartner -Properties MemberOf,PasswordNeverExpires,Enabled

DistinguishedName      : CN=npartner,CN=Users,DC=npartner,DC=local
Enabled                 : True
GivenName               :
MemberOf                : {}
Name                   : npartner
ObjectClass             : user
ObjectGUID              : ac23ae29-1ec8-444a-8075-4861157e4d4c
PasswordNeverExpires   : True
SamAccountName          : npartner
SID                     : S-1-5-21-637894504-1246074459-1714703841-1105
Surname                 :
UserPrincipalName       : npartner@npartner.local

PS C:\Users\Administrator>
```

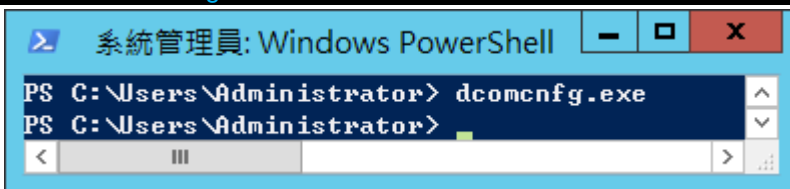
4.3.2 設定 DCOM 權限

(1) 開啟 [Windows PowerShell]



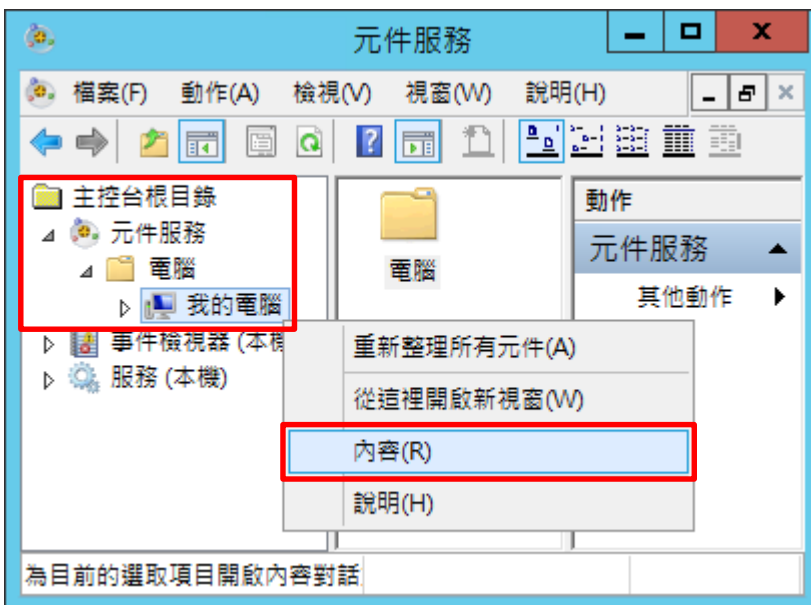
(2) 開啟元件服務

PS C:\> dcomcnfg.exe



(3) 編輯電腦內容

展開 [主控台根目錄] -> [元件服務] -> [電腦] -> 在 [我的電腦] 按滑鼠右鍵 -> 點選 [內容]



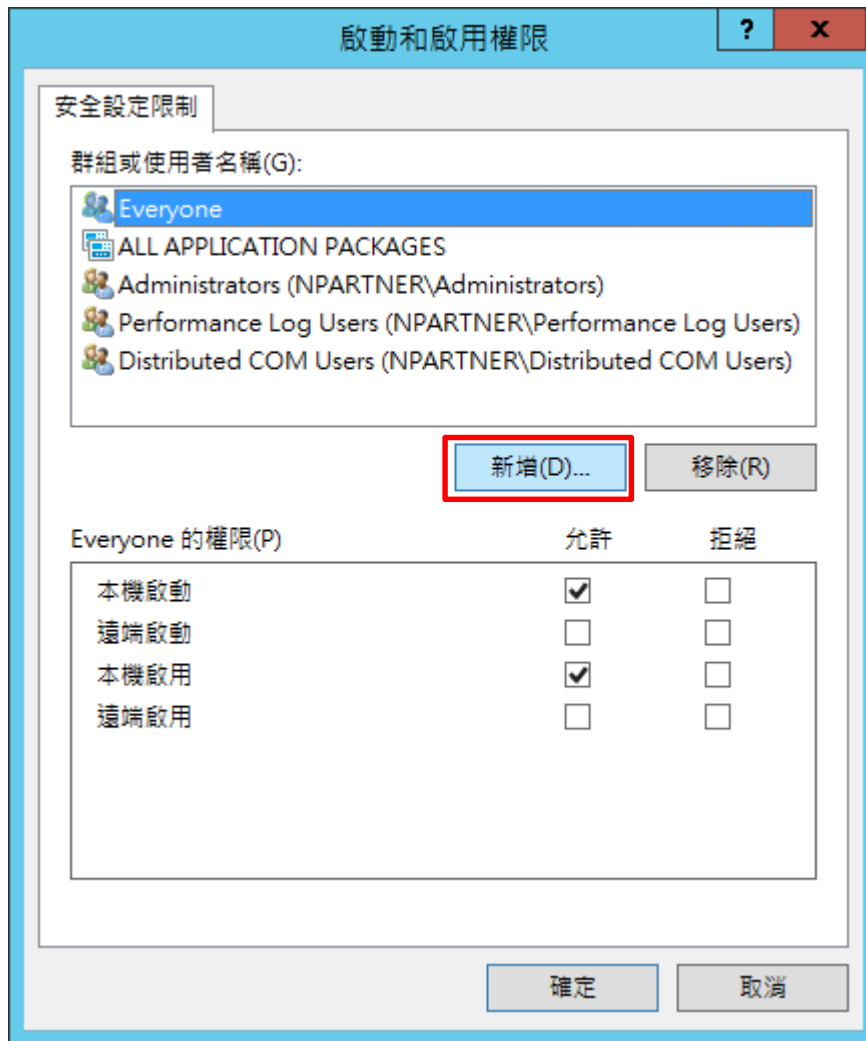
(4) 啟用權限

點選 [COM 安全性] 頁面 -> 啟動和啟用權限，按 [編輯限制]



(5) 新增 DCOM 使用者權限

點選 [新增]



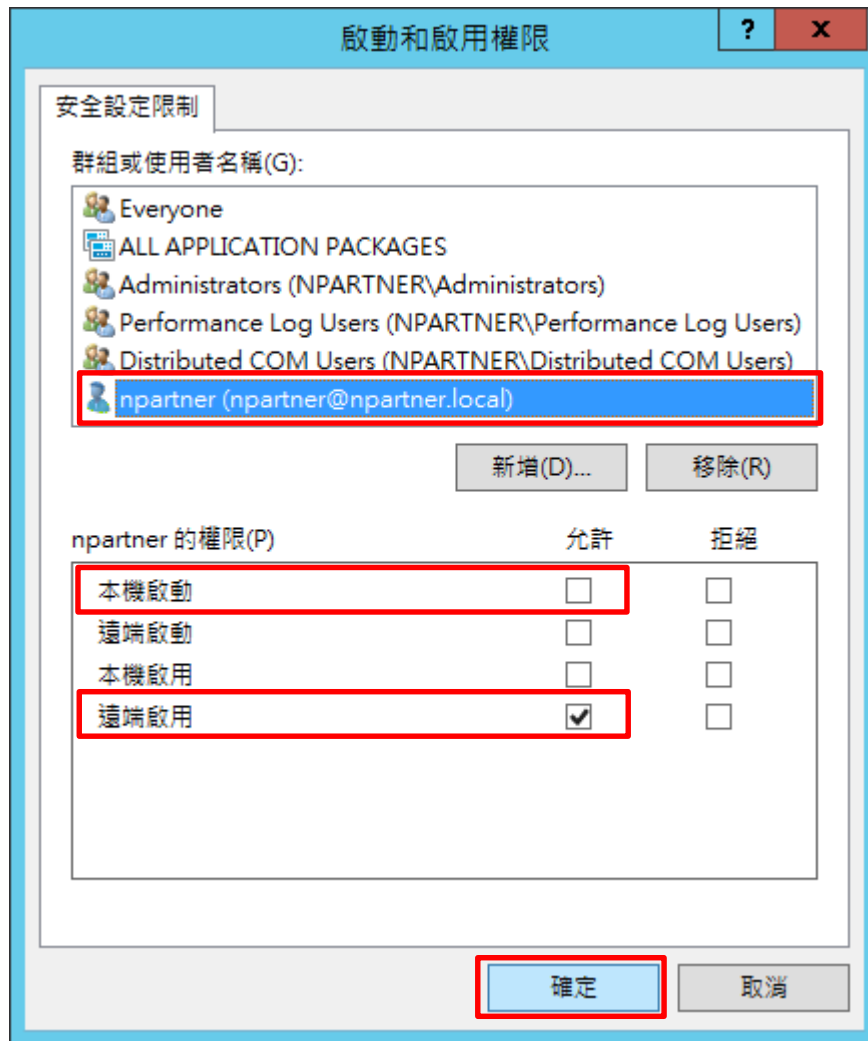
(6) 輸入使用者

輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

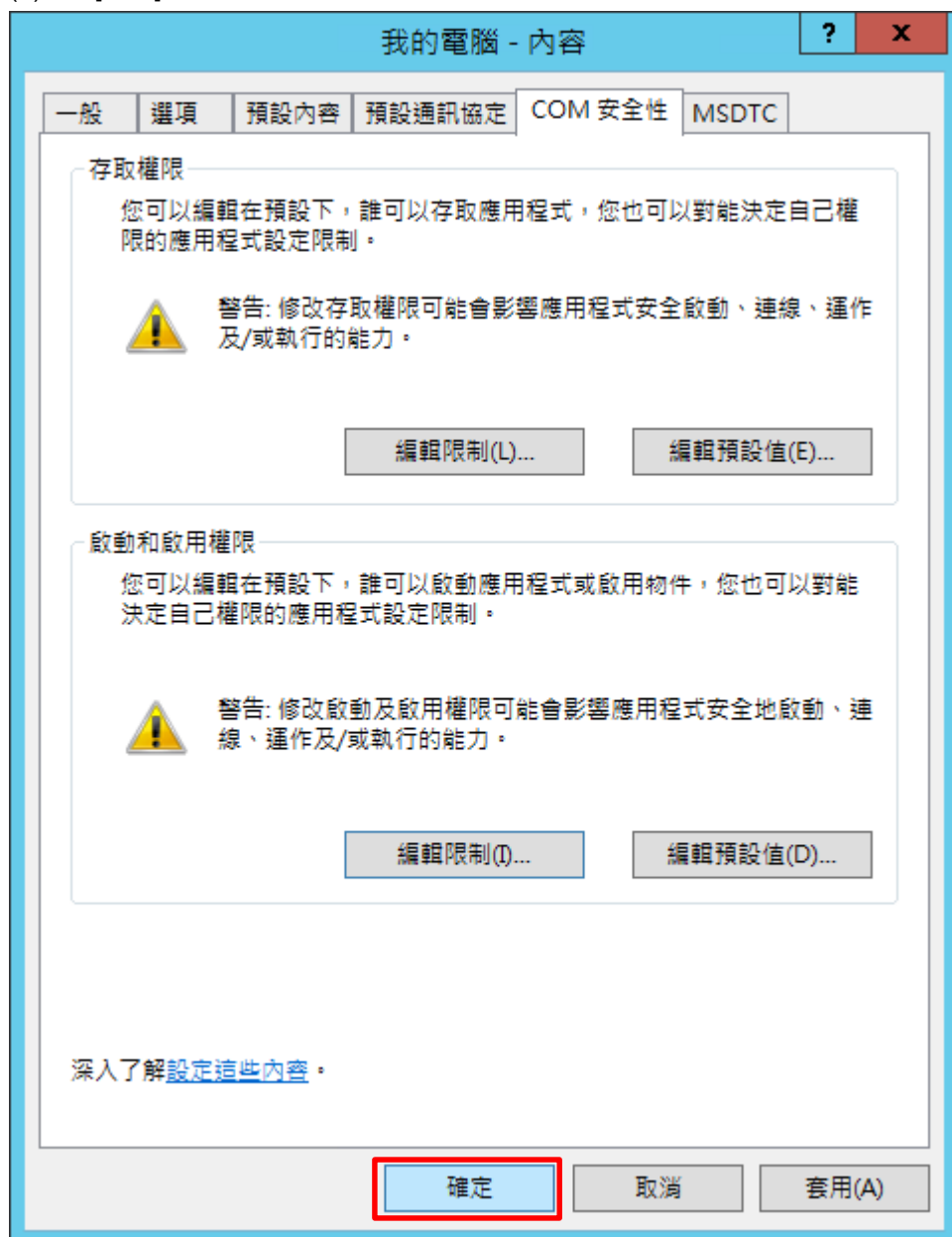


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [本機啟動:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



4.3.3 設定 WMI 權限

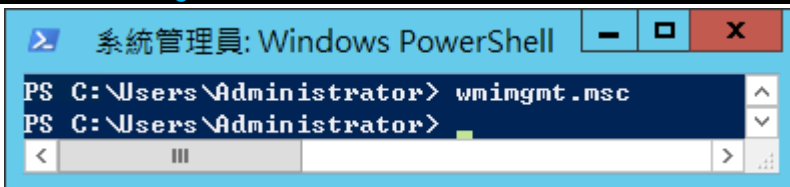
4.3.3.1 設定事件日誌權限

(1) 開啟 [Windows PowerShell]



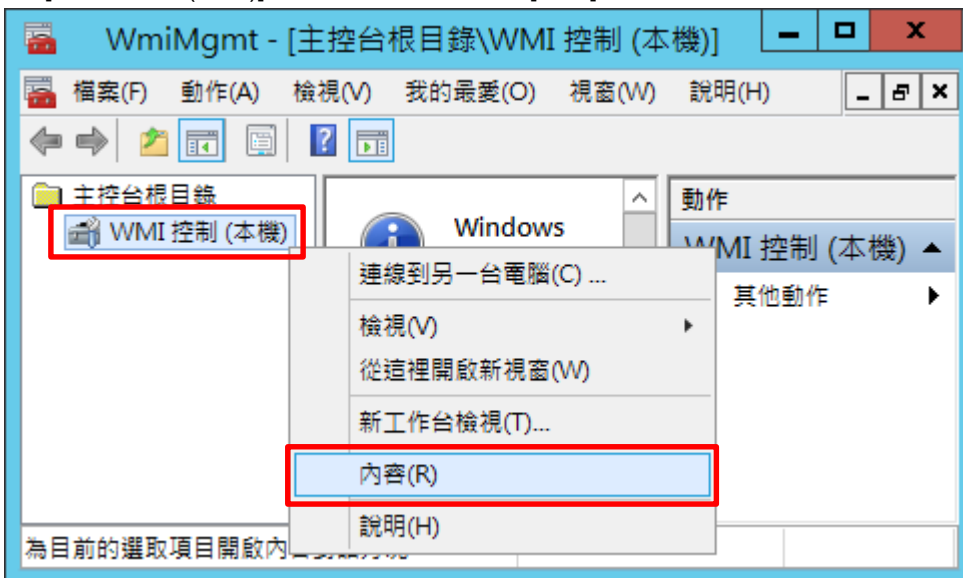
(2) 開啟元件服務

PS C:\> wimgmt.msc



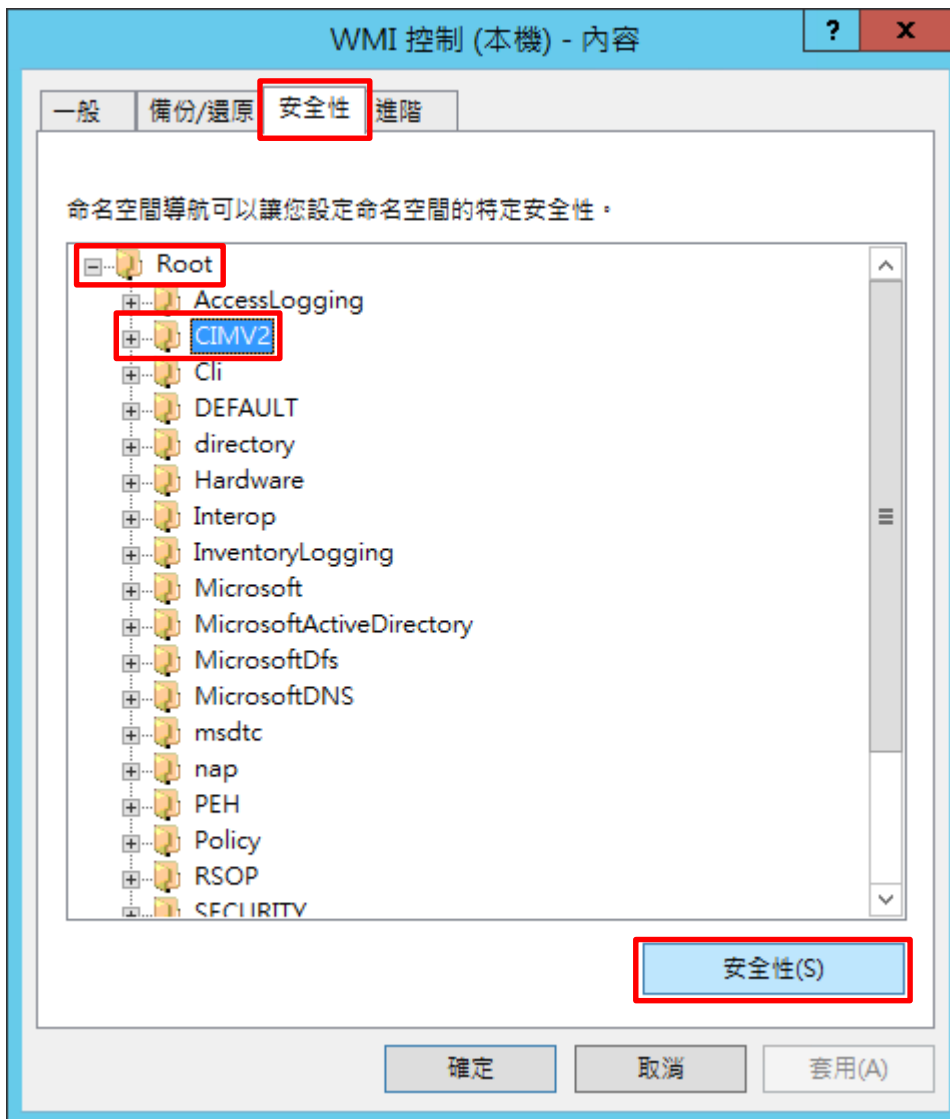
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



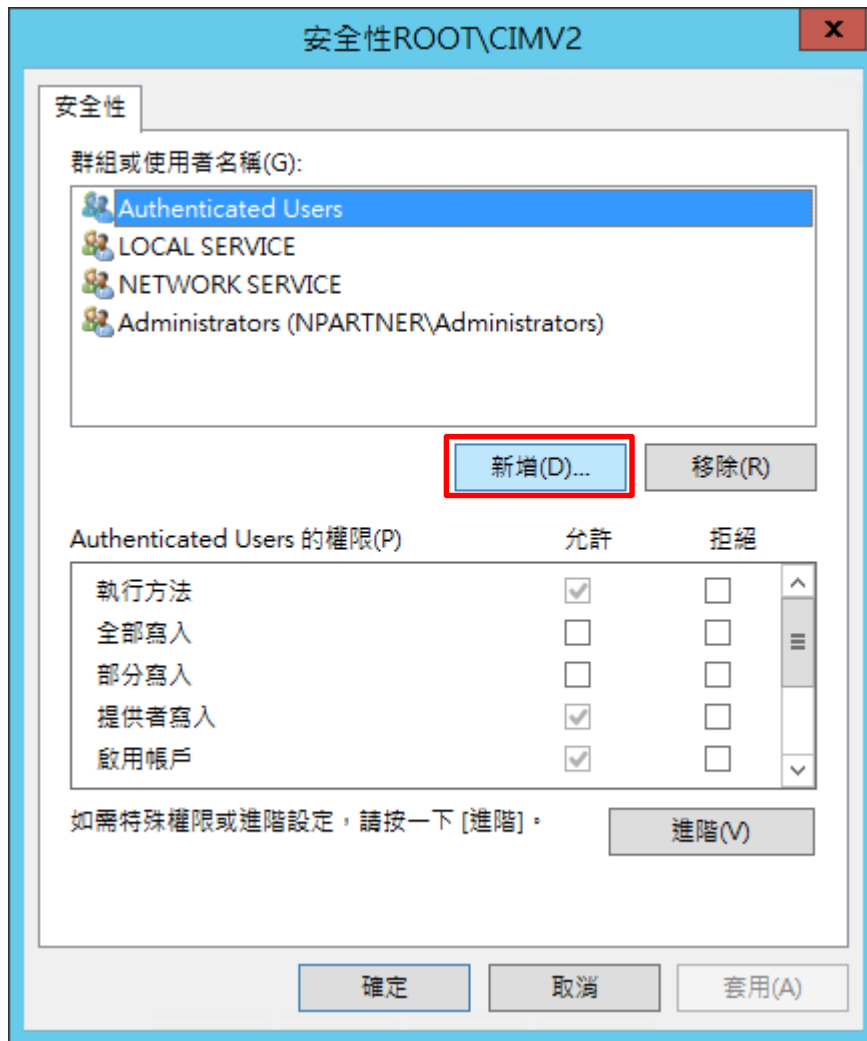
(4) 編輯 CIMV2 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [CIMV2] -> 按 [安全性]



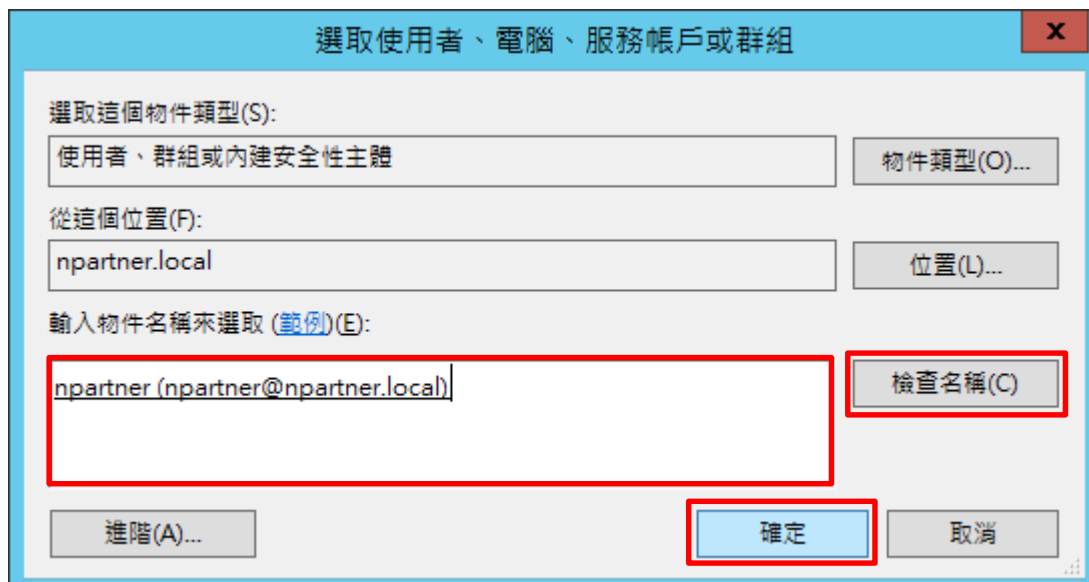
(5) 新增 WMI 使用者權限

按 [新增]



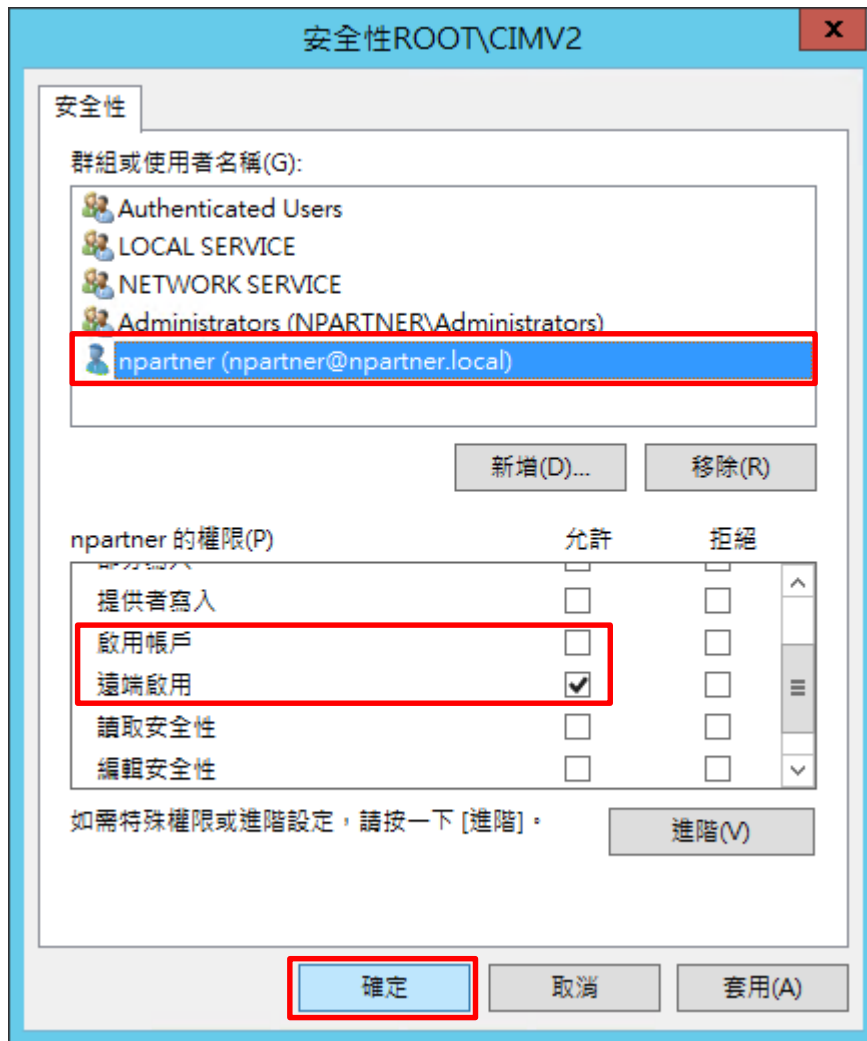
(6) 輸入使用者

輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

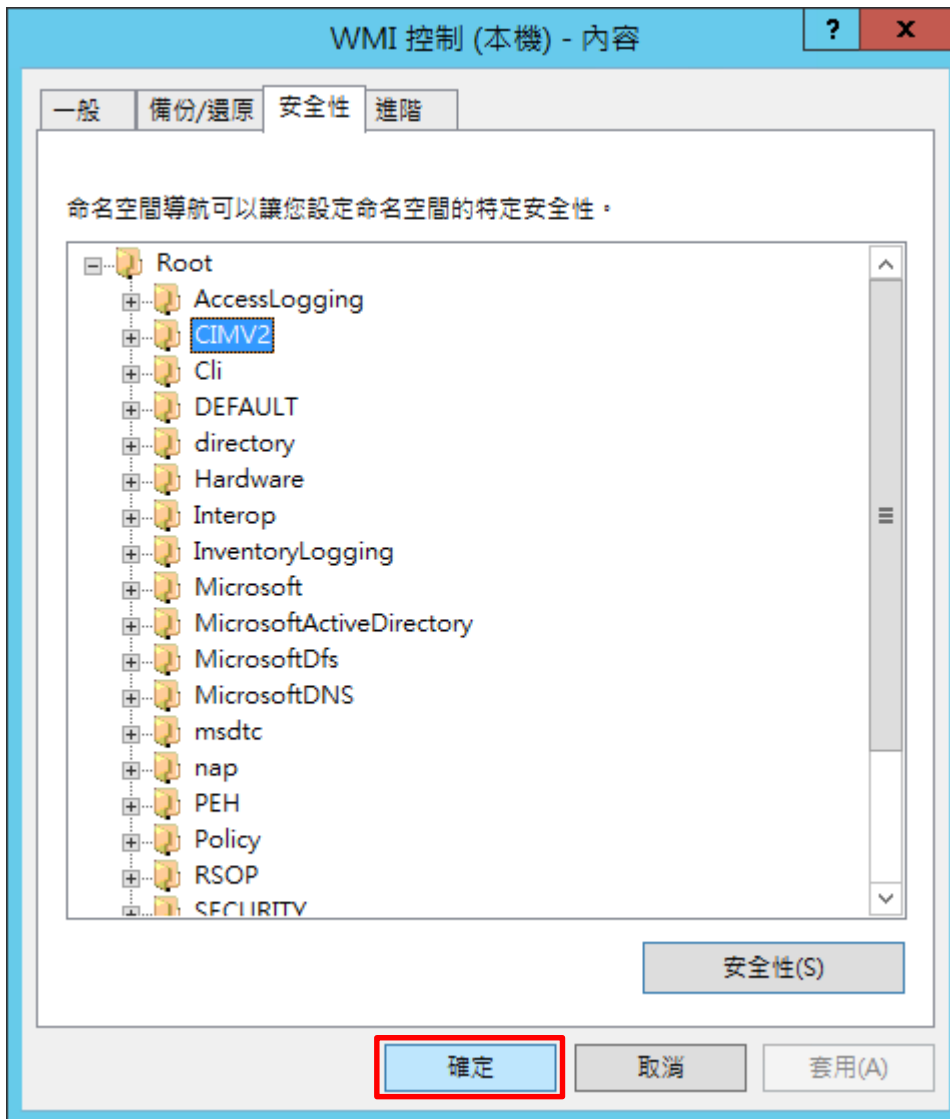


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



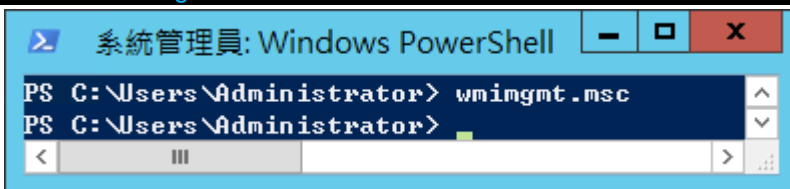
4.3.3.2 設定讀取使用者資料權限

(1) 開啟 [Windows PowerShell]



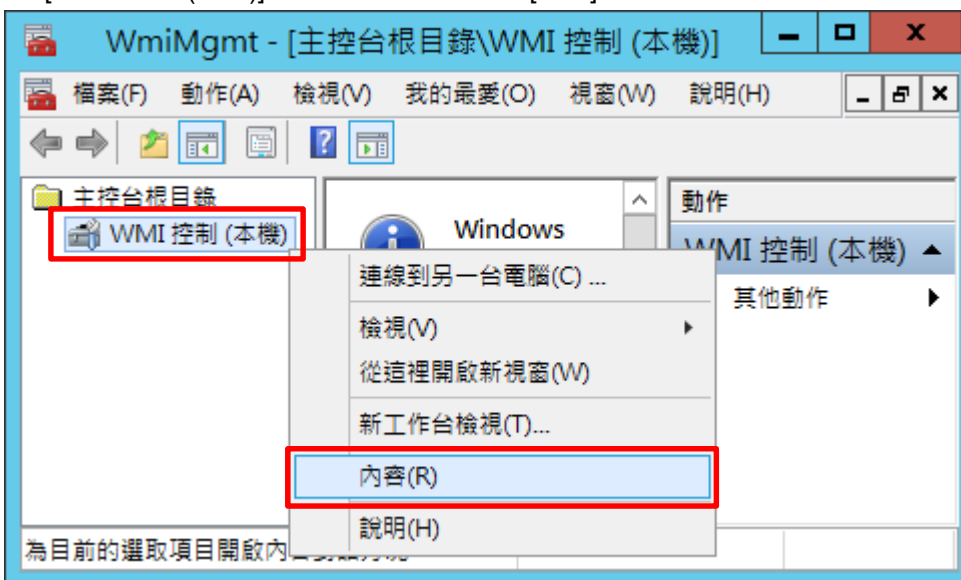
(2) 開啟元件服務

PS C:\> wimgmt.msc



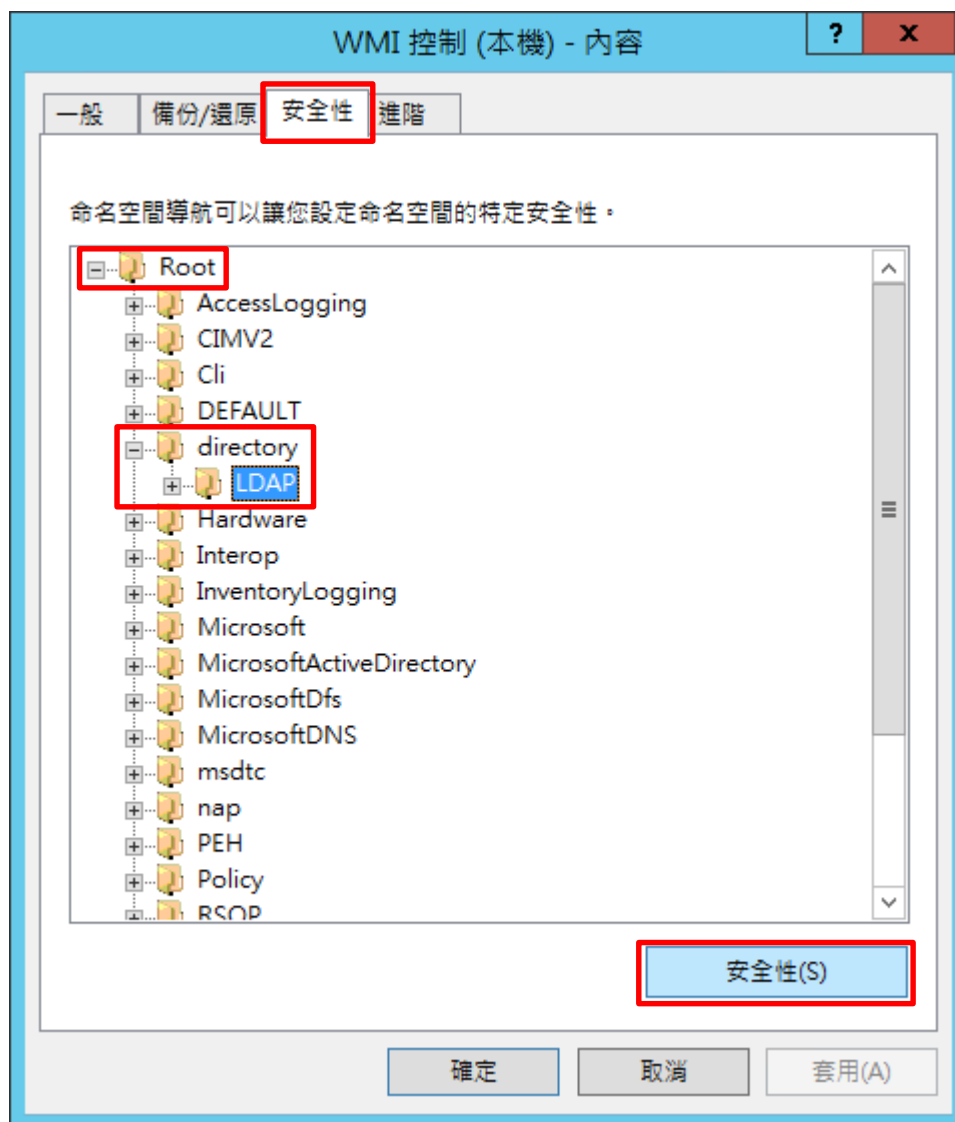
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



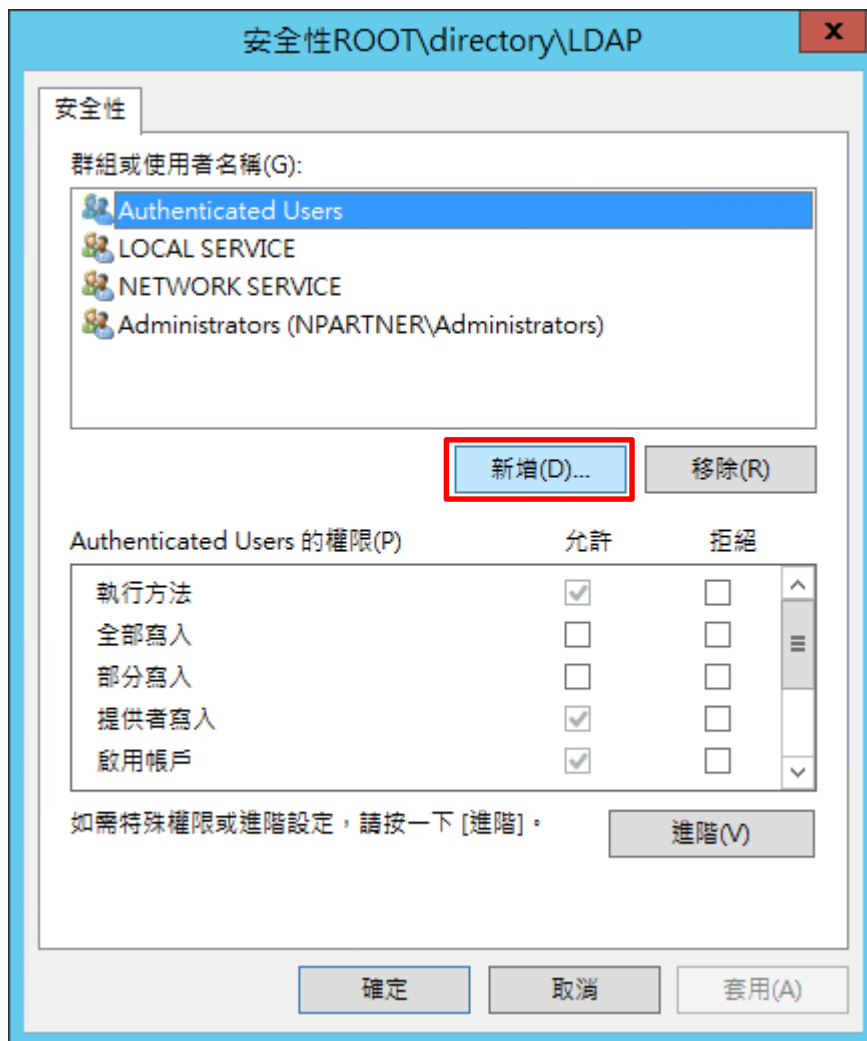
(4) 編輯 LDAP 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [directory] -> [LDAP] -> 按 [安全性]



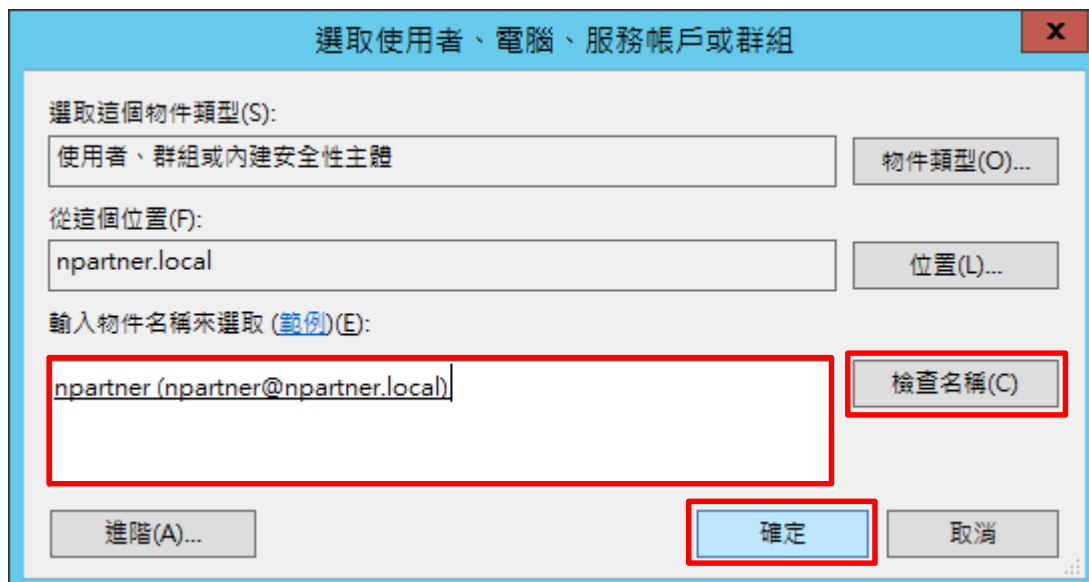
(5) 新增 WMI 使用者權限

按 [新增]



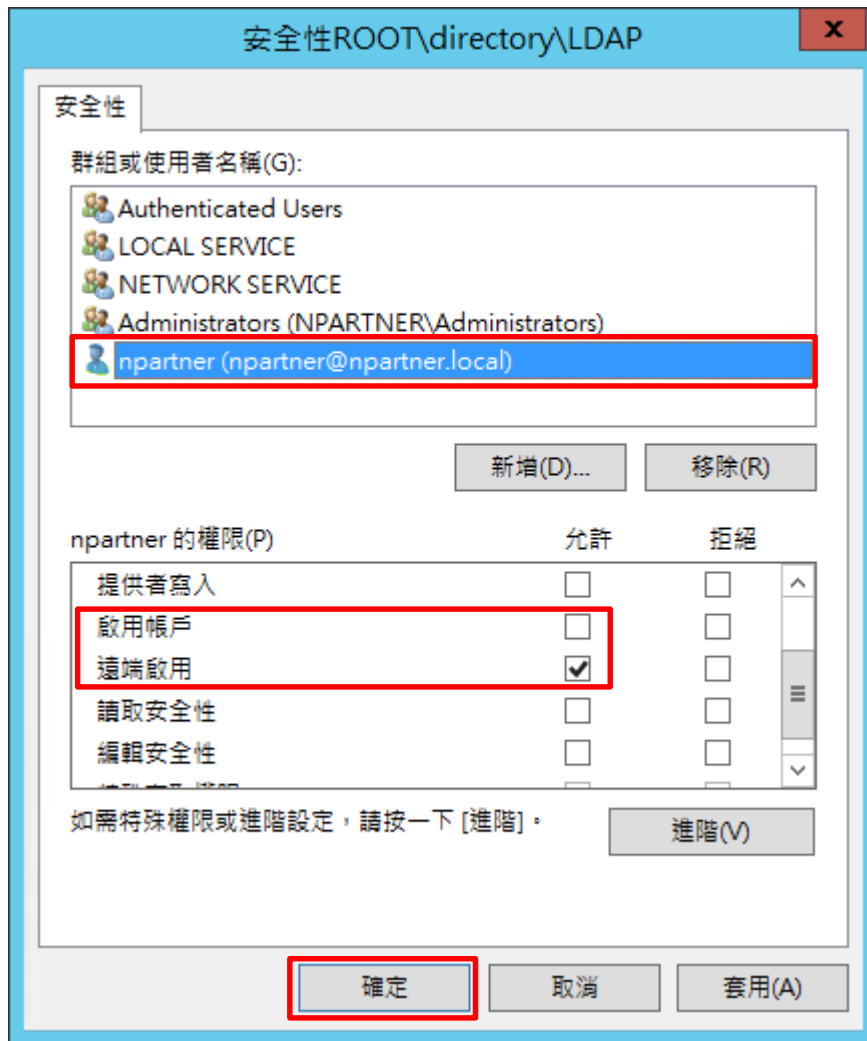
(6) 輸入使用者

輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

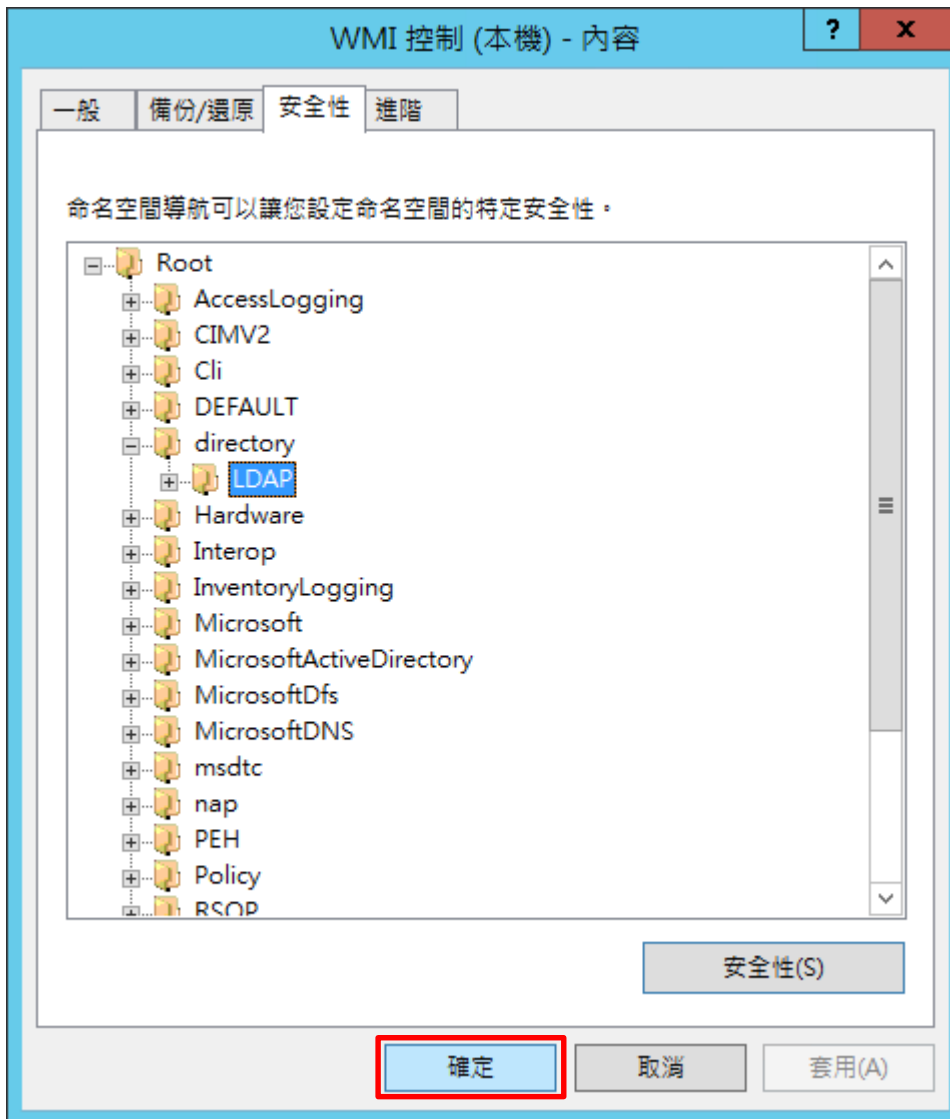


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



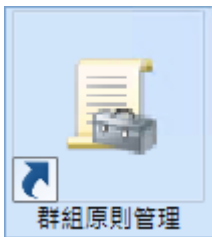
(8) 按 [確定]



4.3.4 設定 Event log 讀取權限

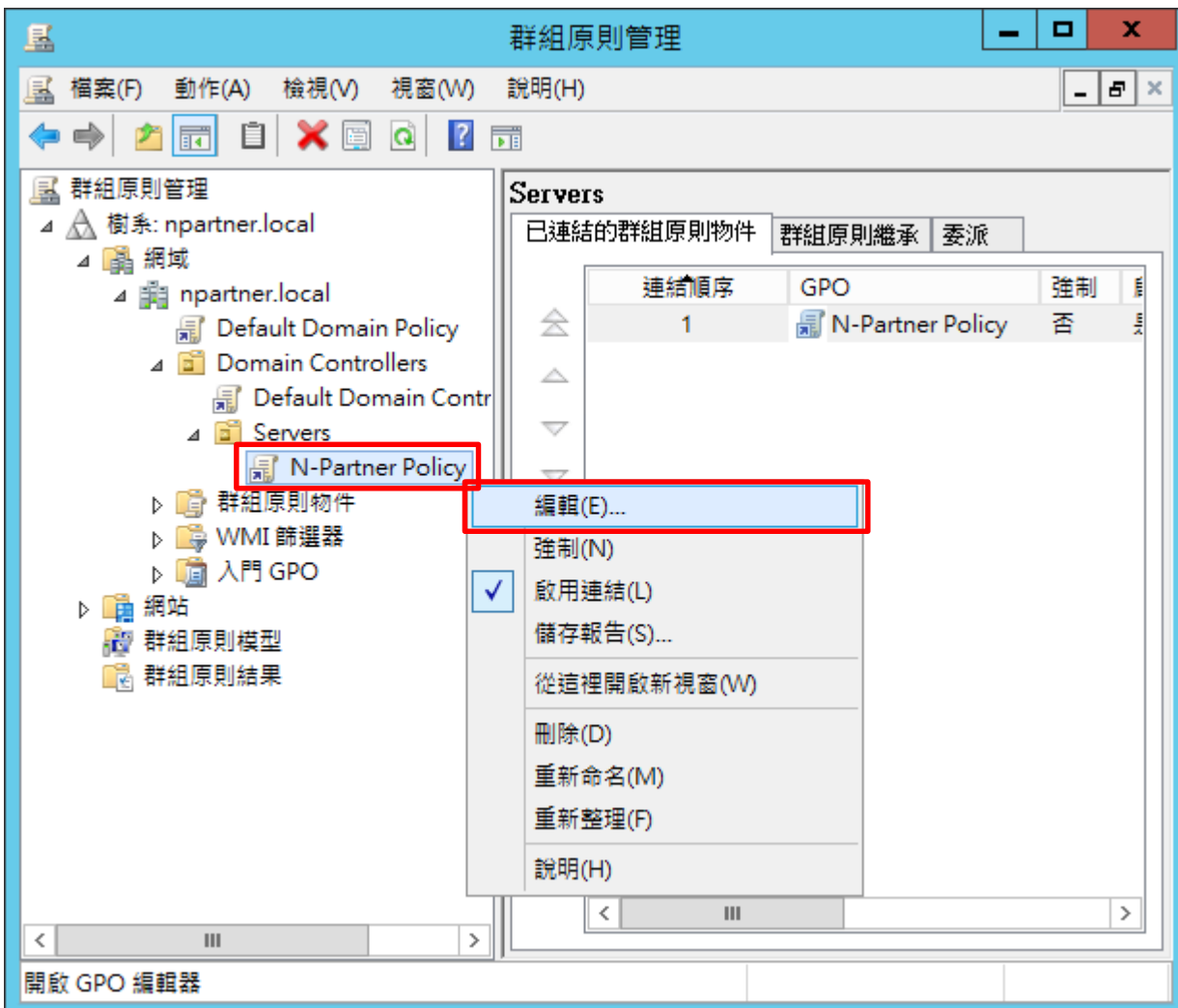
(1) 開啟群組原則管理

開啟 [群組原則管理]




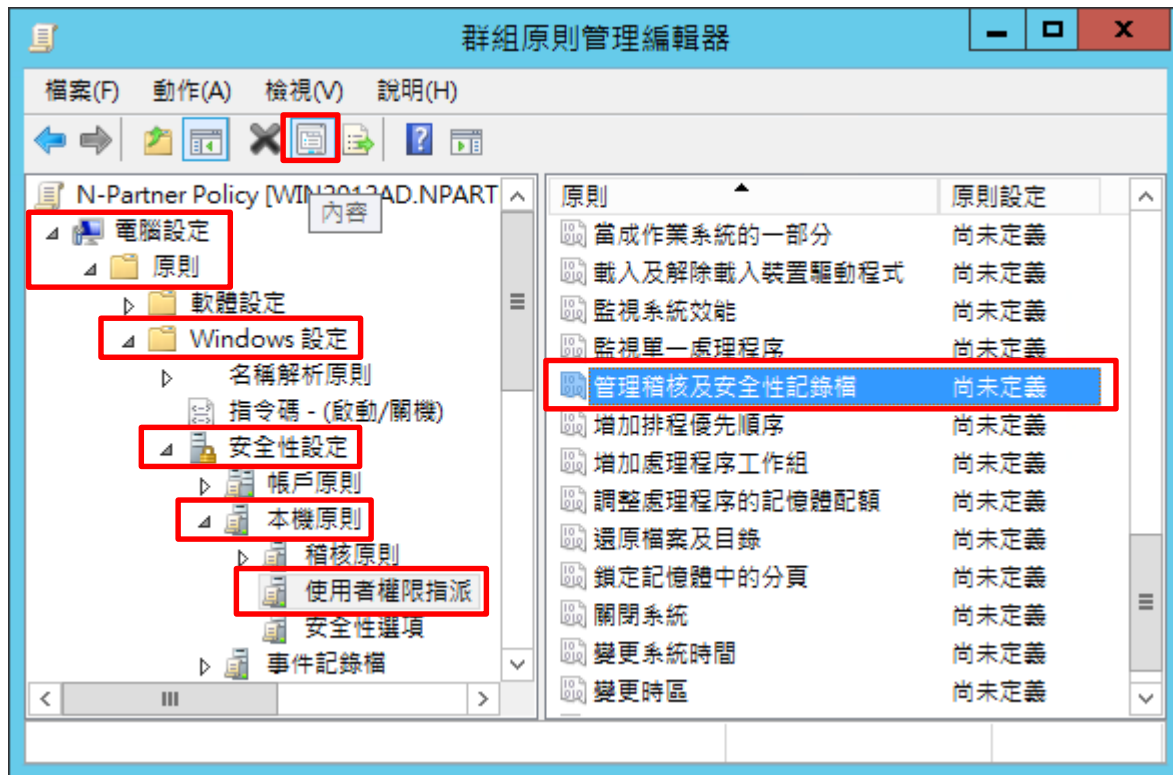
(2) 編輯群組原則物件

在 [N-Partner Policy] 群組原則物件，按滑鼠右鍵 -> 點選 [編輯]



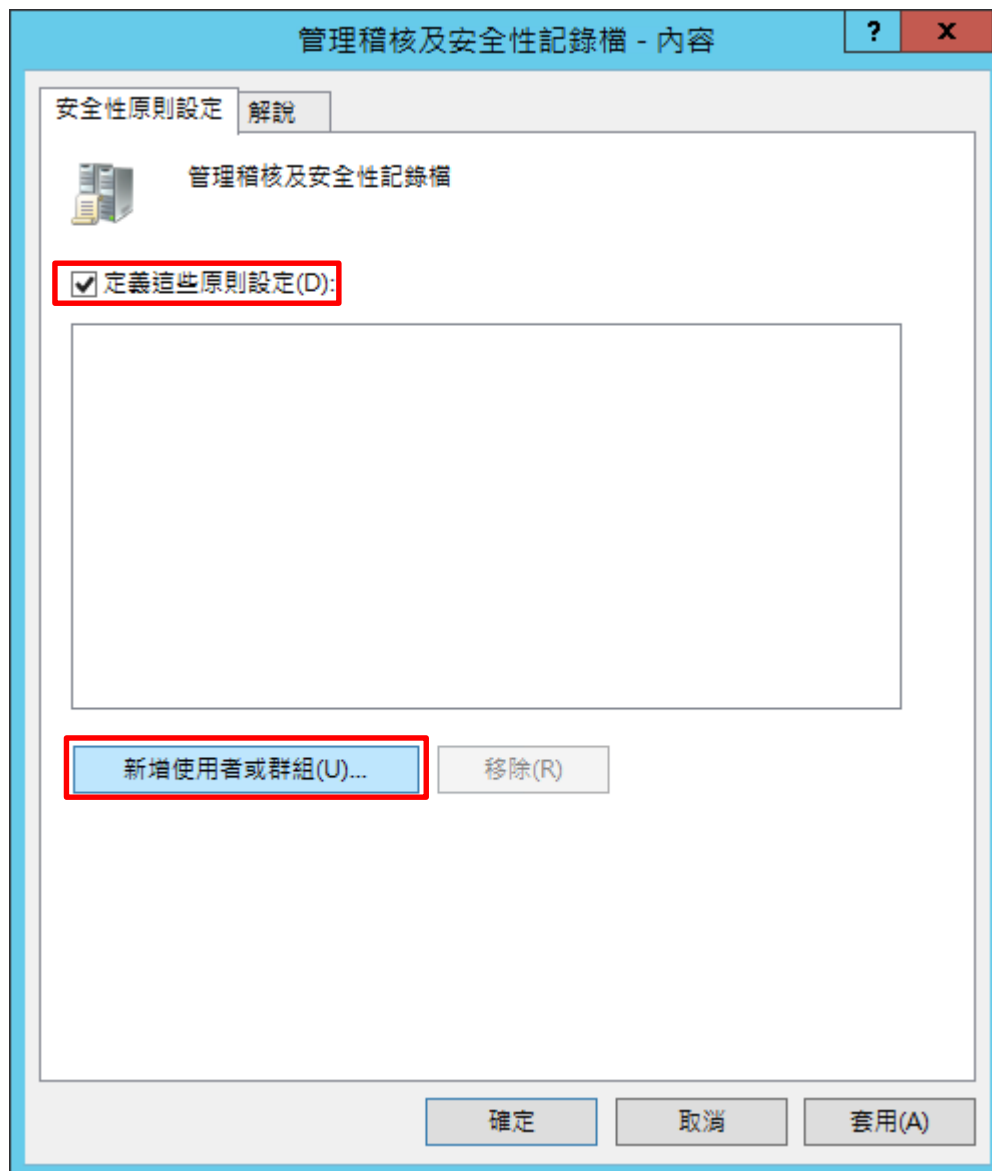
(3) 設定記錄檔

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [使用者權限指派] -> 選擇 [管理稽核及安全記錄檔] 項目 -> 點選  內容



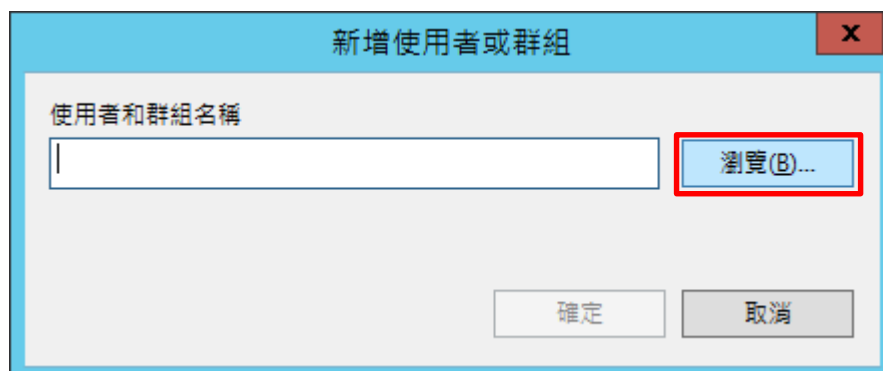
(4) 新增管理稽核使用者

勾選 [定義這些原則設定] -> 按 [新增使用者或群組...]



(5) 搜尋使用者

按 [瀏覽]



(6) 輸入使用者

輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

選取使用者、電腦、服務帳戶或群組

選取這個物件類型(S):
使用者、群組或內建安全性主體 物件類型(O)...

從這個位置(F):
npartner.local 位置(L)...

輸入物件名稱來選取 (範例)(E):
npartner (npartner@npartner.local) 檢查名稱(C)

進階(A)... 確定 取消

(7) 確定使用者

按 [確定]

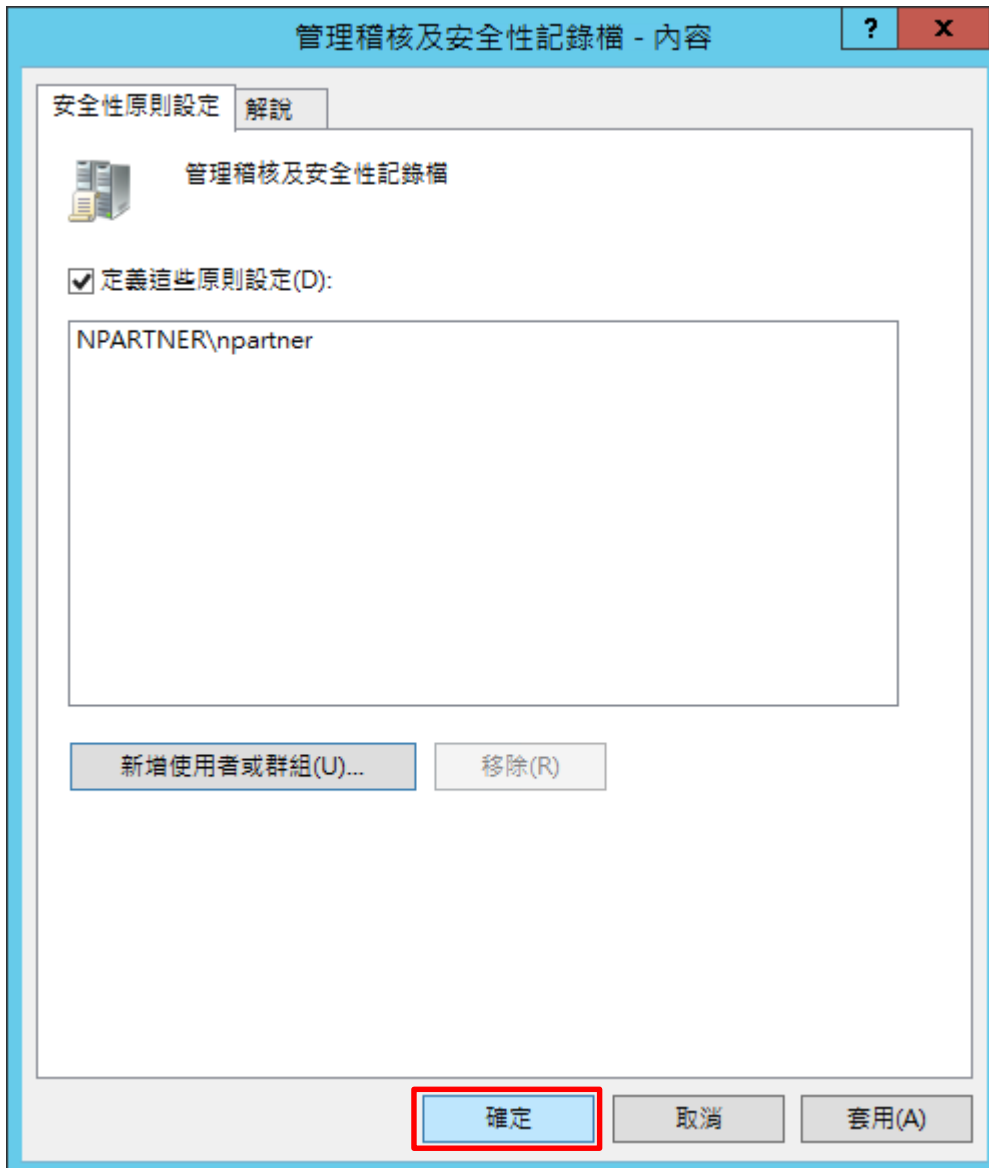
新增使用者或群組

使用者和群組名稱
NPARTNER\mpartner 瀏覽(B)...

確定 取消

(8) 確定設定記錄檔

按 [確定]

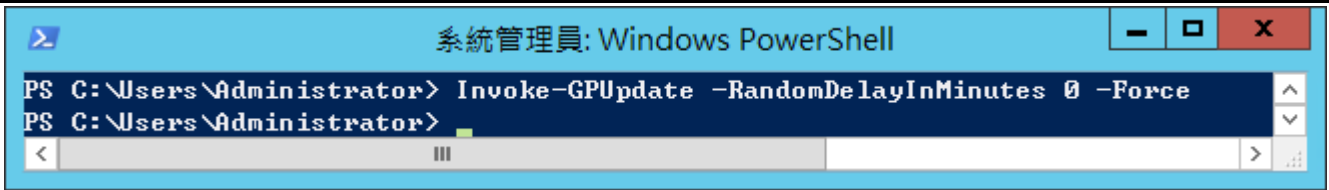


(9) 開啟 [Windows PowerShell]



(10) 更新群組原則

PS C:\> Invoke-GPUdate -RandomDelayInMinutes 0 -Force



```
系統管理員: Windows PowerShell
PS C:\Users\Administrator> Invoke-GPUdate -RandomDelayInMinutes 0 -Force
PS C:\Users\Administrator>
```

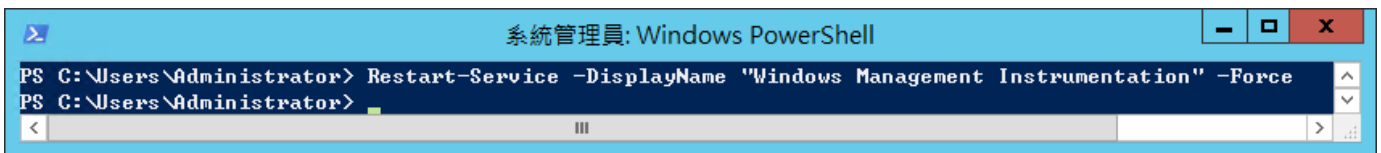

4.3.5 重啟 WMI 服務

(1) 開啟 [Windows PowerShell]



(2) 重啟 WMI 服務

PS C:\> Restart-Service -DisplayName "Windows Management Instrumentation" -Force



(3) 查看 WMI 服務

PS C:\> Get-Service -DisplayName "Windows Management Instrumentation"



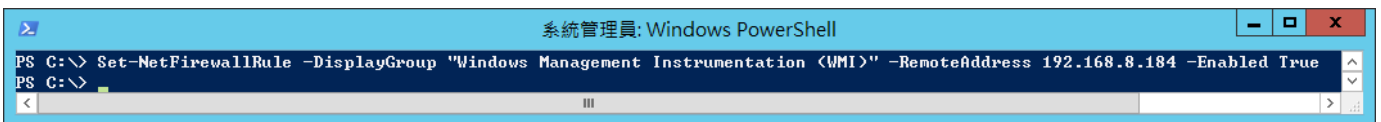
4.4 設定防火牆

(1) 開啟 [Windows PowerShell]



(2) 設定防火牆 · 只允許 N-Reporter IP query WMI

```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.184 -Enabled True
```



紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 查看防火牆 WMI 啟用狀態

```
PS C:\> Get-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -Direction Inbound |
>> Format-Table -Property Name,DisplayName,DisplayGroup,
>> @(<Name='RemoteAddress';Expression={{($PSItem | Get-NetFirewallAddressFilter).RemoteAddress}},
>> Enabled,Direction,Action
```

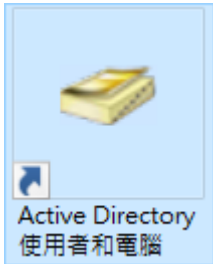


5. Windows 2016

Windows 稽核原則設定 [詳細說明請參考前言的稽核原則建議連結](#)

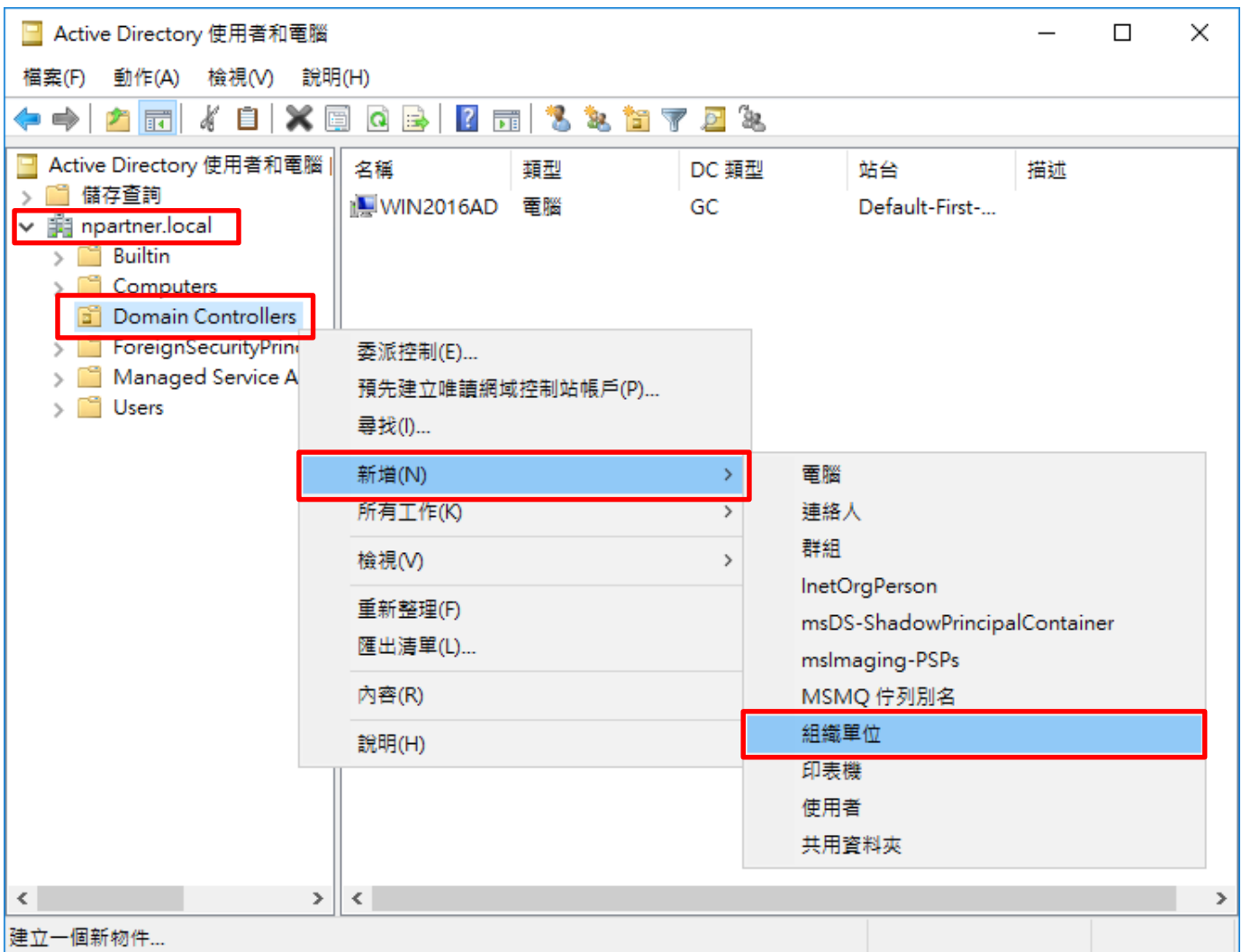
5.1 組織單位設定

(1) 開啟 [Active Directory 使用者和電腦]



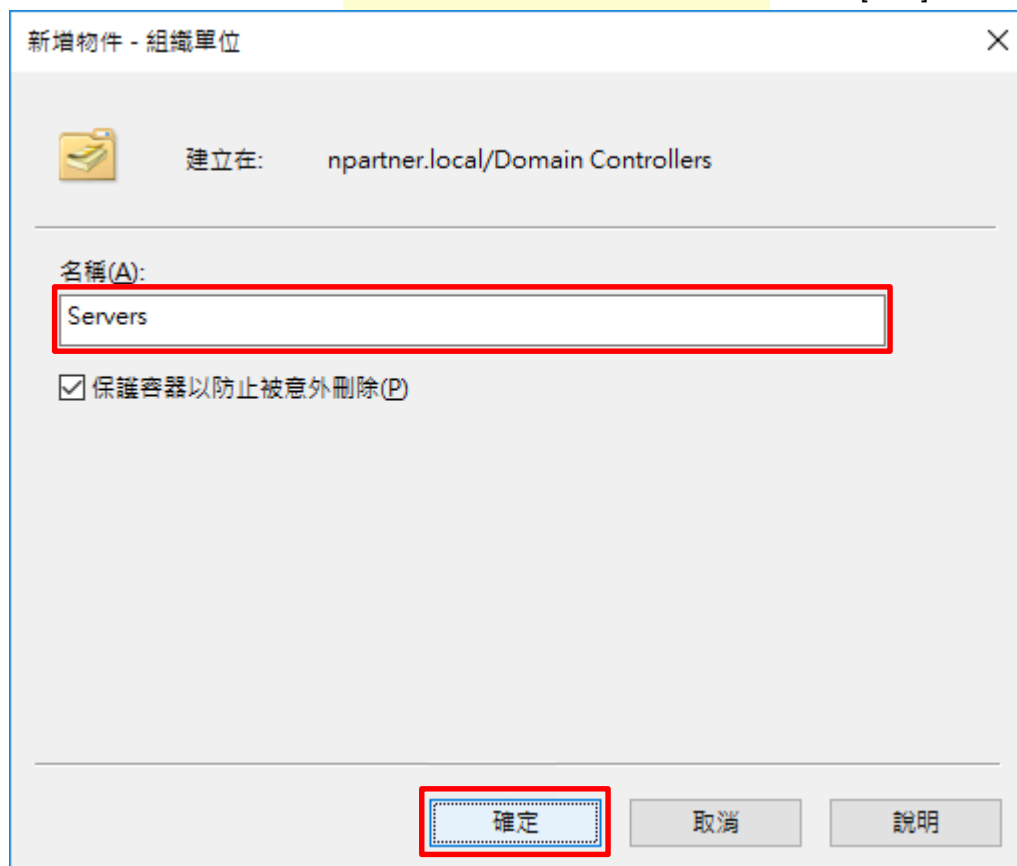
(2) 新增組織單位

[網域名稱] 的 [Domain Controllers] 組織單位按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]



(3) 輸入組織單位名稱

輸入組織單位名稱: Servers 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



新增物件 - 組織單位

建立在: npartner.local/Domain Controllers

名稱(A):
Servers

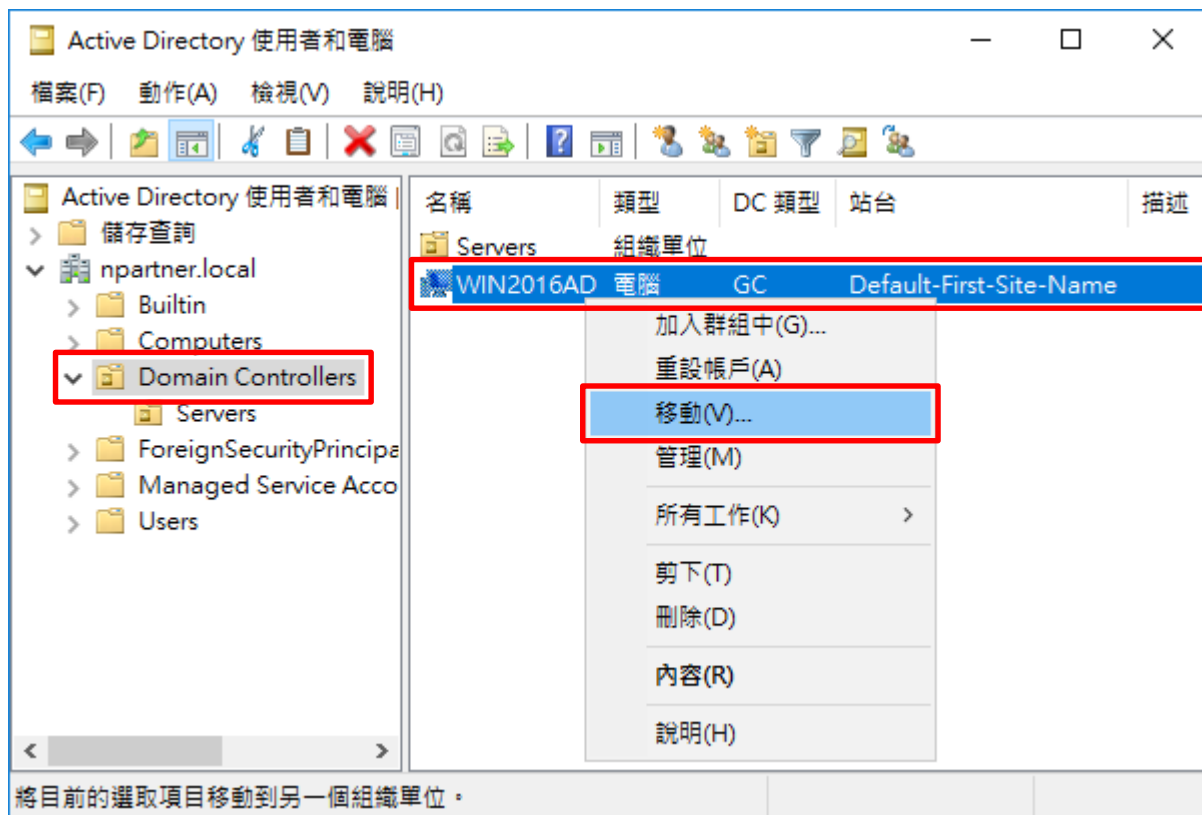
保護容器以防止被意外刪除(P)

確定 取消 說明

(4) 移動伺服器至新的組織單位

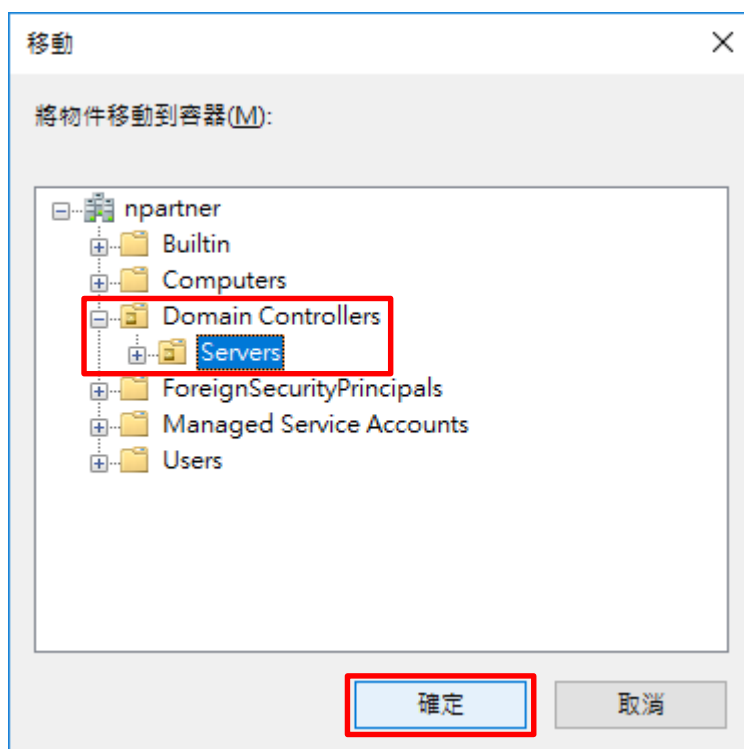
選擇 [Domain Controllers] 組織單位 -> 在 [Win2016AD] 按滑鼠右鍵 · 註：請依客戶環境選擇 Windows AD 主機

-> 點選 [移動]



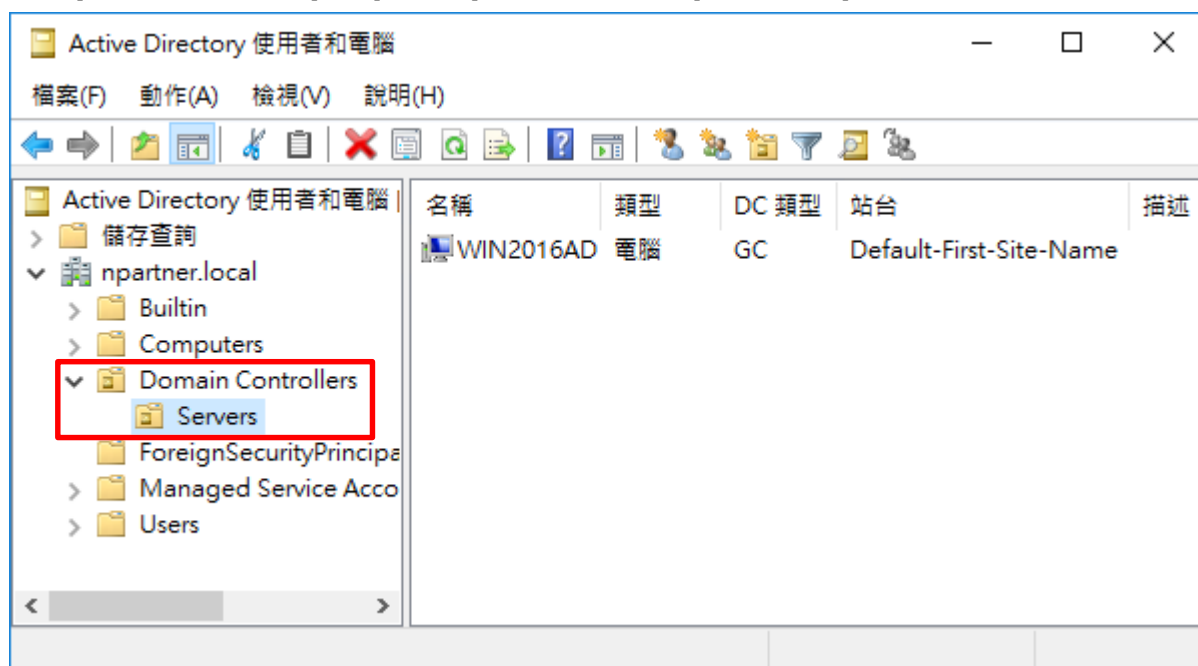
(5) 選擇組織單位

選擇 [Domain Controllers] 的 [Servers] 組織單位 -> 按 [確定]



(6) 確認伺服器已移動至新的組織單位

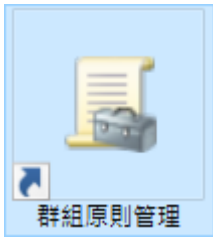
展開 [Domain Controllers] 的 [Servers] 組織單位，確認 [Win2016AD] 伺服器已移動



5.2 群組原則設定

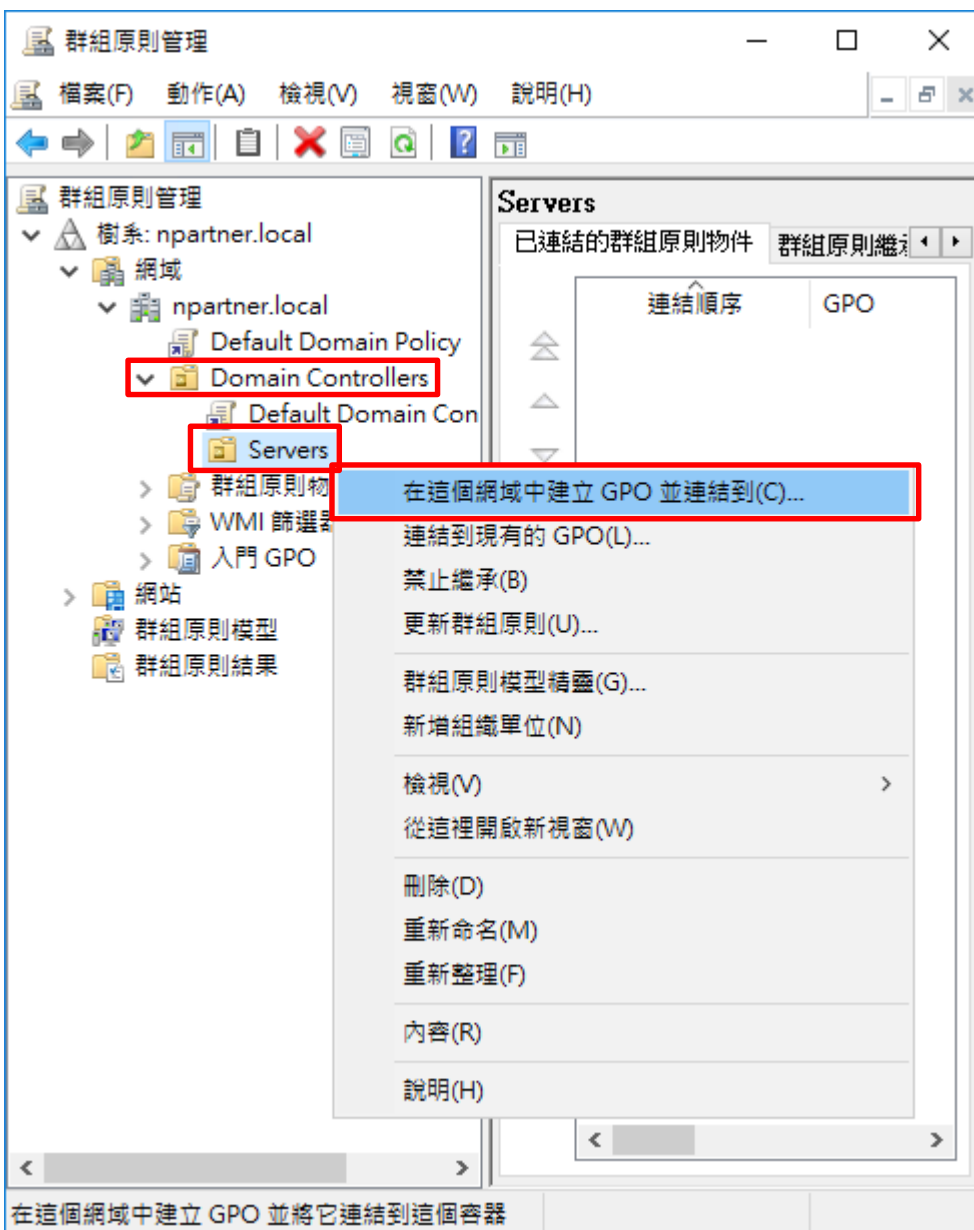
(1) 開啟群組原則管理

開啟 [群組原則管理]



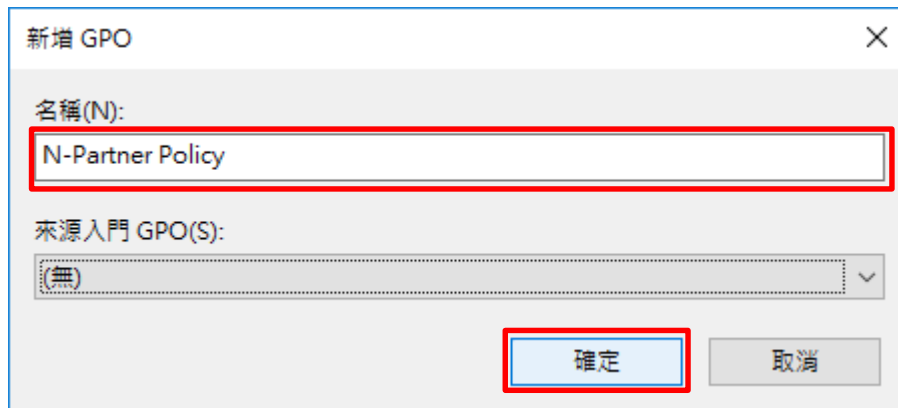
(2) 在 Servers 組織單位，新增群組原則物件

在 [Domain Controllers] 的 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到...]



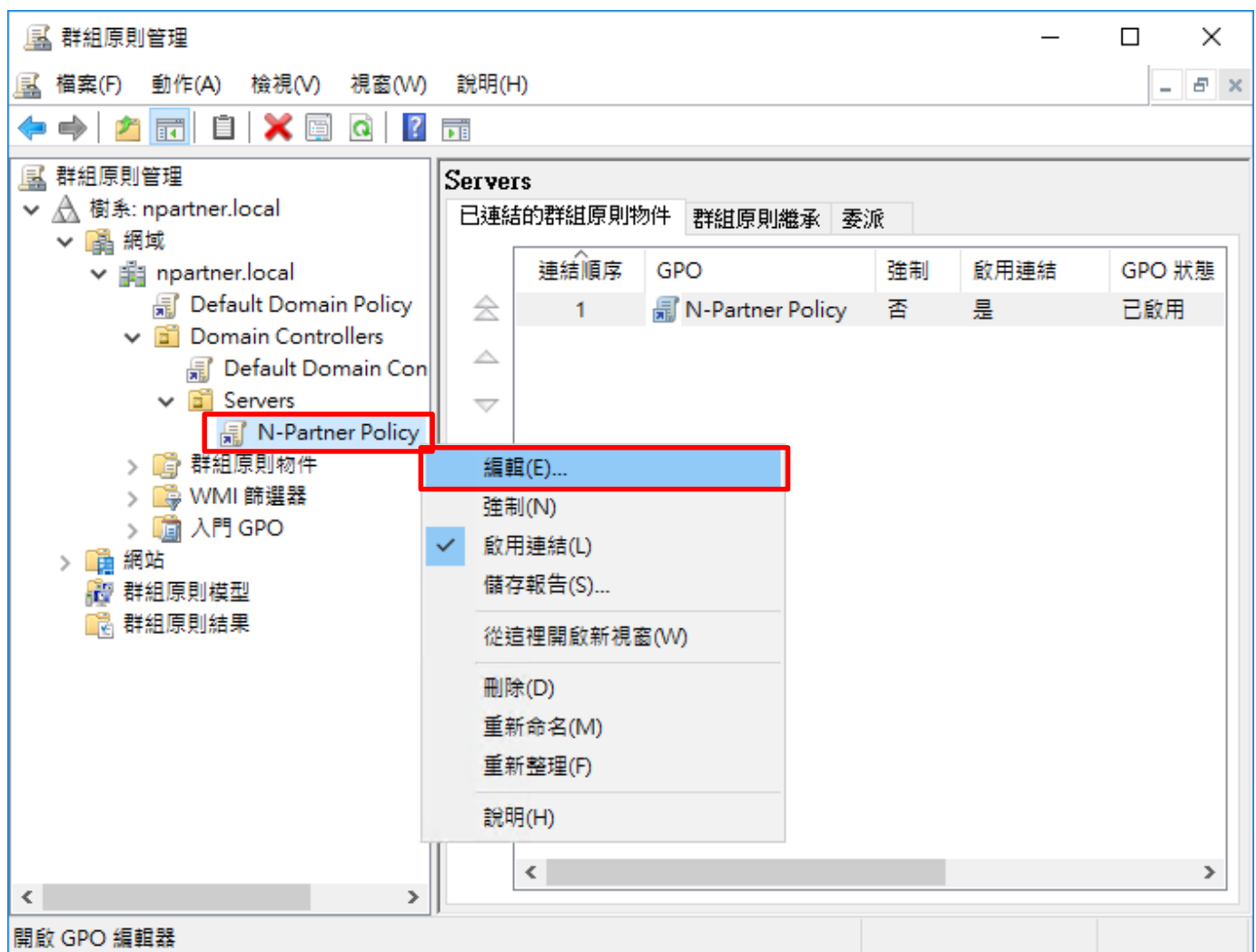
(3) 輸入群組原則物件名稱

輸入群組原則物件名稱: **N-Partner Policy** 註: 請依客戶環境建立群組物件名稱 -> 按 [確定]



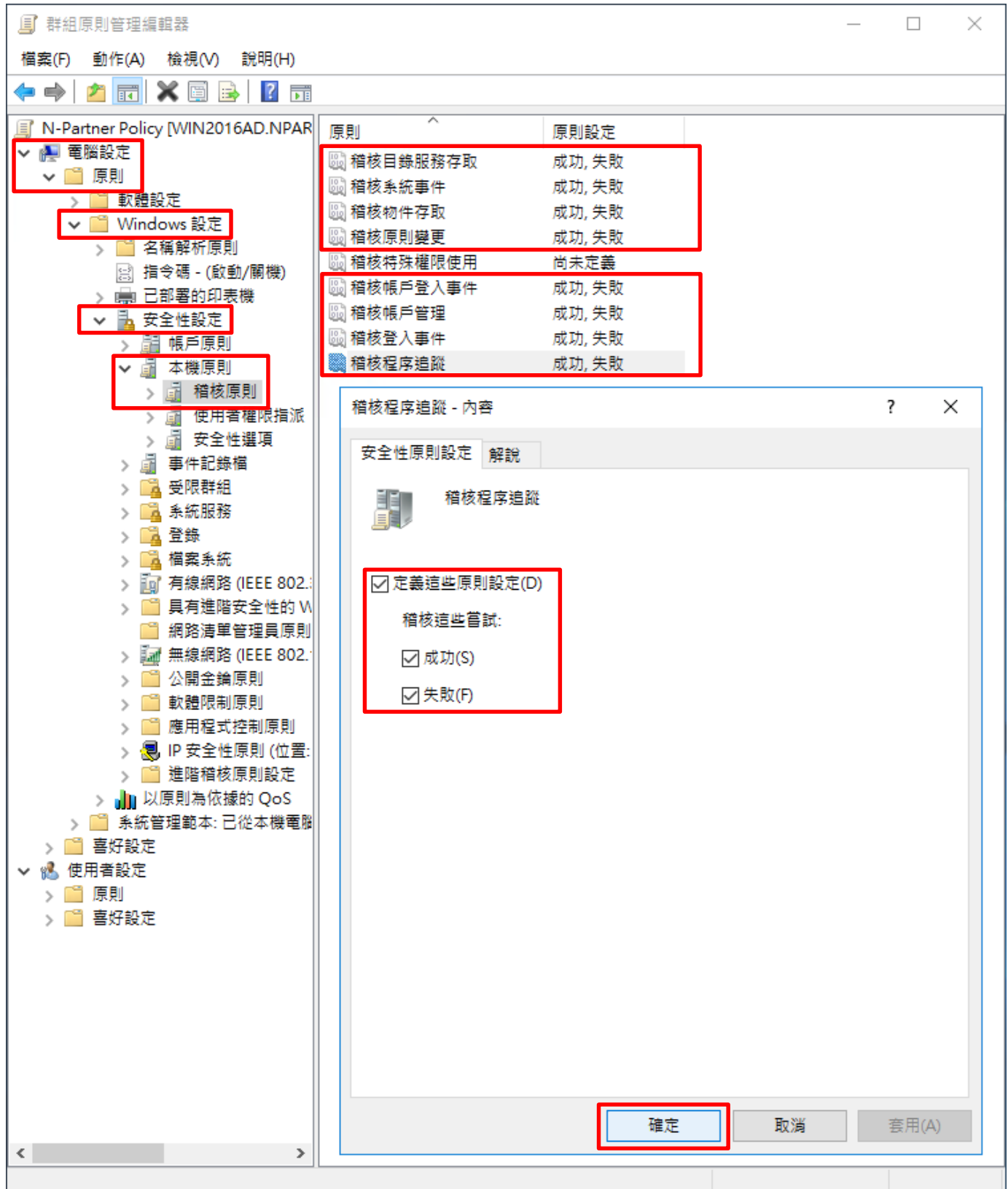
(4) 編輯群組原則物件

在 [N-Partner Policy] 群組原則物件 · 按滑鼠右鍵 -> 點選 [編輯]



(5) 本機原則：稽核原則

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核目錄服務存取], [稽核系統事件], [稽核物件存取], [稽核原則變更], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件], [稽核程序追蹤] 項目 -> 勾選 [定義這些原則設定:] & [成功] & [失敗] -> 按 [確定]



(6) 事件記錄：安全性記錄檔大小最大值

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔大小最大值] 項目 -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]

The screenshot shows the Group Policy Editor window titled "群組原則管理編輯器". The left-hand navigation pane is expanded to show the following path: "電腦設定" (Computer Configuration) > "原則" (Policies) > "Windows 設定" (Windows Settings) > "安全性設定" (Security Settings) > "事件記錄檔" (Event Logs). The right-hand pane displays a list of policies, with "安全性記錄檔大小最大值" (Maximum size of security event logs) selected and highlighted. Below this list, a dialog box titled "安全性記錄檔大小最大值 - 內容" (Maximum size of security event logs - Content) is open. In this dialog, the "安全性原則設定" (Security Policy Settings) tab is active, and the "定義這個原則設定(D)" (Define this policy setting) checkbox is checked. The value "204800" is entered in the text box, followed by "KB". A warning icon and text are visible below the input field, stating: "修改這個設定可能影響與用戶端、服務及應用程式間的相容性。如需其他資訊，請參閱[安全性記錄檔大小最大值](#)。(Q823659)". At the bottom of the dialog, the "確定" (OK) button is highlighted with a red box.

原則	原則設定
不允許本機來賓存取安全性記錄檔	尚未定義
不允許本機來賓存取系統記錄檔	尚未定義
不允許本機來賓存取應用程式記錄檔	尚未定義
安全性記錄檔大小最大值	204800 KB
安全性記錄檔保持方法	尚未定義
安全性記錄檔保留天數	尚未定義
系統記錄檔大小最大值	尚未定義
系統記錄檔保持方法	尚未定義
系統記錄檔保留天數	尚未定義
應用程式記錄保持方法	尚未定義
應用程式記錄檔大小最大值	尚未定義
應用程式記錄檔保留天數	尚未定義

(7) 事件記錄：安全性記錄檔大小最大值

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔保持方法] 項目 -> 勾選 [定義這個原則設定] -> 點選 [視需要覆寫事件] -> 按 [確定]

群組原則管理編輯器

檔案(F) 動作(A) 檢視(V) 說明(H)

N-Partner Policy [WIN2016AD.NPAR]

電腦設定

原則

軟體設定

Windows 設定

名稱解析原則

指令碼 - (啟動/關機)

已部署的印表機

安全性設定

帳戶原則

本機原則

事件記錄檔

受限群組

系統服務

登錄

檔案系統

有線網路 (IEEE 802.3)

具有進階安全性的 W

網路清單管理員原則

無線網路 (IEEE 802.11)

公開金鑰原則

軟體限制原則

應用程式控制原則

IP 安全性原則 (位置)

進階稽核原則設定

以原則為依據的 QoS

系統管理範本: 已從本機電腦

喜好設定

使用者設定

原則

喜好設定

原則	原則設定
不允許本機來賓存取安全性記錄檔	尚未定義
不允許本機來賓存取系統記錄檔	尚未定義
不允許本機來賓存取應用程式記錄檔	尚未定義
安全性記錄檔大小最大值	204800 KB
安全性記錄檔保持方法	尚未定義
安全性記錄檔保留天數	尚未定義
系統記錄檔大小最大值	尚未定義
系統記錄檔保持方法	尚未定義
系統記錄檔保留天數	尚未定義
應用程式記錄保持方法	尚未定義
應用程式記錄檔大小最大值	尚未定義
應用程式記錄檔保留天數	尚未定義

安全性記錄檔保持方法 - 內容

安全性原則設定 解說

安全性記錄檔保持方法

定義這個原則設定(D)

依日期覆寫事件(O)

視需要覆寫事件(V)

不要覆寫事件 (以手動方式清除記錄)(N)

修改這個設定可能影響與用戶端、服務及應用程式間的相容性。如需其他資訊，請參閱[安全性記錄檔保持方法](#)。(Q823659)

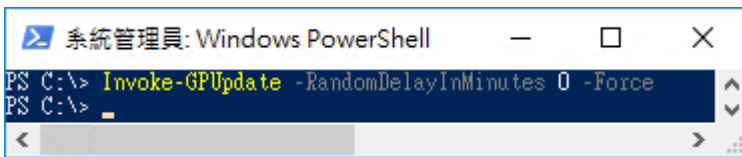
確定 取消 套用(A)

(8) 開啟 [Windows PowerShell]



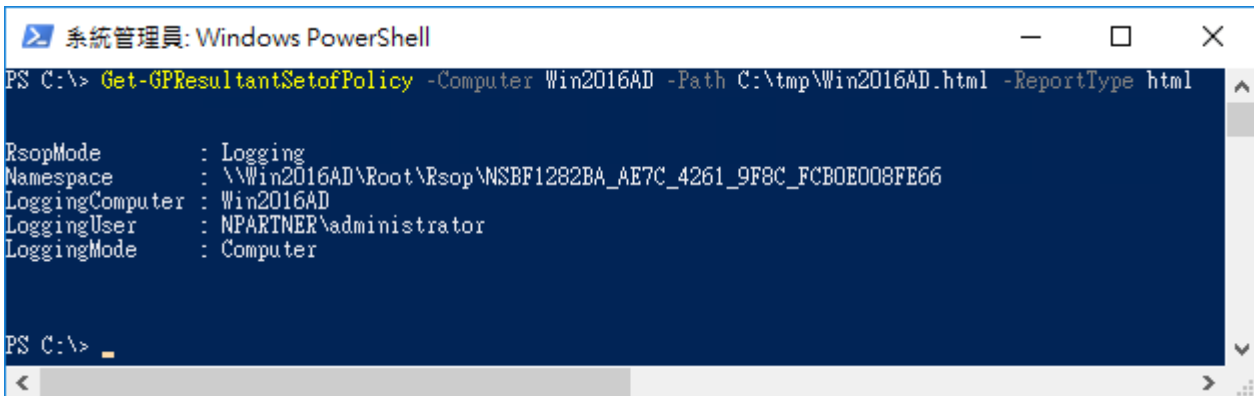
(9) 更新群組原則

```
PS C:\> Invoke-GPUdate -RandomDelayInMinutes 0 -Force
```



(10) 產生伺服器群組原則報表

```
PS C:\> Get-GPResultantSetofPolicy -Computer Win2016AD -Path C:\tmp\Win2016AD.html -ReportType html
```



紅色文字部位請輸入 Windows AD 伺服器名稱和資料夾路徑檔案名稱

(11) 開啟報表 · 確認 Windows 2016 AD 伺服器 · 套用 N-Partner Policy 群組原則

The screenshot displays the Windows Group Policy console. The left pane shows the following hierarchy:

- 原則 (Policies)
 - Windows 設定 (Windows Settings)
 - 安全性設定 (Security Settings)
 - 帳戶原則/密碼規則 (Account Policies/Password Policies) - 顯示 (Visible)
 - 帳戶原則/帳戶鎖定原則 (Account Policies/Account Lockout Policies) - 顯示 (Visible)
 - 帳戶原則/Kerberos 原則 (Account Policies/Kerberos Policies) - 顯示 (Visible)
 - 本機原則/稽核原則 (Local Policies/Audit Policies) - 隱藏 (Hidden)

原則 (Policy)	設定 (Setting)	優勢 GPO (Linked GPO)
稽核目錄服務存取 (Audit Directory Service Access)	成功, 失敗 (Success, Failure)	N-Partner Policy
稽核系統事件 (Audit System Events)	成功, 失敗 (Success, Failure)	N-Partner Policy
稽核物件存取 (Audit Object Access)	成功, 失敗 (Success, Failure)	N-Partner Policy
稽核原則變更 (Audit Policy Change)	成功, 失敗 (Success, Failure)	N-Partner Policy
稽核帳戶登入事件 (Audit Account Logon Events)	成功, 失敗 (Success, Failure)	N-Partner Policy
稽核帳戶管理 (Audit Account Management)	成功, 失敗 (Success, Failure)	N-Partner Policy
稽核登入事件 (Audit Logon Events)	成功, 失敗 (Success, Failure)	N-Partner Policy
稽核程序追蹤 (Audit Program Execution)	成功, 失敗 (Success, Failure)	N-Partner Policy
 - 本機原則/使用者權限指派 (Local Policies/User Rights Assignments) - 顯示 (Visible)
 - 本機原則/安全性選項 (Local Policies/Security Options) - 顯示 (Visible)
 - 事件記錄檔 (Event Log) - 隱藏 (Hidden)

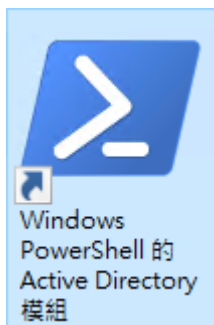
原則 (Policy)	設定 (Setting)	優勢 GPO (Linked GPO)
安全性記錄檔保持方法 (Security Log Retention Method)	視需要而定 (As Required)	N-Partner Policy
安全性記錄檔容量最大值 (Security Log Capacity Maximum)	204800 KB	N-Partner Policy
 - 公開金鑰原則/憑證服務用戶端 - 自動註冊設定 (Public Key Policies/Certificate Services Client - Auto Registration Settings) - 顯示 (Visible)
 - 公開金鑰原則/加密檔案系統 (Public Key Policies/Encrypting File System) - 顯示 (Visible)
 - 系統管理範本 (System Management Templates) - 顯示 (Visible)

5.3 新增非管理帳號

5.3.1 新增使用者

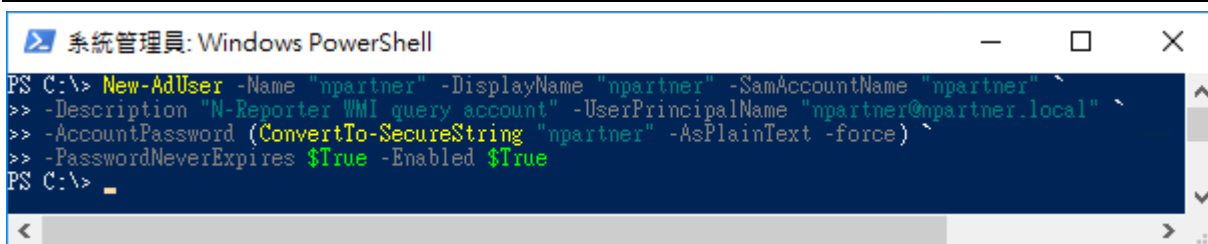
(1) 開啟 AD 使用者和電腦

開啟 [Windows PowerShell 的 Active Directory 模組]



(2) 新增帳號

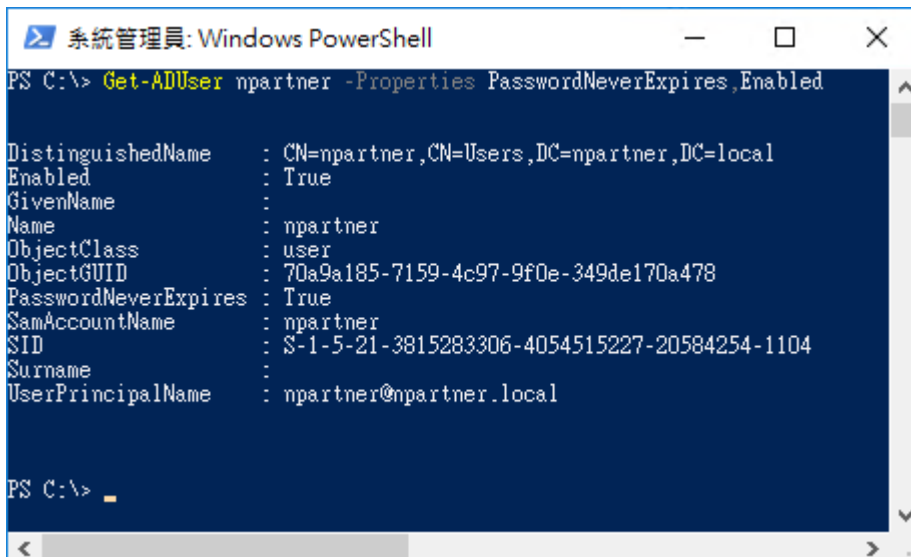
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True
```

A screenshot of a Windows PowerShell terminal window titled "系統管理員: Windows PowerShell". The terminal shows the execution of the New-AdUser command with the following parameters: -Name "npartner", -DisplayName "npartner", -SamAccountName "npartner", -Description "N-Reporter WMI query account", -UserPrincipalName "npartner@npartner.local", -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force), and -PasswordNeverExpires \$True -Enabled \$True. The prompt returns to PS C:\>.

紅色文字部位請輸入帳號密碼及網域資訊

(3) 查看帳號狀態

```
PS C:\> Get-ADUser npartner -Properties PasswordNeverExpires,Enabled
```

A screenshot of a Windows PowerShell terminal window titled "系統管理員: Windows PowerShell". The terminal shows the execution of the Get-ADUser npartner -Properties PasswordNeverExpires,Enabled command. The output is as follows:
DistinguishedName : CN=npartner,CN=Users,DC=npartner,DC=local
Enabled : True
GivenName :
Name : npartner
ObjectClass : user
ObjectGUID : 70a9a185-7159-4c97-9f0e-349de170a478
PasswordNeverExpires : True
SamAccountName : npartner
SID : S-1-5-21-3815283306-4054515227-20584254-1104
Surname :
UserPrincipalName : npartner@npartner.local
The prompt returns to PS C:\>.

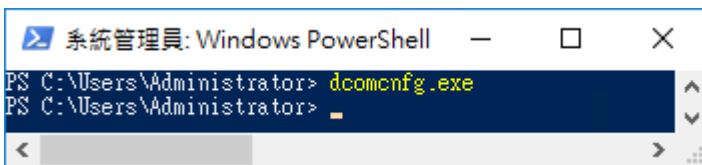
5.3.2 設定 DCOM 權限

(1) 開啟 [Windows PowerShell]



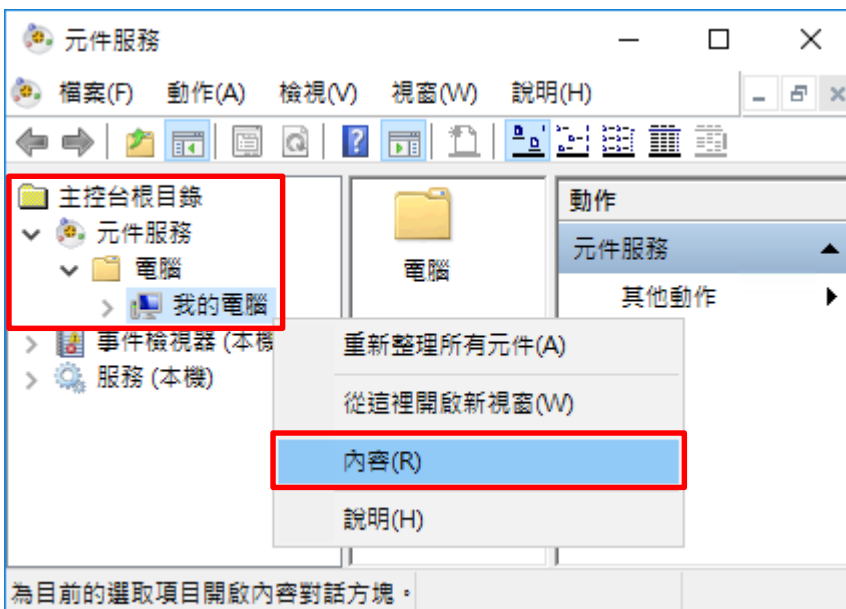
(2) 開啟元件服務

```
PS C:\> dcomcnfg.exe
```



(3) 編輯電腦內容

展開 [主控台根目錄], [元件服務], [電腦] -> 在 [我的電腦] 按滑鼠右鍵 -> 點選 [內容]



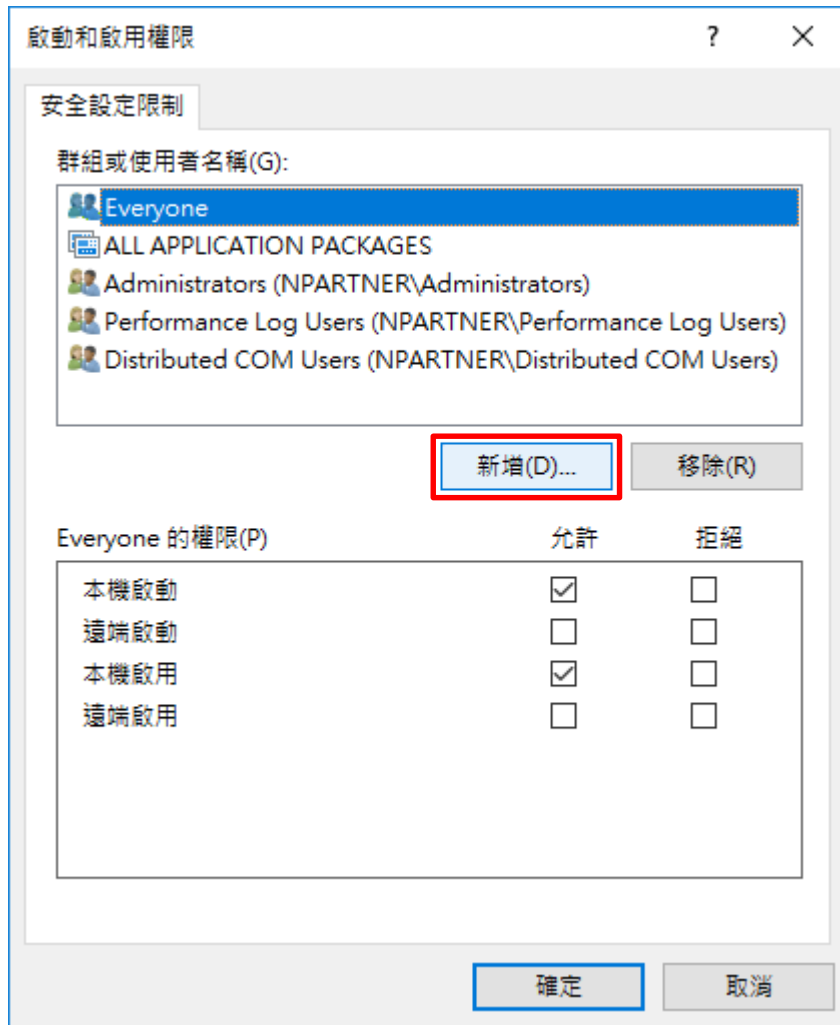
(4) 啟用權限

點選 [COM 安全性] 頁面 -> 啟動和啟用權限，按 [編輯限制]



(5) 新增 DCOM 使用者權限

點選 [新增]



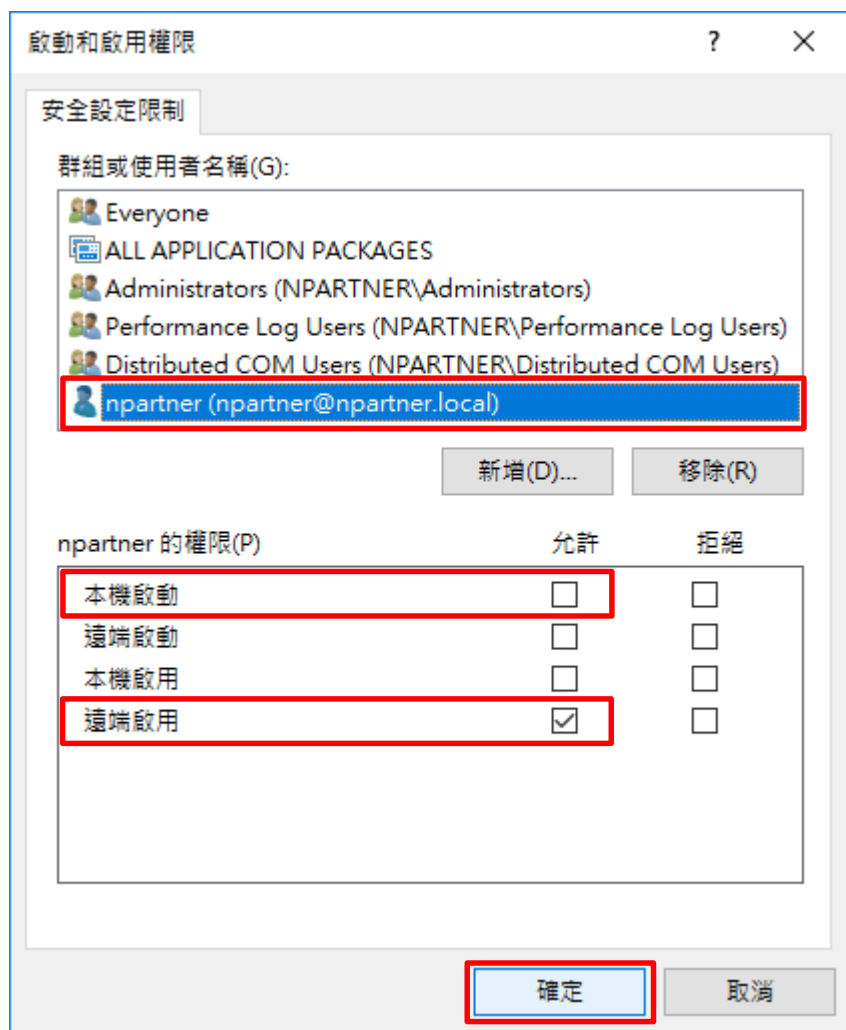
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]



(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [本機啟動:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



5.3.3 設定 WMI 權限

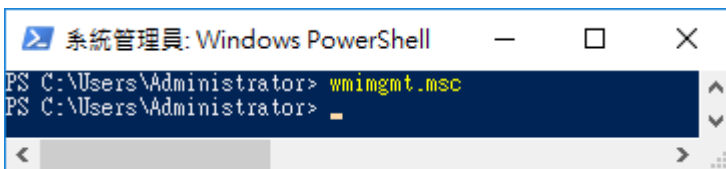
5.3.3.1 設定事件日誌權限

(1) 開啟 [Windows PowerShell]



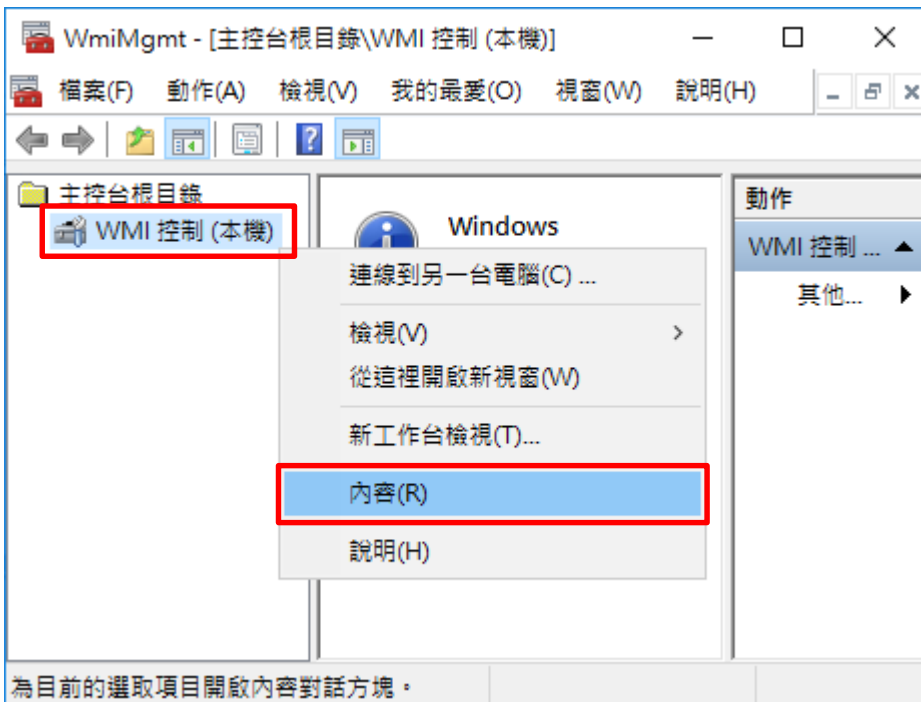
(2) 開啟元件服務

```
PS C:\> wimgmt.msc
```



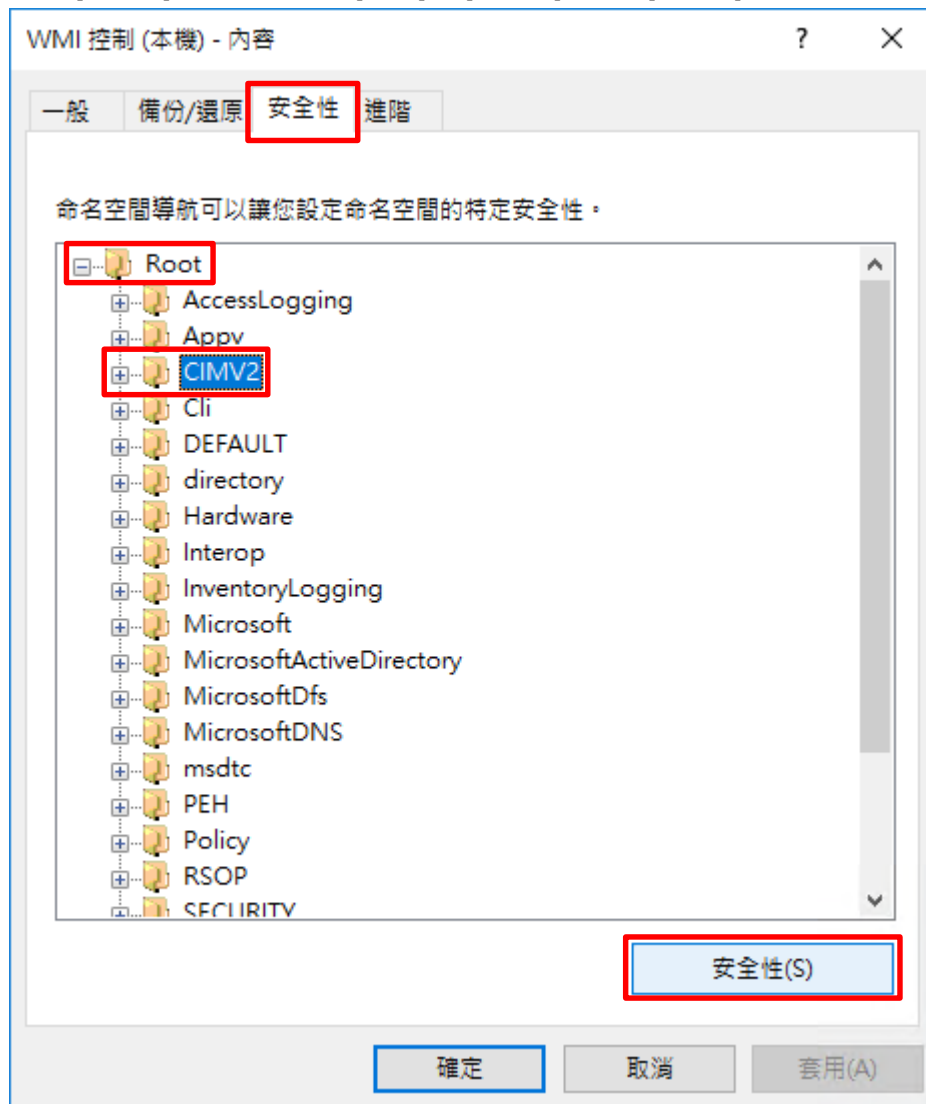
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



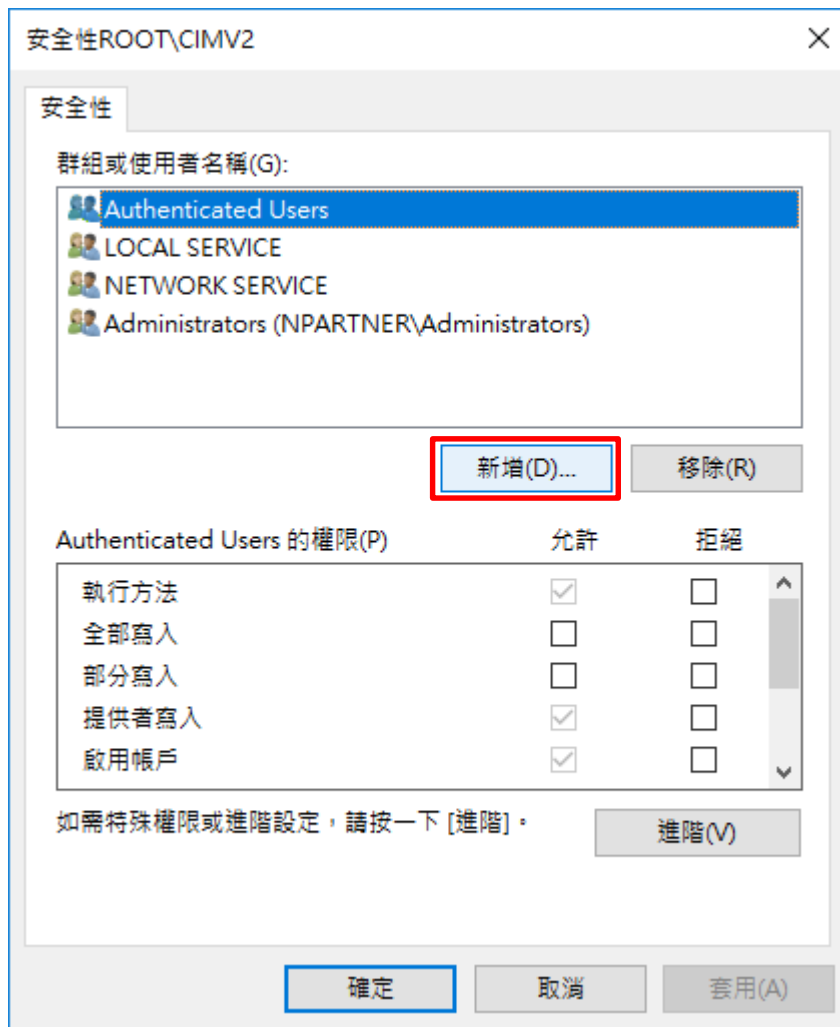
(4) 編輯 CIMV2 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [CIMV2] -> 按 [安全性]



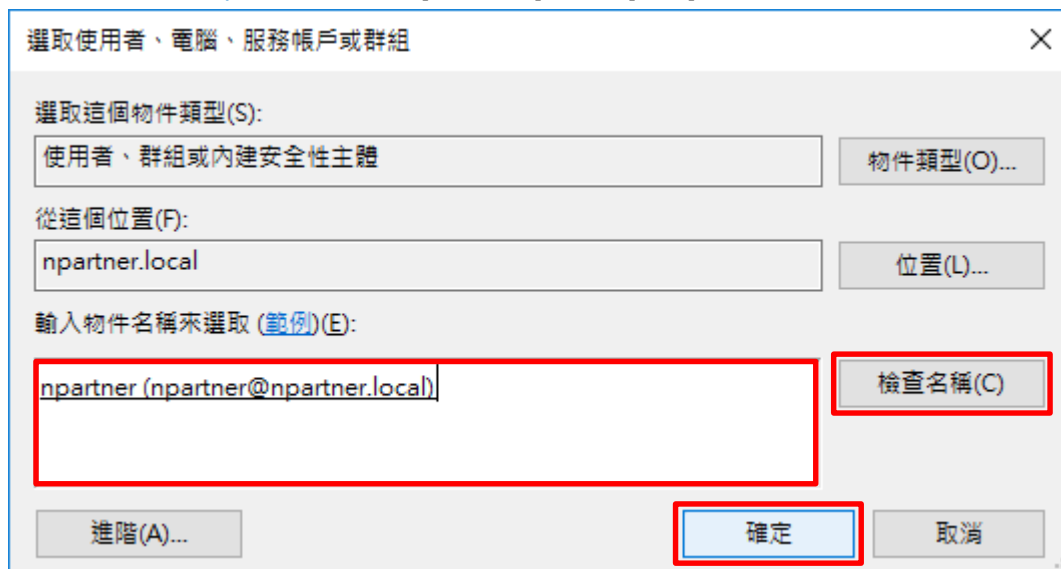
(5) 新增 WMI 使用者權限

按 [新增]



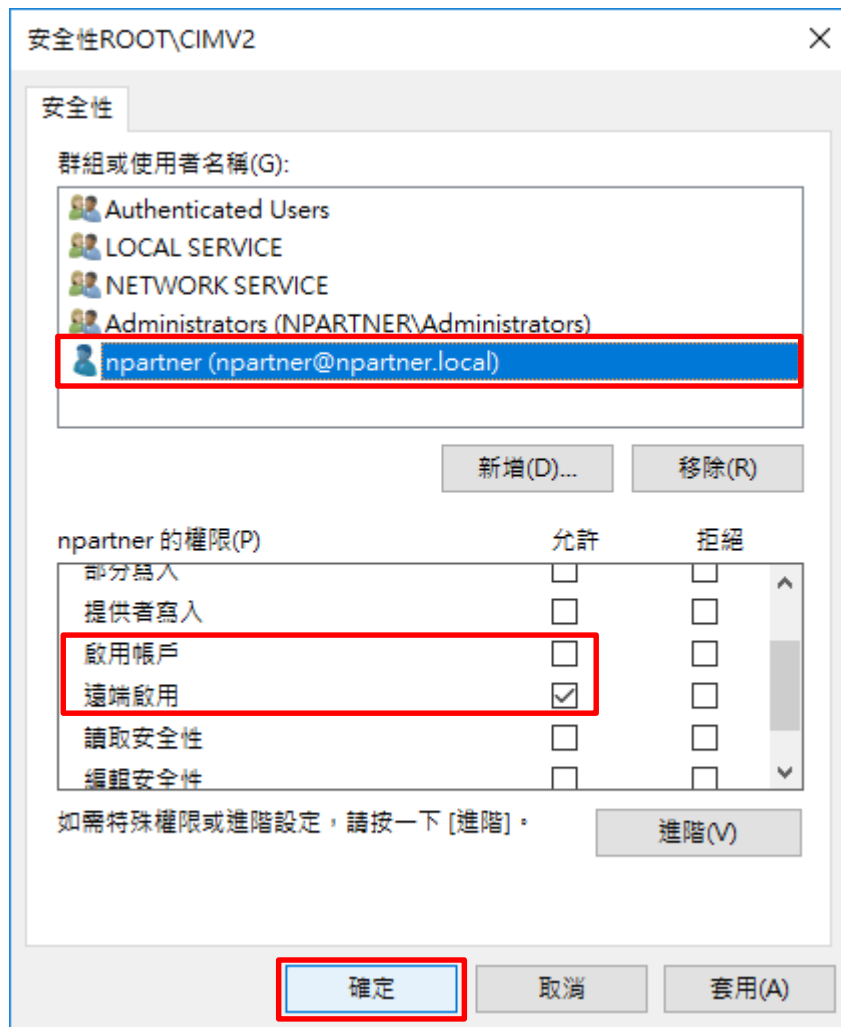
(6) 輸入使用者

輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

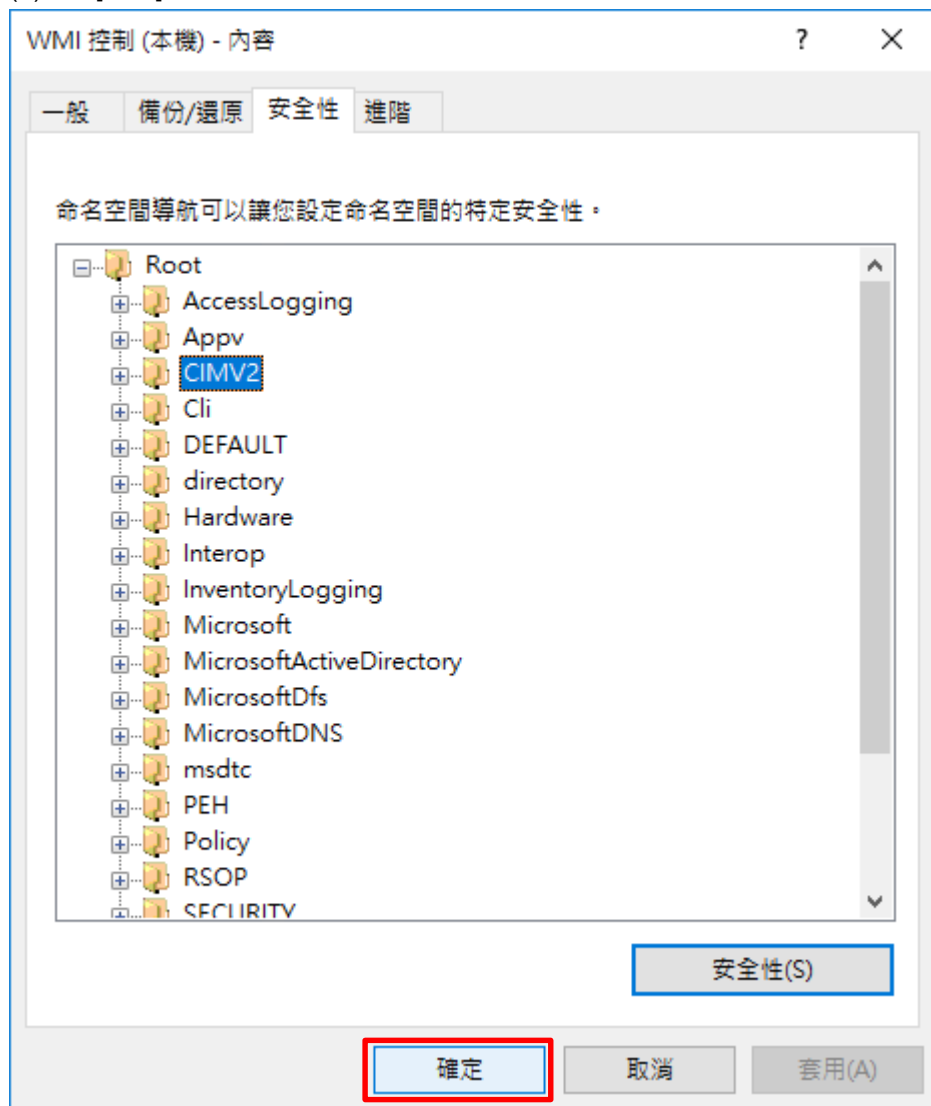


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



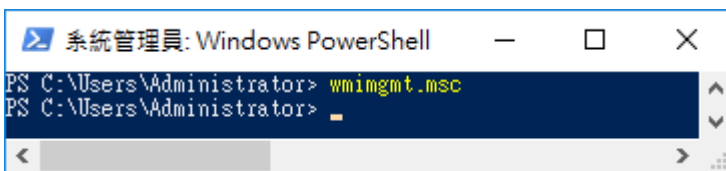
5.3.3.2 設定讀取使用者資料權限

(1) 開啟 [Windows PowerShell]



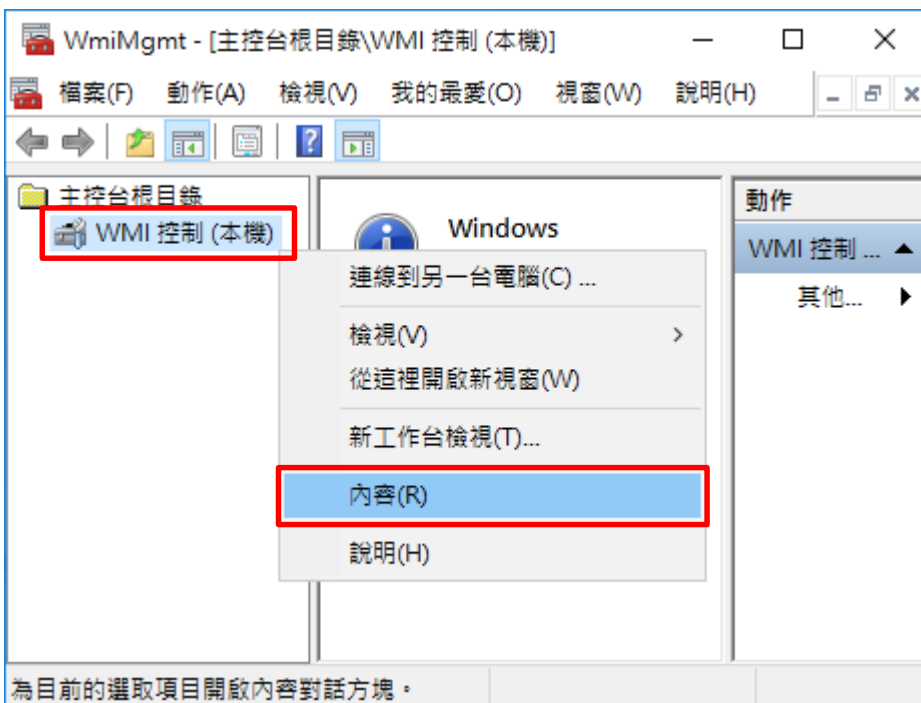
(2) 開啟元件服務

```
PS C:\> wimgmt.msc
```



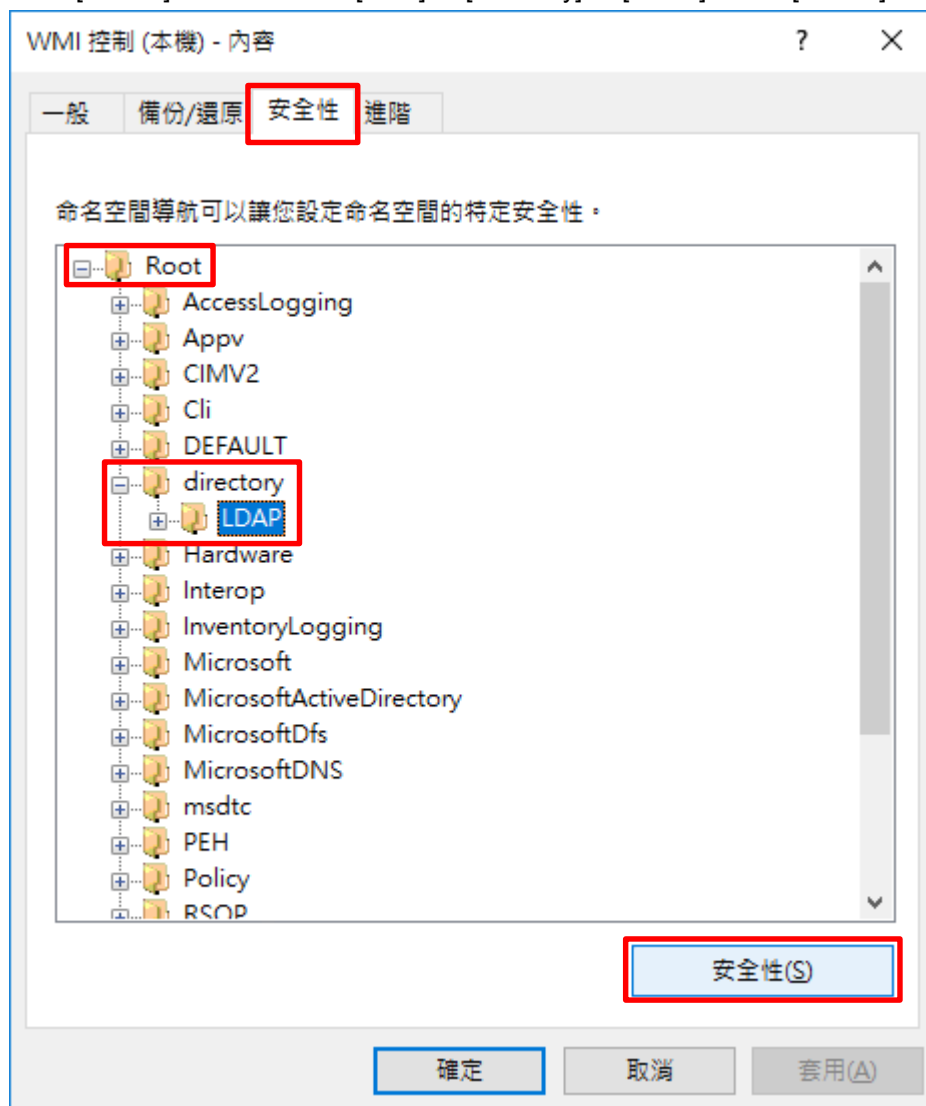
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



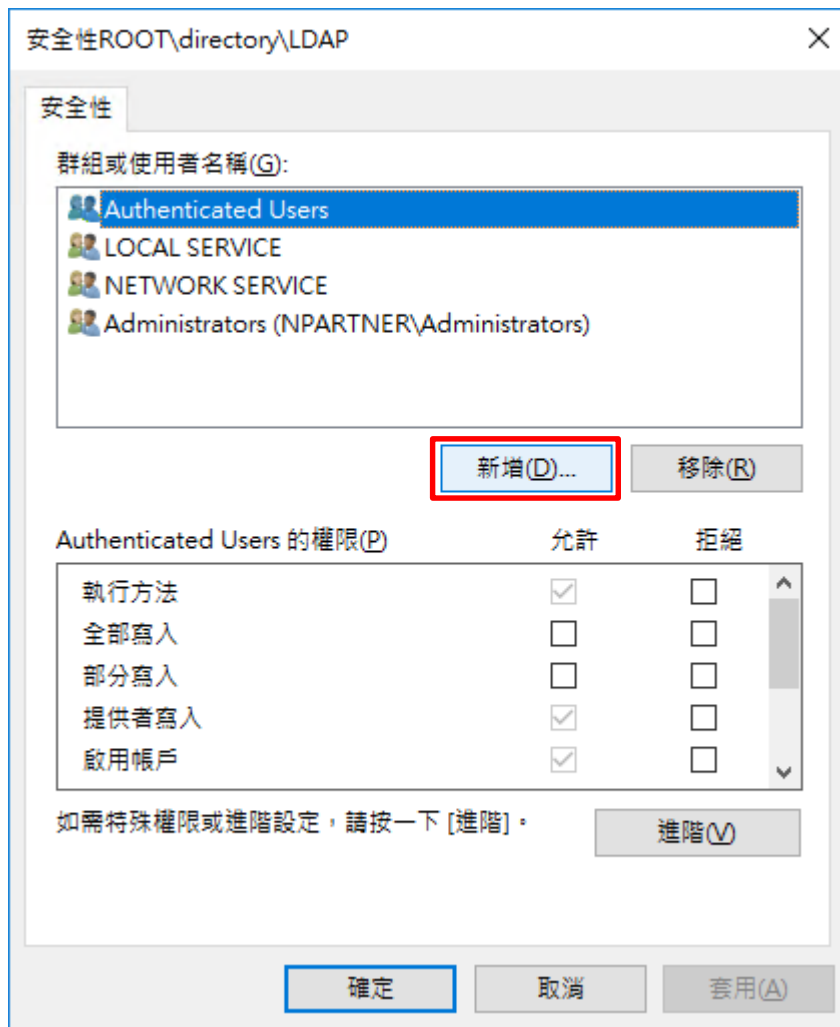
(4) 編輯 LDAP 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [directory] -> 按 [安全性]



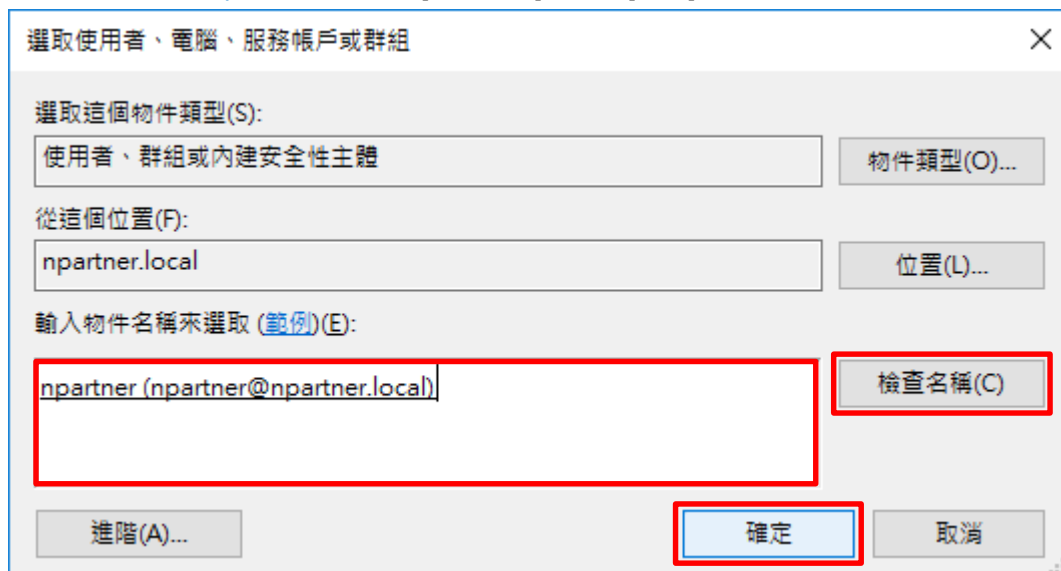
(5) 新增 WMI 使用者權限

按 [新增]



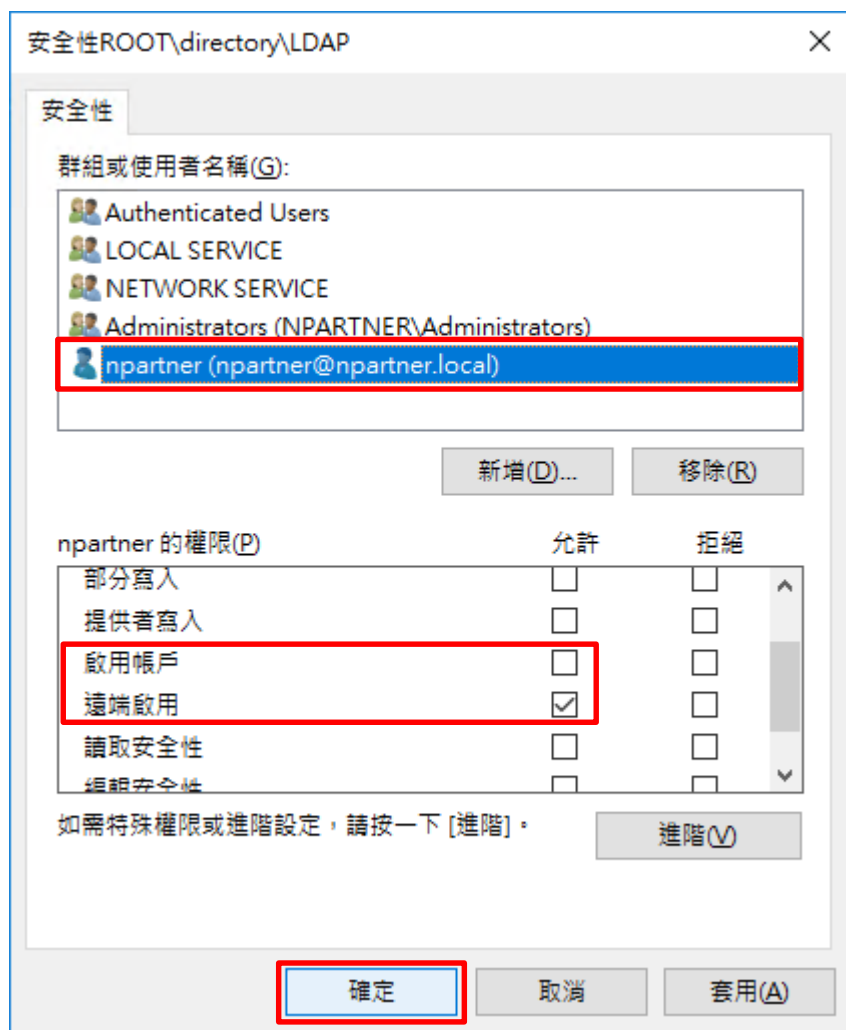
(6) 輸入使用者

輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

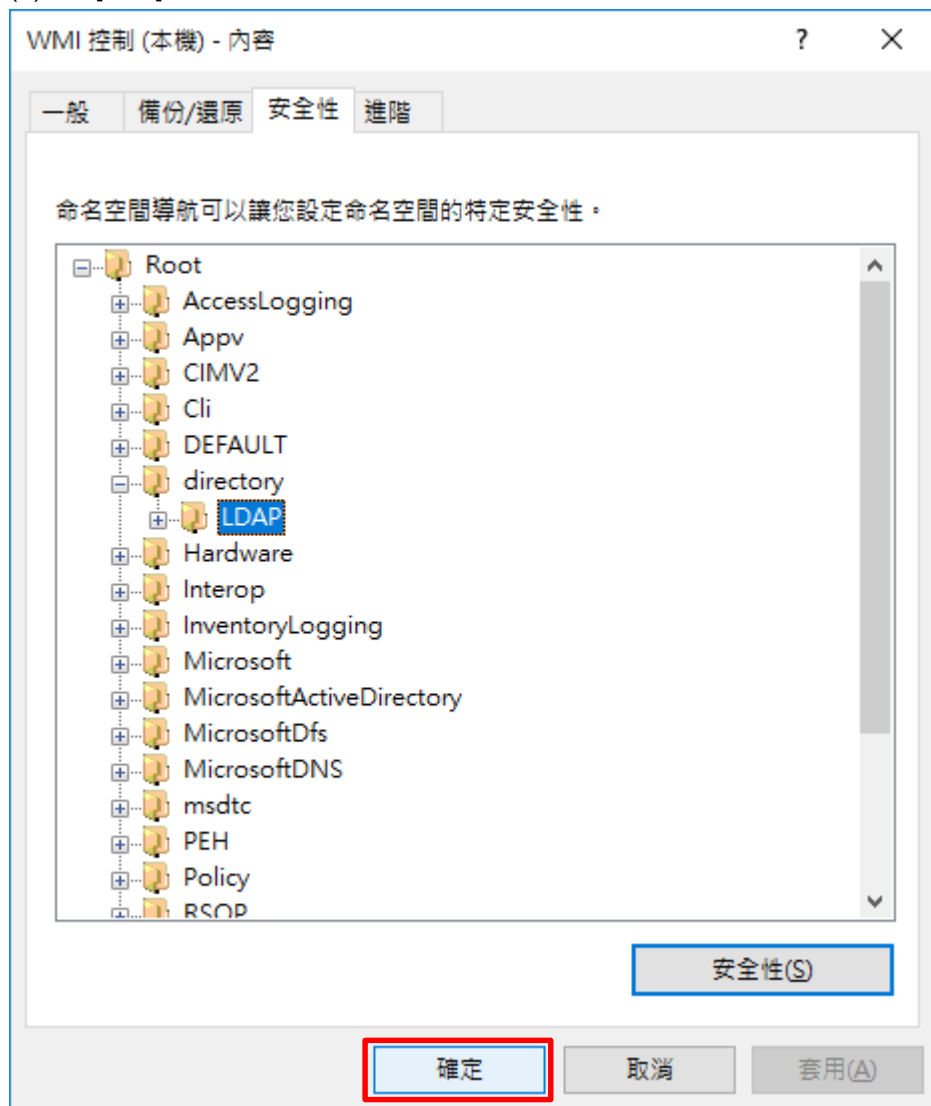


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]

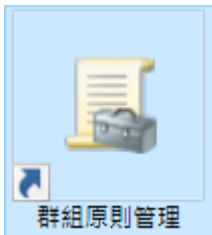


(8) 按 [確定]



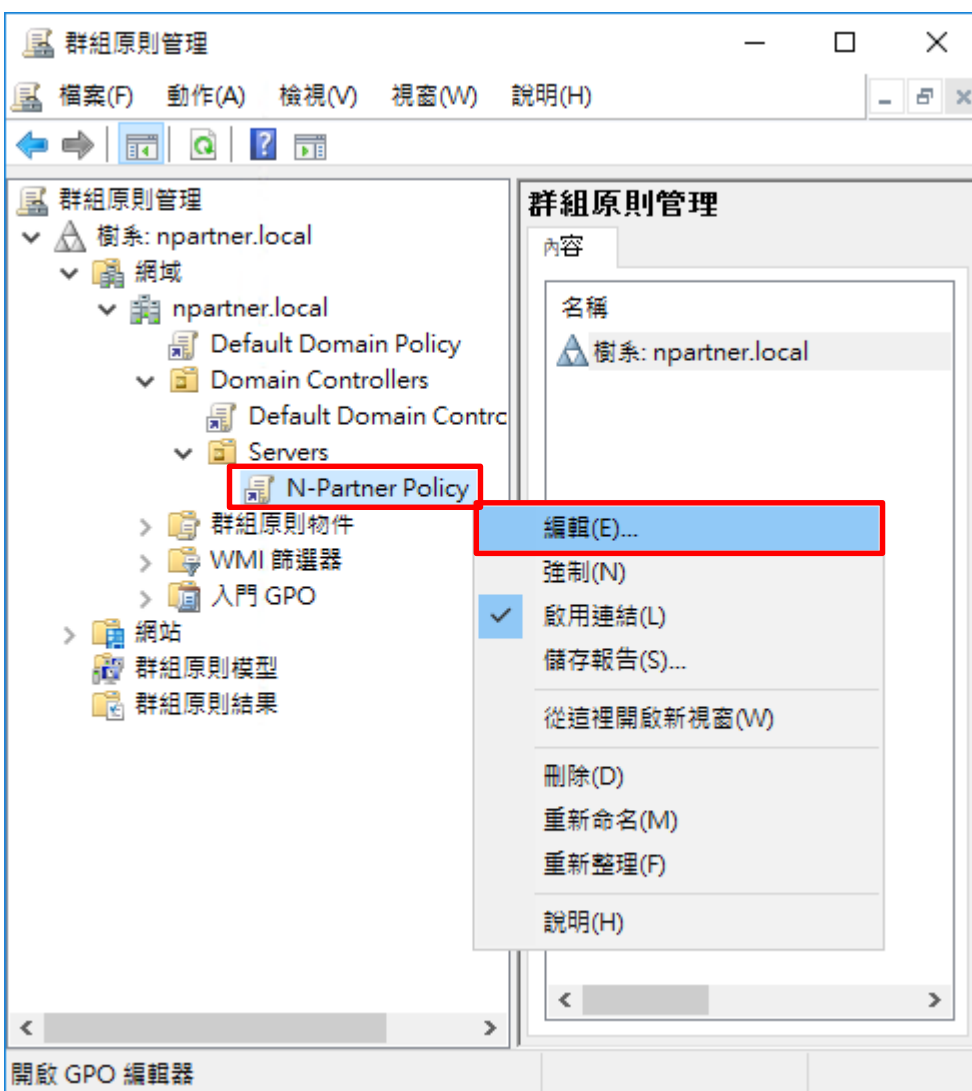
5.3.4 設定 Event log 讀取權限

(1) 開啟 [群組原則管理]




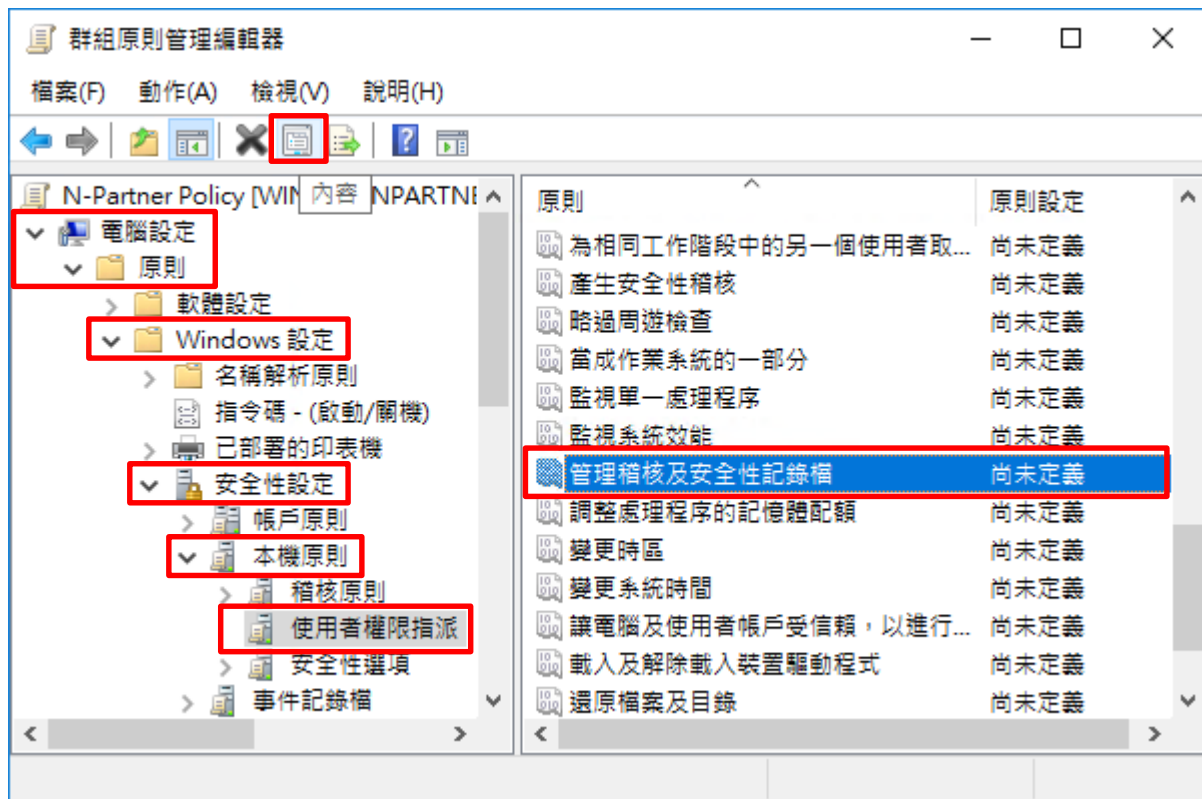
(2) 編輯群組原則物件

在 [N-Partner Policy] 群組原則物件，按滑鼠右鍵 -> 點選 [編輯]



(3) 設定記錄檔

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [使用者權限指派] -> 選擇 [管理稽核及安全記錄檔] 項目 -> 點選  內容



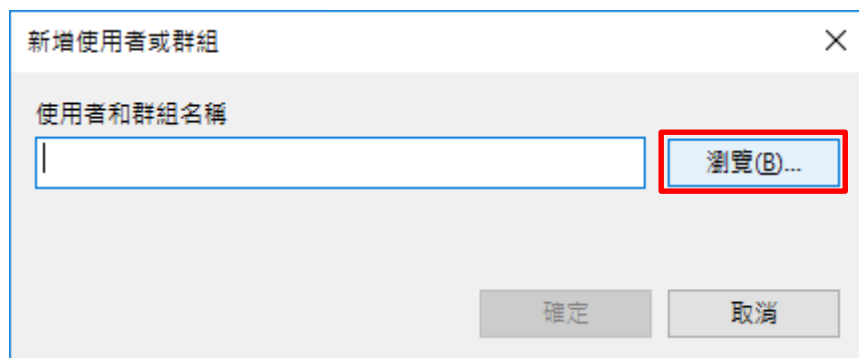
(4) 新增管理稽核使用者

勾選 [定義這些原則設定] -> 按 [新增使用者或群組...]



(5) 搜尋使用者

按 [瀏覽]



(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

選取使用者、電腦、服務帳戶或群組

選取這個物件類型(S):
使用者、服務帳戶、群組或內建安全性主體

物件類型(O)...

從這個位置(F):
npartner.local

位置(L)...

輸入物件名稱來選取 (範例)(E):
npartner (npartner@npartner.local)

檢查名稱(C)

進階(A)...

確定

取消

(7) 確定使用者

按 [確定]

新增使用者或群組

使用者和群組名稱
NPARTNER\npartner

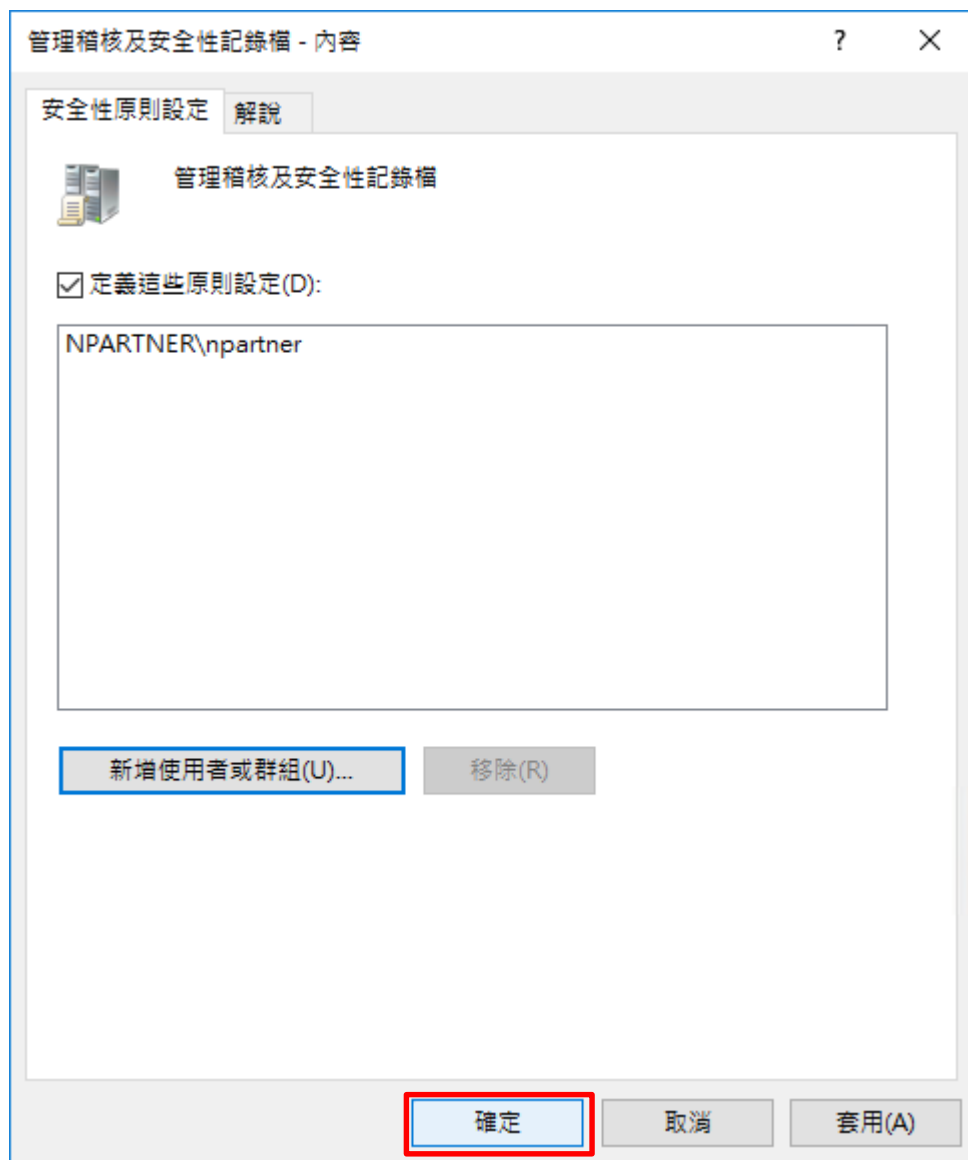
瀏覽(B)...

確定

取消

(8) 確定設定記錄檔

按 [確定]

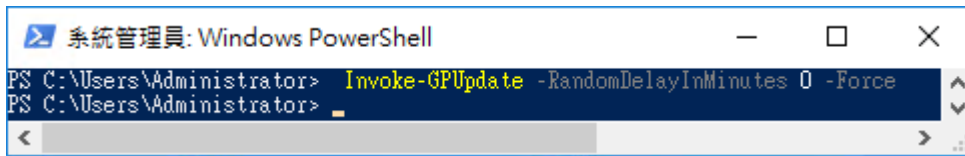


(9) 開啟 [Windows PowerShell]



(10) 更新群組原則

PS C:\> Invoke-GPUdate -RandomDelayInMinutes 0 -Force



```
系統管理員: Windows PowerShell
PS C:\Users\Administrator> Invoke-GPUdate -RandomDelayInMinutes 0 -Force
PS C:\Users\Administrator>
```

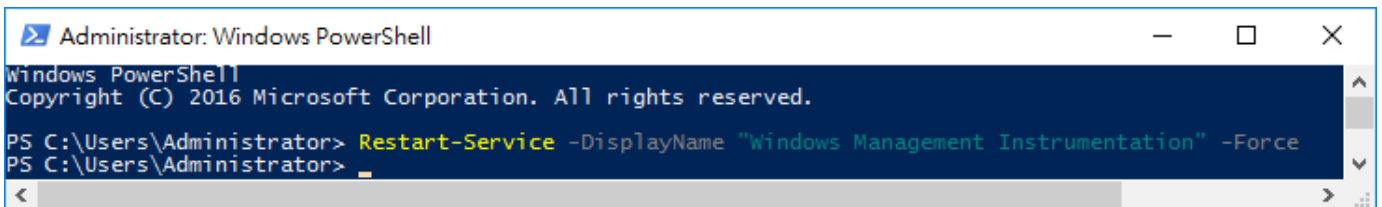
5.3.5 重啟 WMI 服務

(1) 開啟 [Windows PowerShell]



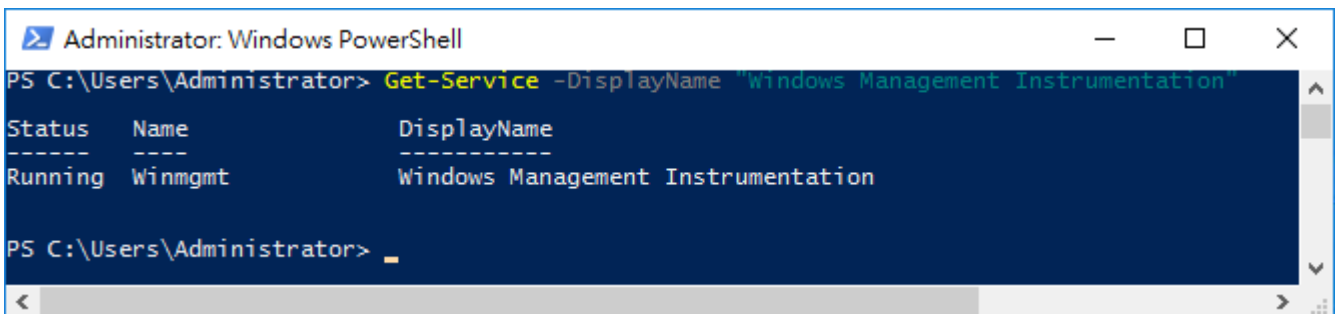
(2) 重啟 WMI 服務

```
PS C:\> Restart-Service -DisplayName "Windows Management Instrumentation" -Force
```



(3) 查看 WMI 服務

```
PS C:\> Get-Service -DisplayName "Windows Management Instrumentation"
```



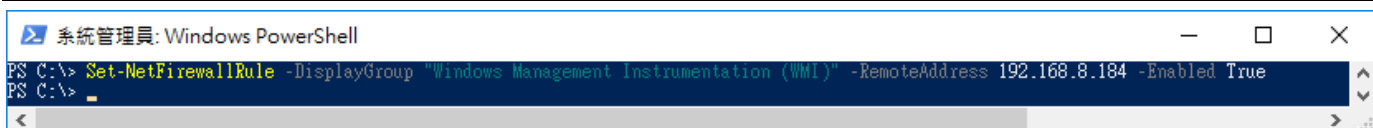
5.4 設定防火牆

(1) 開啟 [Windows PowerShell]



(2) 設定防火牆 · 只允許 N-Reporter IP query WMI

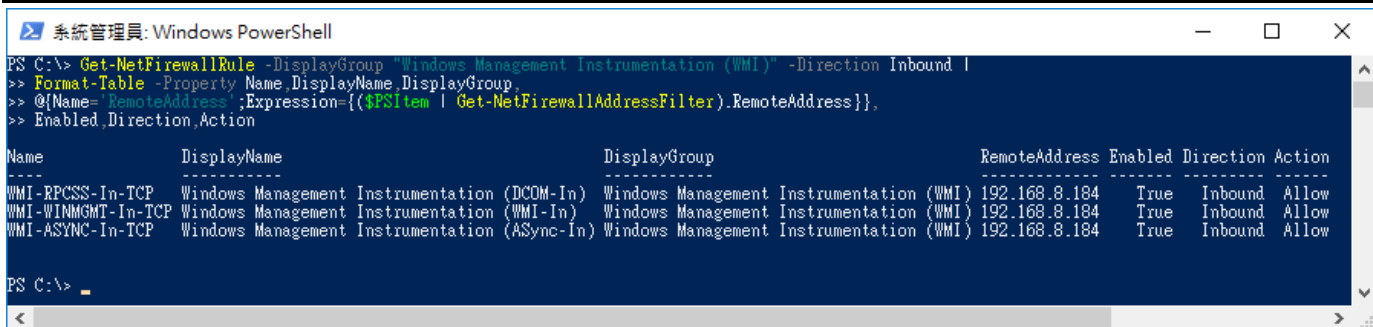
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.184 -Enabled True
```



紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 查看防火牆 WMI 啟用狀態

```
PS C:\> Get-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -Direction Inbound |  
>> Format-Table -Property Name,DisplayName,DisplayGroup,  
>> @{Name='RemoteAddress';Expression={($PSItem | Get-NetFirewallAddressFilter).RemoteAddress}},  
>> Enabled,Direction,Action
```

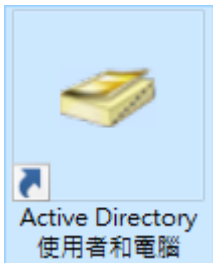


6. Windows 2019

Windows 稽核原則設定 [詳細說明請參考前言的稽核原則建議連結](#)

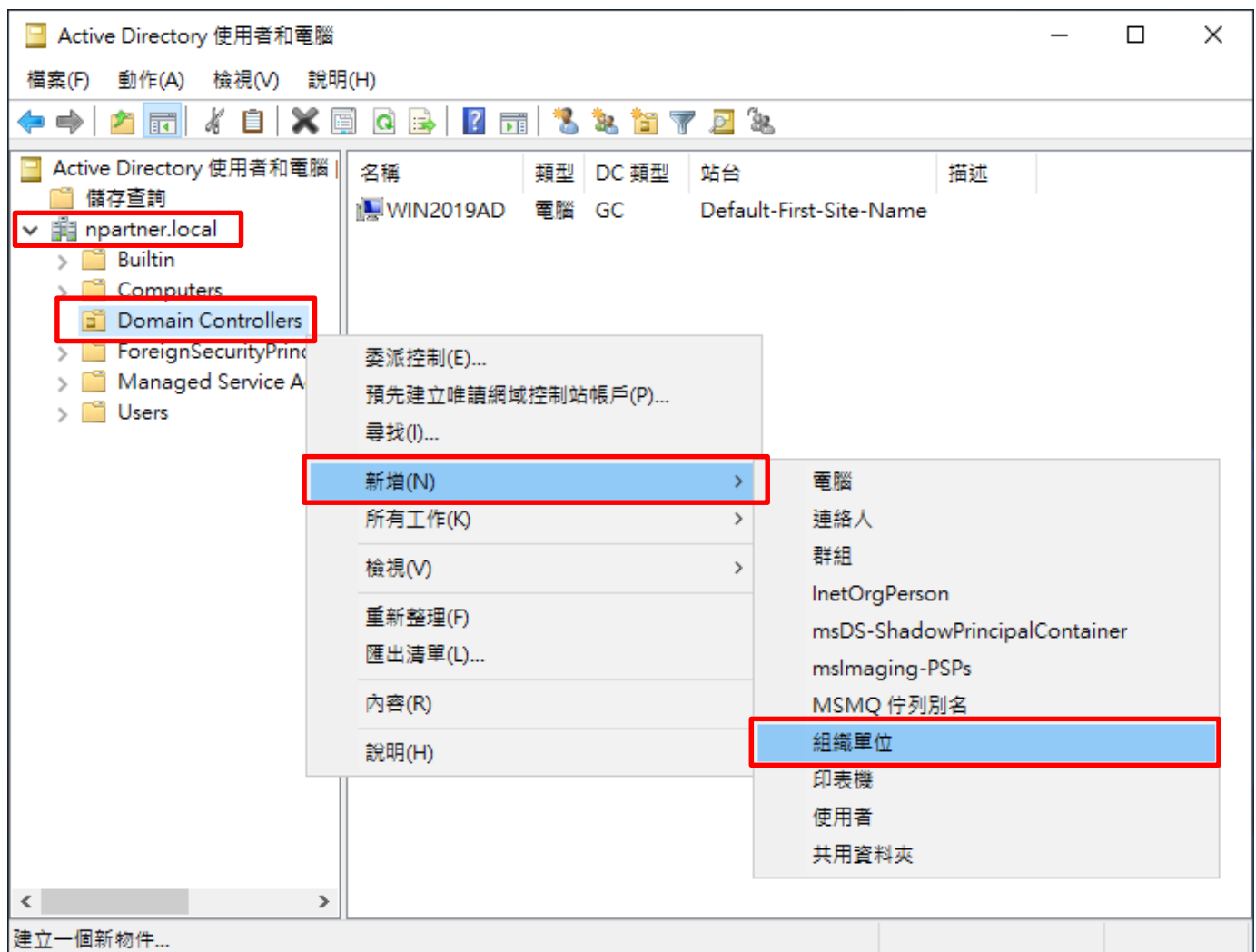
6.1 組織單位設定

(1) 開啟 [Active Directory 使用者和電腦]



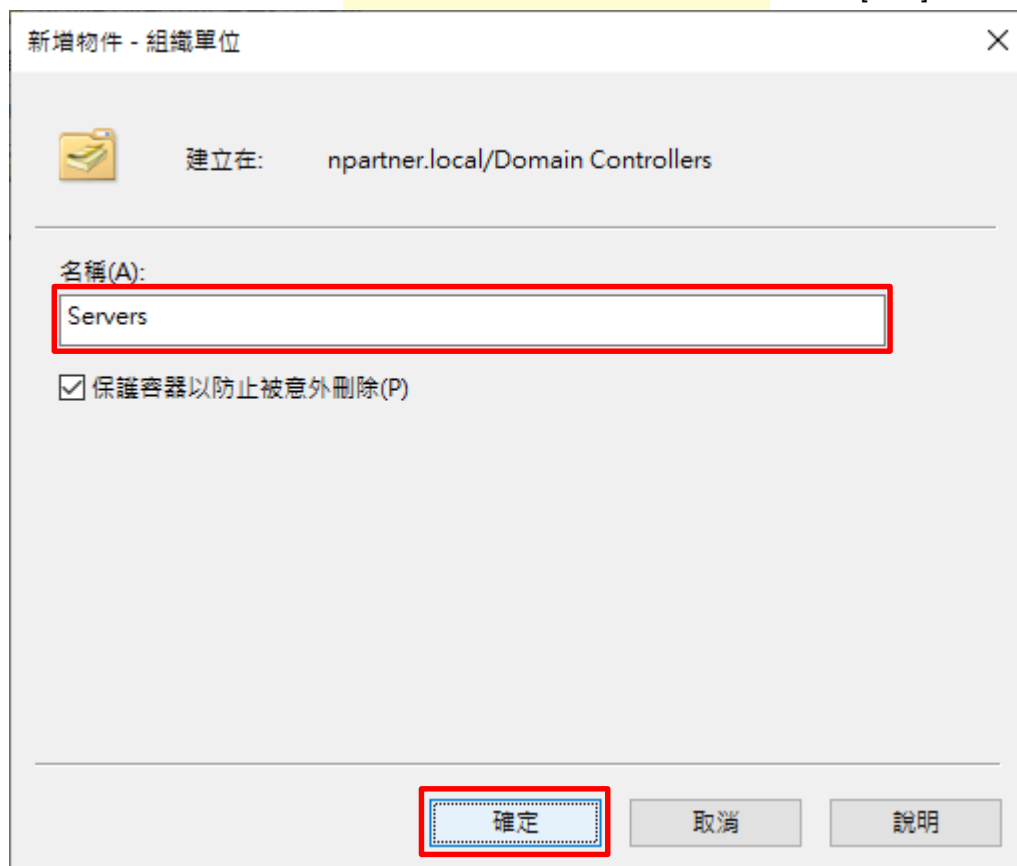
(2) 新增組織單位

[網域名稱] 的 [Domain Controllers] 組織單位 · 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]



(3) 輸入組織單位名稱

輸入組織單位名稱: Servers 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



新增物件 - 組織單位

建立在: npartner.local/Domain Controllers

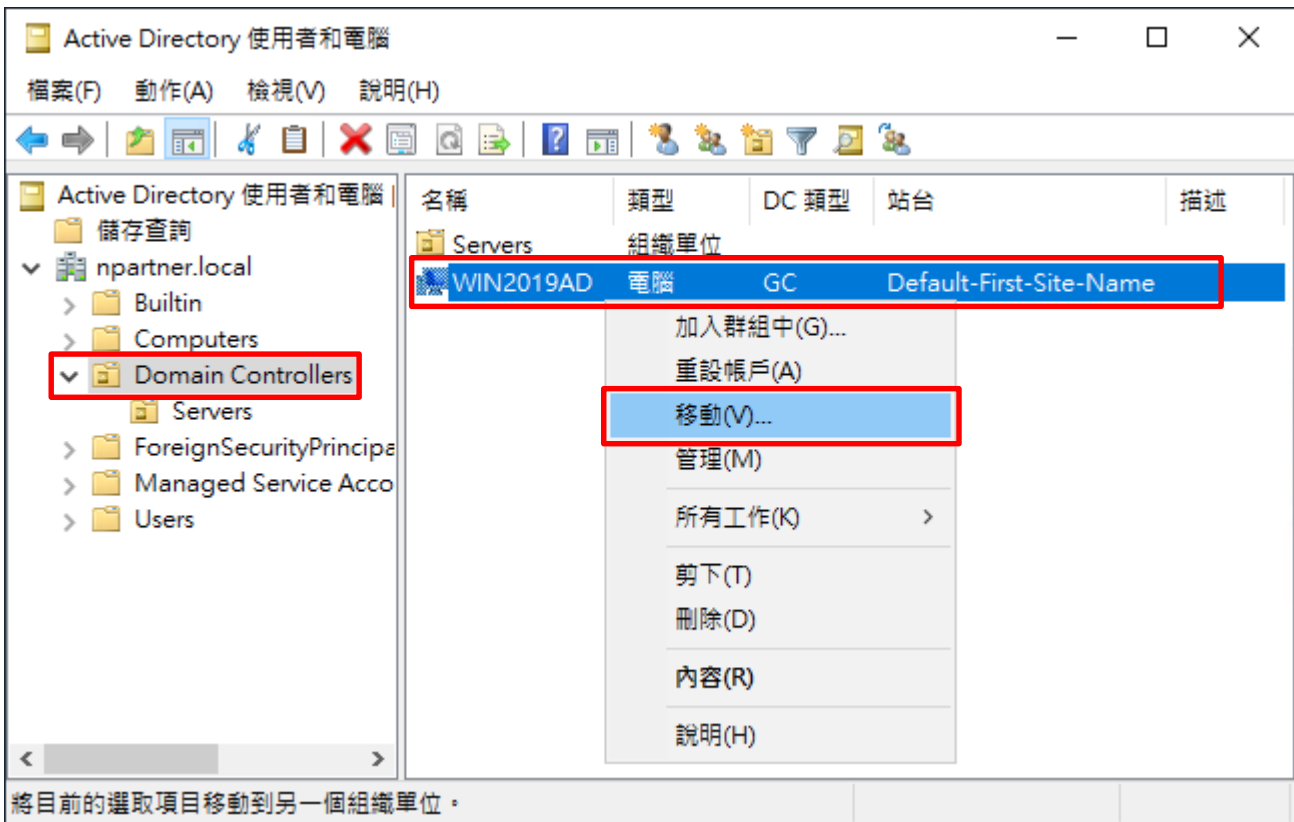
名稱(A):
Servers

保護容器以防止被意外刪除(P)

確定 取消 說明

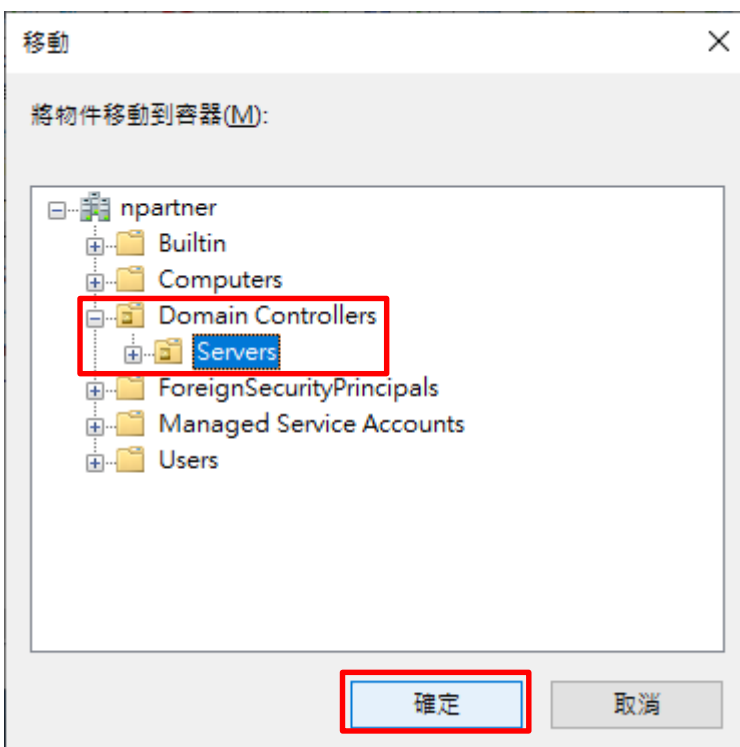
(4) 移動伺服器至新的組織單位

選擇 [Domain Controllers] 組織單位 -> 在 [Win2019AD] 按滑鼠右鍵，註：請依客戶環境選擇 Windows AD 主機
-> 點選 [移動]



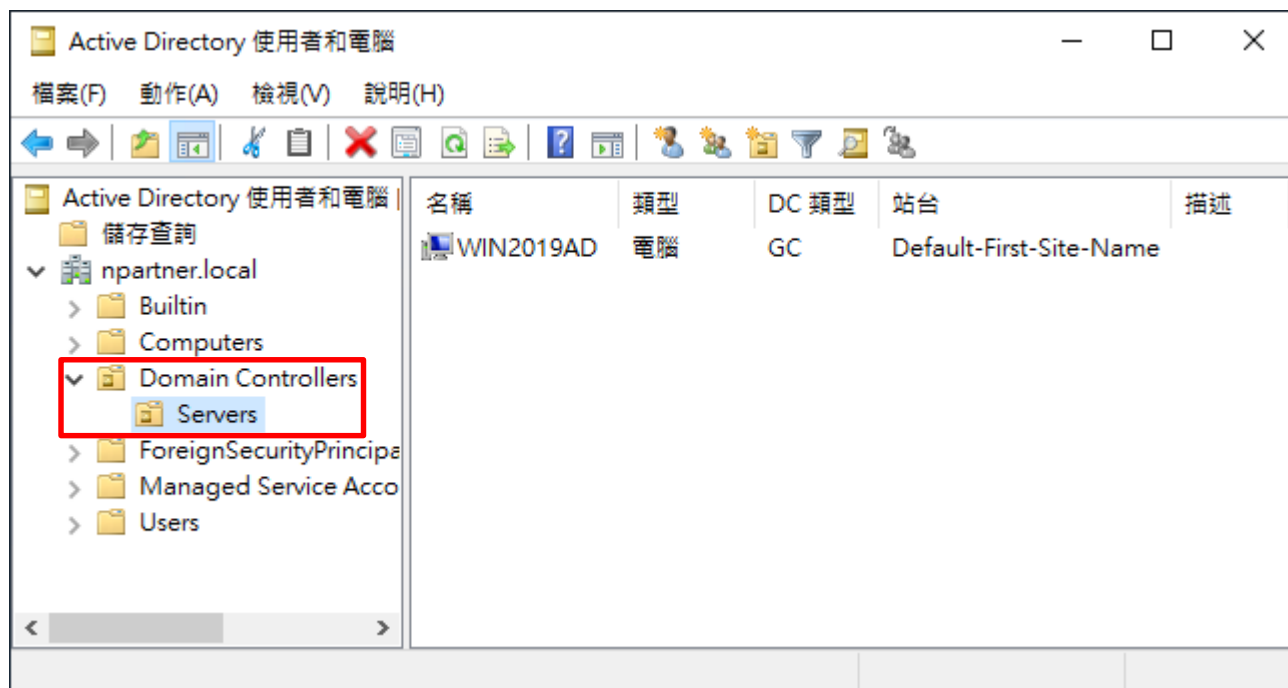
(5) 選擇組織單位

選擇 [Domain Controllers] 的 [Servers] 組織單位 -> 按 [確定]



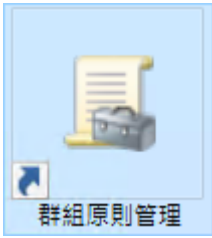
(6) 確認伺服器已移動至新的組織單位

展開 [Domain Controllers] 的 [Servers] 組織單位，確認 [Win2019AD] 伺服器已移動



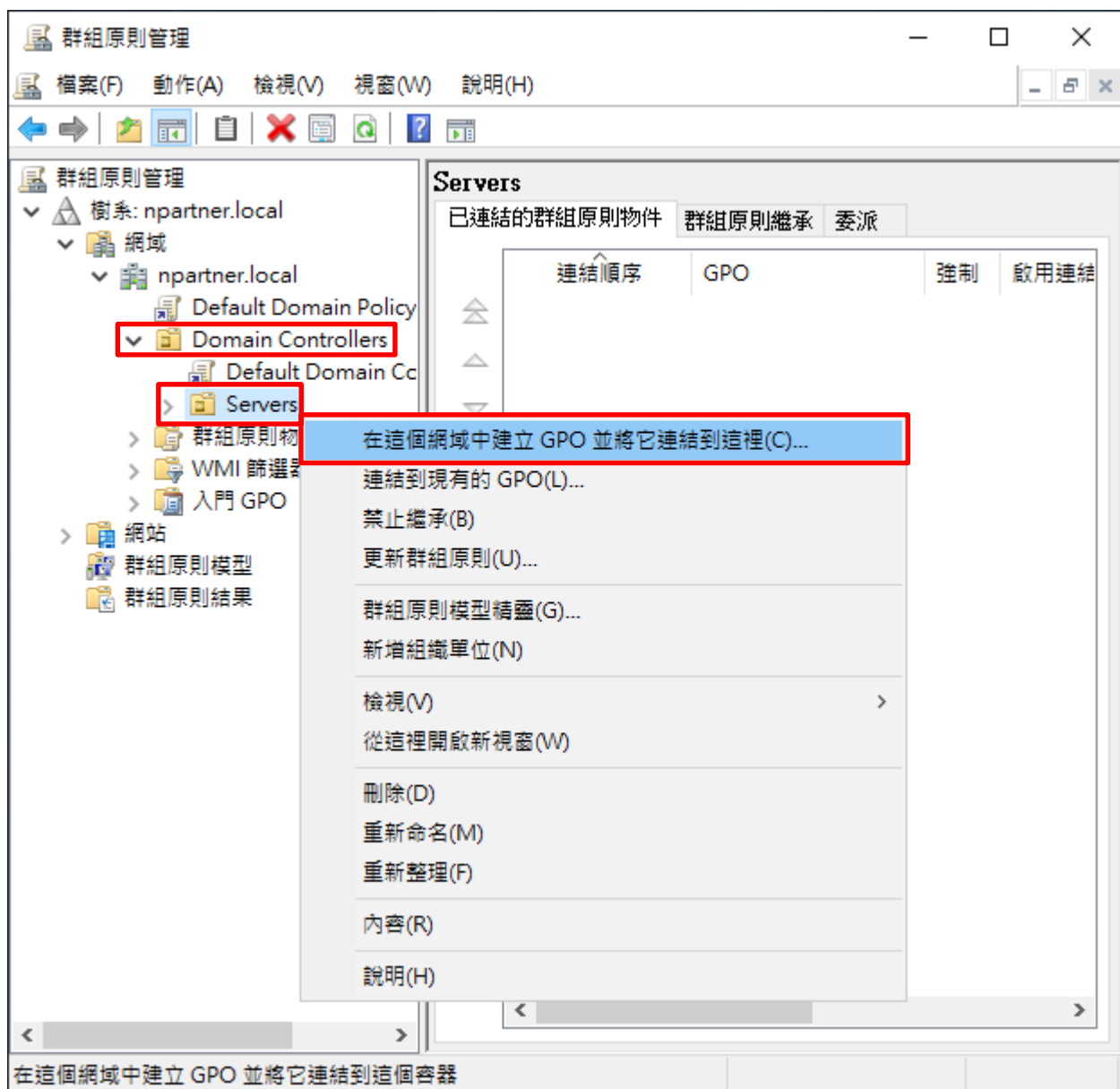
6.2 群組原則設定

(1) 開啟 [群組原則管理]



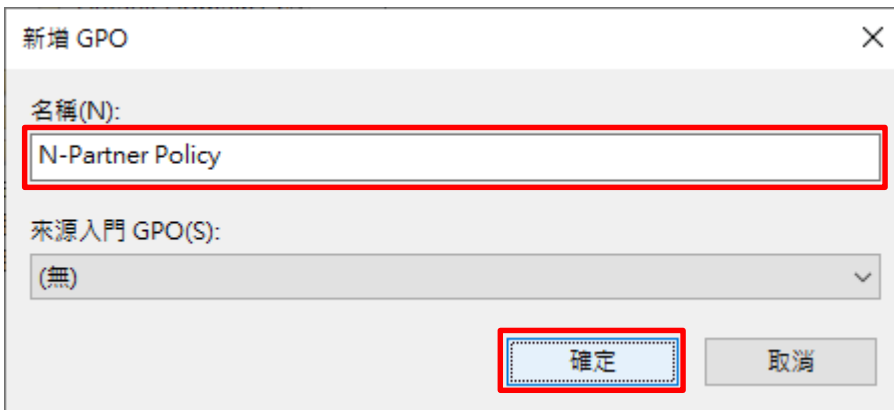
(2) 在 Servers 組織單位，新增群組原則物件

在 [Domain Controllers] 的 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到...]



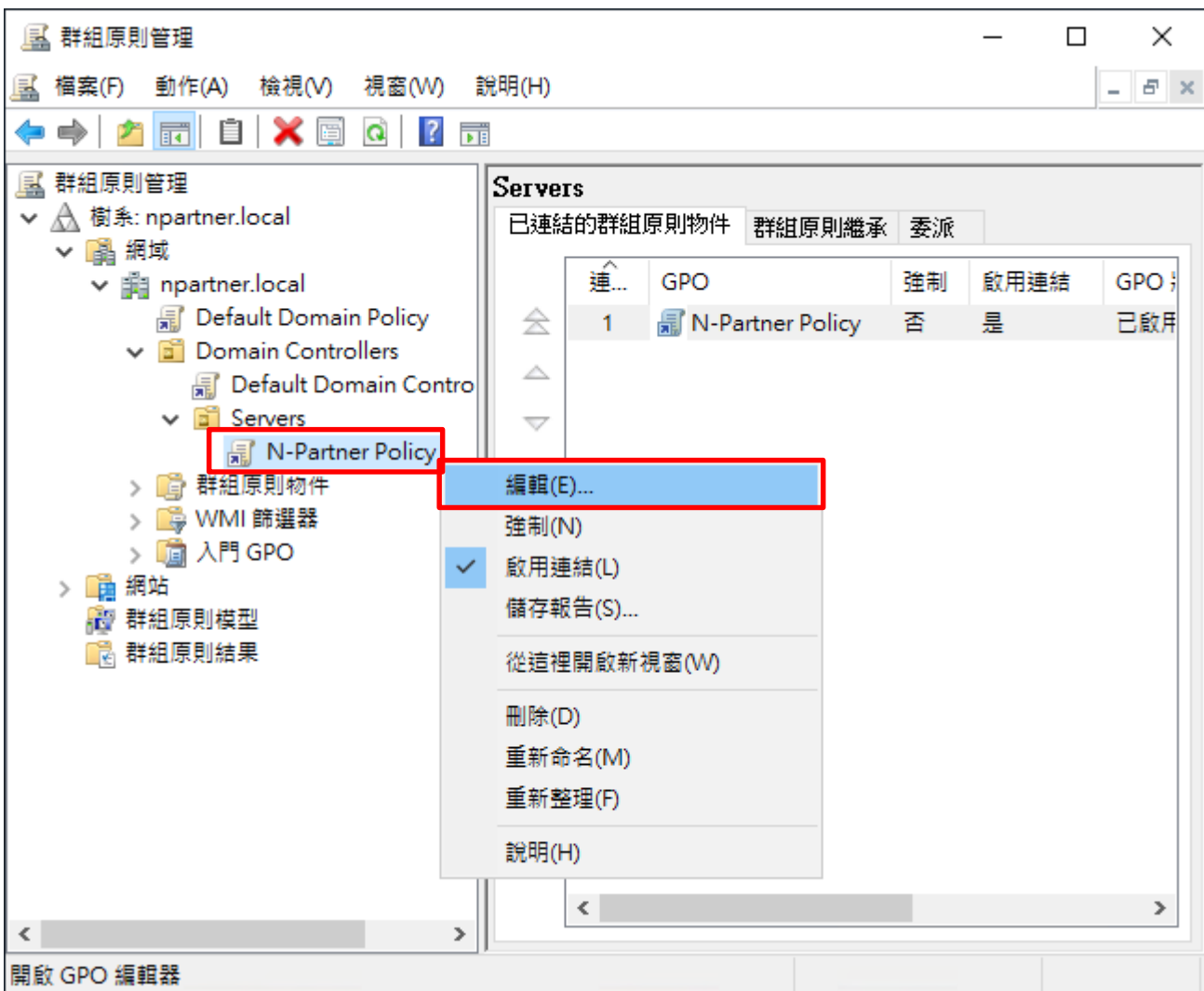
(3) 輸入群組原則物件名稱

輸入群組原則物件名稱: **N-Partner Policy** 註: 請依客戶環境建立群組物件名稱 -> 按 [確定]



(4) 編輯群組原則物件

在 [N-Partner Policy] 群組原則物件 · 按滑鼠右鍵 -> 點選 [編輯]



(5) 本機原則：稽核原則

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核目錄服務存取], [稽核系統事件], [稽核物件存取], [稽核原則變更], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件], [稽核程序追蹤] 項目 -> 勾選 [定義這些原則設定:] & [成功] & [失敗] -> 按 [確定]

群組原則管理編輯器

檔案(F) 動作(A) 檢視(V) 說明(H)

N-Partner Policy [WIN2019AD.NPA]

電腦設定

原則

軟體設定

Windows 設定

名稱解析原則

指令碼 - (啟動/關機)

已部署的印表機

安全性設定

帳戶原則

本機原則

稽核原則

使用者權限指派

安全性選項

事件記錄檔

受限群組

系統服務

登錄

檔案系統

有線網路 (IEEE 802)

具有進階安全性的 V

網路清單管理員原則

無線網路 (IEEE 802)

公開金鑰原則

軟體限制原則

應用程式控制原則

IP 安全性原則 (位置)

進階稽核原則設定

以原則為依據的 QoS

系統管理範本: 已從本機電

喜好設定

使用者設定

原則

喜好設定

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

稽核程序追蹤 - 內容

安全性原則設定 解說

稽核程序追蹤

定義這些原則設定(D)

稽核這些嘗試:

成功(S)

失敗(F)

確定 取消 套用(A)

(6) 事件記錄：安全性記錄檔大小最大值

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔大小最大值] 項目 -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]

The screenshot shows the Group Policy Management console for the 'N-Partner Policy [WIN2019AD.NPA]'. The left-hand navigation pane is expanded to show the following path: 電腦設定 (Computer Configuration) > 原則 (Policies) > Windows 設定 (Windows Settings) > 安全性設定 (Security Settings) > 事件記錄檔 (Event Log). The right-hand pane displays a list of policies, with '安全性記錄檔大小最大值' (Maximum size of security event log) selected and highlighted. The value for this policy is set to 204800 KB. Below the main console, a dialog box titled '安全性記錄檔大小最大值 - 內容' (Maximum size of security event log - Content) is open. In this dialog, the '定義這個原則設定(D)' (Define this policy setting) checkbox is checked. The value '204800' is entered in the text box, followed by 'KB' in the unit dropdown. A warning icon and text are visible at the bottom of the dialog, stating: '修改這個設定可能影響與用戶端、服務及應用程式間的相容性。如需其他資訊，請參閱[安全性記錄檔大小最大值](#)。(Q823659)'. The '確定' (OK) button is highlighted with a red box.

原則	原則設定
不允許本機來賓存取安全性記錄檔	尚未定義
不允許本機來賓存取系統記錄檔	尚未定義
不允許本機來賓存取應用程式記錄檔	尚未定義
安全性記錄檔大小最大值	204800 KB
安全性記錄檔保持方法	尚未定義
安全性記錄檔保留天數	尚未定義
系統記錄檔大小最大值	尚未定義
系統記錄檔保持方法	尚未定義
系統記錄檔保留天數	尚未定義
應用程式記錄保持方法	尚未定義
應用程式記錄檔大小最大值	尚未定義
應用程式記錄檔保留天數	尚未定義

(7) 事件記錄：安全性記錄檔大小最大值

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔保持方法] 項目 -> 勾選 [定義這個原則設定] -> 點選 [視需要覆寫事件] -> 按 [確定]

群組原則管理編輯器

檔案(F) 動作(A) 檢視(V) 說明(H)

N-Partner Policy [WIN2019AD.NPA]

原則	原則設定
不允許本機來賓存取安全性記錄檔	尚未定義
不允許本機來賓存取系統記錄檔	尚未定義
不允許本機來賓存取應用程式記錄檔	尚未定義
安全性記錄檔大小最大值	204800 KB
安全性記錄檔保持方法	視需要而定
安全性記錄檔保留天數	尚未定義
系統記錄檔大小最大值	尚未定義
系統記錄檔保持方法	尚未定義
系統記錄檔保留天數	尚未定義
應用程式記錄保持方法	尚未定義
應用程式記錄檔大小最大值	尚未定義
應用程式記錄檔保留天數	尚未定義

安全性記錄檔保持方法 - 內容

安全性原則設定 解說

安全性記錄檔保持方法

定義這個原則設定(D)

依日期覆寫事件(O)

視需要覆寫事件(V)

不要覆寫事件 (以手動方式清除記錄)(N)

修改這個設定可能影響與用戶端、服務及應用程式間的相容性。
如需其他資訊，請參閱[安全性記錄檔保持方法](#)。(Q823659)

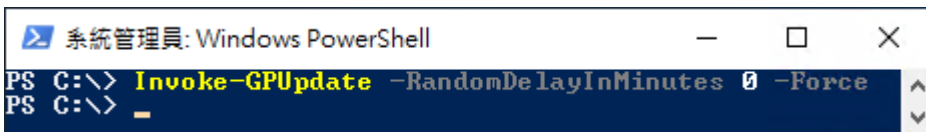
確定 取消 套用(A)

(8) 開啟 [Windows PowerShell]



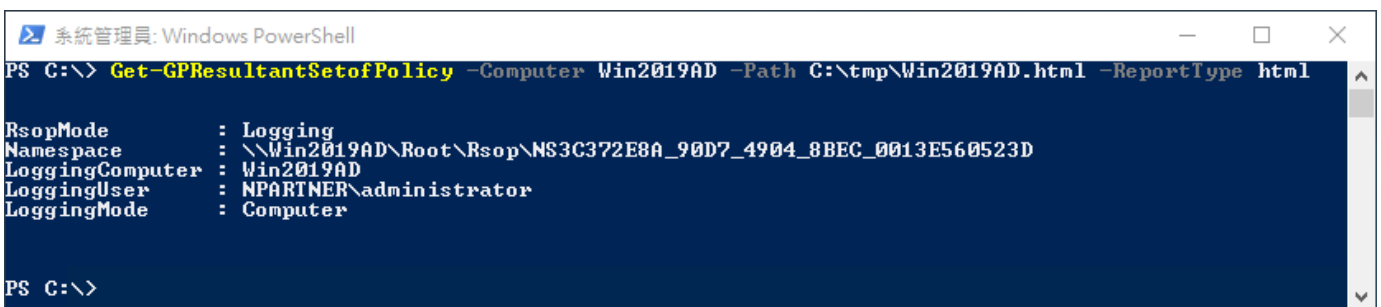
(9) 更新群組原則

```
PS C:\> Invoke-GPUUpdate -RandomDelayInMinutes 0 -Force
```



(10) 產生伺服器群組原則報表

```
PS C:\> Get-GPResultantSetofPolicy -Computer Win2019AD -Path C:\tmp\Win2019AD.html -ReportType html
```



紅色文字部位請輸入 Windows AD 伺服器名稱和資料夾路徑檔案名稱

(11) 開啟報表 · 確認 Windows 2019 AD 伺服器 · 套用 N-Partner Policy 群組原則

原則	設定	優勢 GPO
Windows 設定		
安全性設定		
帳戶原則/密碼規則		
帳戶原則/帳戶鎖定原則		
帳戶原則/Kerberos 原則		
本機原則/稽核原則		
原則	設定	優勢 GPO
稽核目錄服務存取	成功, 失敗	N-Partner Policy
稽核系統事件	成功, 失敗	N-Partner Policy
稽核物件存取	成功, 失敗	N-Partner Policy
稽核原則變更	成功, 失敗	N-Partner Policy
稽核帳戶登入事件	成功, 失敗	N-Partner Policy
稽核帳戶管理	成功, 失敗	N-Partner Policy
稽核登入事件	成功, 失敗	N-Partner Policy
稽核程序追蹤	成功, 失敗	N-Partner Policy
本機原則/使用者權限指派		
本機原則/安全性選項		
事件記錄檔		
原則	設定	優勢 GPO
安全性記錄檔保持方法	視需要而定	N-Partner Policy
安全性記錄檔容量最大值	204800 KB	N-Partner Policy
公開金鑰原則/憑證服務用戶端 - 自動註冊設定		
公開金鑰原則/加密檔案系統		

6.3 新增非管理帳號

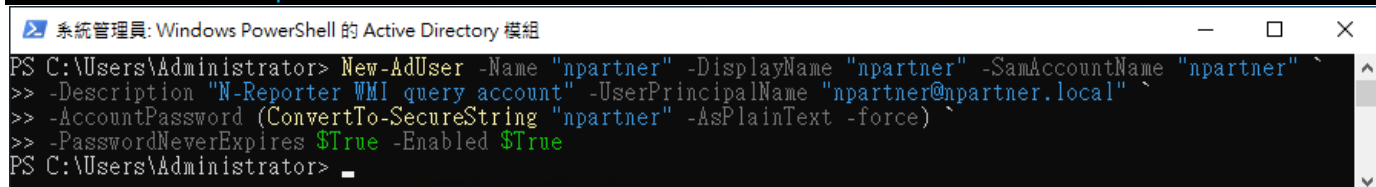
6.3.1 新增使用者

(1) 開啟 [Windows PowerShell 的 Active Directory 模組]



(2) 新增帳號

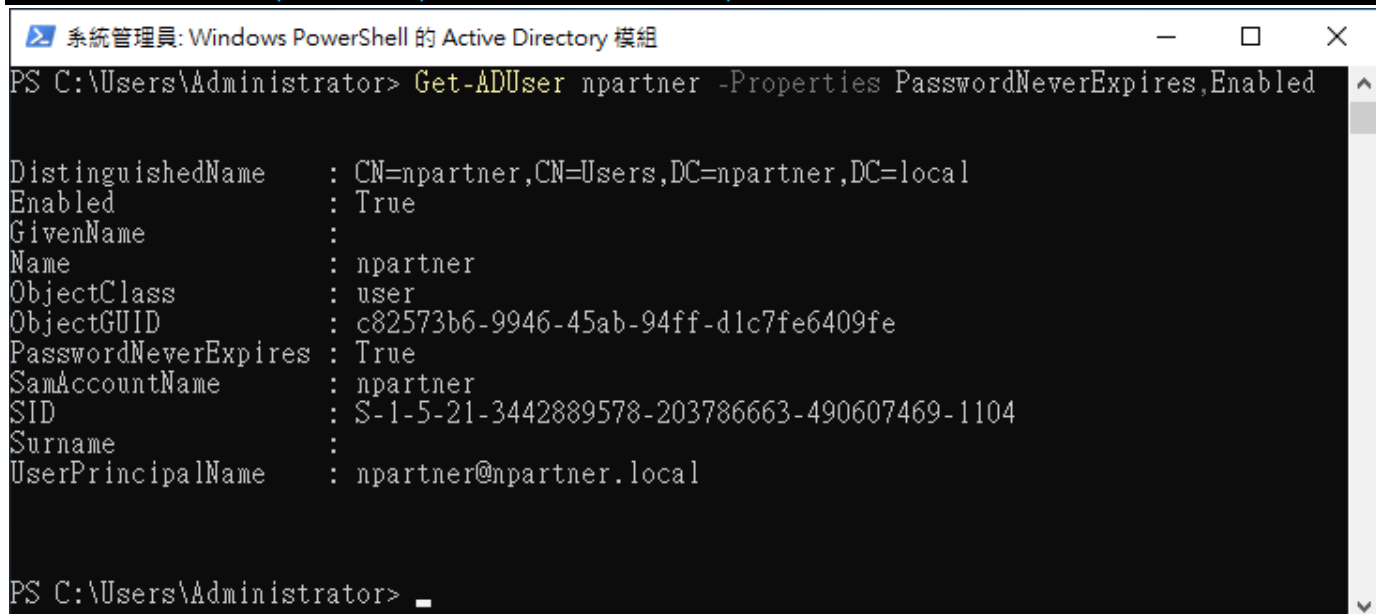
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True
```



紅色文字部位請輸入帳號密碼及網域資訊

(3) 查看帳號狀態

```
PS C:\> Get-ADUser npartner -Properties PasswordNeverExpires,Enabled
```



```
DistinguishedName      : CN=npartner,CN=Users,DC=npartner,DC=local
Enabled                 : True
GivenName               :
Name                    : npartner
ObjectClass             : user
ObjectGUID              : c82573b6-9946-45ab-94ff-d1c7fe6409fe
PasswordNeverExpires   : True
SamAccountName          : npartner
SID                     : S-1-5-21-3442889578-203786663-490607469-1104
Surname                 :
UserPrincipalName       : npartner@npartner.local

PS C:\Users\Administrator>
```

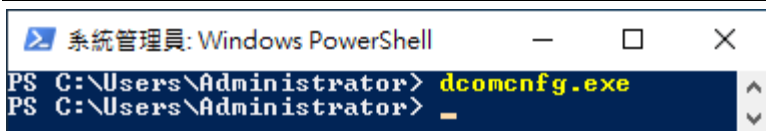
6.3.2 設定 DCOM 權限

(1) 開啟 [Windows PowerShell]



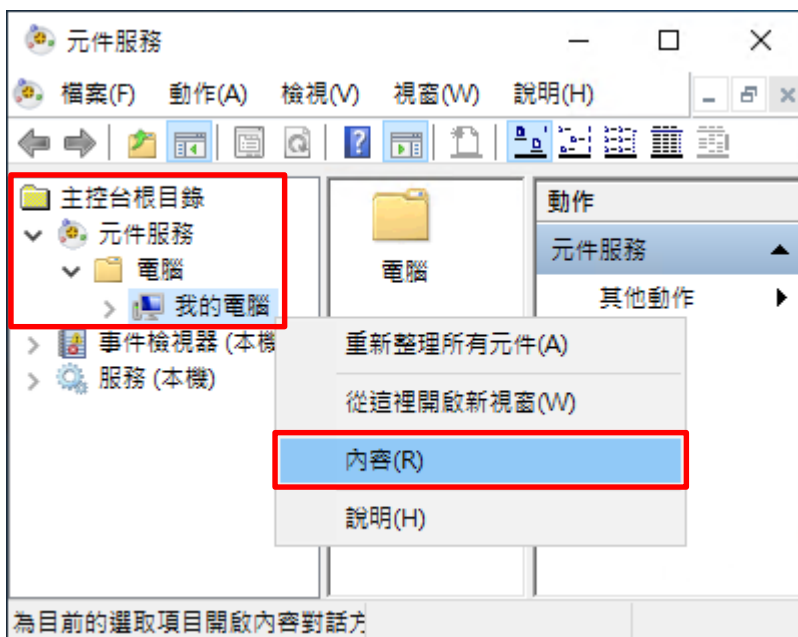
(2) 開啟元件服務

```
PS C:\> dcomcnfg.exe
```



(3) 編輯電腦內容

展開 [主控台根目錄], [元件服務], [電腦] -> 在 [我的電腦] 按滑鼠右鍵 -> 點選 [內容]



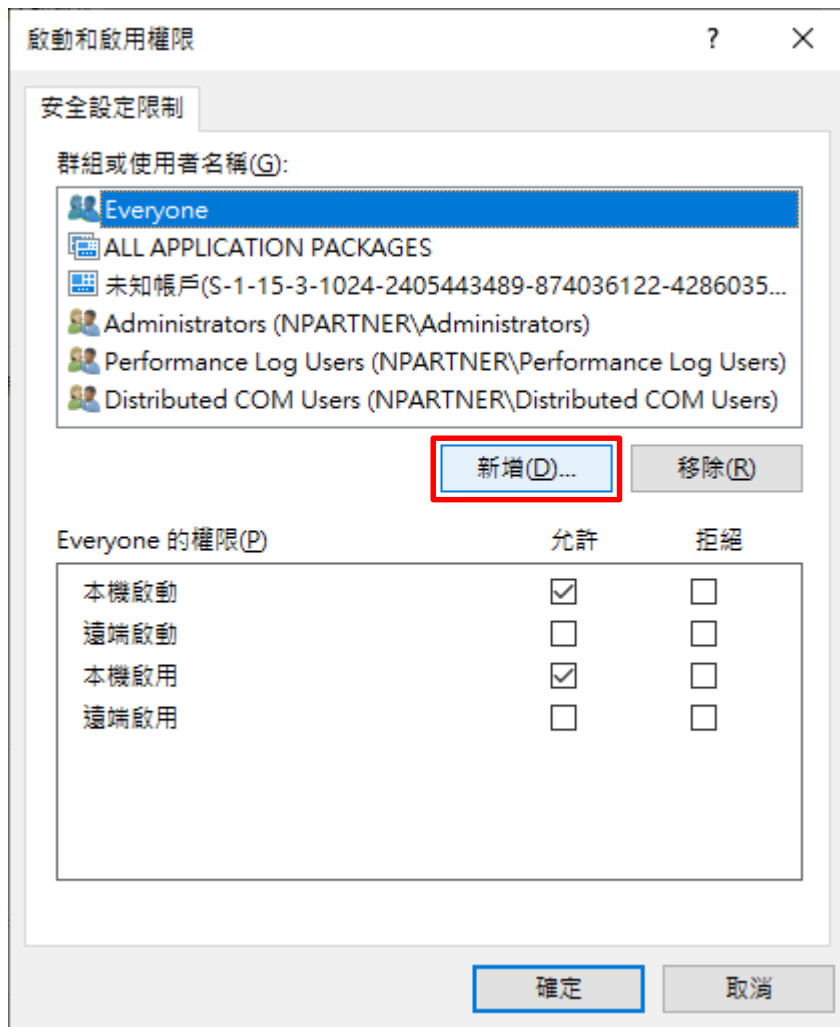
(4) 啟用權限

點選 [COM 安全性] 頁面 -> 啟動和啟用權限，按 [編輯限制]



(5) 新增 DCOM 使用者權限

點選 [新增]



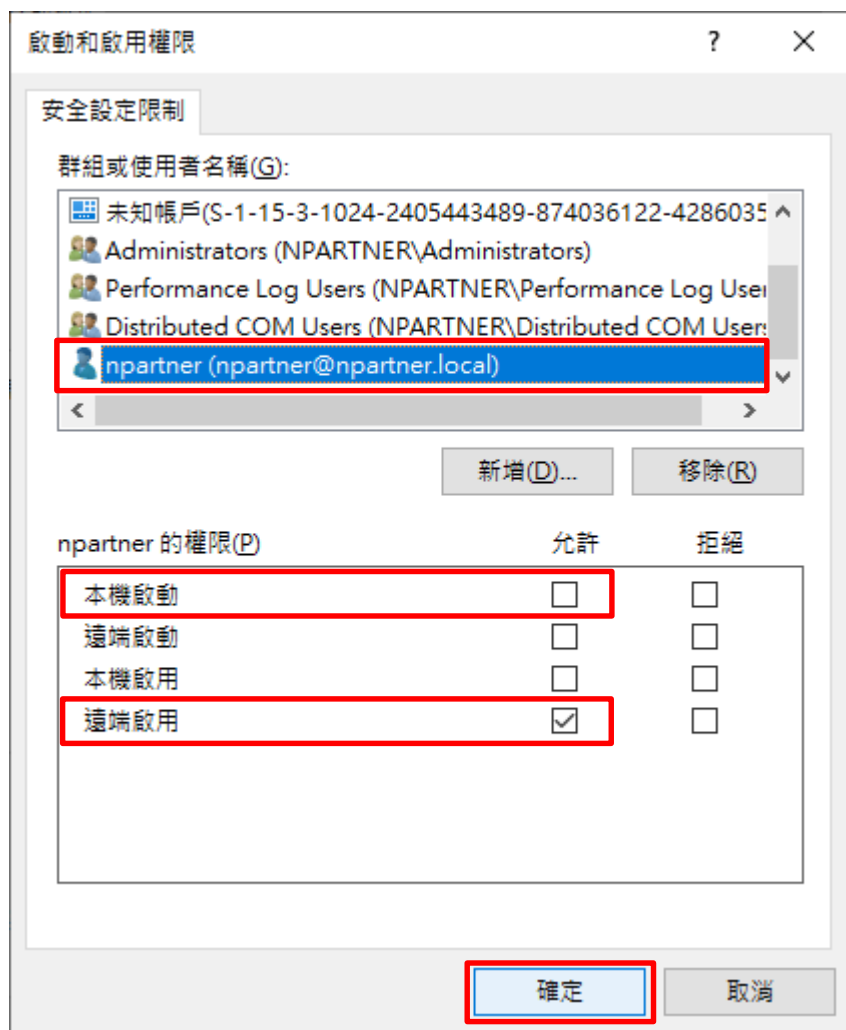
(6) 輸入使用者

輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]



(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [本機啟動:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 確定使用者權限

按 [確定]



6.3.3 設定 WMI 權限

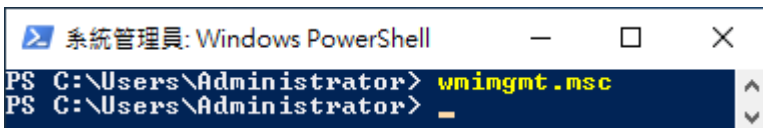
6.3.3.1 設定事件日誌權限

(1) 開啟 [Windows PowerShell]



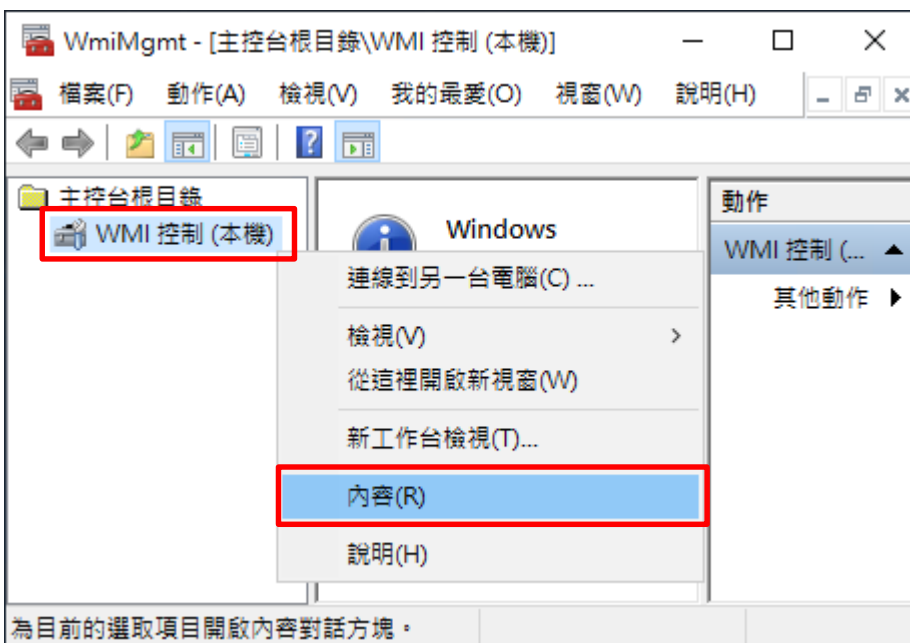
(2) 開啟元件服務

```
PS C:\> wimgmt.msc
```



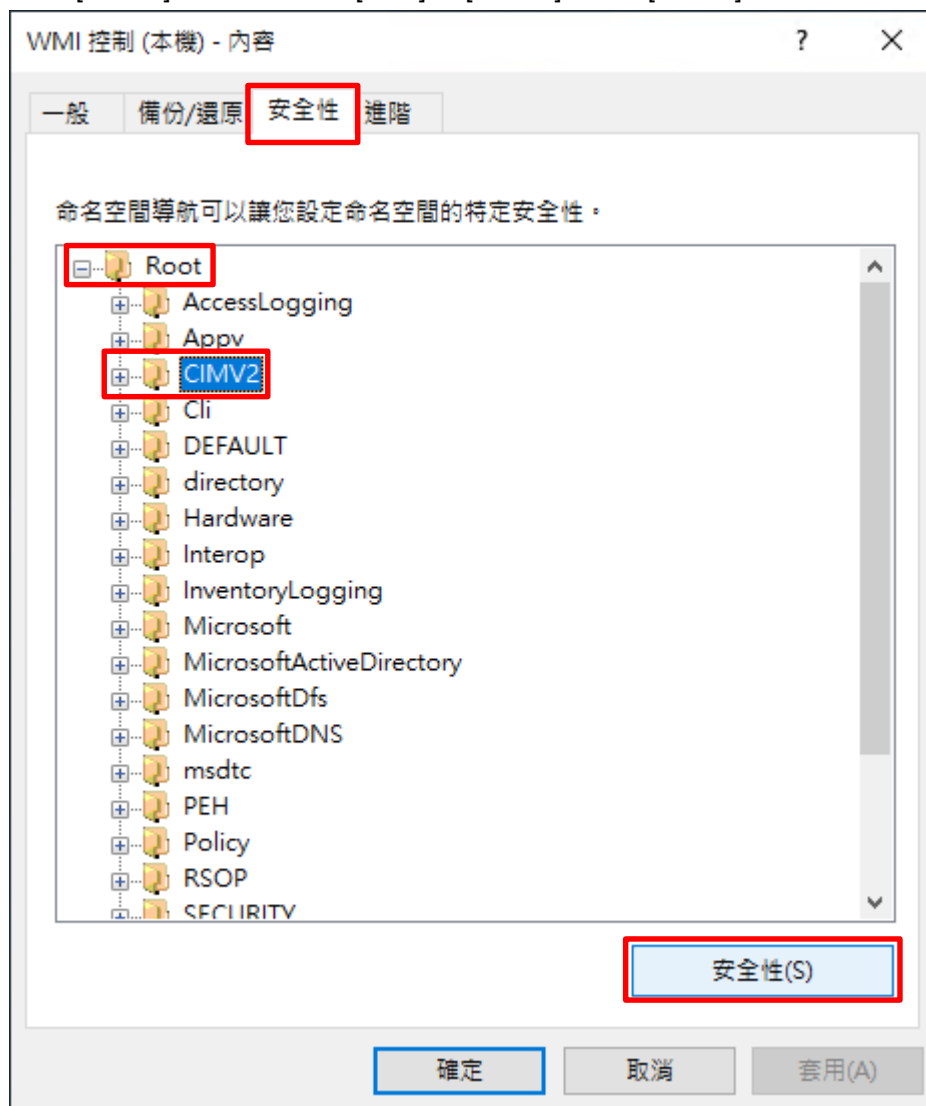
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



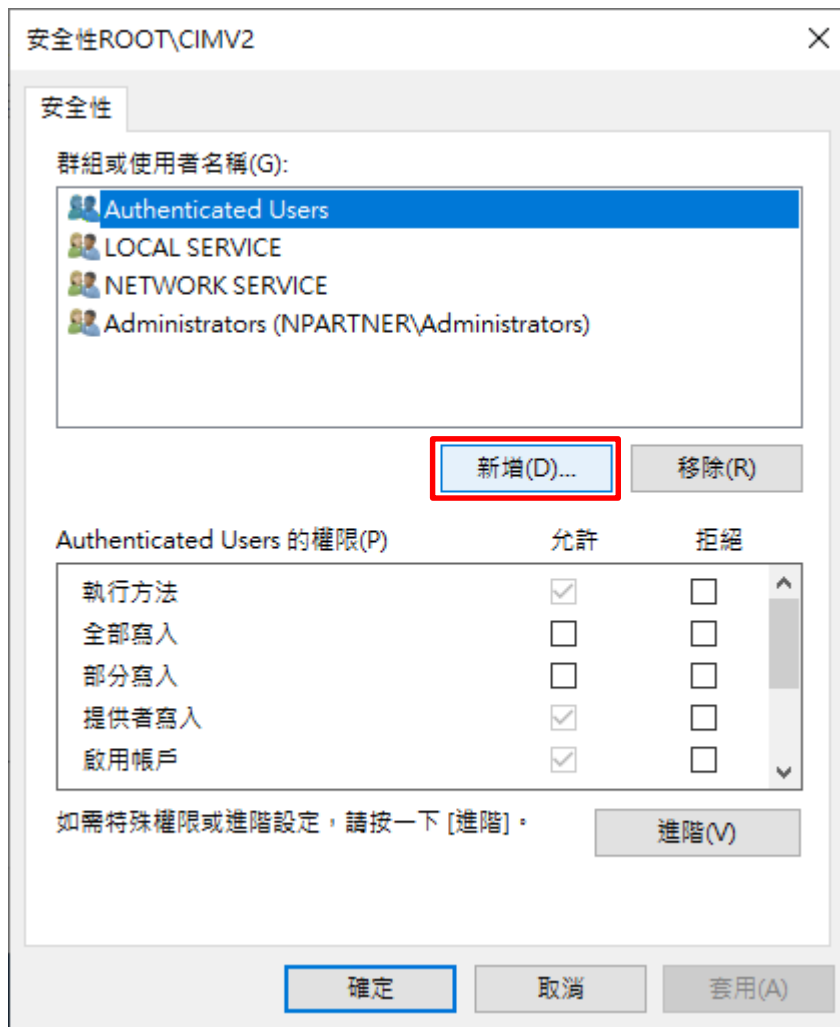
(4) 編輯 CIMV2 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [CIMV2] -> 按 [安全性]



(5) 新增 WMI 使用者權限

按 [新增]



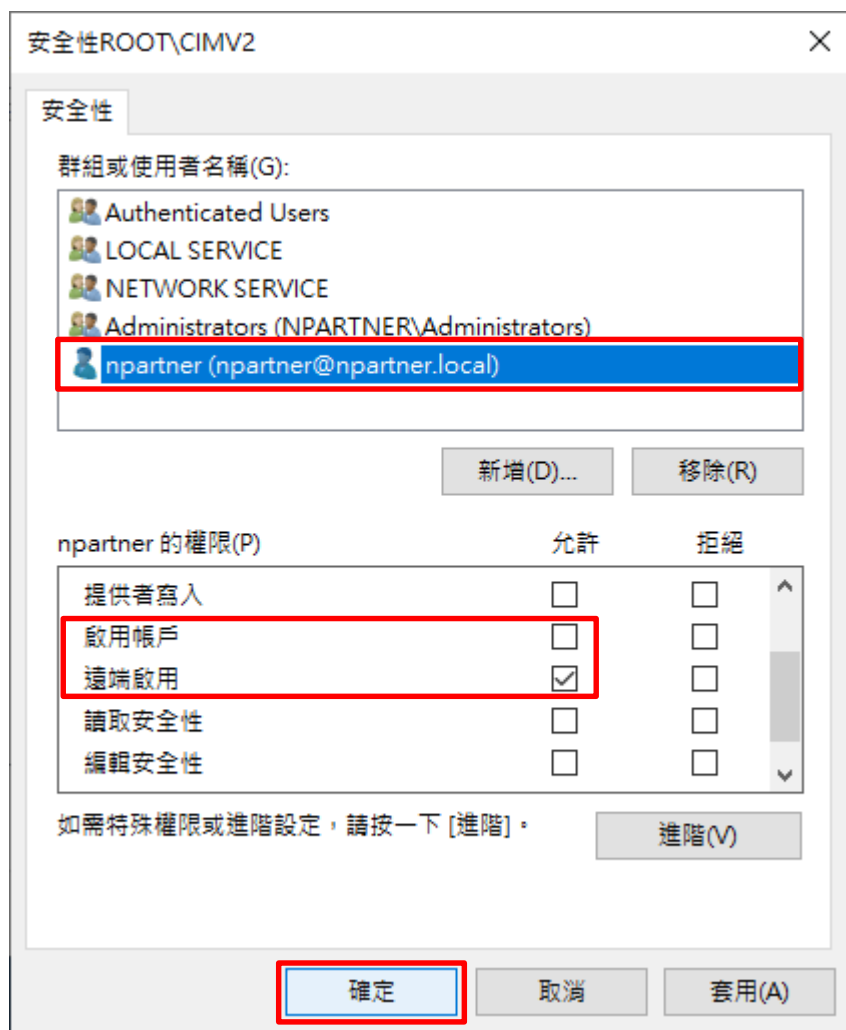
(6) 輸入使用者

輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]



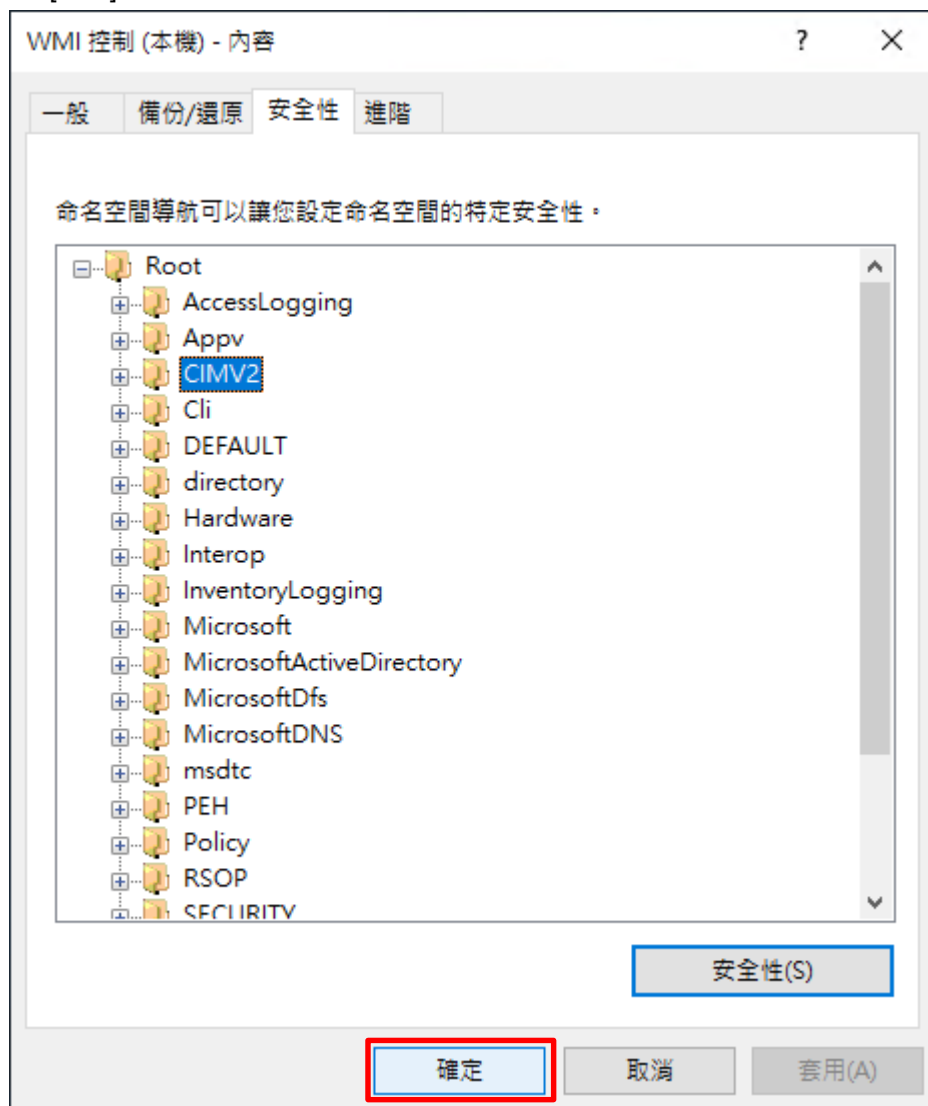
(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 確定使用者權限

按 [確定]



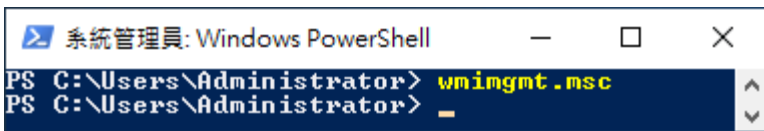
6.3.3.2 設定讀取使用者資料權限

(1) 開啟 [Windows PowerShell]



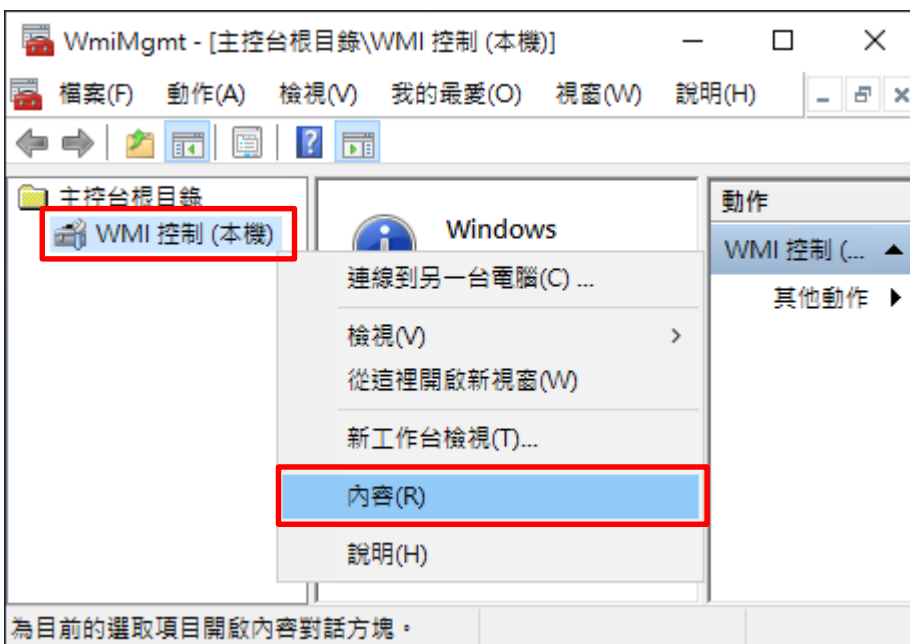
(2) 開啟元件服務

```
PS C:\> wimgmt.msc
```



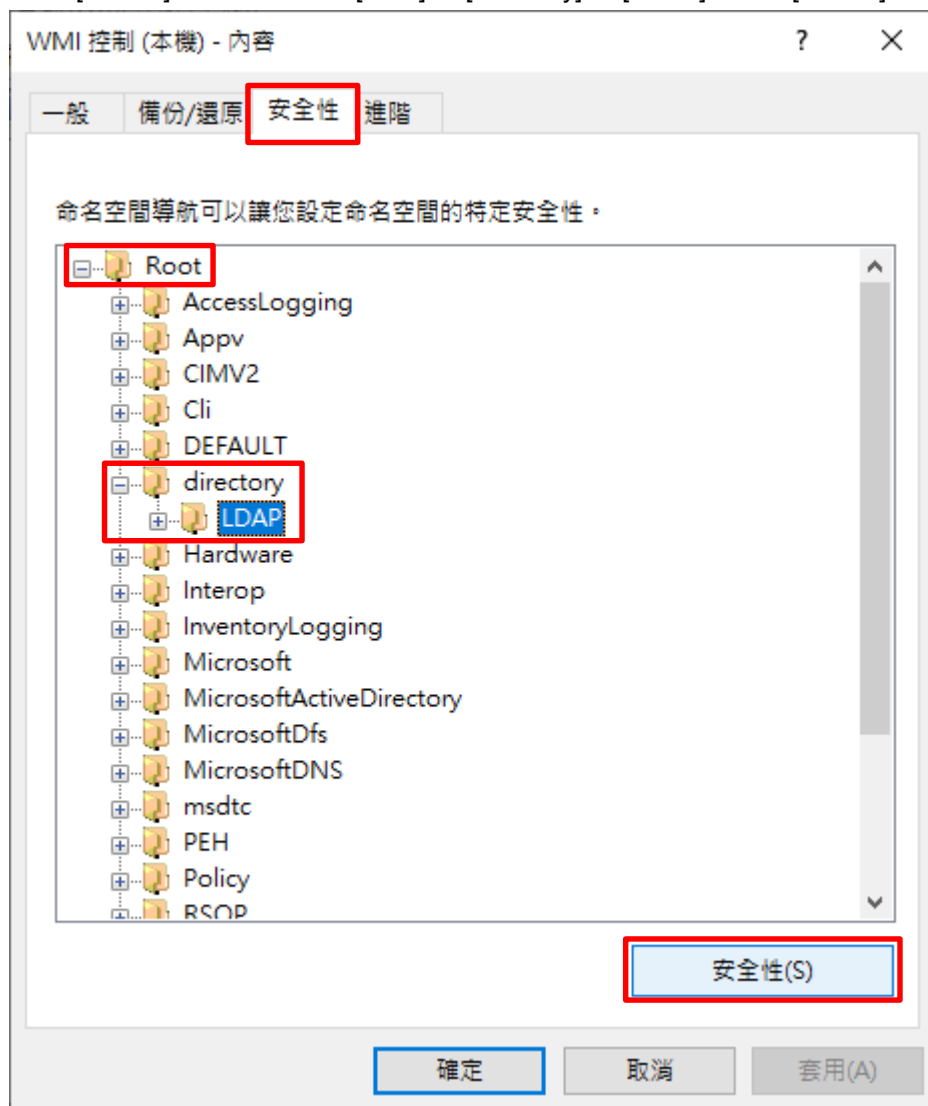
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



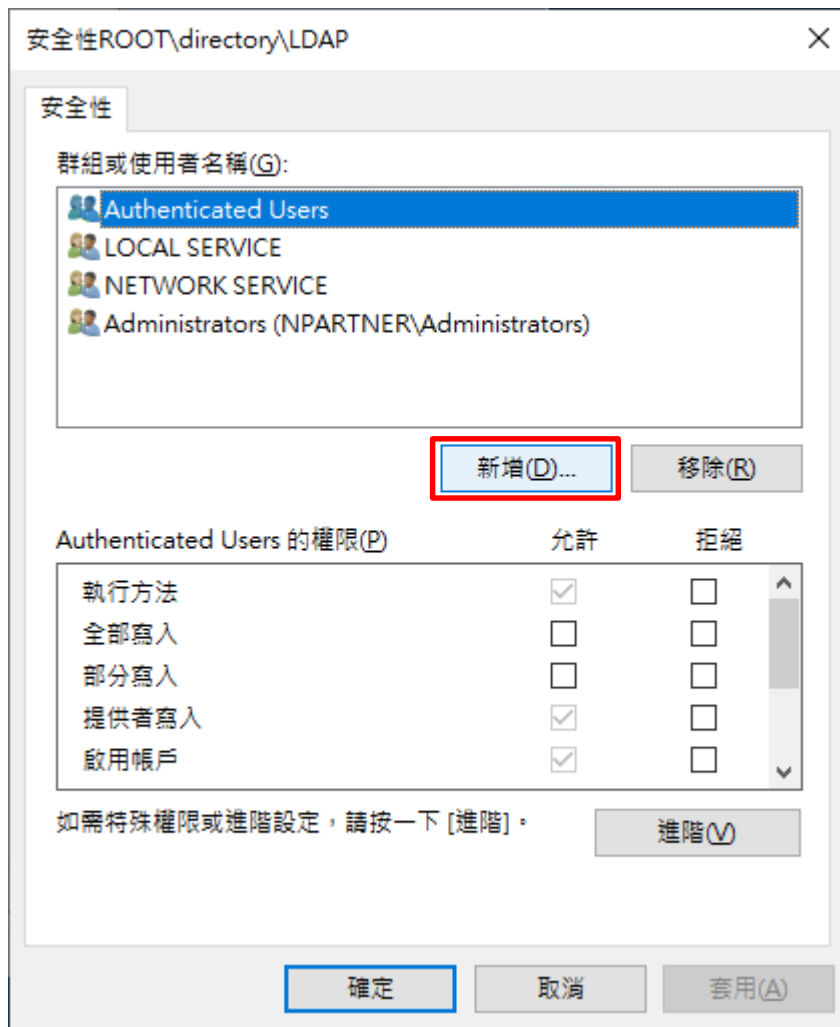
(4) 編輯 LDAP 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [directory] -> 按 [安全性]



(5) 新增 WMI 使用者權限

按 [新增]



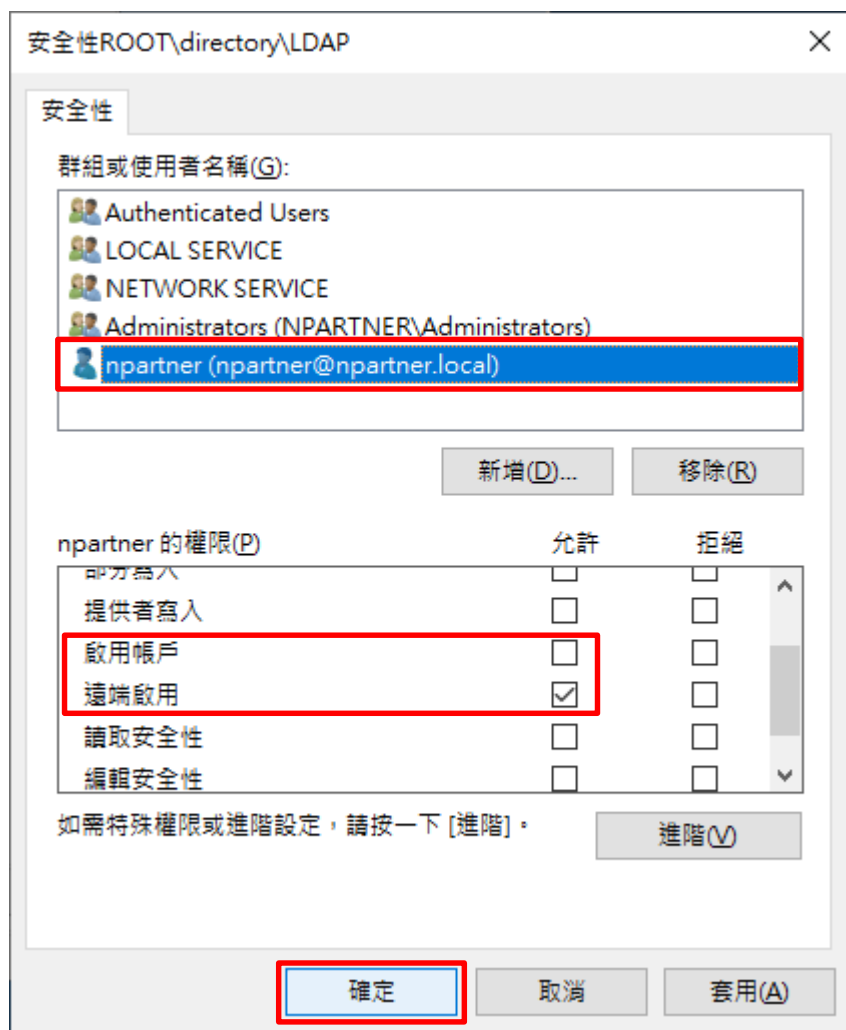
(6) 輸入使用者

輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]



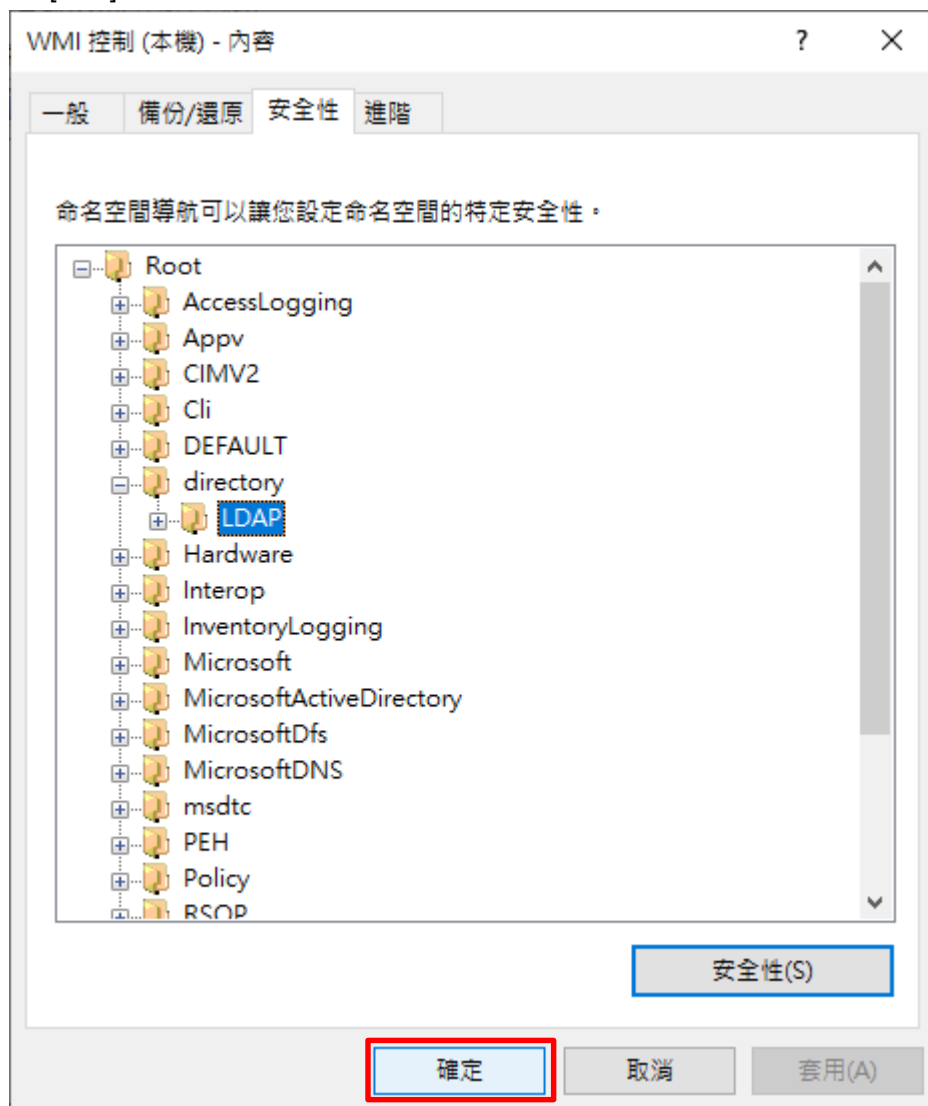
(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 確定使用者權限

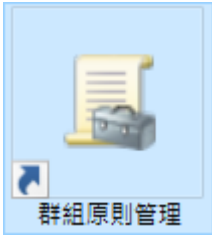
按 [確定]



6.3.4 設定 Event log 讀取權限

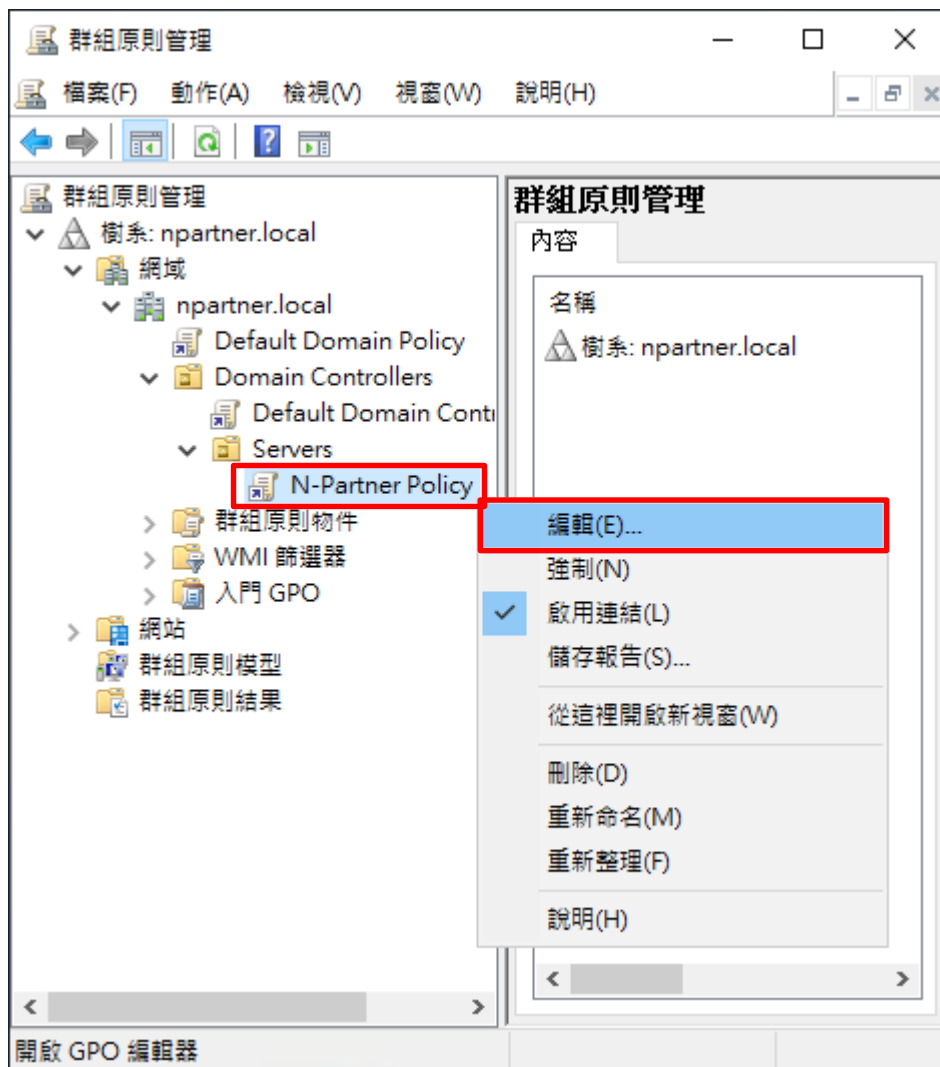
(1) 開啟群組原則管理

開啟 [群組原則管理]




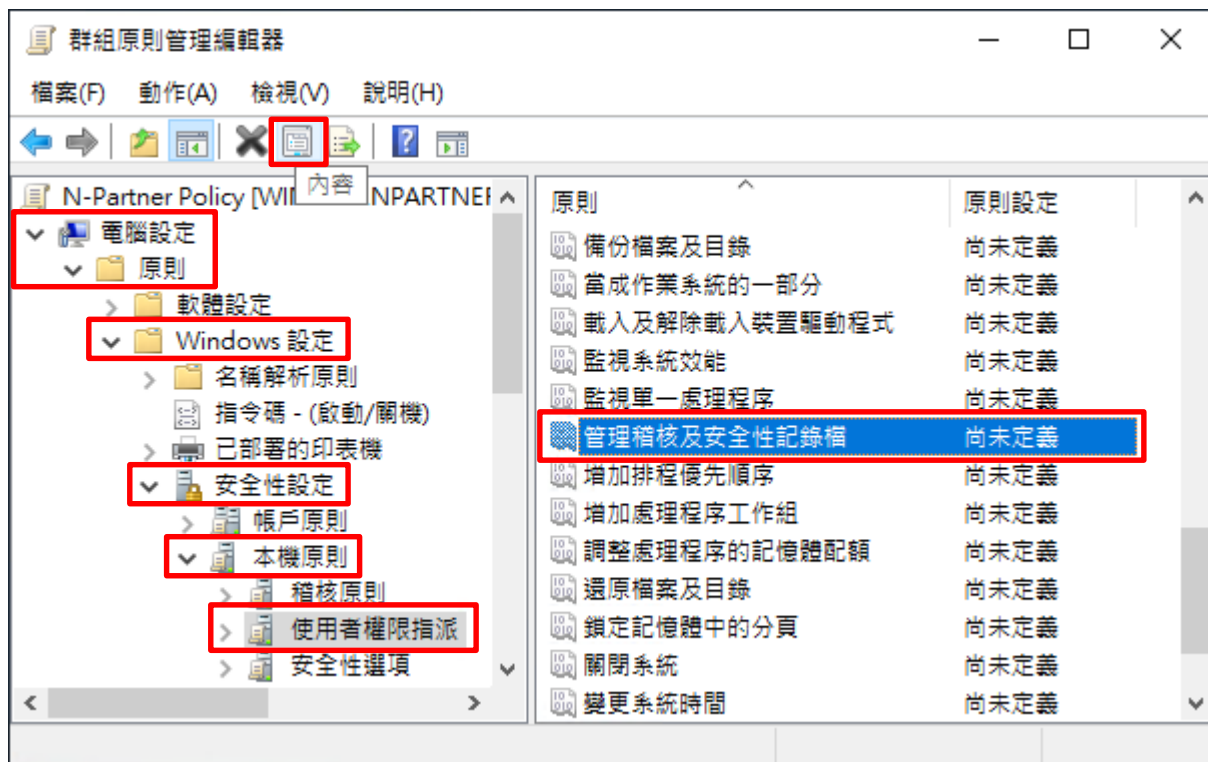
(2) 編輯群組原則物件

在 [N-Partner Policy] 群組原則物件，按滑鼠右鍵 -> 點選 [編輯]



(3) 設定記錄檔

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [使用者權限指派] -> 選擇 [管理稽核及安全記錄檔] 項目 -> 點選  內容



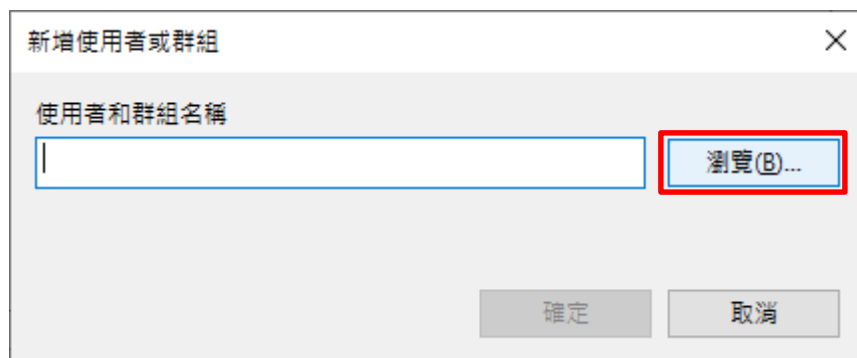
(4) 新增管理稽核使用者

勾選 [定義這些原則設定] -> 按 [新增使用者或群組...]



(5) 搜尋使用者

按 [瀏覽]



(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

選取使用者、電腦、服務帳戶或群組

選取這個物件類型(S):
使用者、服務帳戶、群組或內建安全性主體

物件類型(O)...

從這個位置(F):
npartner.local

位置(L)...

輸入物件名稱來選取 (範例)(E):
npartner (npartner@npartner.local)

檢查名稱(C)

進階(A)... 確定 取消

(7) 確定使用者

按 [確定]

新增使用者或群組

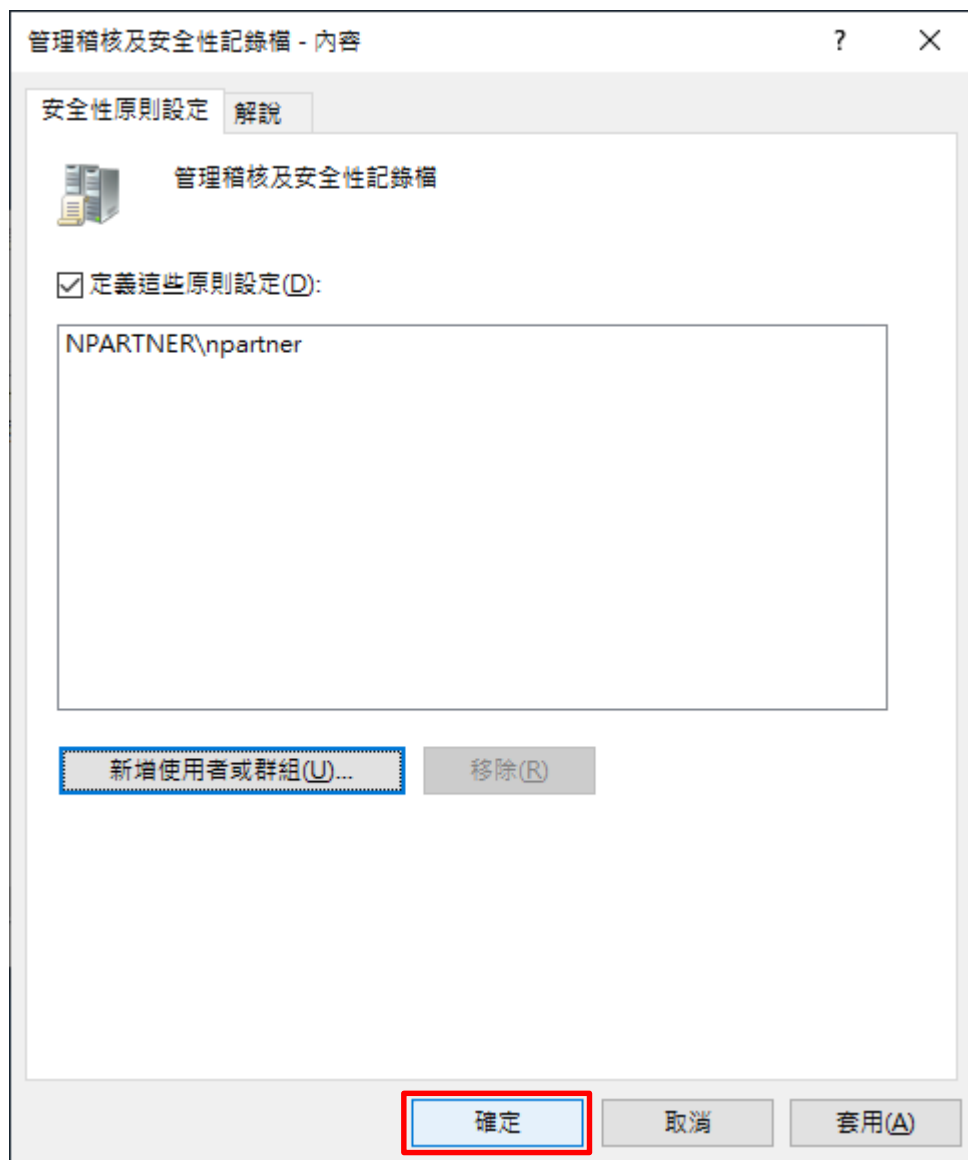
使用者和群組名稱
NPARTNER\npartner

瀏覽(B)...

確定 取消

(8) 確定設定記錄檔

按 [確定]



(9) 開啟 [Windows PowerShell]



(10) 更新群組原則

PS C:\> Invoke-GPUdate -RandomDelayInMinutes 0 -Force



```
系統管理員: Windows PowerShell
PS C:\Users\Administrator> Invoke-GPUdate -RandomDelayInMinutes 0 -Force
PS C:\Users\Administrator> _
```

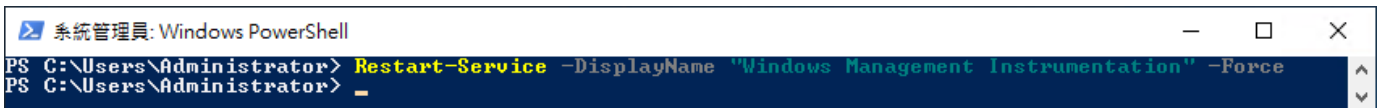
6.3.5 重啟 WMI 服務

(1) 開啟 [Windows PowerShell]



(2) 重啟 WMI 服務

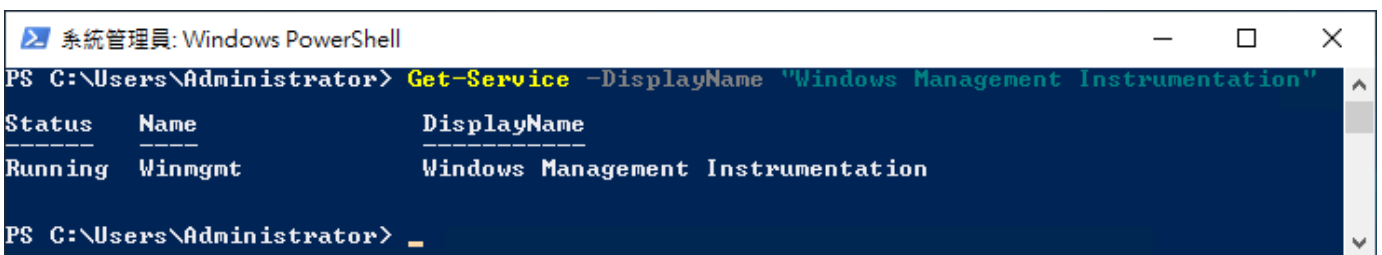
```
PS C:\> Restart-Service -DisplayName "Windows Management Instrumentation" -Force
```

A screenshot of a Windows PowerShell terminal window titled "系統管理員: Windows PowerShell". The terminal shows the command `Restart-Service -DisplayName "Windows Management Instrumentation" -Force` being executed. The prompt `PS C:\Users\Administrator>` is visible before and after the command.

```
系統管理員: Windows PowerShell
PS C:\Users\Administrator> Restart-Service -DisplayName "Windows Management Instrumentation" -Force
PS C:\Users\Administrator> _
```

(3) 查看 WMI 服務

```
PS C:\> Get-Service -DisplayName "Windows Management Instrumentation"
```

A screenshot of a Windows PowerShell terminal window titled "系統管理員: Windows PowerShell". The terminal shows the command `Get-Service -DisplayName "Windows Management Instrumentation"` being executed. The output is a table with columns for Status, Name, and DisplayName. The prompt `PS C:\Users\Administrator>` is visible before and after the command.

```
系統管理員: Windows PowerShell
PS C:\Users\Administrator> Get-Service -DisplayName "Windows Management Instrumentation"
Status      Name          DisplayName
-----
Running     Winmgmt      Windows Management Instrumentation
PS C:\Users\Administrator> _
```

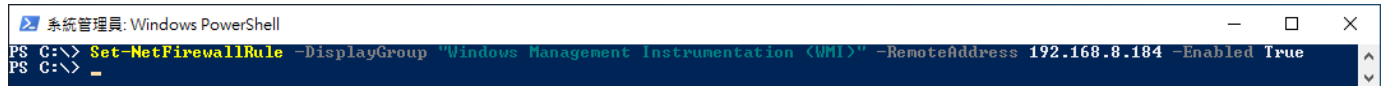
6.4 設定防火牆

(1) 開啟 [Windows PowerShell]



(2) 設定防火牆，只允許 N-Reporter IP query WMI

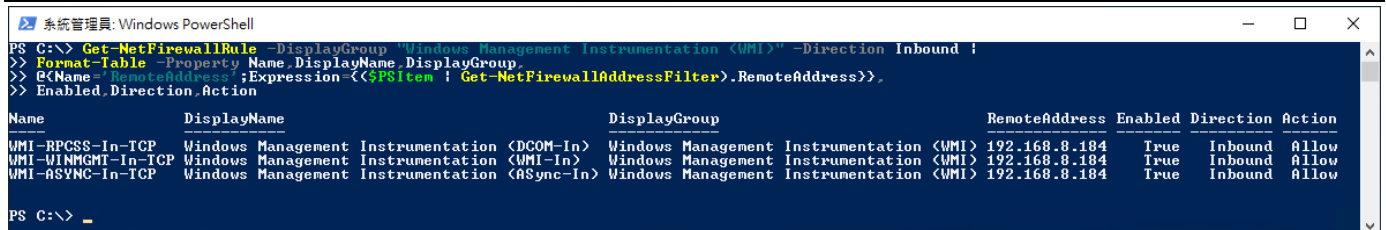
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.184 -Enabled True
```

A screenshot of a Windows PowerShell terminal window. The title bar reads "系統管理員: Windows PowerShell". The command prompt shows the command: `PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.184 -Enabled True`. The prompt is now `PS C:\> _`.

紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 查看防火牆 WMI 啟用狀態

```
PS C:\> Get-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -Direction Inbound |  
>> Format-Table -Property Name,DisplayName,DisplayGroup,  
>> @{Name='RemoteAddress';Expression={$PSItem | Get-NetFirewallAddressFilter}.RemoteAddress},  
>> Enabled,Direction,Action
```

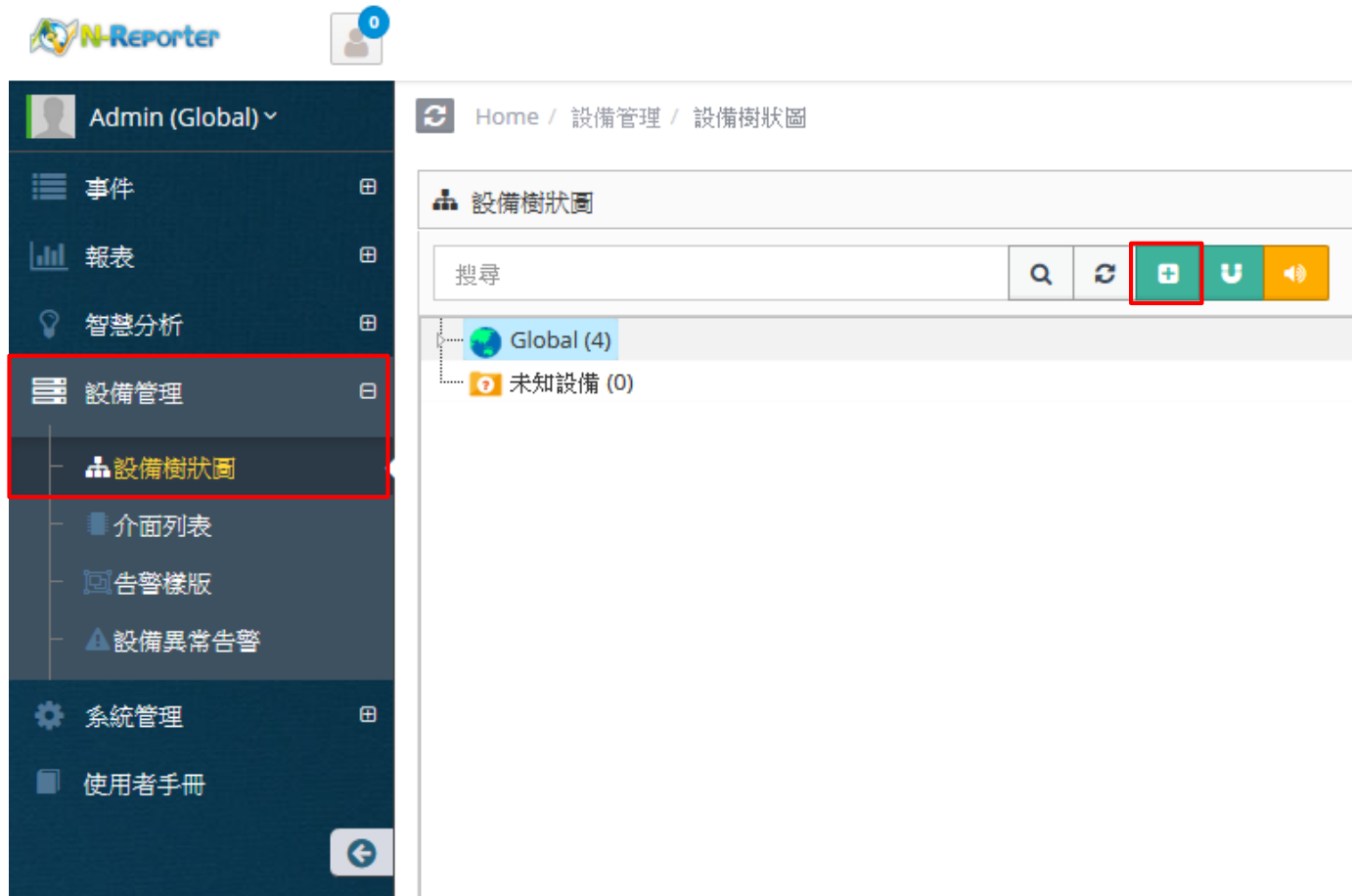
A screenshot of a Windows PowerShell terminal window. The title bar reads "系統管理員: Windows PowerShell". The command prompt shows the command: `PS C:\> Get-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -Direction Inbound | Format-Table -Property Name,DisplayName,DisplayGroup, @{Name='RemoteAddress';Expression={$PSItem | Get-NetFirewallAddressFilter}.RemoteAddress}, Enabled,Direction,Action`. The output is a table with 8 columns: Name, DisplayName, DisplayGroup, RemoteAddress, Enabled, Direction, and Action. The output shows three rules for WMI, all enabled and allowing inbound traffic from 192.168.8.184.

Name	DisplayName	DisplayGroup	RemoteAddress	Enabled	Direction	Action
WMI-RPCSS-In-TCP	Windows Management Instrumentation (DCOM-In)	Windows Management Instrumentation (WMI)	192.168.8.184	True	Inbound	Allow
WMI-WINMGMT-In-TCP	Windows Management Instrumentation (WMI-In)	Windows Management Instrumentation (WMI)	192.168.8.184	True	Inbound	Allow
WMI-ASync-In-TCP	Windows Management Instrumentation (ASync-In)	Windows Management Instrumentation (WMI)	192.168.8.184	True	Inbound	Allow

7. N-Reporter

(1) 新增 Windows AD WMI 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]



The screenshot displays the N-Reporter web application interface. On the left is a dark blue sidebar menu with the following items: 'Admin (Global) v', '事件' (Events), '報表' (Reports), '智慧分析' (Smart Analysis), '設備管理' (Device Management) - highlighted with a red box, '設備樹狀圖' (Device Tree) - also highlighted with a red box, '介面列表' (Interface List), '告警樣版' (Alert Templates), '設備異常告警' (Device Abnormal Alerts), '系統管理' (System Management), and '使用者手冊' (User Manual). The main content area shows the breadcrumb 'Home / 設備管理 / 設備樹狀圖'. Below this is a search bar with a search icon, a refresh icon, a green '+ Add' button (highlighted with a red box), a green 'U' button, and a yellow speaker icon. The device tree shows a 'Global (4)' folder containing a '未知設備 (0)' (Unknown Devices) item.

7.1 Windows 2003 或之前版本作業系統

(2) 設定 Windows AD WMI 設備

輸入名稱和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [Windows 2003 AD Server (WMI)] 和編碼方式: [BIG5]

-> 選擇設備 Icon: [icon-host] -> 輸入 Windows AD 的 Login Account 和 Login Password -> 點選接收狀態: [啟用]

-> 按 [確定]

新增設備

設備基本設定

名稱
WindowsAD-192.168.1.183

IP
192.168.1.183

設備種類
 Syslog Flow SNMP

Syslog 相關設定

資料格式
Windows 2003 AD Server (WMI)

Facility

編碼方式
BIG5

設備進階設定

ICMP 告警樣板
N/A

設備 Icon
icon-host

Login Account
npartner

Login Password
.....

接收狀態
 啟用 停用

暫無資料告警
 啟用 Syslog/Flow 暫無資料告警

資料保留天數

確定 取消

7.2 Windows 2008 或之後版本作業系統

(2) 設定 Windows AD WMI 設備

輸入名稱和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [Windows 2008/2012 AD Server (WMI)] 和編碼方式: [UTF-8] -> 選擇設備 Icon: [icon-host] -> 輸入 Windows AD 的 Login Account 和 Login Password -> 點選接收狀態: [啟用] -> 按 [確定]

新增設備

設備基本設定

名稱
WindowsAD-192.168.1.183

IP
192.168.1.183

設備種類
 Syslog Flow SNMP

Syslog 相關設定

資料格式
Windows 2008/2012 AD Server (WMI)

Facility

編碼方式
UTF-8

設備進階設定

ICMP 告警樣板
----- N/A -----

設備 Icon
icon-host

Login Account
npartner

Login Password
.....

接收狀態
 啟用 停用

暫無資料告警
 啟用 Syslog/Flow 暫無資料告警

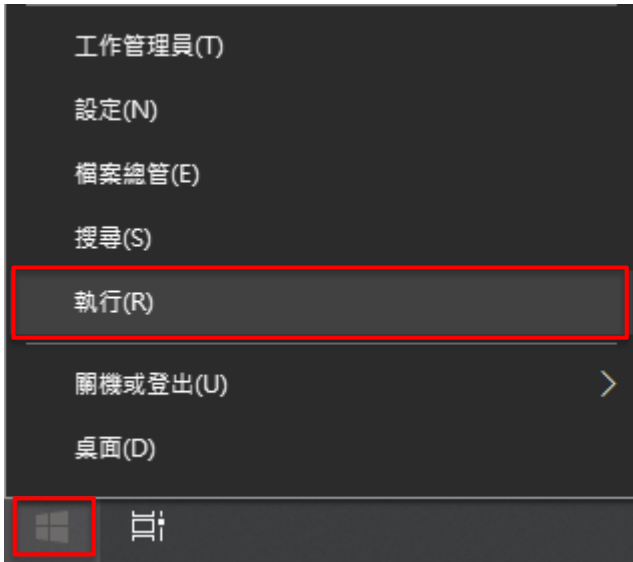
資料保留天數

確定 取消

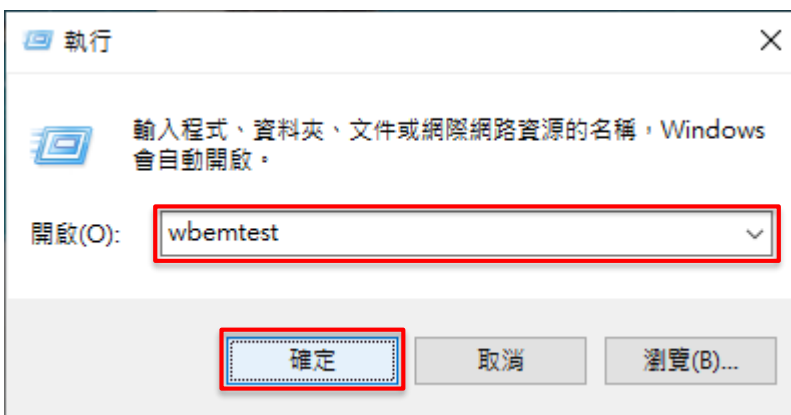
8. 問題排除

8.1 WMI Query Language 檢查

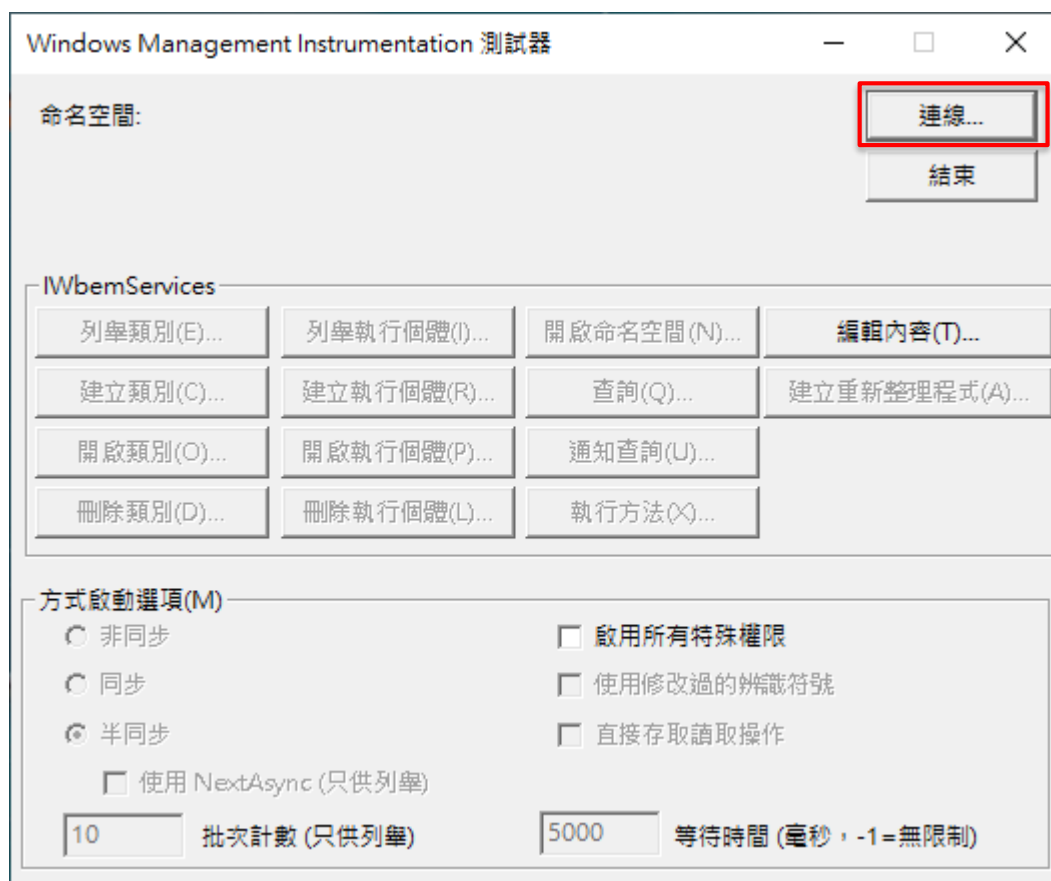
(1) 按  -> 點選 [執行]



(2) 輸入 `wbemtest` -> 按 [確定]



(3) 按 [連線]



(4) 檢查事件日誌；輸入命名空間 \\<Windows AD IP>root\cimv2 -> 使用者帳號和密碼 -> 按 [連線]

連線

命名空間
\\192.168.1.183\root\cimv2

連線

取消

連線:
使用: IWbemLocator (Namespaces)
傳回: IWbemServices 完成: Synchronous

認證
使用者(U): npartner
密碼(P): *****
授權(A):

地區設定(L)

如何解譯空白密碼(H)
 NULL 空白

模擬等級(I)
 識別
 模擬
 委派

驗證等級(V)
 無 封包
 連線 封包完整性
 呼叫 封包私密性

(5) 按 [查詢]

Windows Management Instrumentation 測試器

命名空間:
\\192.168.1.183\root\cimv2

連線...
結束

IWbemServices

列舉類別(E)...	列舉執行個體(I)...	開啟命名空間(N)...	編輯內容(T)...
建立類別(C)...	建立執行個體(R)...	查詢(Q)...	建立重新整理程式(A)...
開啟類別(O)...	開啟執行個體(P)...	通知查詢(U)...	
刪除類別(D)...	刪除執行個體(L)...	執行方法(X)...	

方式啟動選項(M)

非同步 啟用所有特殊權限

同步 使用修改過的辨識符號

半同步 直接存取讀取操作

使用 NextAsync (只供列舉)

10 批次計數 (只供列舉) 5000 等待時間 (毫秒, -1=無限制)

(6) 輸入查詢 `Select * FROM Win32_NTLogEvent` -> 按 [套用]

查詢

輸入查詢

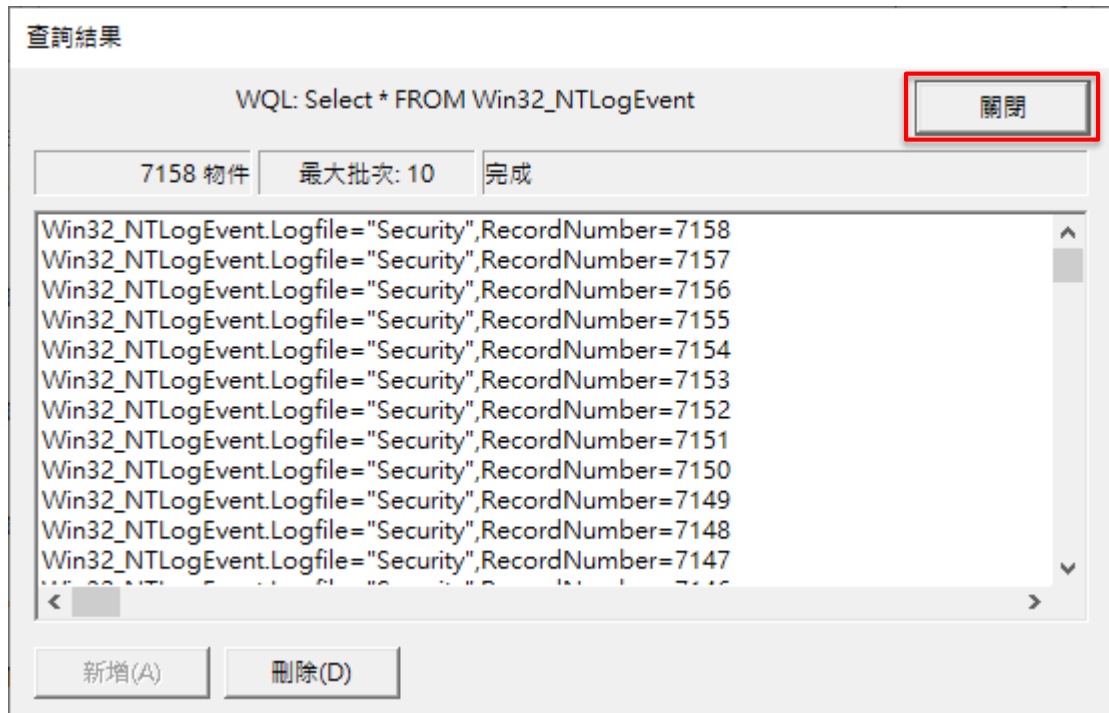
Select * FROM Win32_NTLogEvent

查詢類型

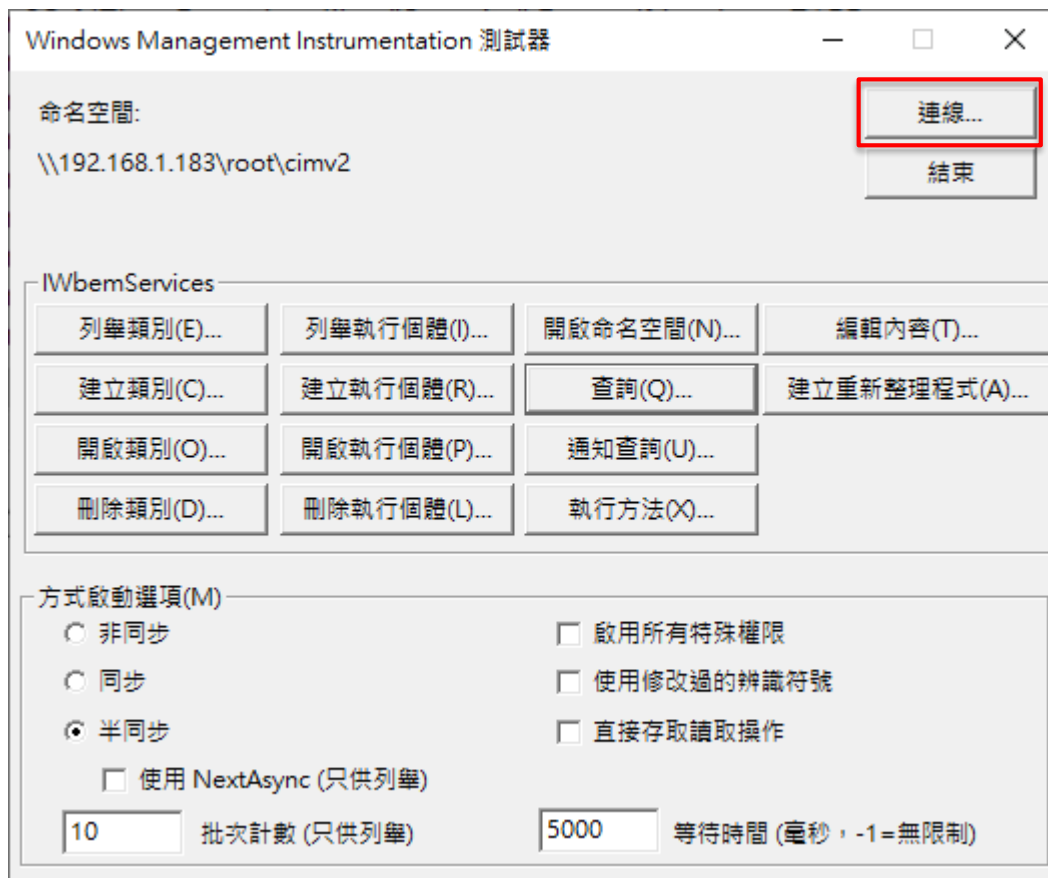
WQL 抓取類別原型

套用
取消

(7) 顯示查詢到資料 -> 按 [關閉]



(8) 按 [連線]



(9) 檢查使用者資料；輸入命名空間 \\<Windows AD IP>\root\directory\LDAP -> 使用者帳號和密碼 -> 按 [連線]

連線

命名空間
\\192.168.1.183\root\directory\LDAP

連線

取消

連線:
使用: IWbemLocator (Namespaces)
傳回: IWbemServices 完成: Synchronous

認證
使用者(U): npartner
密碼(P): *****
授權(A):

地區設定(L)

如何解譯空白密碼(H)
 NULL 空白

模擬等級(I)
 識別
 模擬
 委派

驗證等級(V)
 無 封包
 連線 封包完整性
 呼叫 封包私密性

(10) 按 [查詢]

Windows Management Instrumentation 測試器

命名空間:
\\192.168.1.183\root\directory\LDAP

連線...
結束

IWbemServices

列舉類別(E)...	列舉執行個體(I)...	開啟命名空間(N)...	編輯內容(T)...
建立類別(C)...	建立執行個體(R)...	查詢(Q)...	建立重新整理程式(A)...
開啟類別(O)...	開啟執行個體(P)...	通知查詢(U)...	
刪除類別(D)...	刪除執行個體(L)...	執行方法(X)...	

方式啟動選項(M)

非同步 啟用所有特殊權限

同步 使用修改過的辨識符號

半同步 直接存取讀取操作

使用 NextAsync (只供列舉)

10 批次計數 (只供列舉) 5000 等待時間 (毫秒, -1=無限制)

(11) 輸入查詢 `Select * FROM ds_user` -> 按 [套用]

查詢

輸入查詢

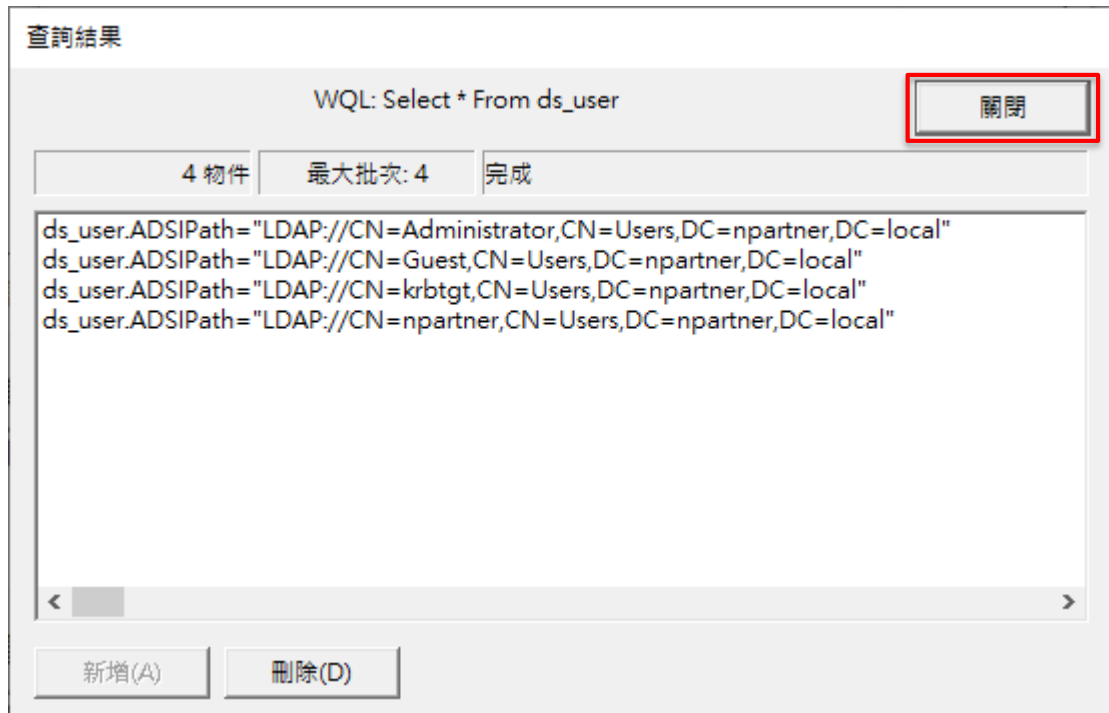
Select * FROM ds_user

查詢類型

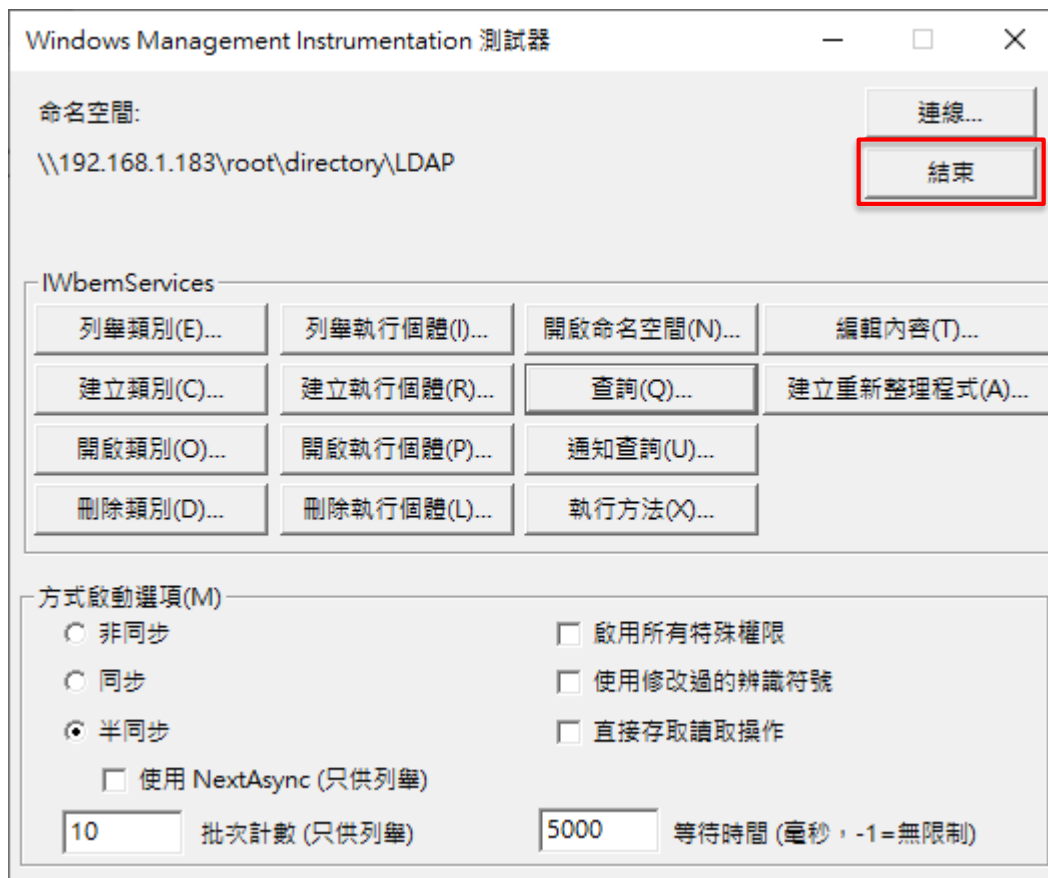
WQL 抓取類別原型

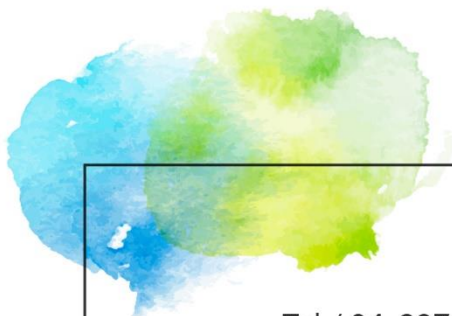
套用
取消

(12) 顯示查詢到資料 -> 按 [關閉]



(13) 檢查結果：可以查詢到日誌和使用者資料；按 [結束] 關閉 WMI 測試器





Tel / 04-23752865 Fax / 04-23757458
業務詢問 / sales@npartnertech.com
技術詢問 / support@npartnertech.com