N-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

商標

目錄

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

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

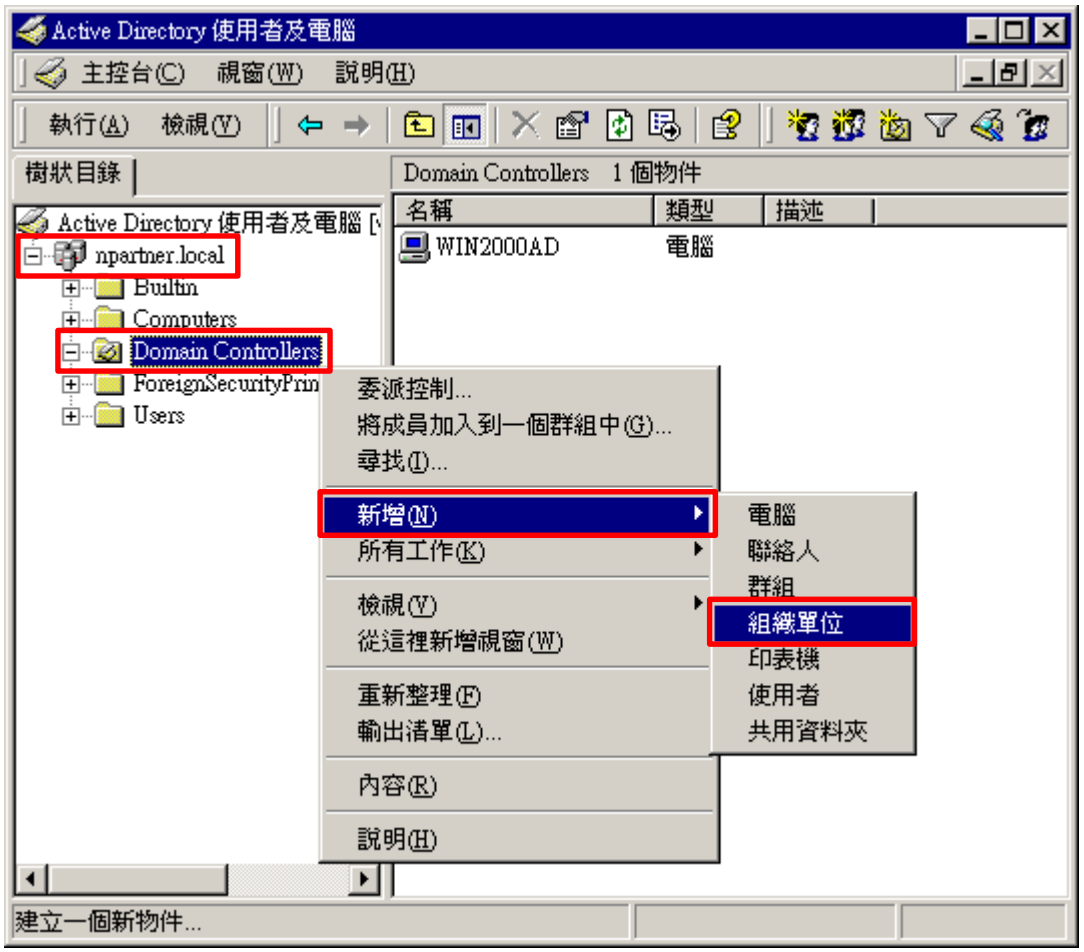
Windows 稽核原則設定 詳細說明請參考**前言**的稽核原則建議連結

1.1 組織單位設定

(1) 開啟 [Active Directory 使用者和電腦]

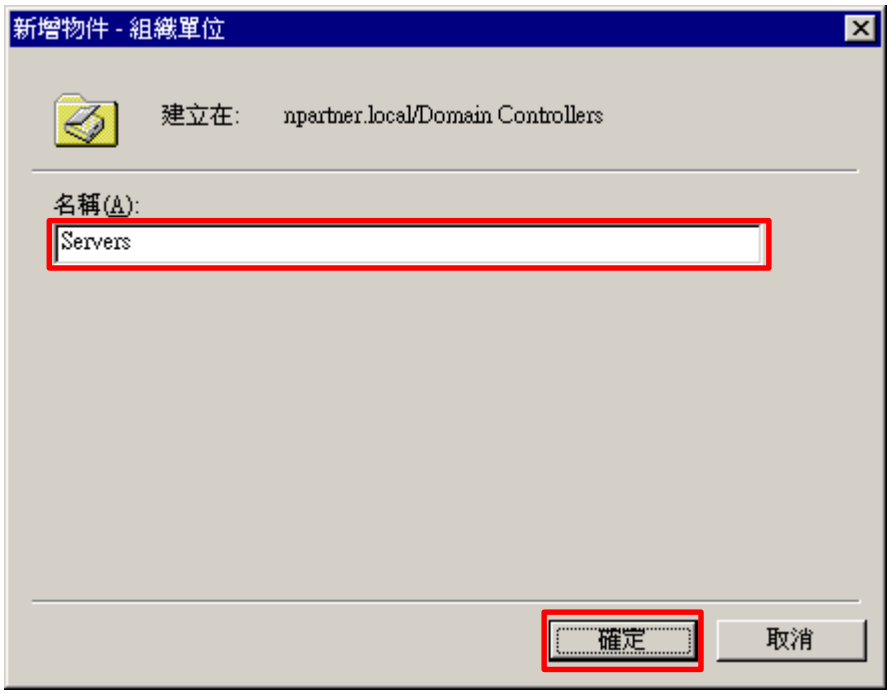
(2) 新增組織單位

[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]



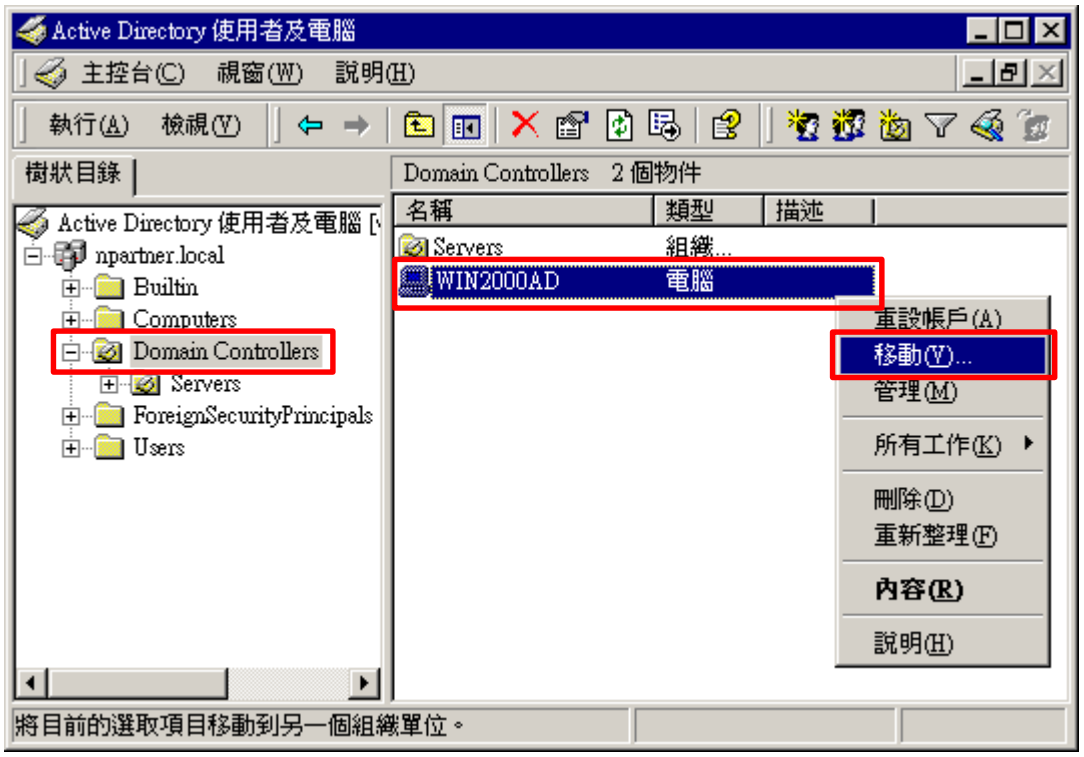
(3) 輸入組織單位名稱

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]

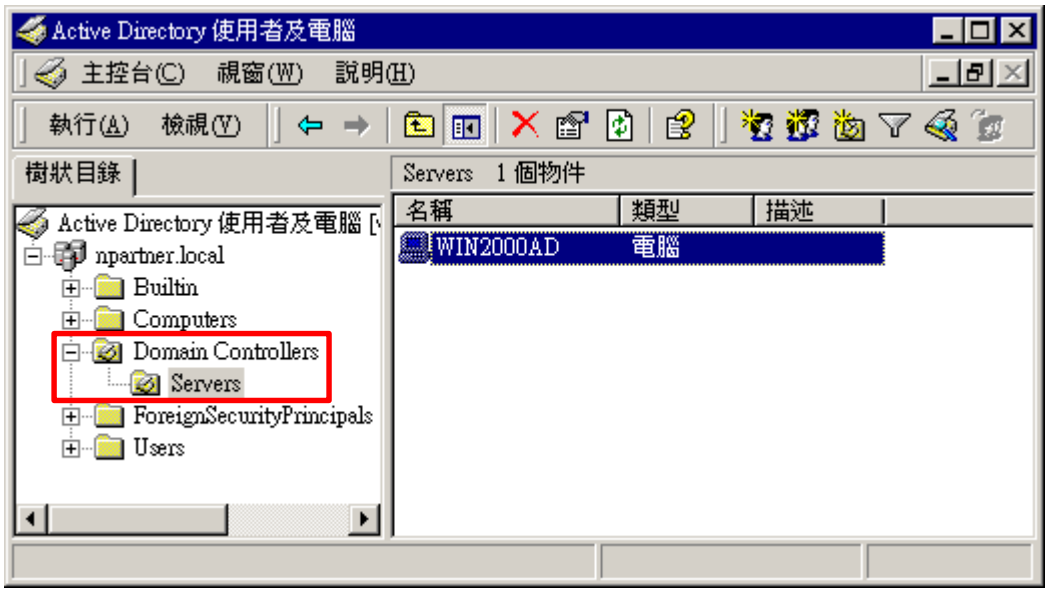


(5) 選擇組織單位

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。



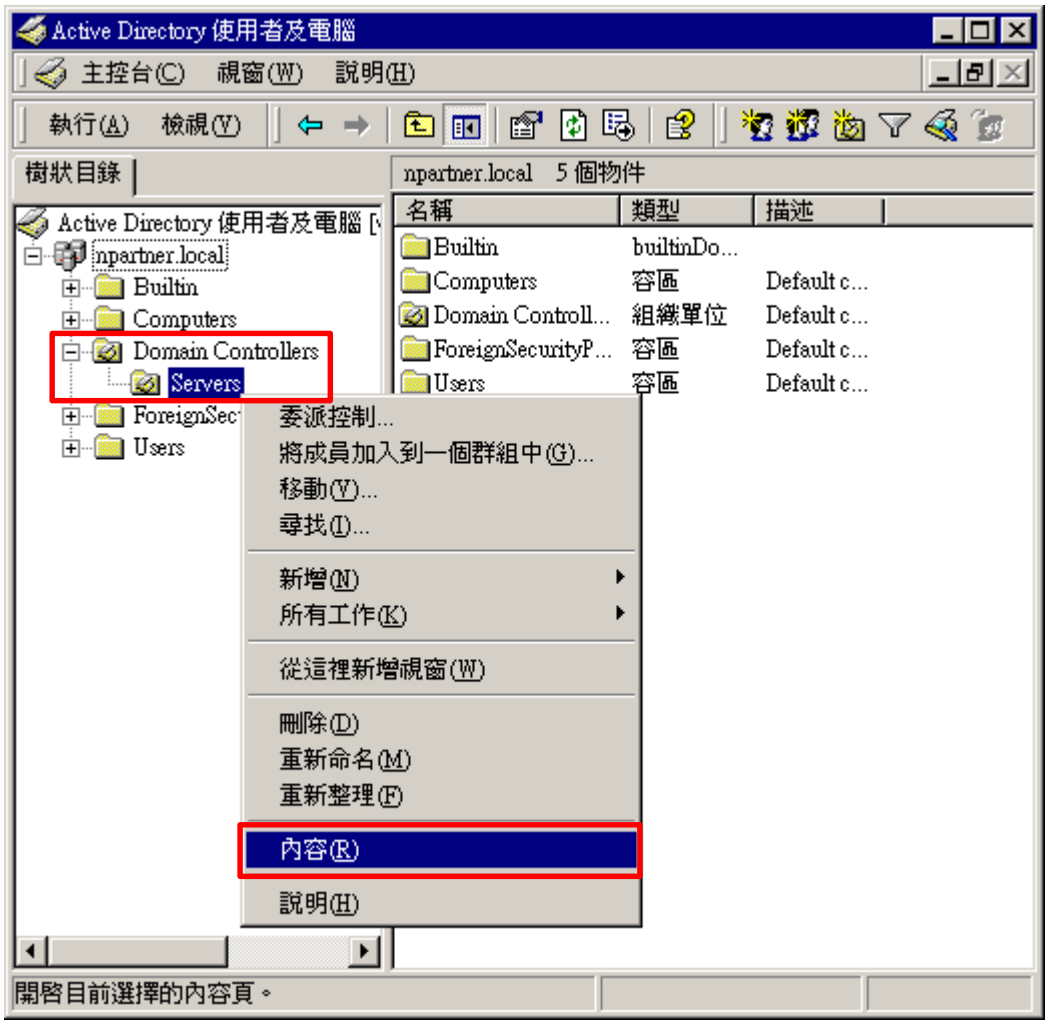
1.2 群組原則設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

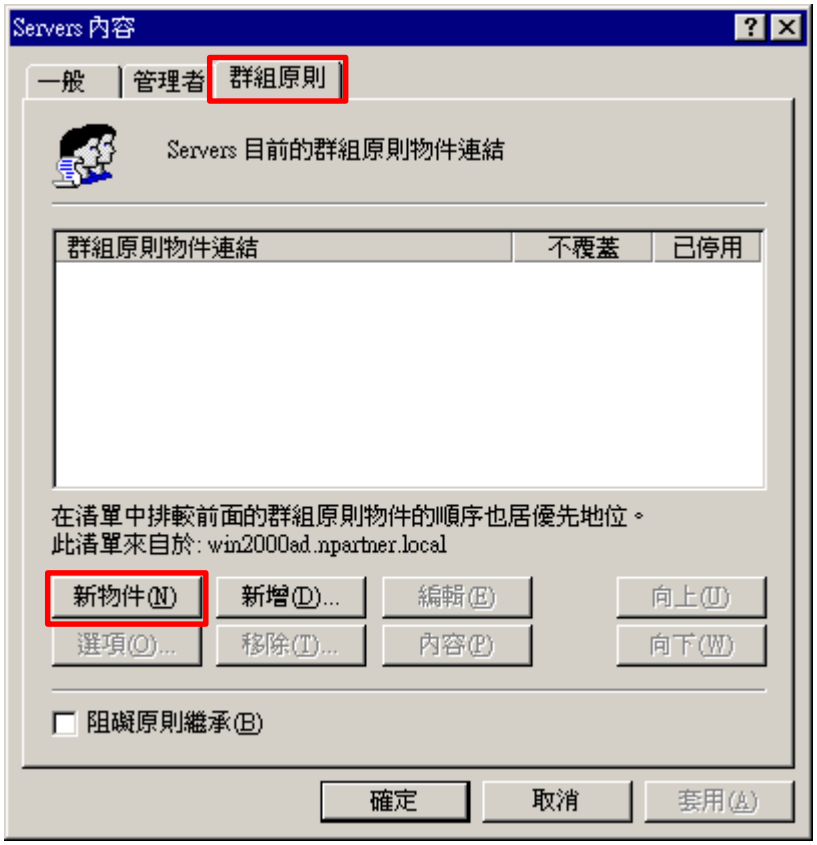
(2) Domain Controllers 的 Servers 組織單位，點選內容

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



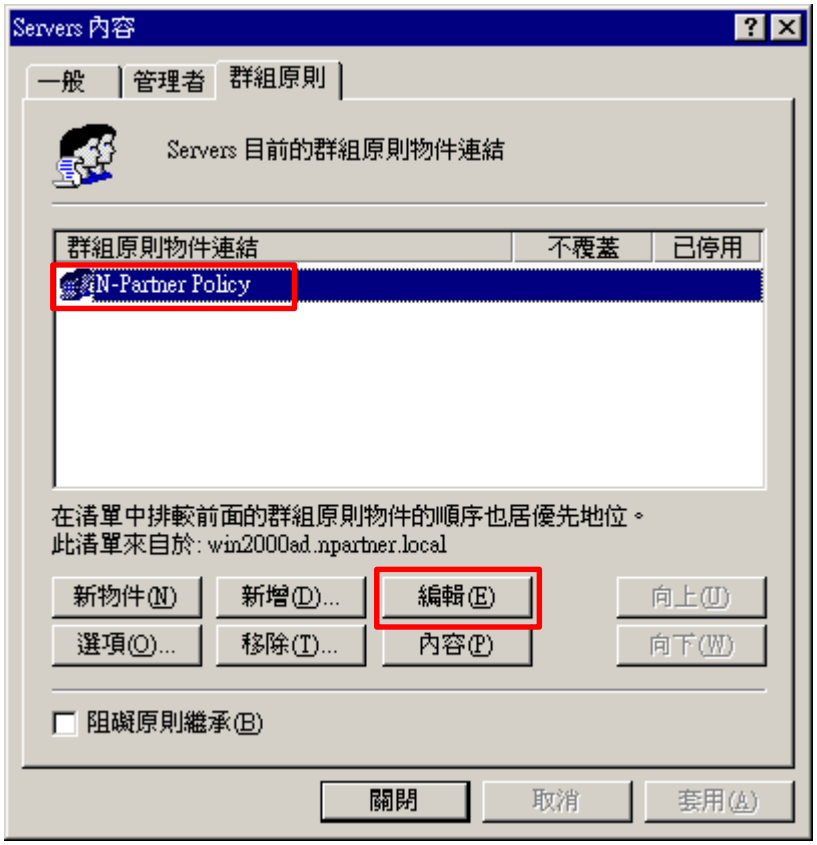
(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按 [新物件]



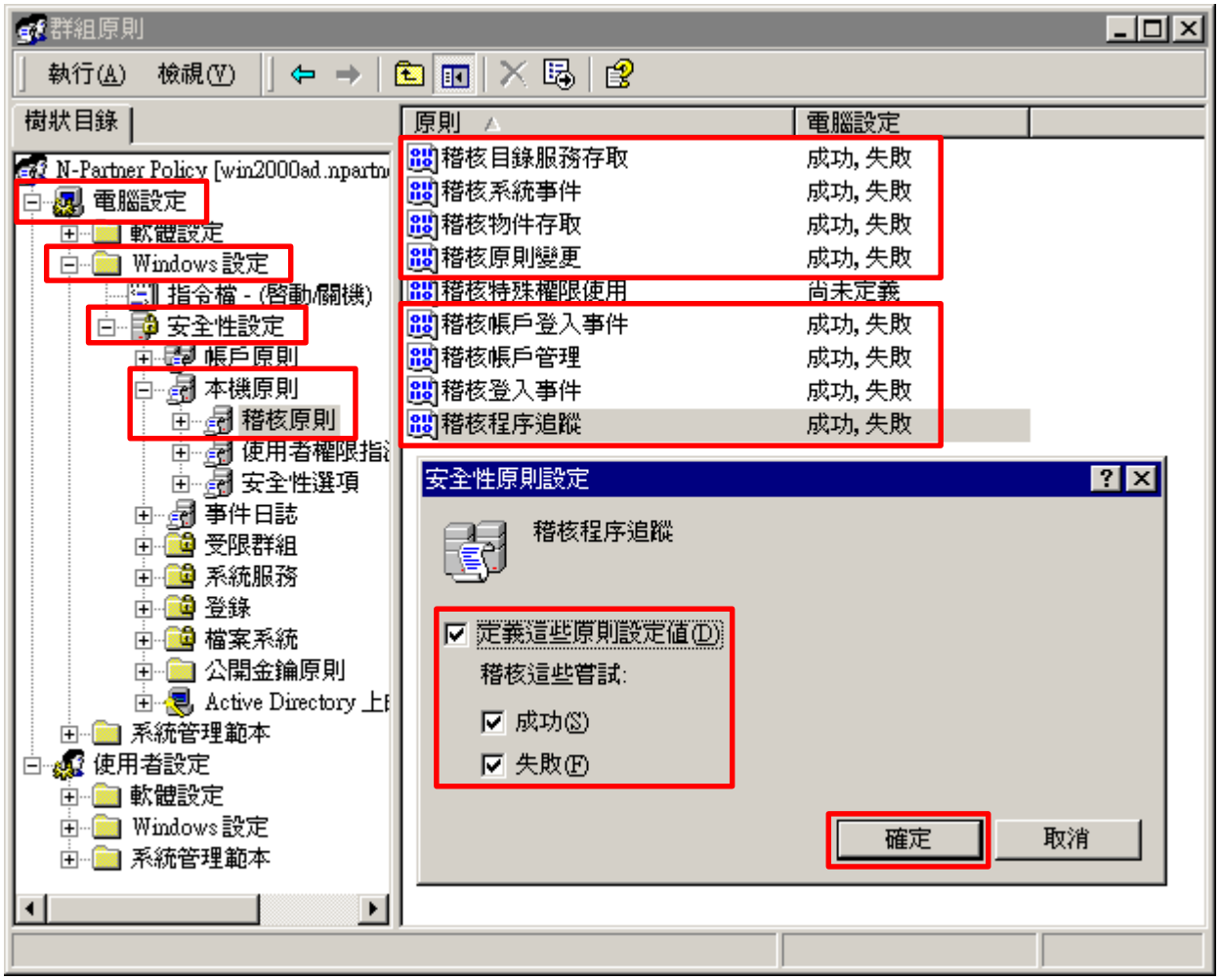
(4) 編輯群組原則物件

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]



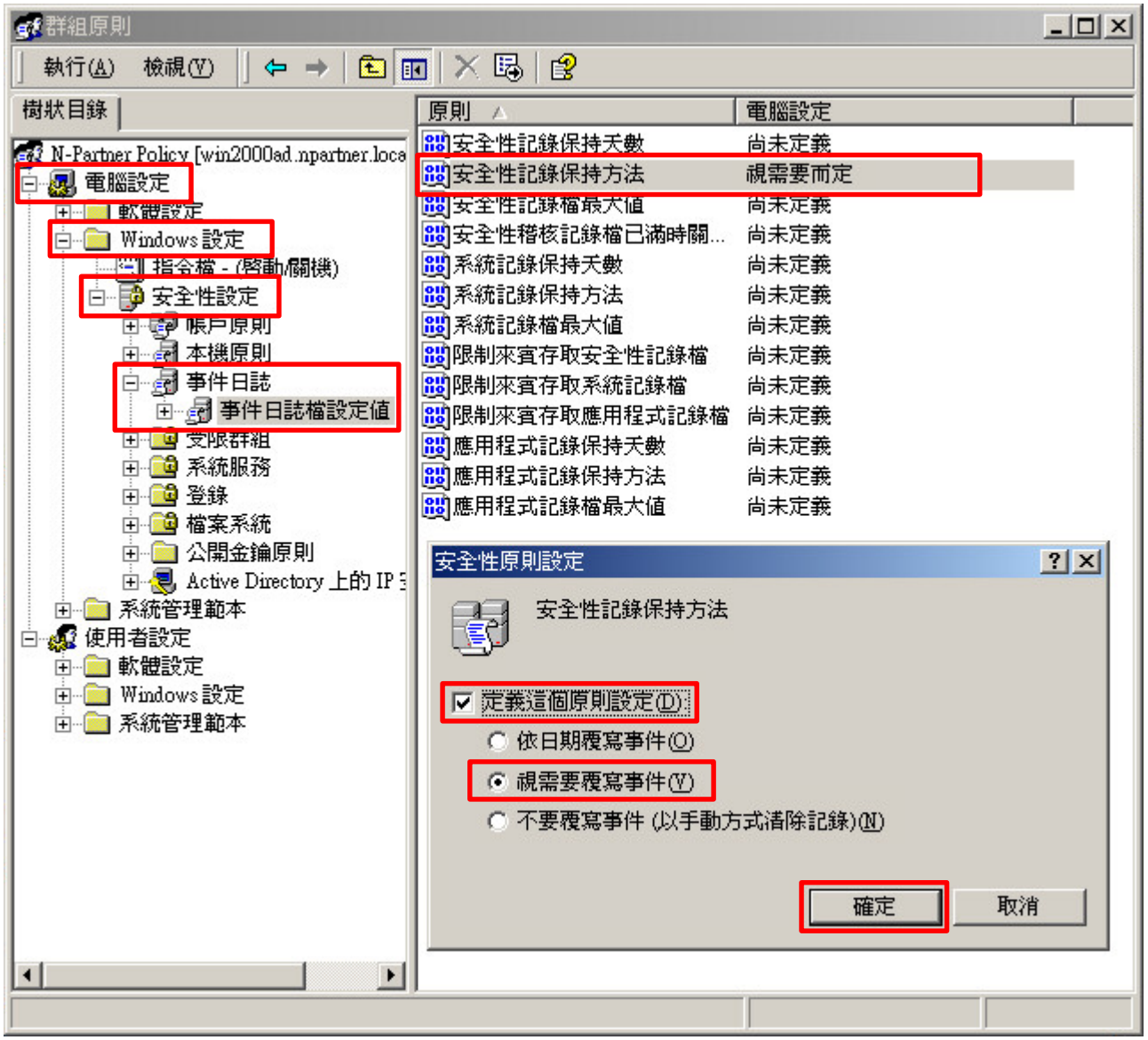
(5) 本機原則：稽核原則

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]



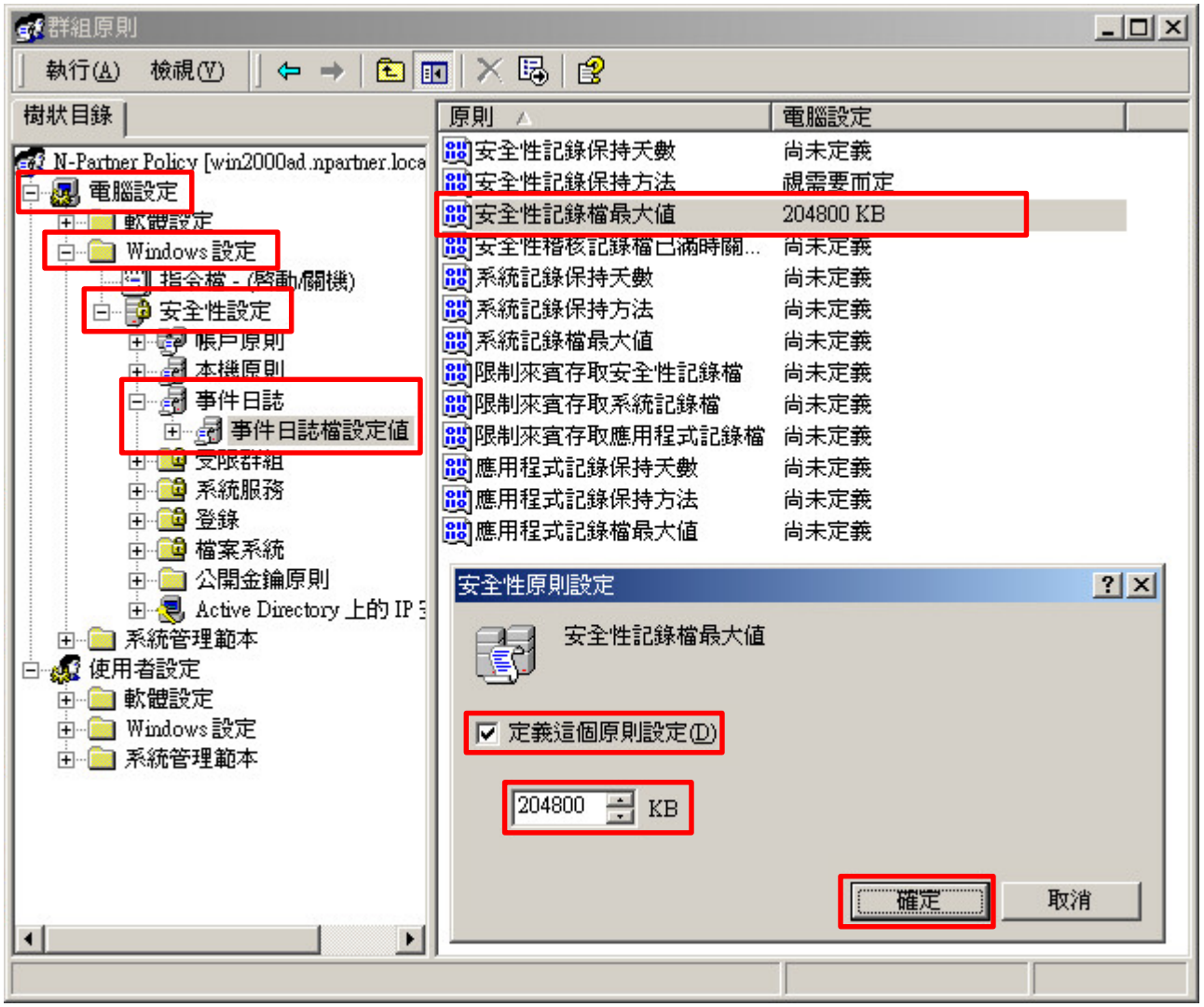
(6) 事件日誌：安全性記錄保持方法

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。

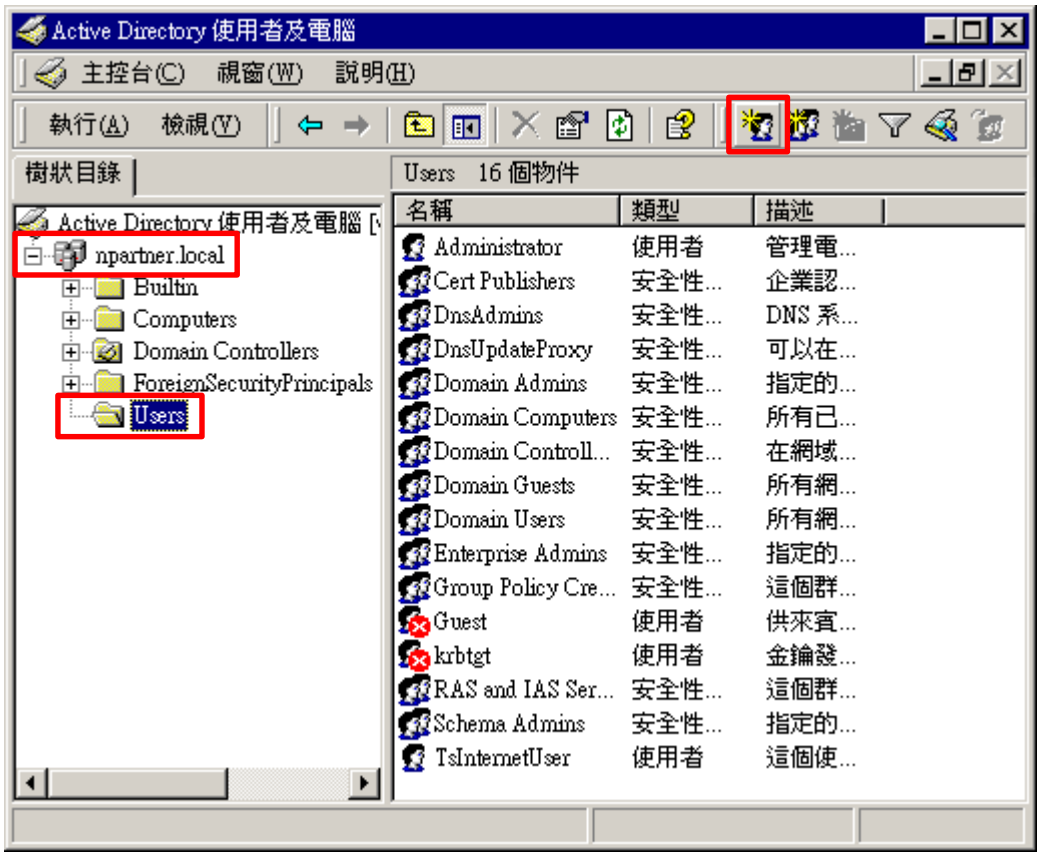
```
C:\> secedit /refreshpolicy machine_policy /enforce
```

1.3 新增非管理帳號

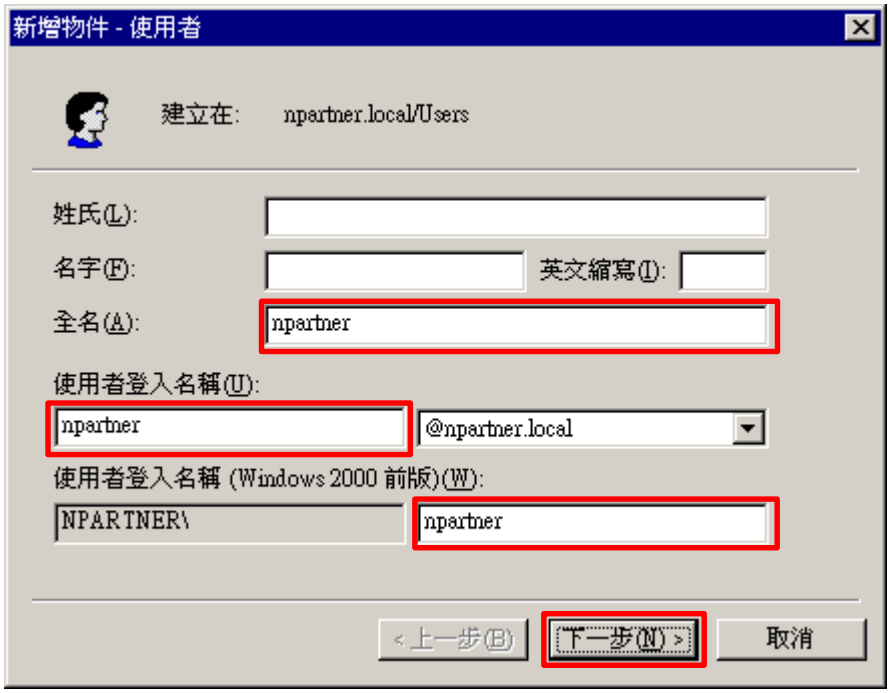
1.3.1 新增使用者

(1) 開啟 [Active Directory 使用者和電腦]

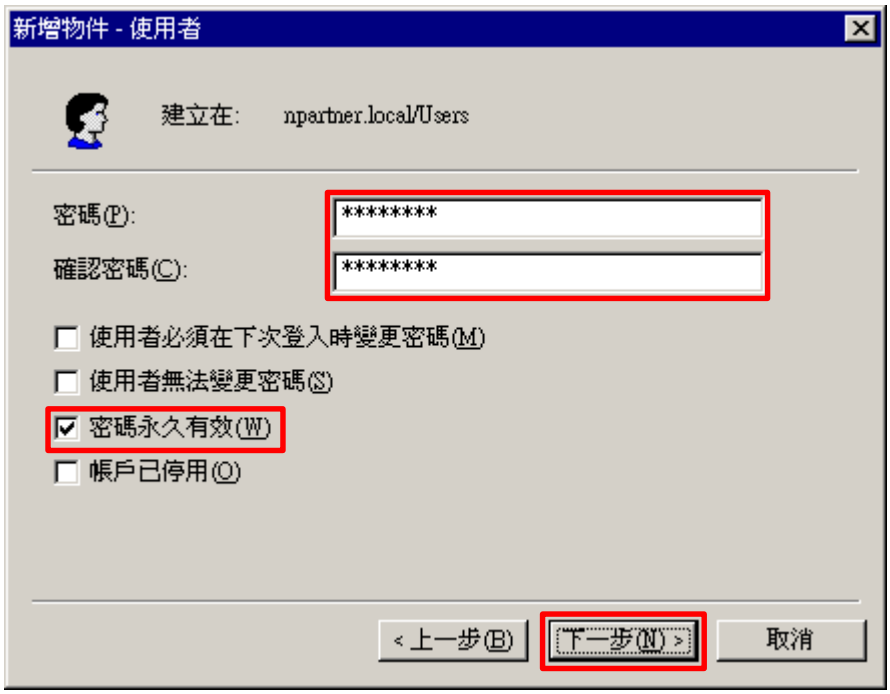
(2) [網域名稱] 的 [Users] 組織單位 註：請依客戶環境選擇組織單位 -> 按  [建立新使用者]



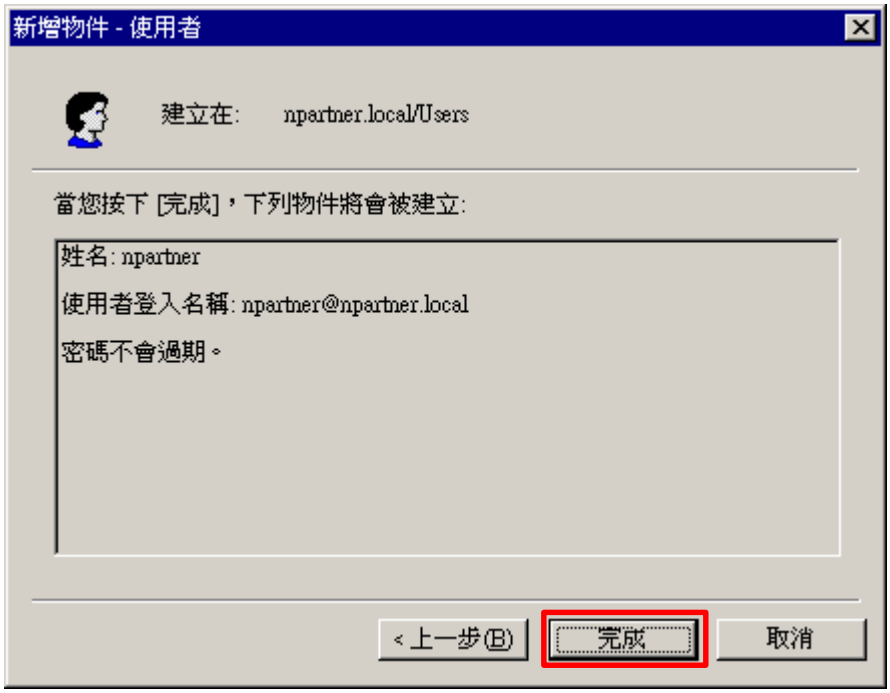
(3) 輸入 全名, 使用者登入名稱 -> 按 [下一步]



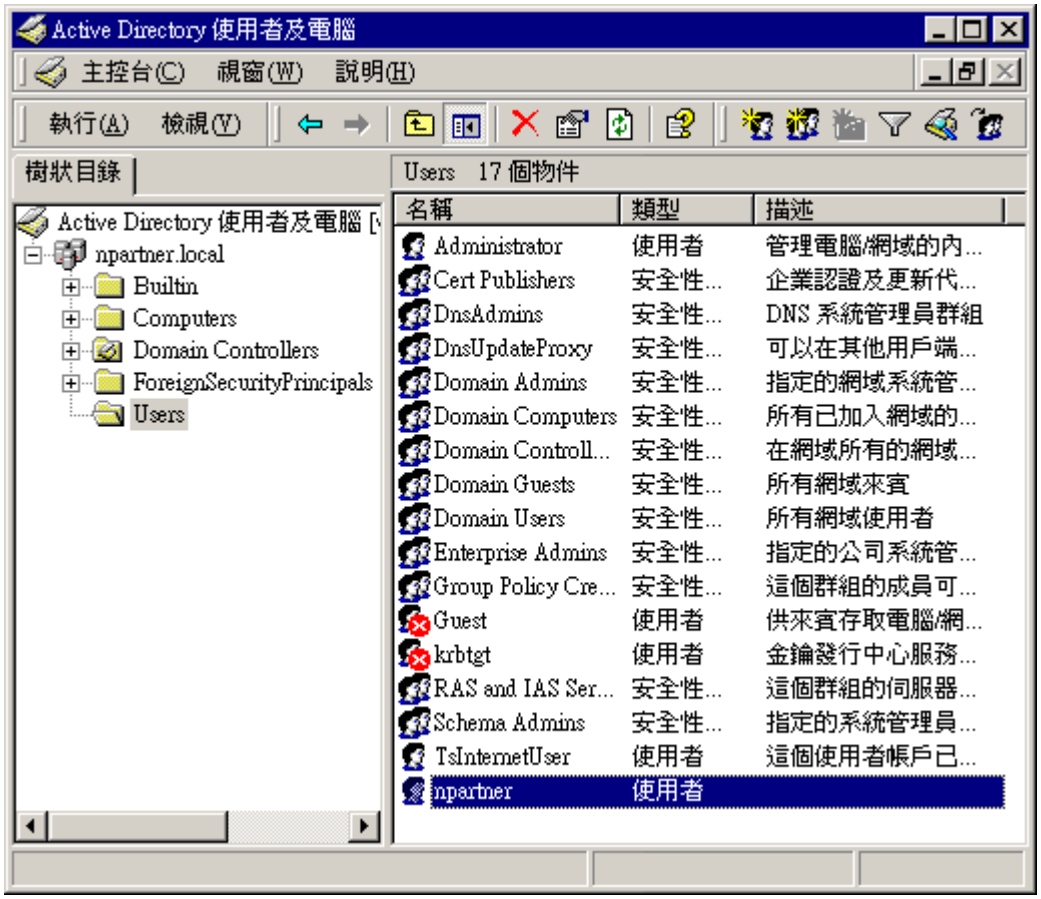
(4) 輸入 密碼, 確認密碼 -> 勾選 [密碼永久有效] -> 按 [下一步]



(5) 按 [完成]

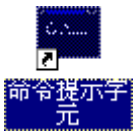


(6) 顯示帳號情形



1.3.2 設定 DCOM 權限

(1) 開啟 [命令提示字元]

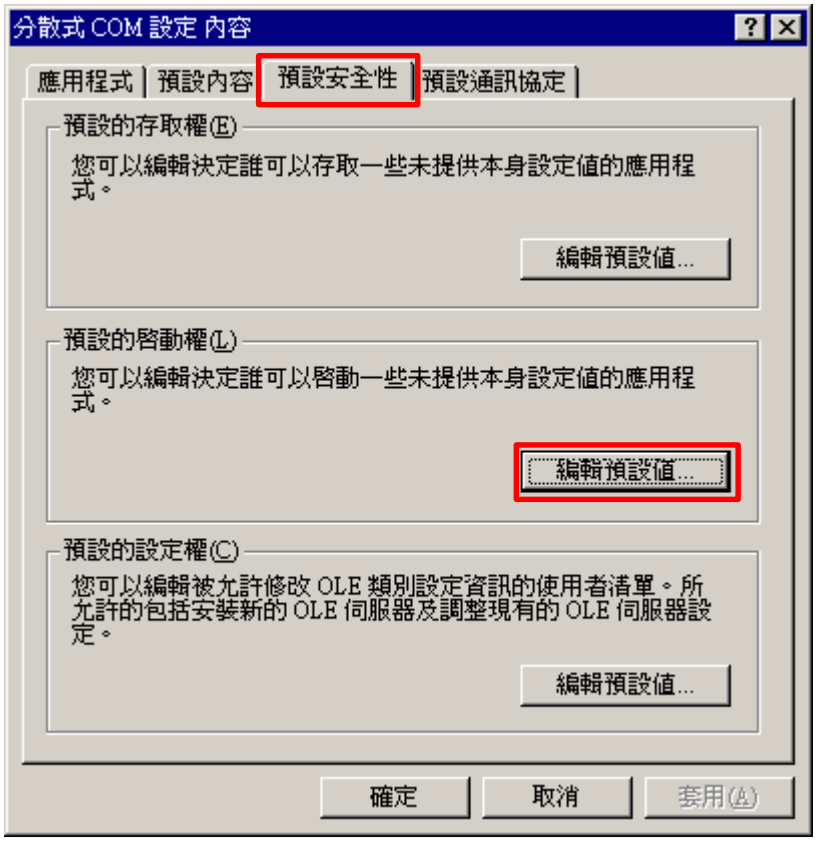


(2) 開啟元件服務

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

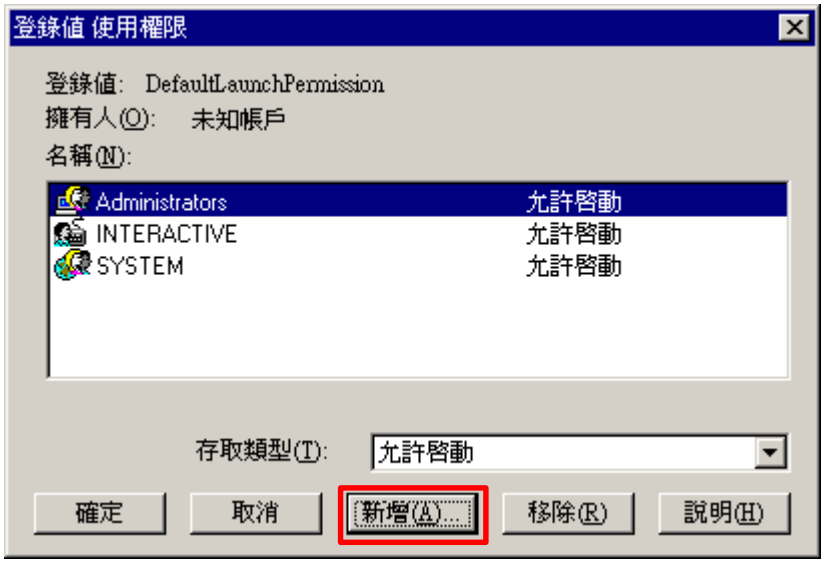
(3) 啟用權限

點選 [預設安全性] 頁面 -> 預設的啟動權，按 [編輯預設值]



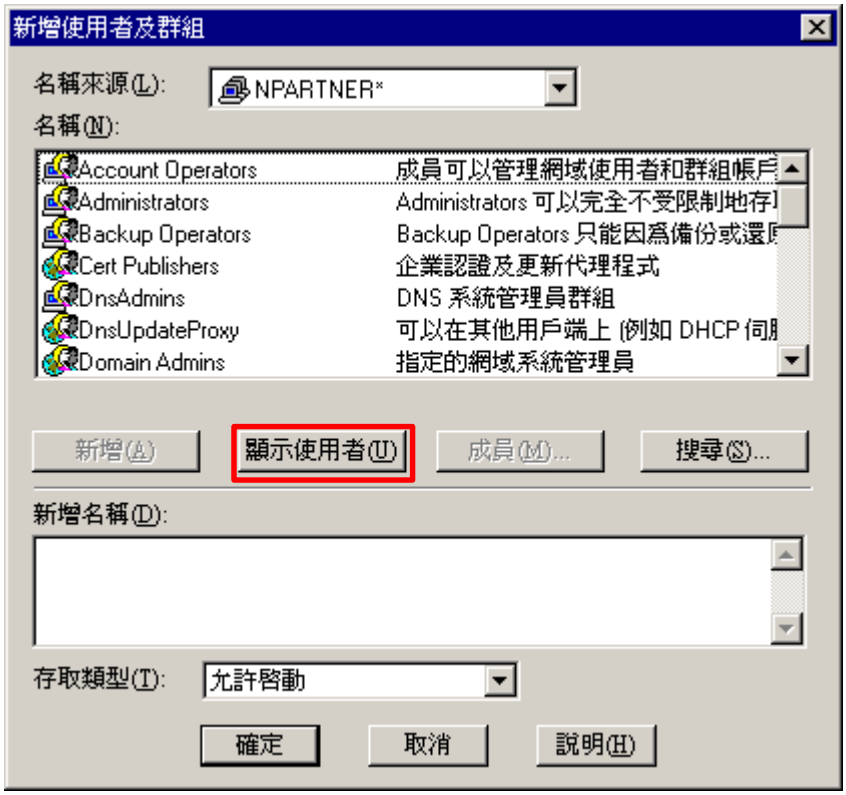
(4) 新增使用者權限

點選 [新增...]



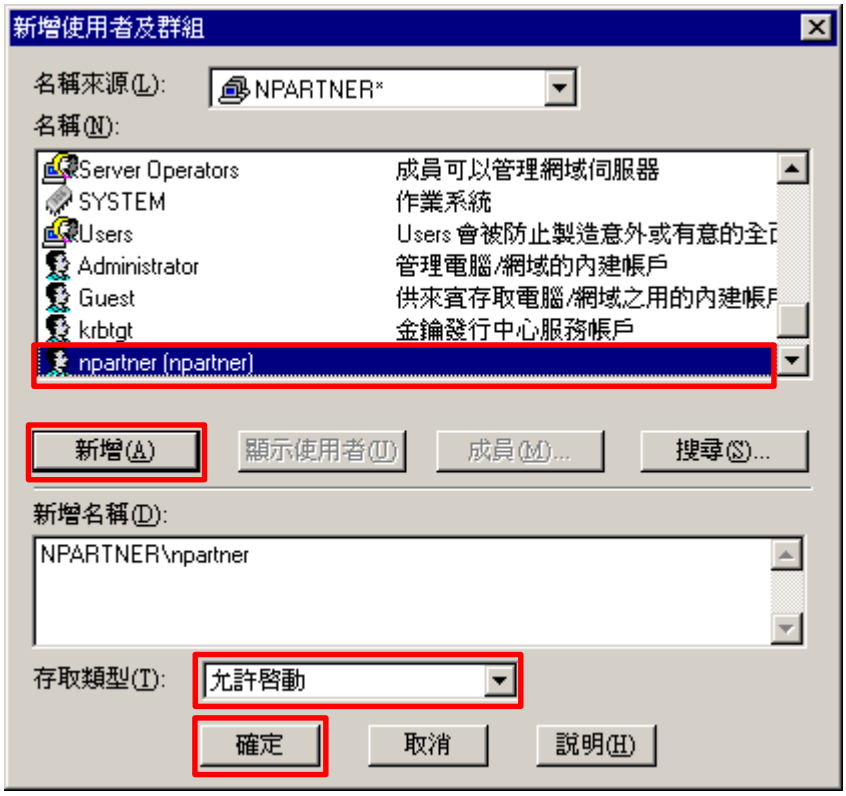
(5) 顯示使用者

按 [顯示使用者]

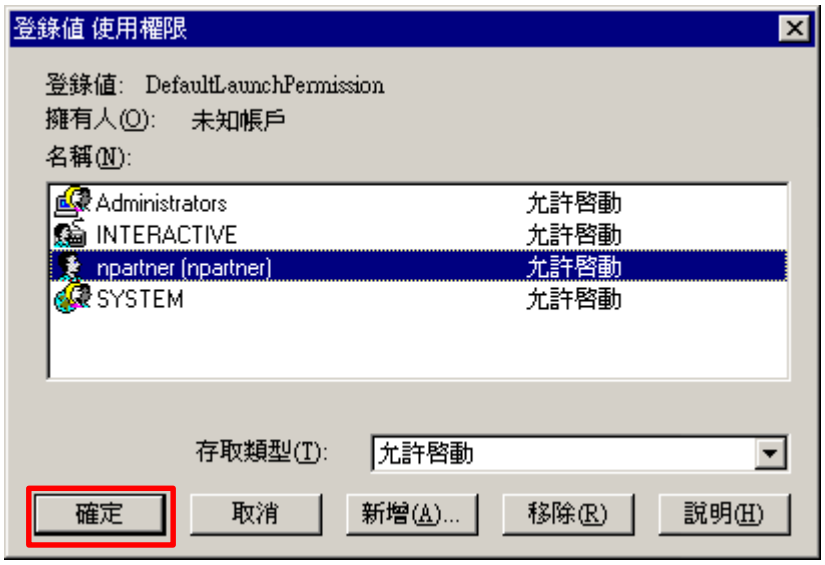


(6) 輸入使用者

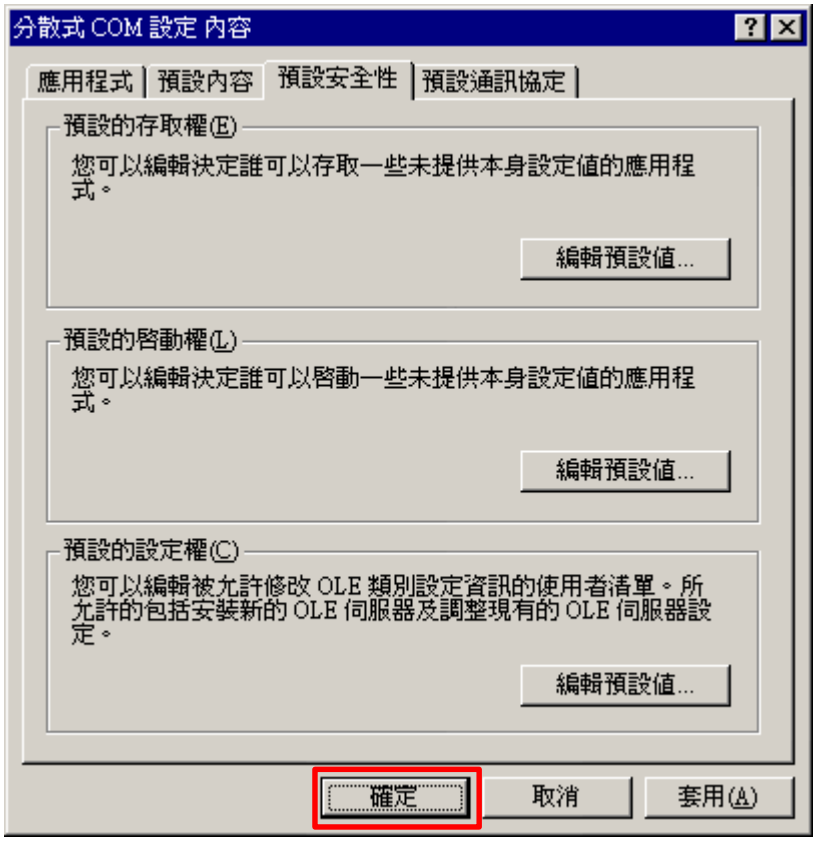
點選使用者帳號 本例 npartner -> 按 [新增] -> 存取類型: 點選 [允許啟動] -> 按 [確定]



(7) 按 [確定]



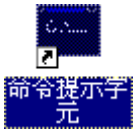
(8) 按 [確定]



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]

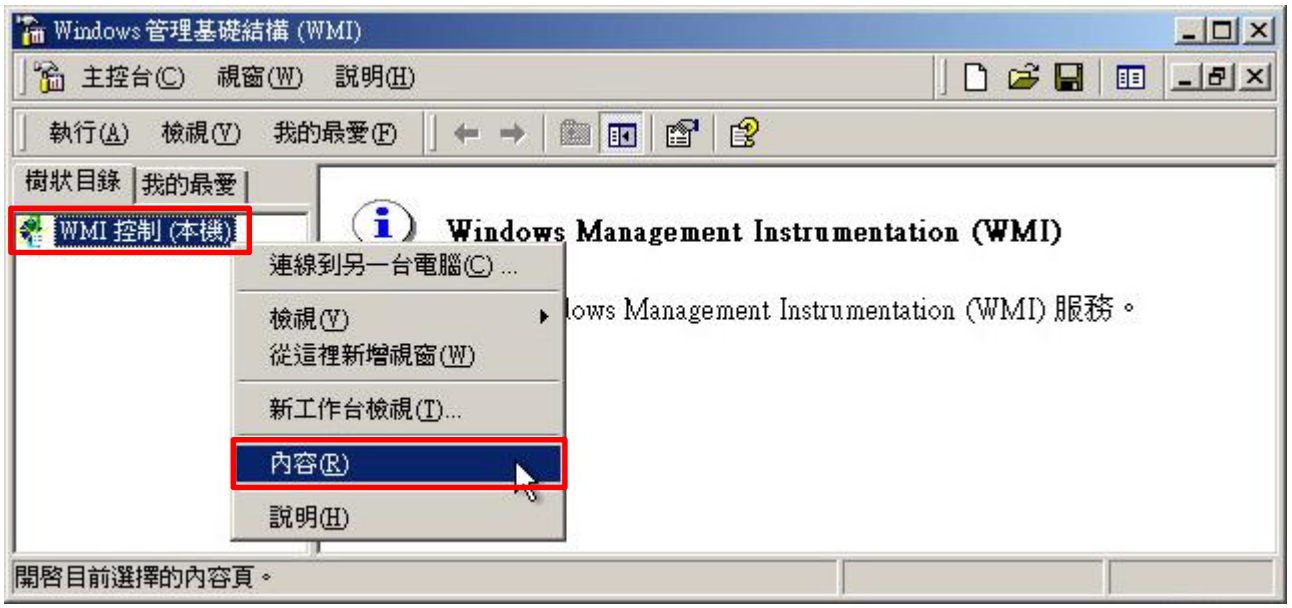


(2) 開啟 WMI 控制

```
C:\> wmimgmt.msc
```

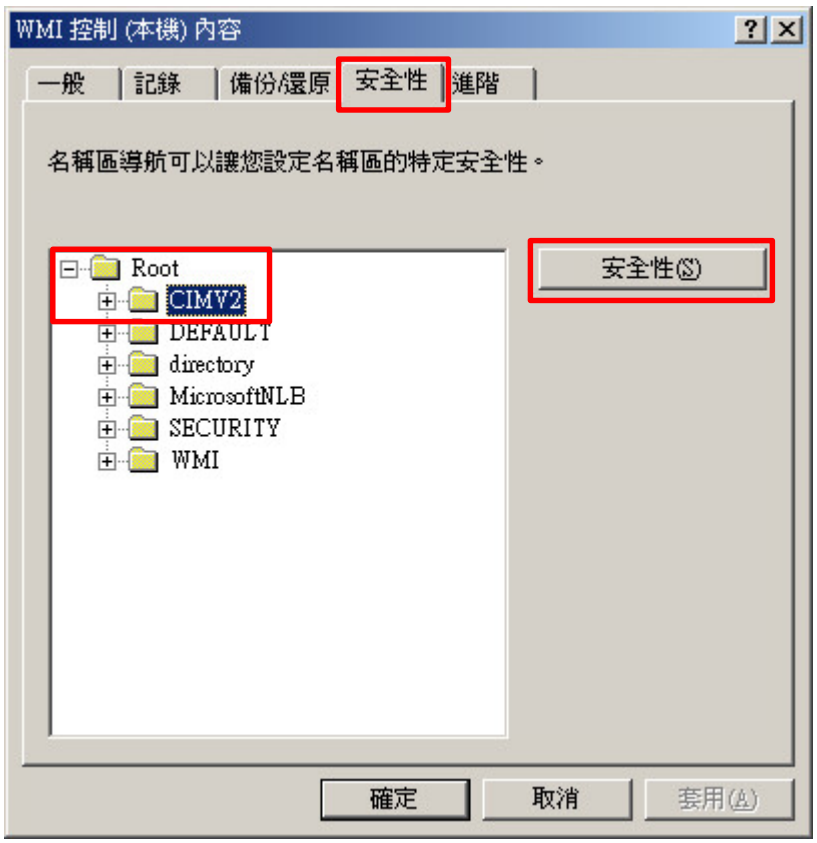
(3) 編輯 WMI 控制

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]

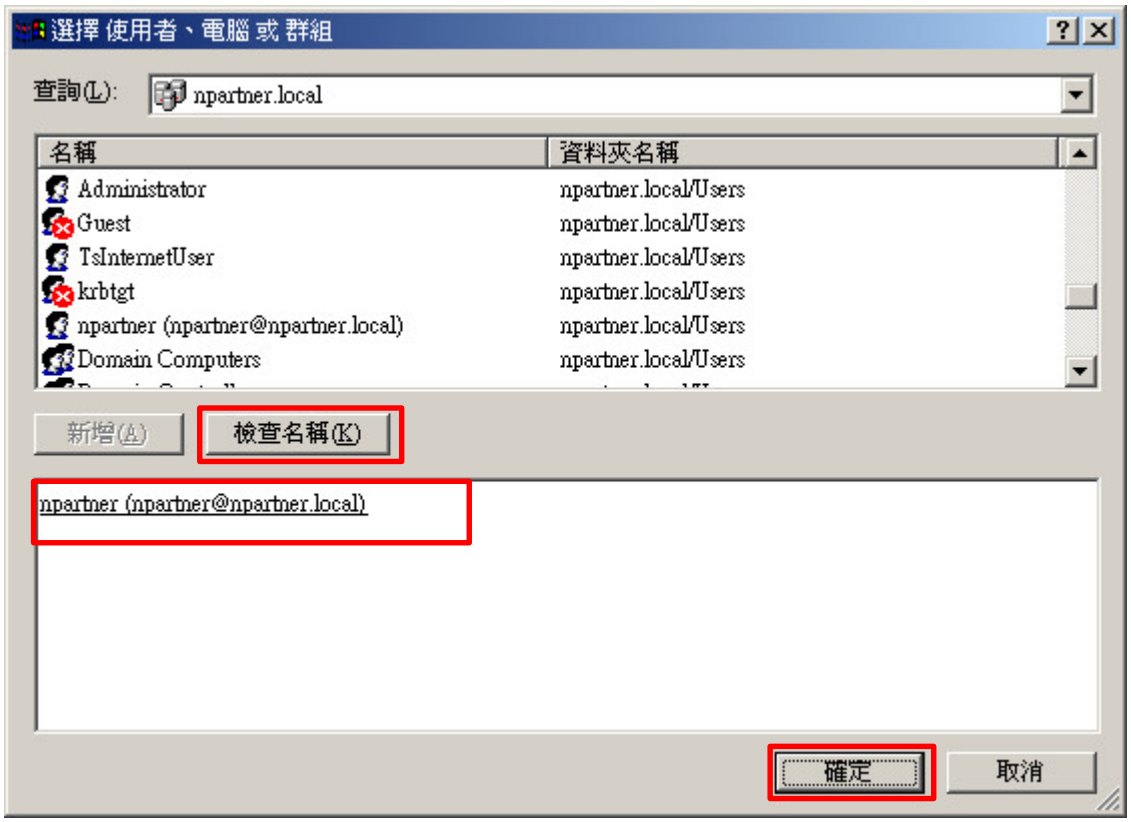


(5) 新增 WMI 使用者權限

按 [新增]

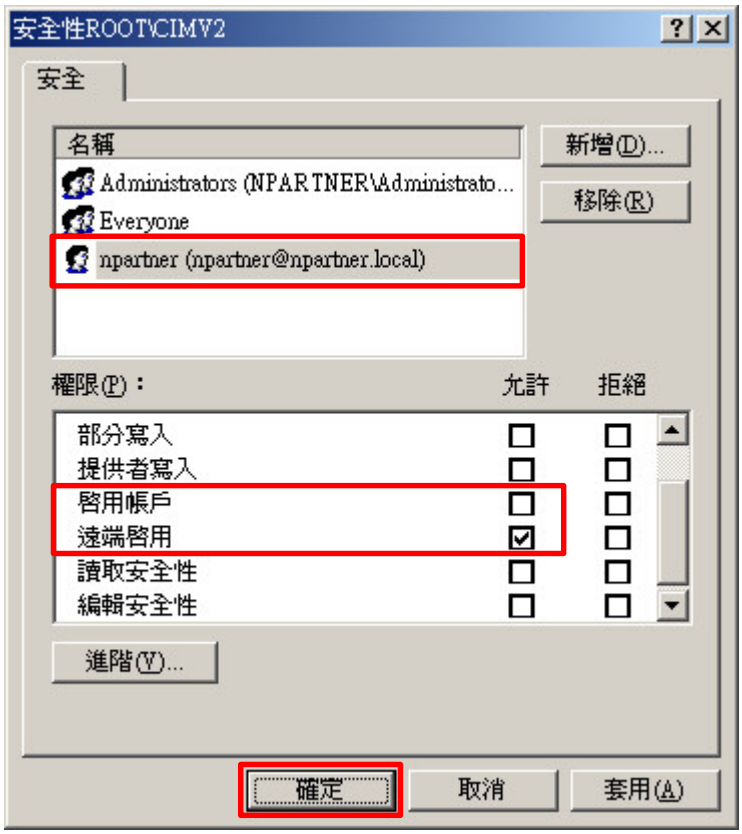
(6) 輸入使用者

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

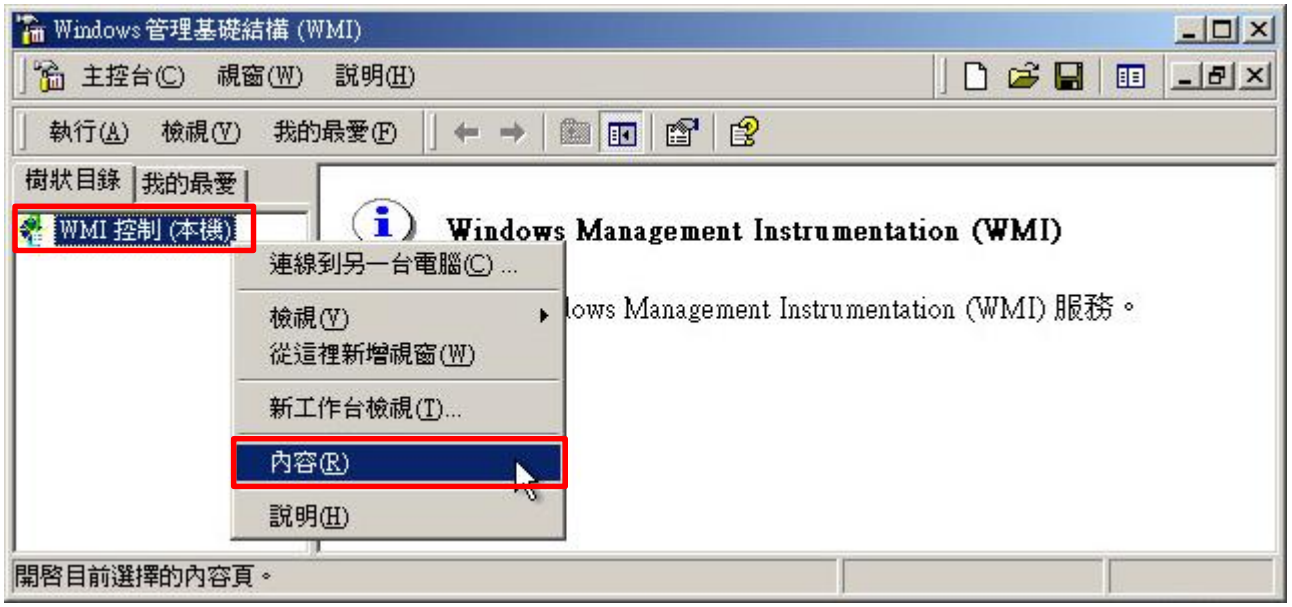
(1) 開啟 [命令提示字元]

(2) 開啟 WMI 控制

```
C:\> wmimgmt.msc
```

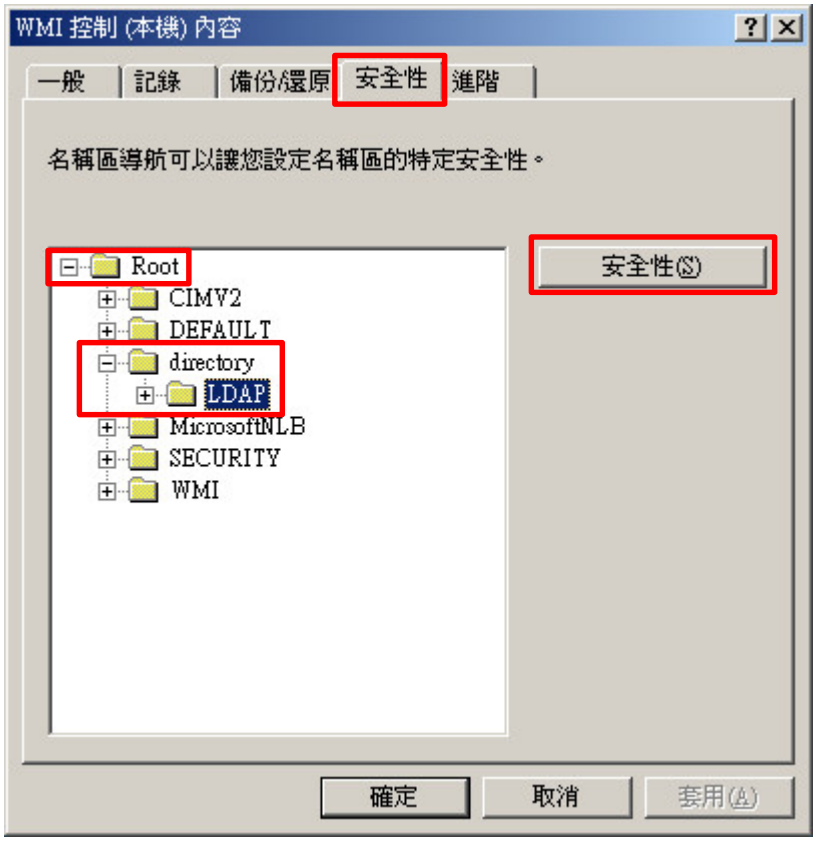
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



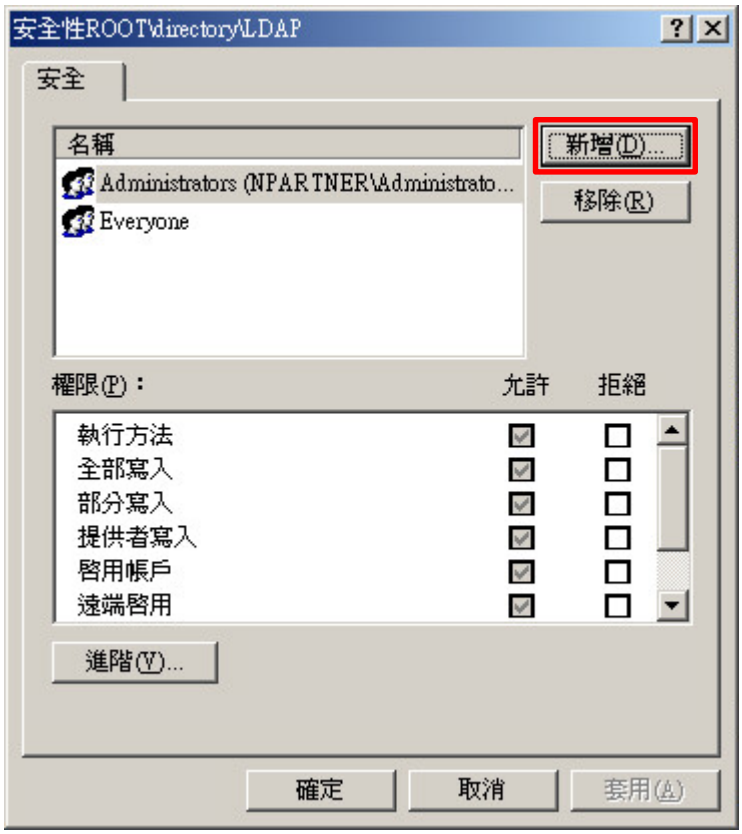
(4) 編輯 LDAP 安全性

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



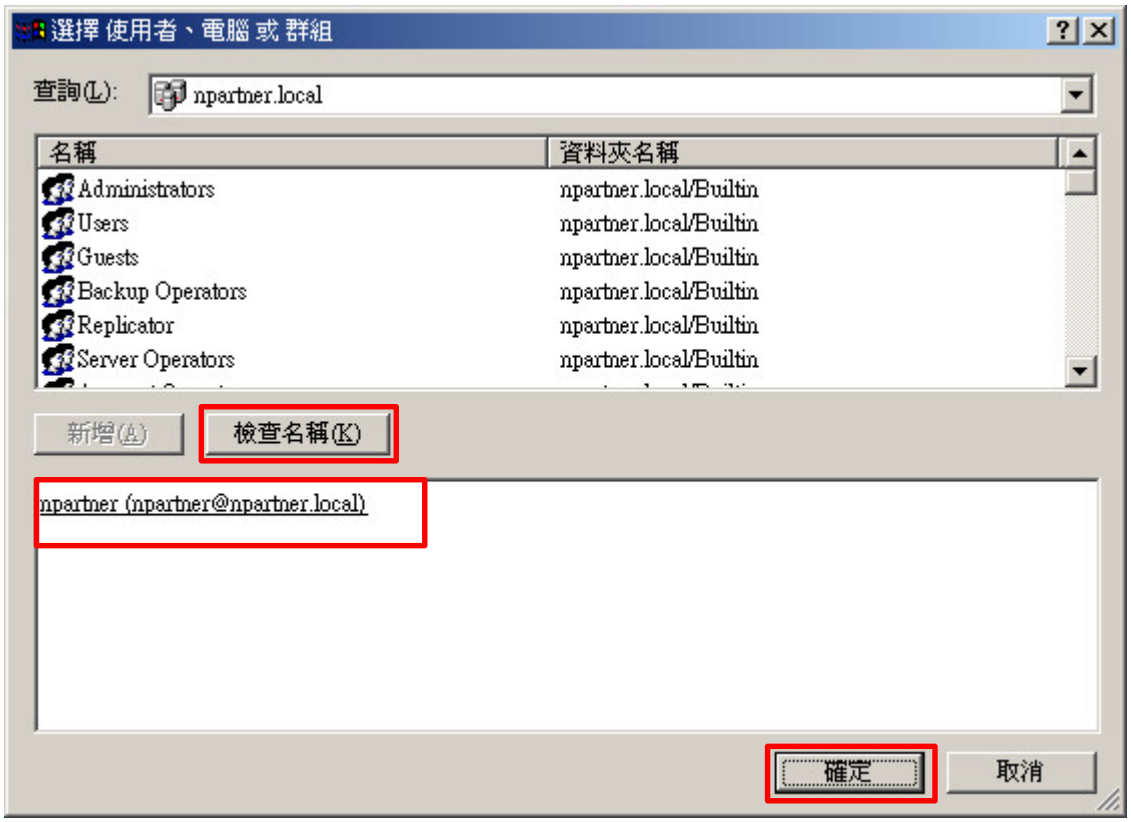
(5) 新增 WMI 使用者權限

按 [新增]



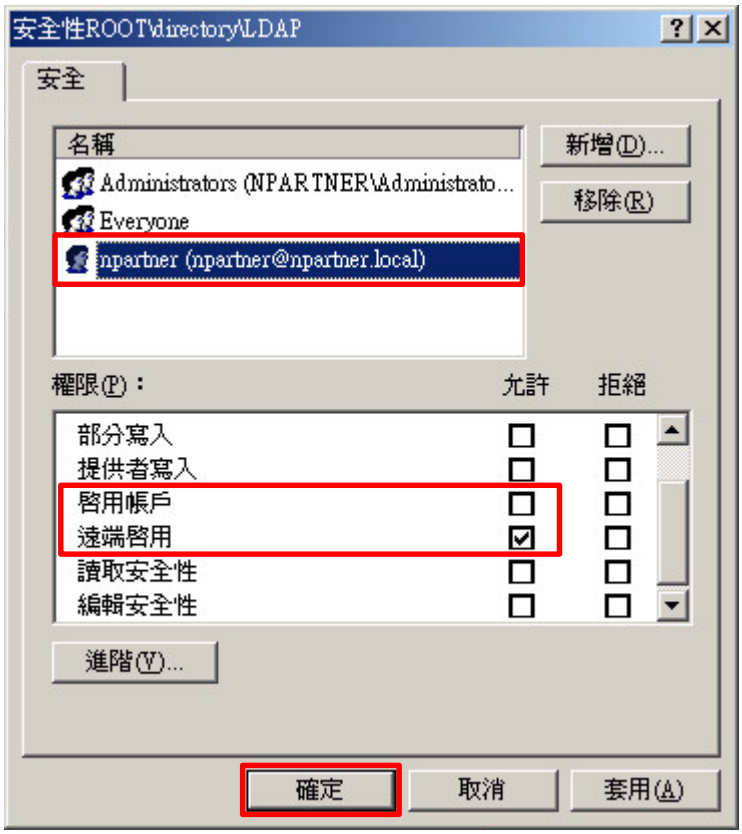
(6) 輸入使用者

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]

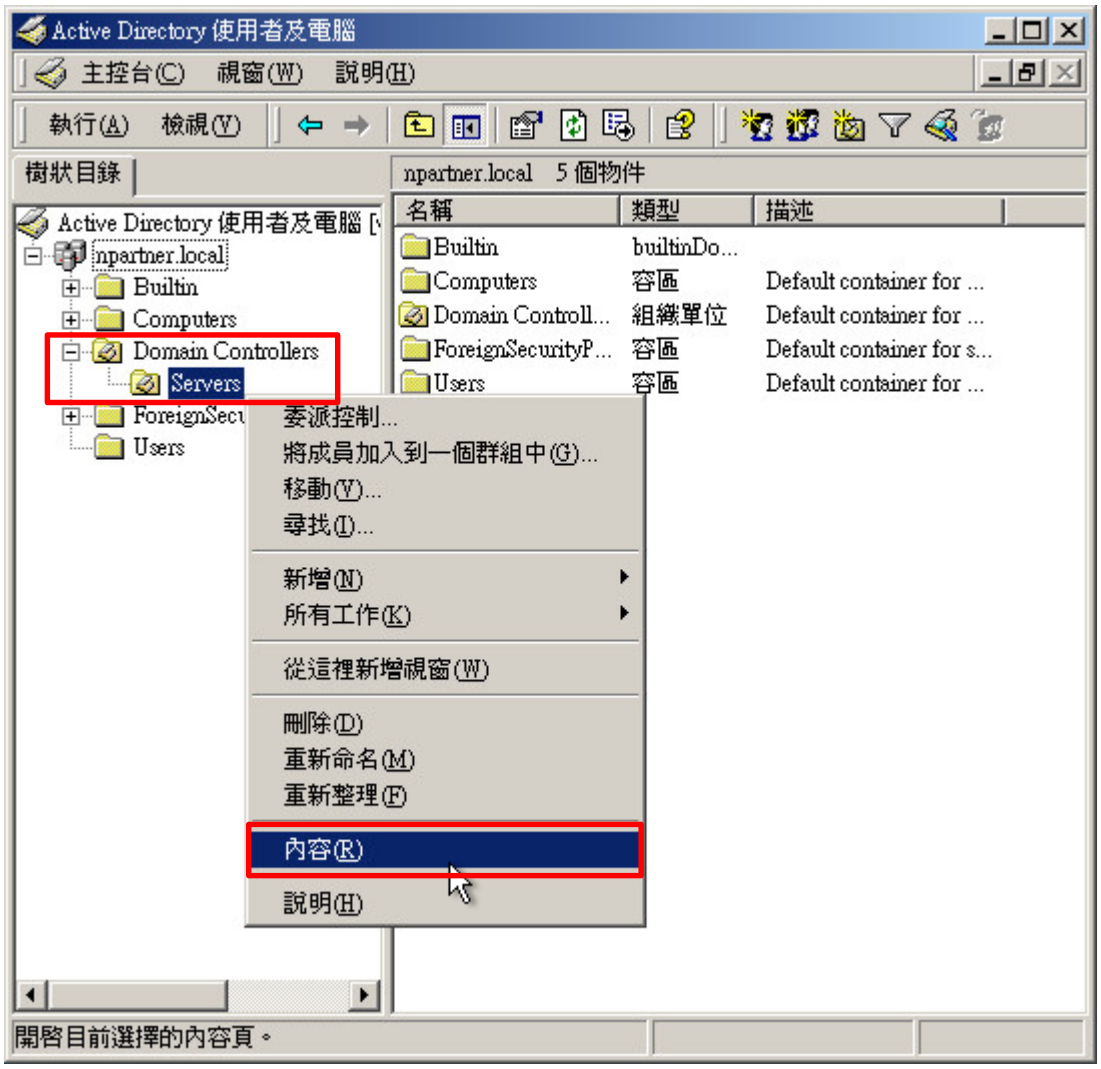
1.3.4 設定 Event log 讀取權限

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

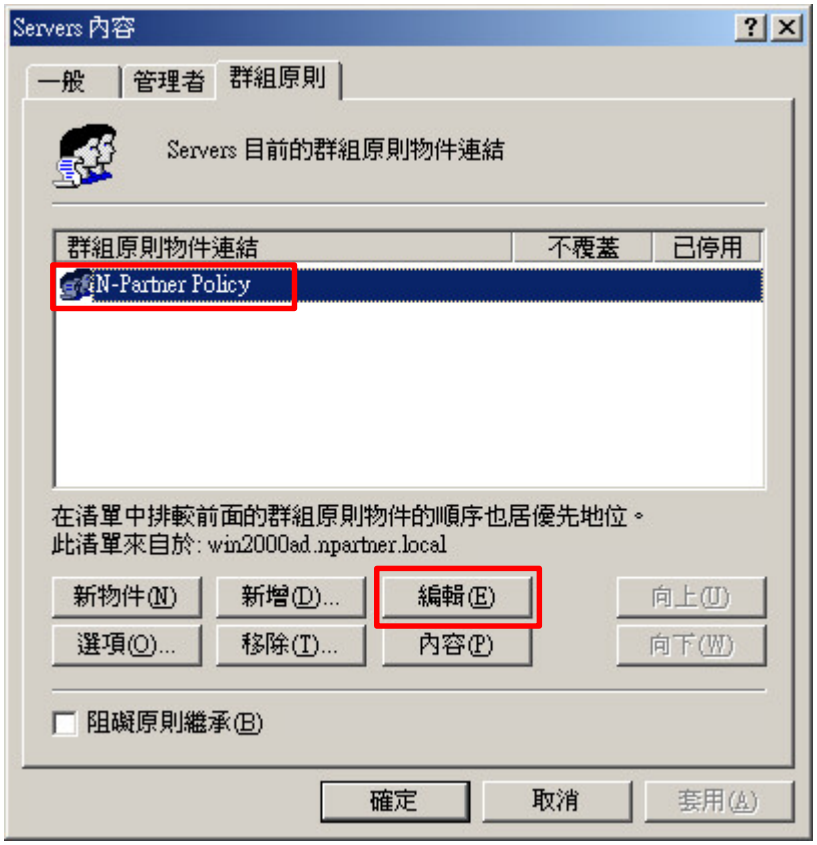
(2) Domain Controllers 的 Servers 組織單位，點選內容

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



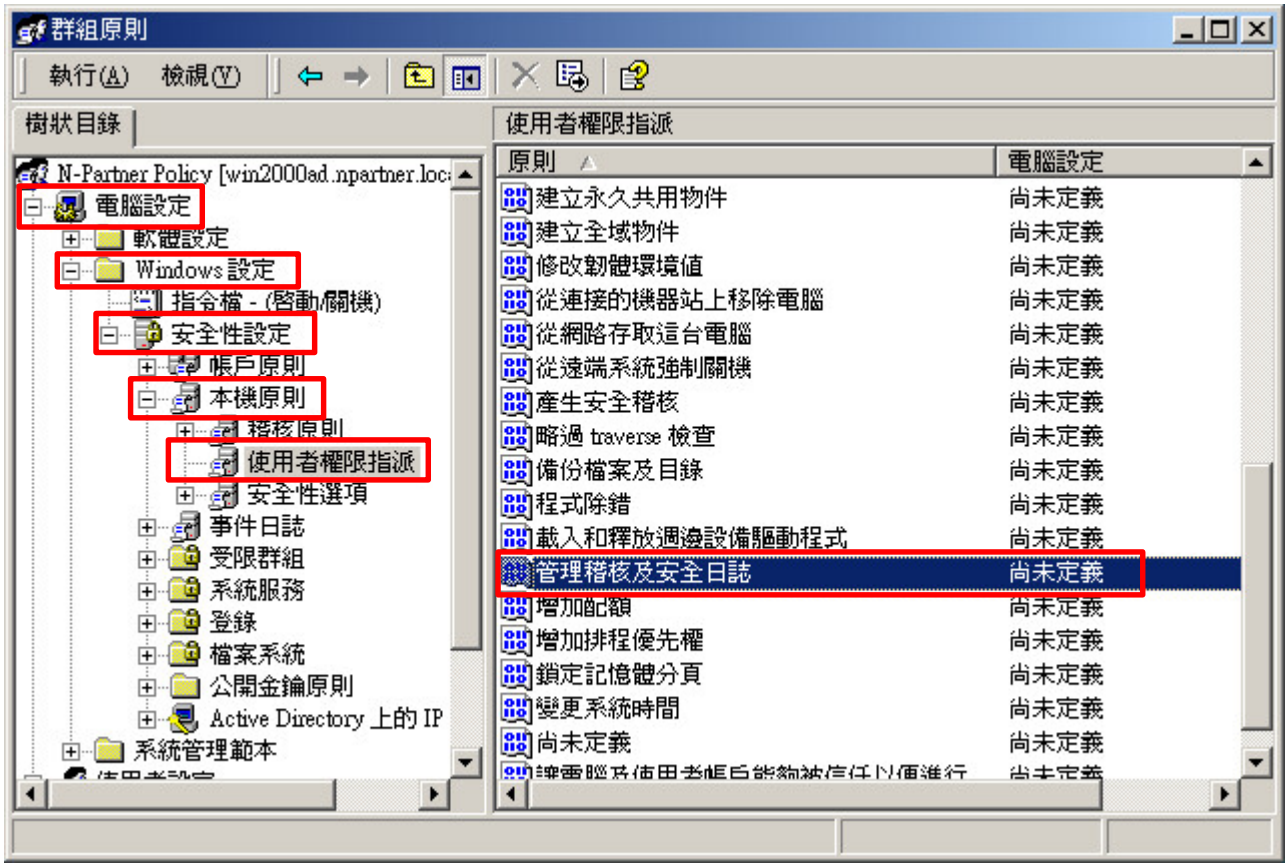
(3) 編輯群組原則物件

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] -> 按 [新增...]

(6) 搜尋使用者

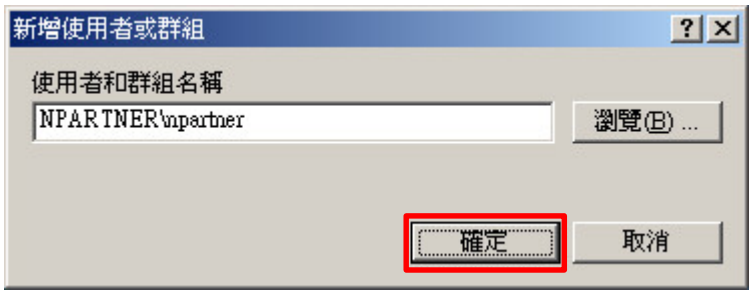
按 [瀏覽]

(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

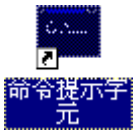
按 [確定]



(9) 確定設定記錄檔

按 [確定]

(10) 開啟 [命令提示字元]

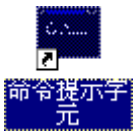


(11) 更新群組原則

```
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

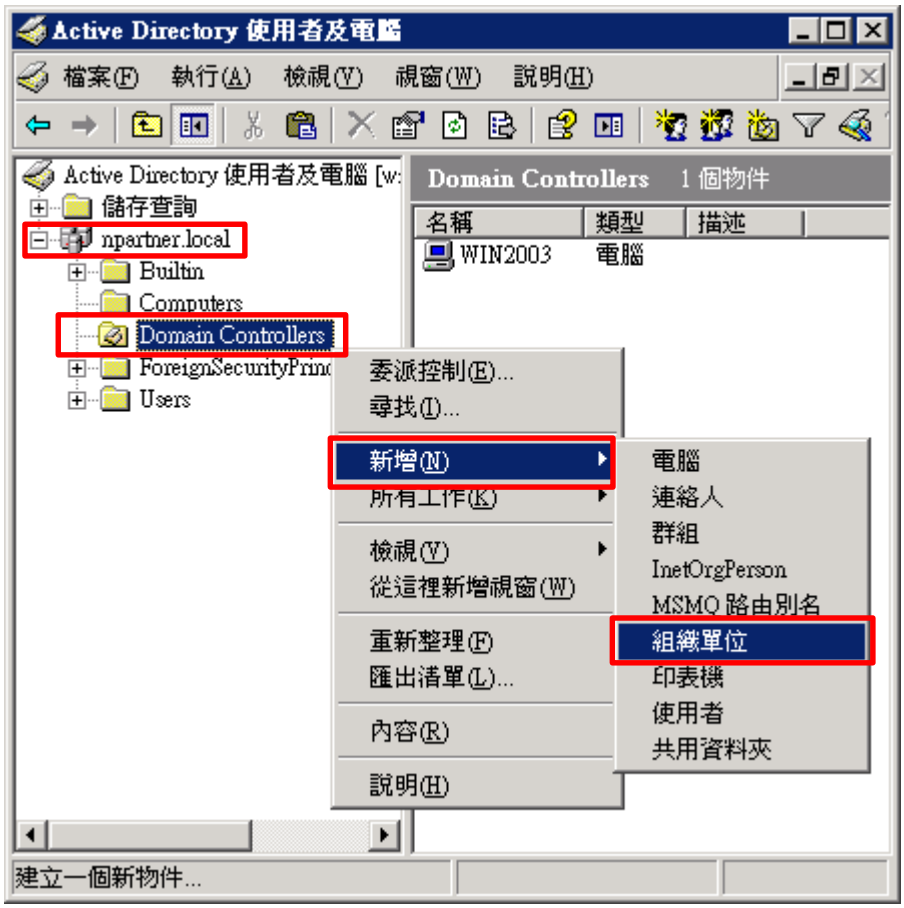
Windows 稽核原則設定 詳細說明請參考**前言**的稽核原則建議連結

2.1 組織單位設定

(1) 開啟 [Active Directory 使用者和電腦]

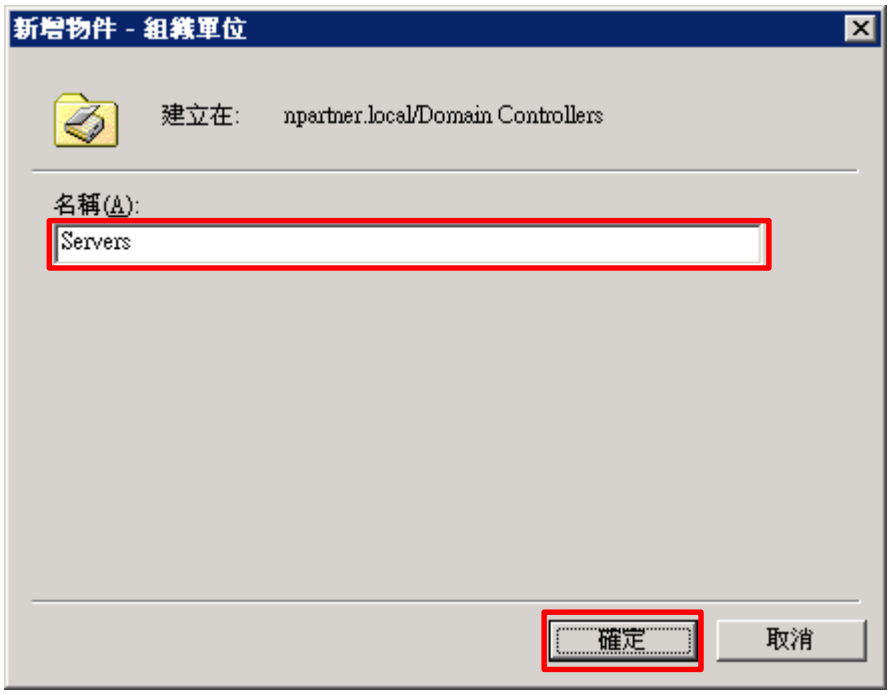
(2) 新增組織單位

[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]



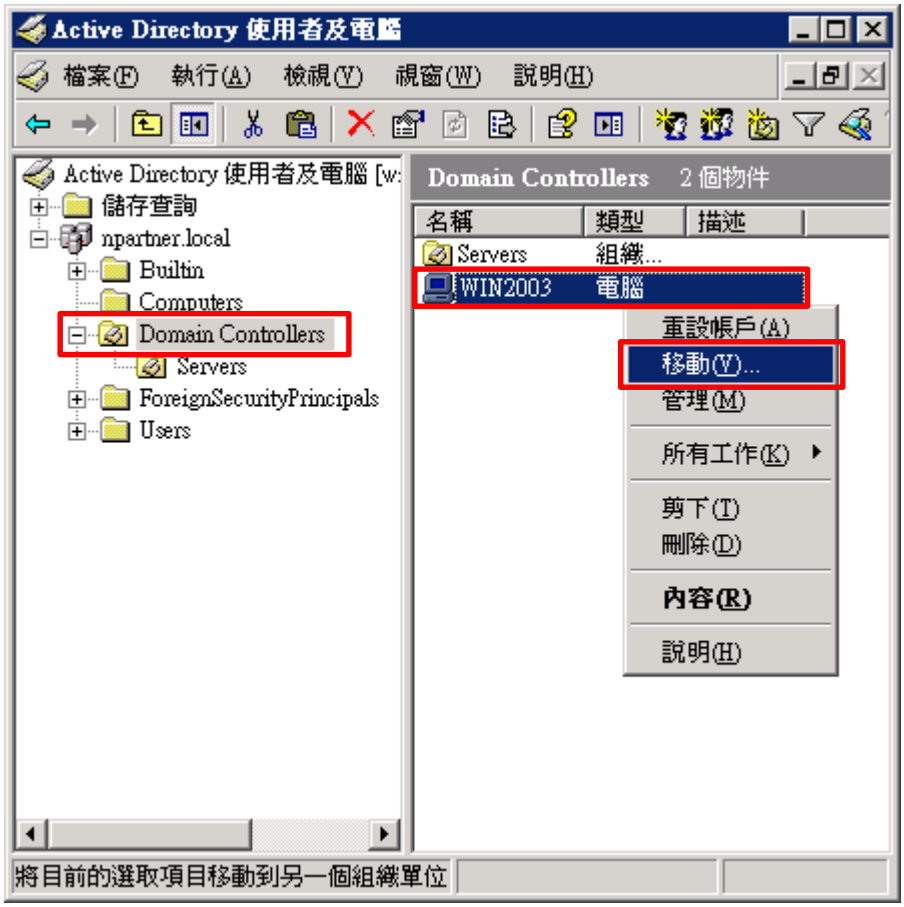
(3) 輸入組織單位名稱

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 註：請依客戶環境選擇 Windows AD 主機 -> 點選 [移動]

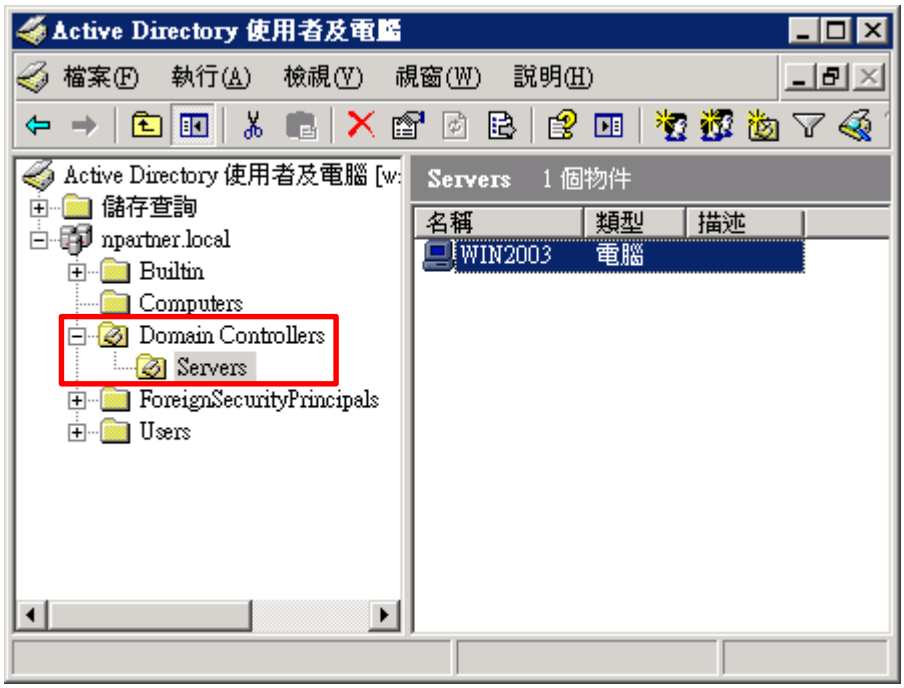


(5) 選擇組織單位

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。



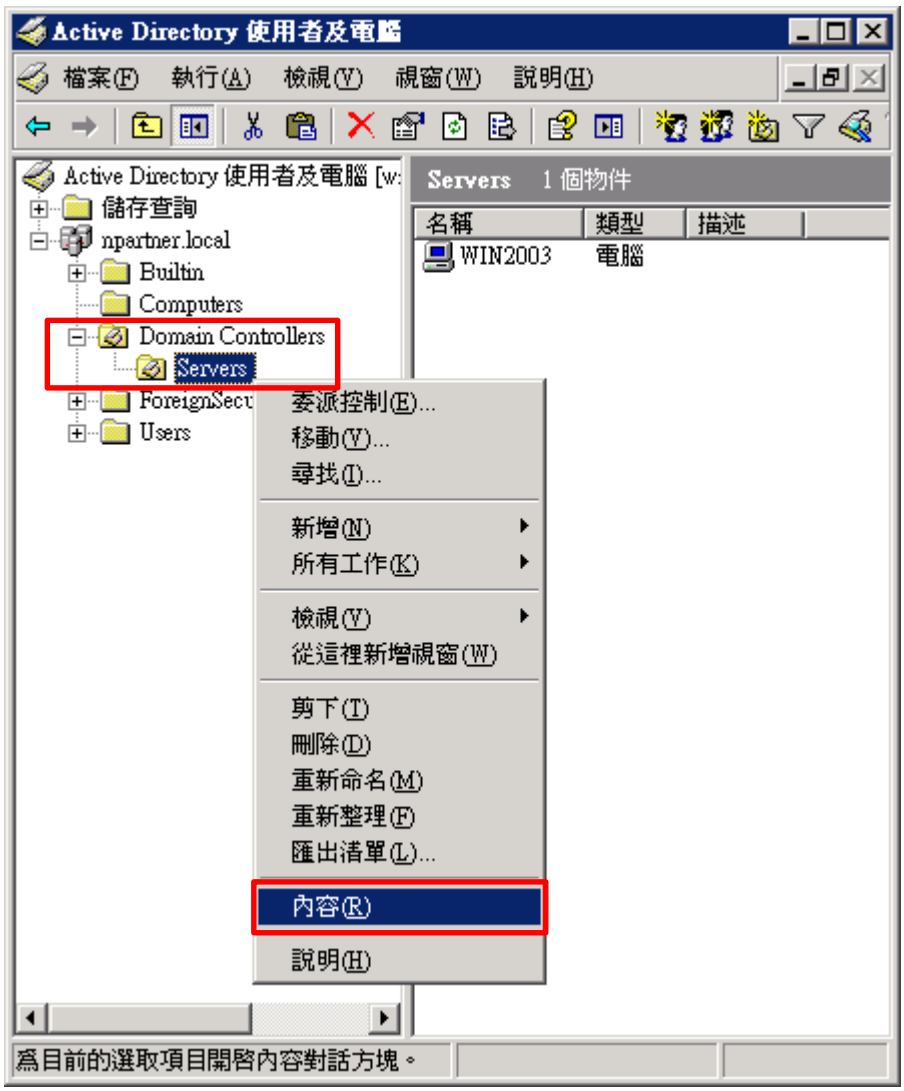
2.2 群組原則設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

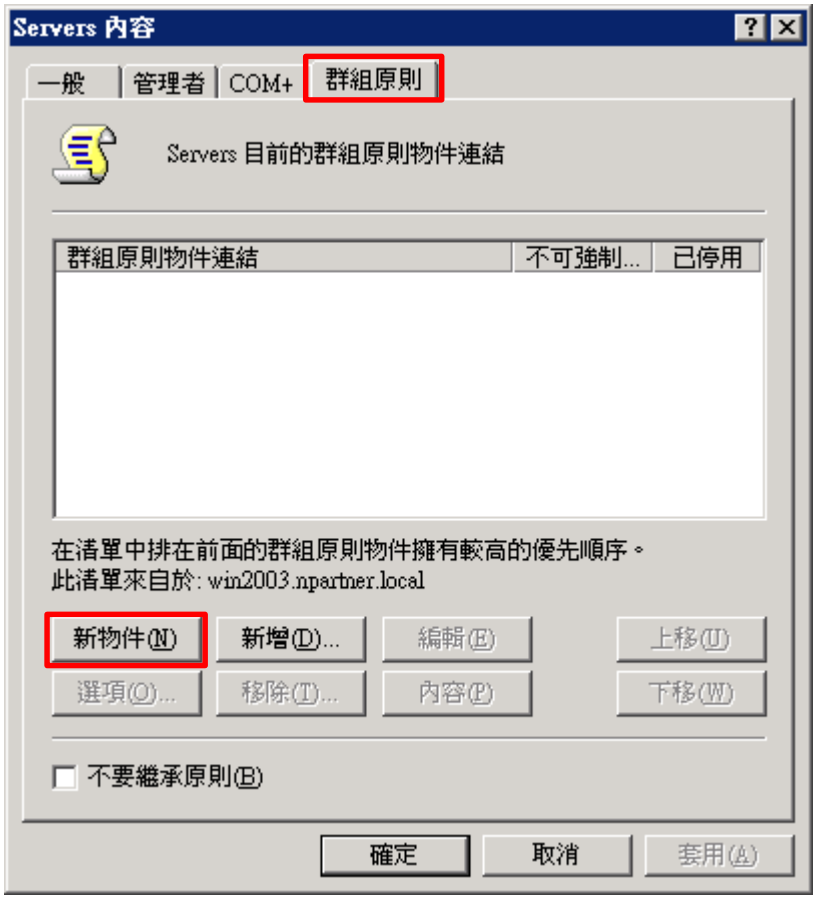
(2) Domain Controllers 的 Servers 組織單位，點選內容

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



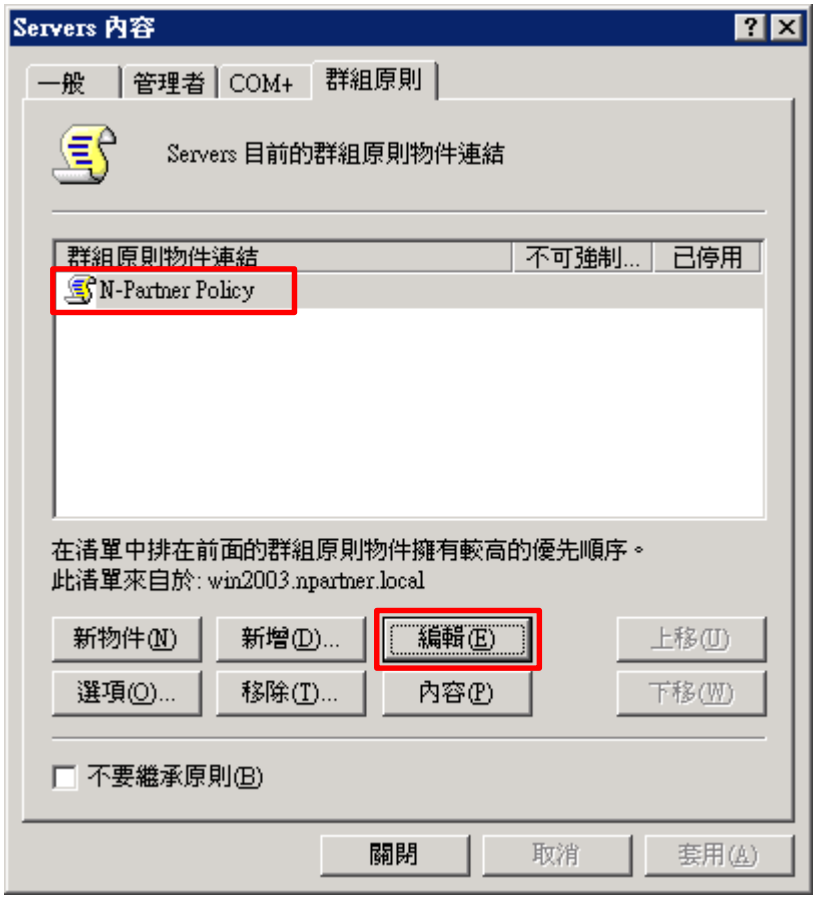
(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按 [新物件]



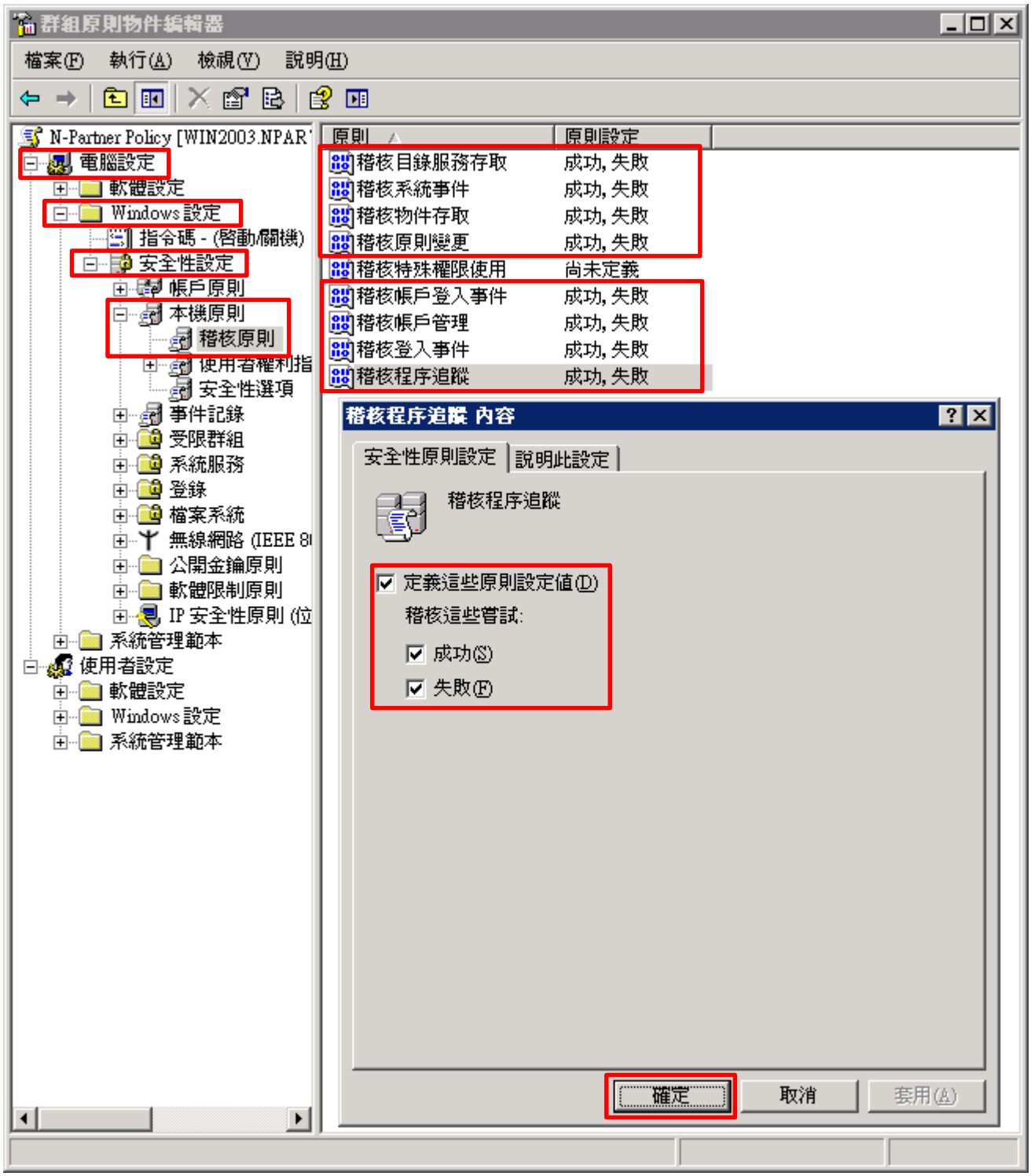
(4) 編輯群組原則物件

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]



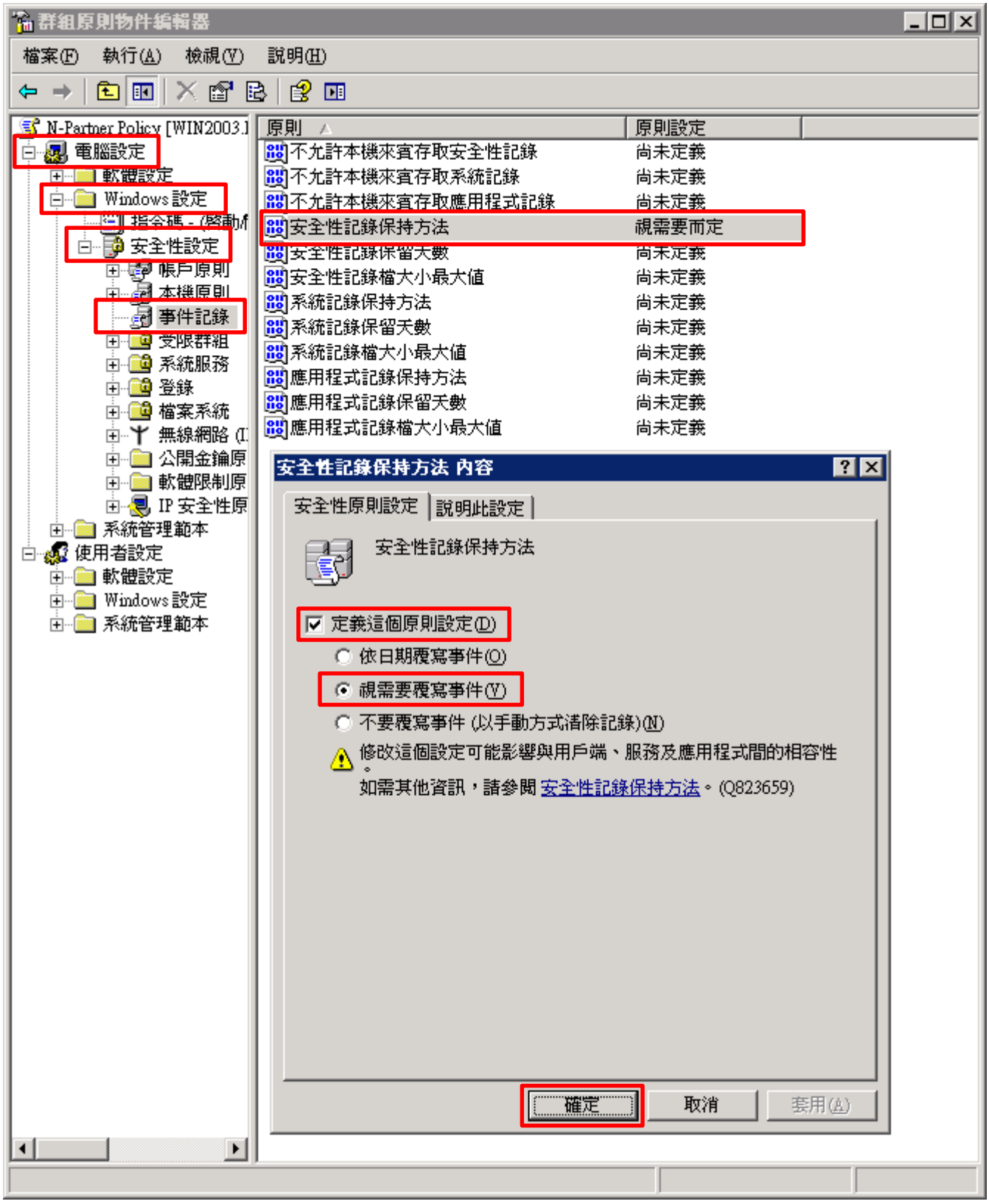
(5) 本機原則：稽核原則

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]



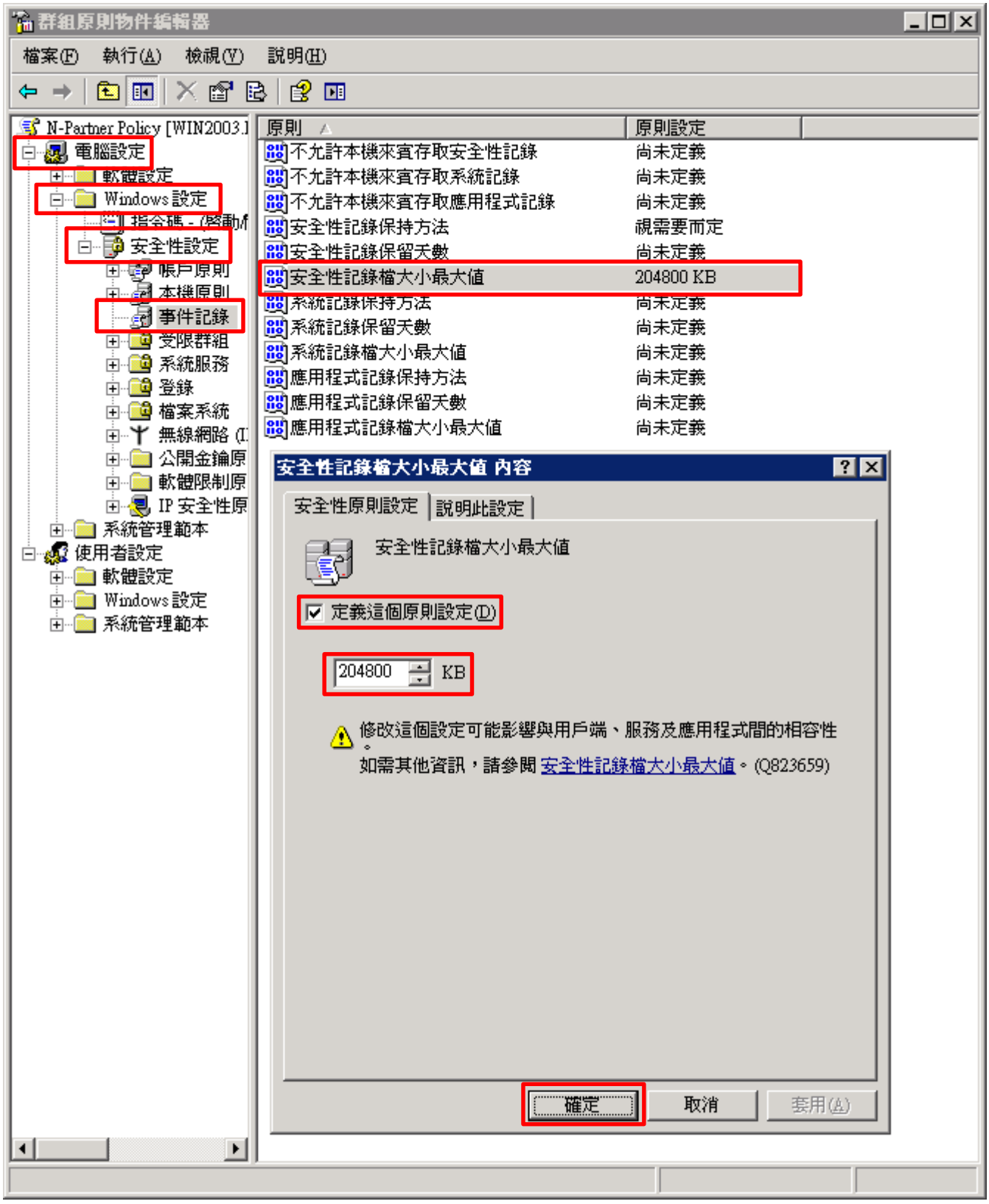
(6) 事件記錄：安全性記錄保持方法

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]



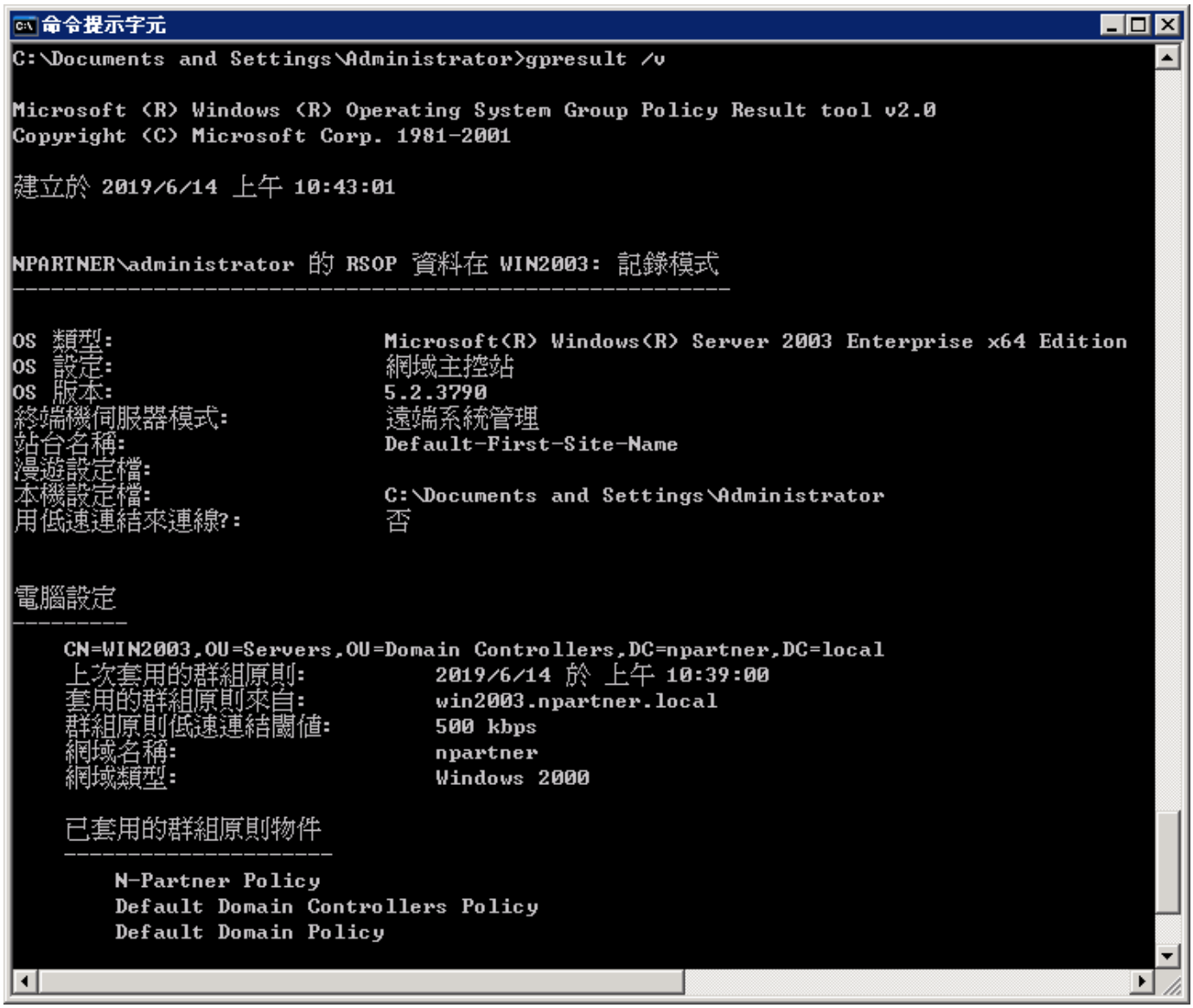
(8) 開啟 [命令提示字元]

(9) 更新群組原則

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

(10) 查看群組原則套用情形

```
C:\> gpresult /v
```



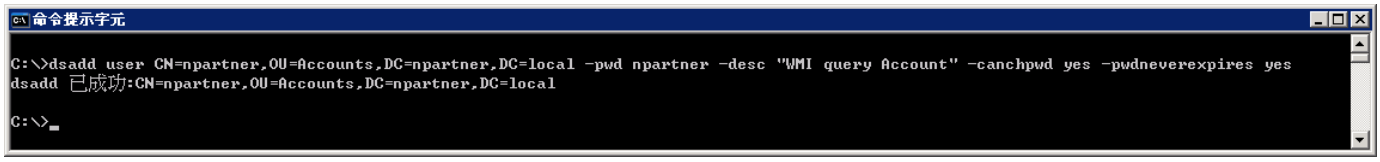
2.3 新增非管理帳號

2.3.1 新增使用者

(1) 開啟 [命令提示字元]

(2) 新增帳號

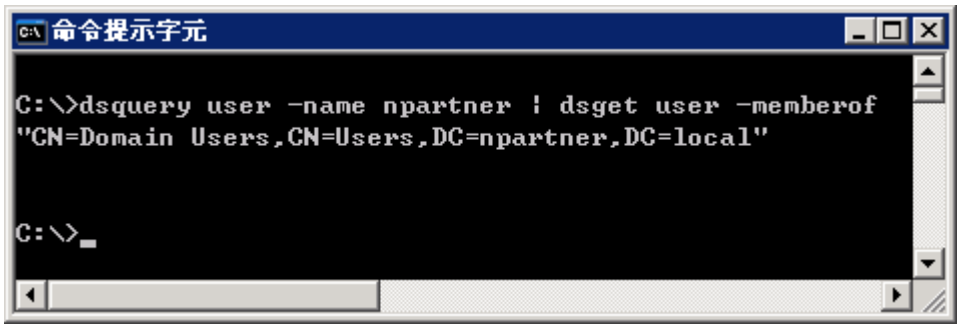
```
C:\> dsadd user CN=npartner,OU=Accounts,DC=npartner,DC=local -pwd npartner -desc "WMI query Account" -canchpwd yes -pwdneverexpires yes
```



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

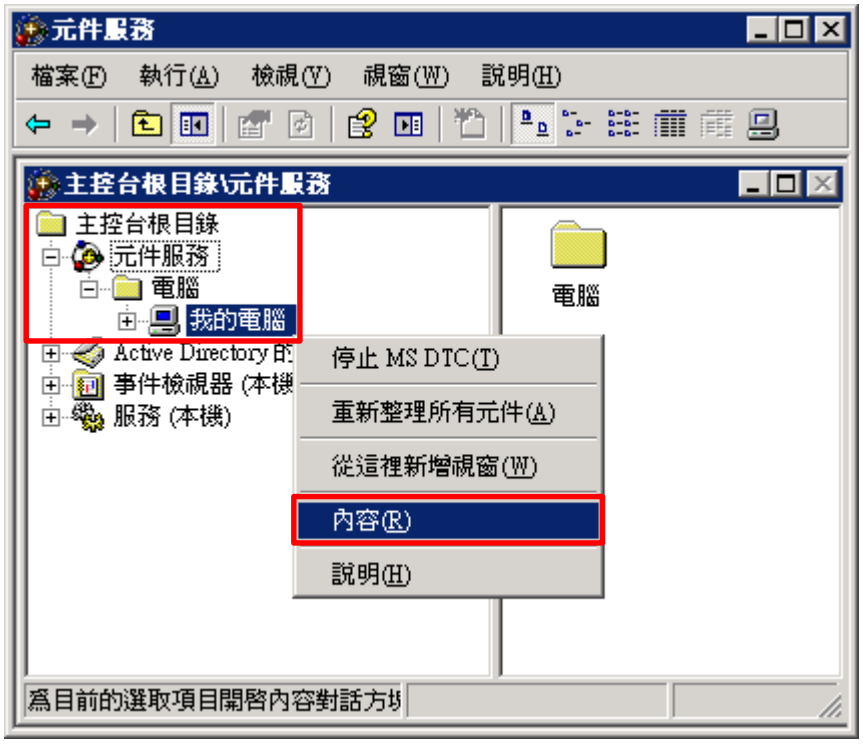
(1) 開啟 [命令提示字元]

(2) 開啟元件服務

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

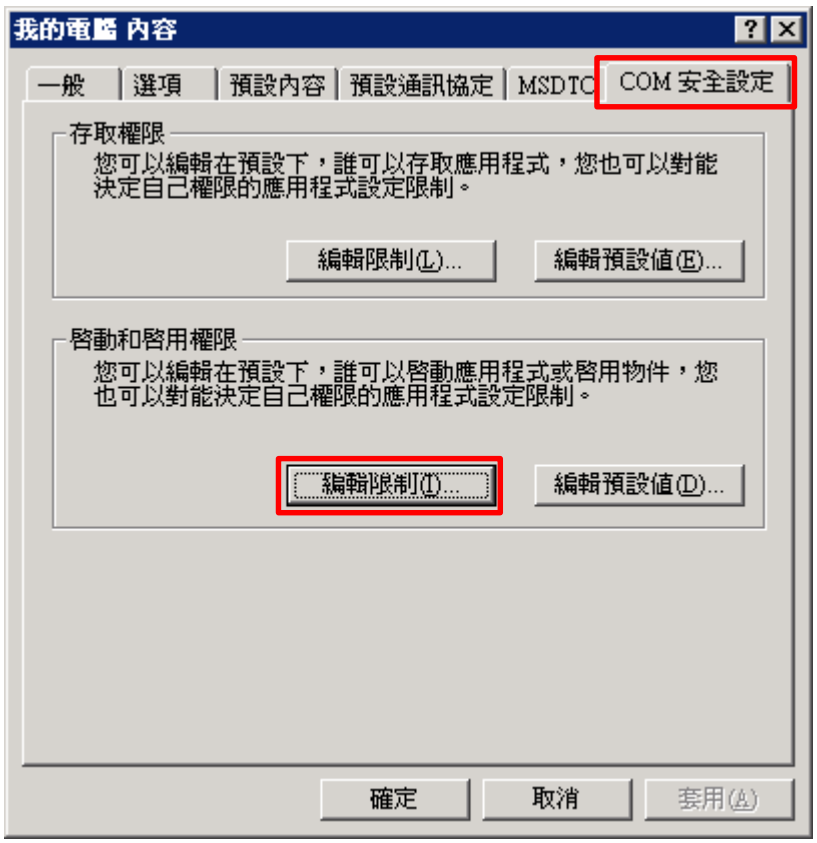
(3) 編輯電腦內容

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]

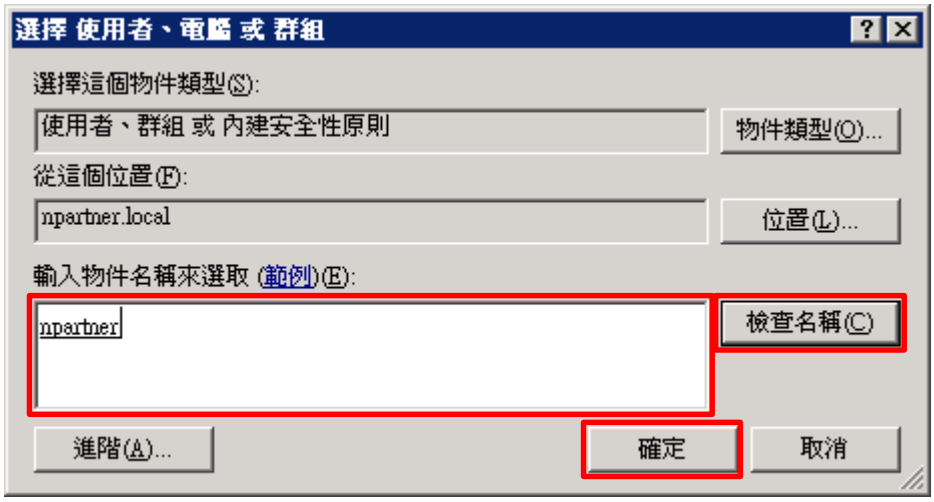


(5) 新增 DCOM 使用者權限

點選 [新增]

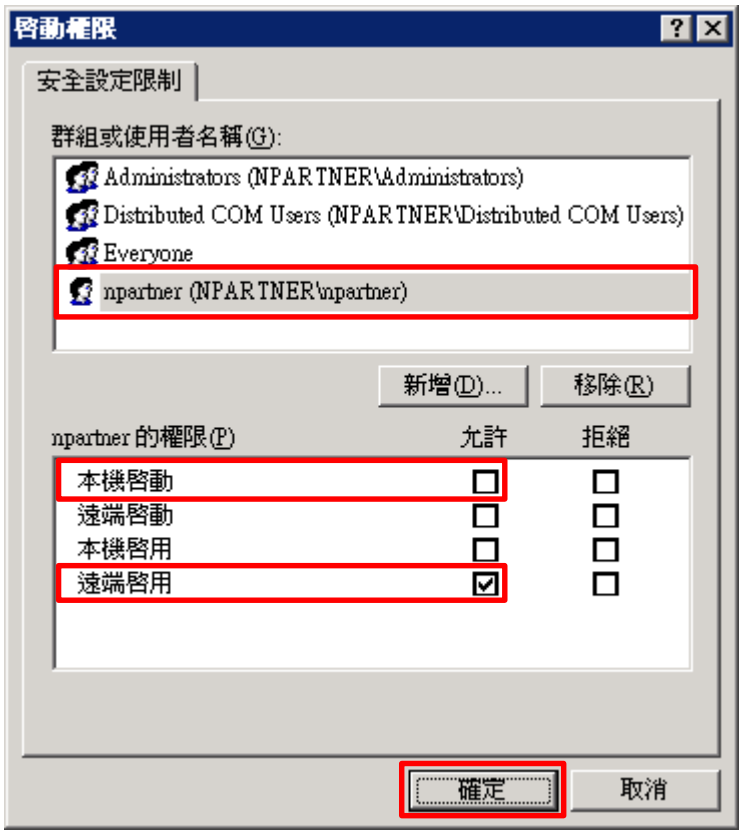
(6) 輸入使用者

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

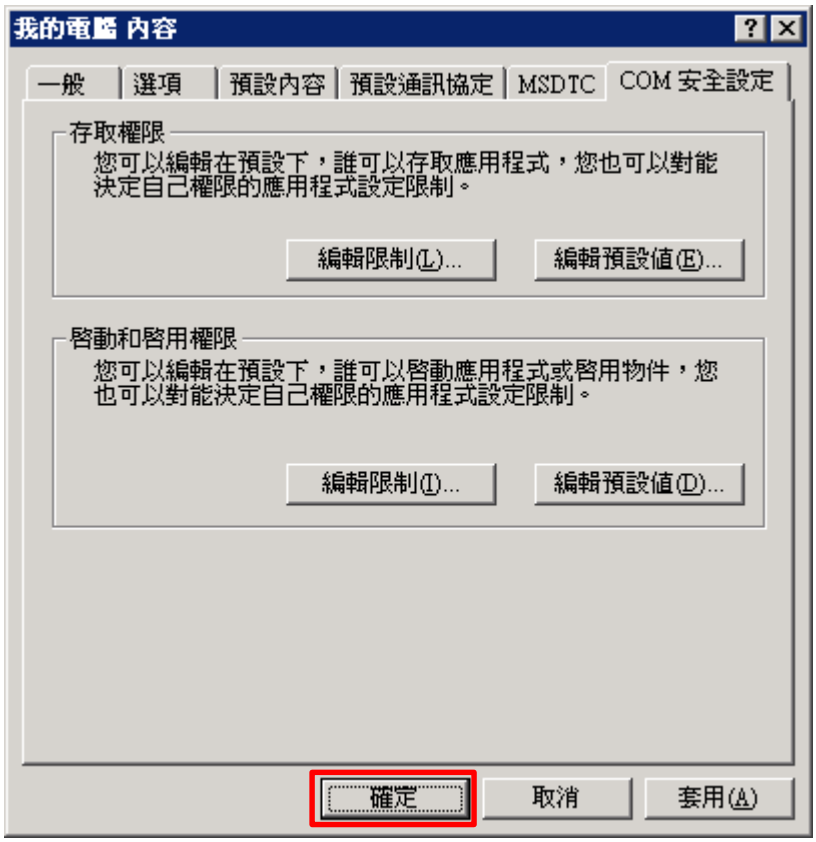


(7) 設定使用者權限

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

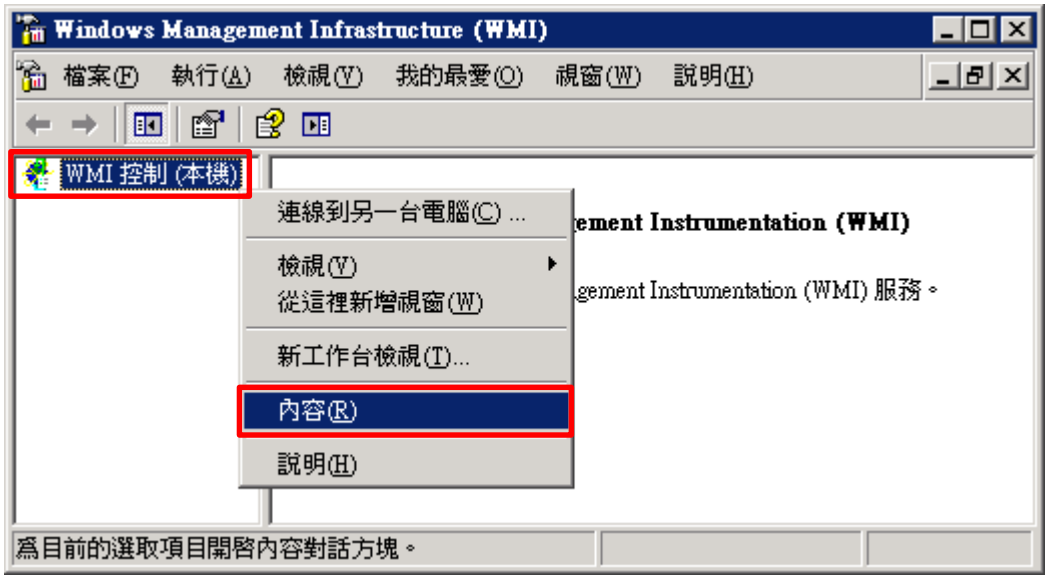
(1) 開啟 [命令提示字元]

(2) 開啟 WMI 控制

```
C:\> wmimgmt.msc
```

(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]

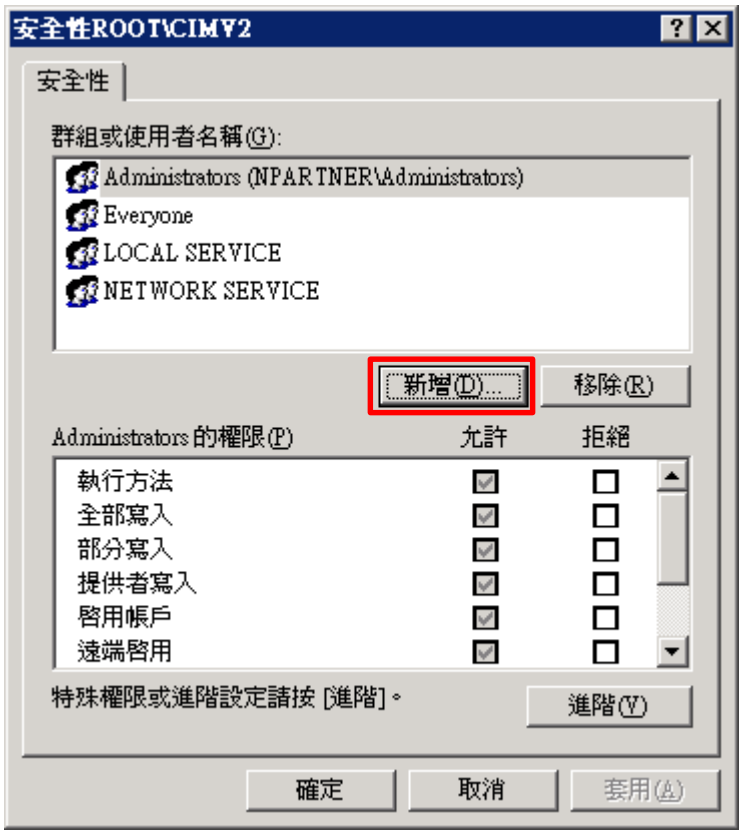


(4) 編輯 CIMV2 安全性

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

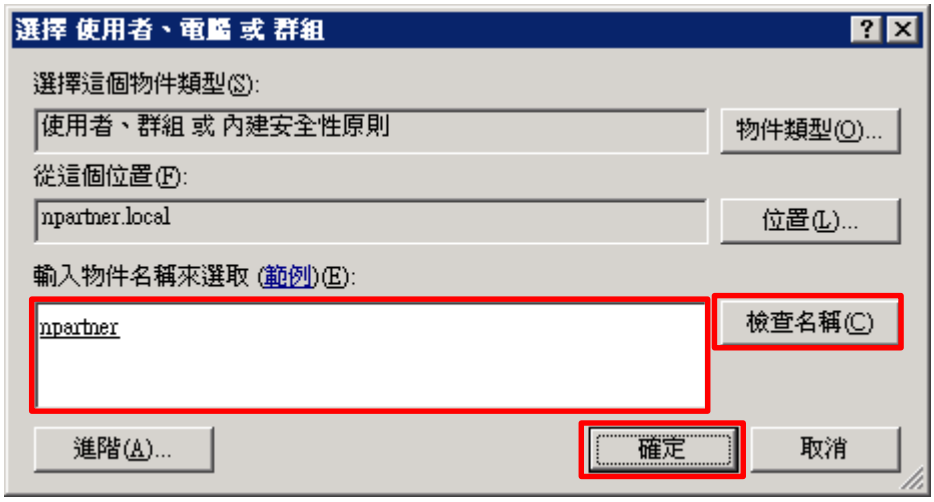
(5) 新增 WMI 使用者權限

按 [新增]



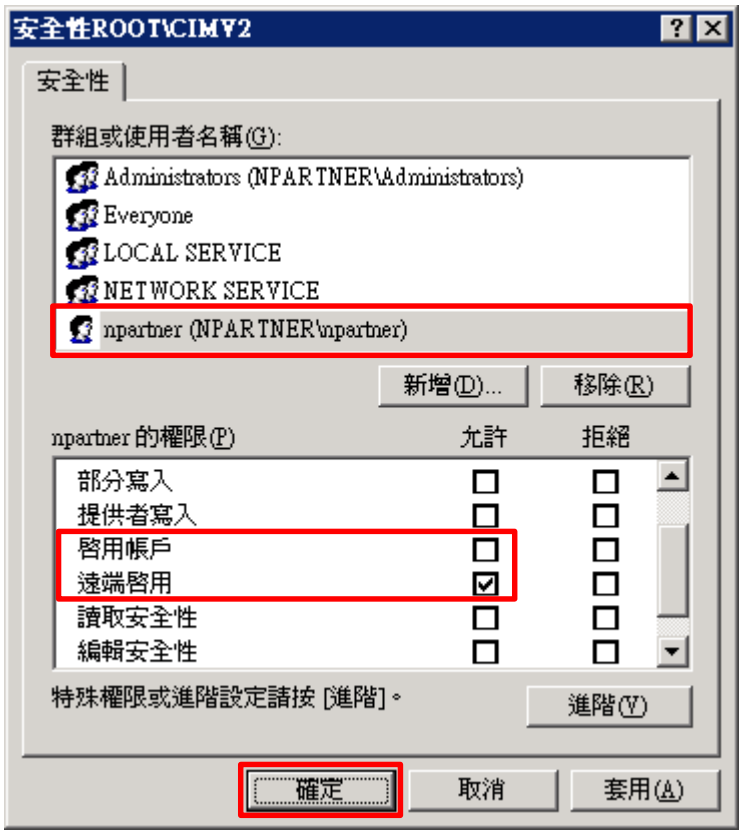
(6) 輸入使用者

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

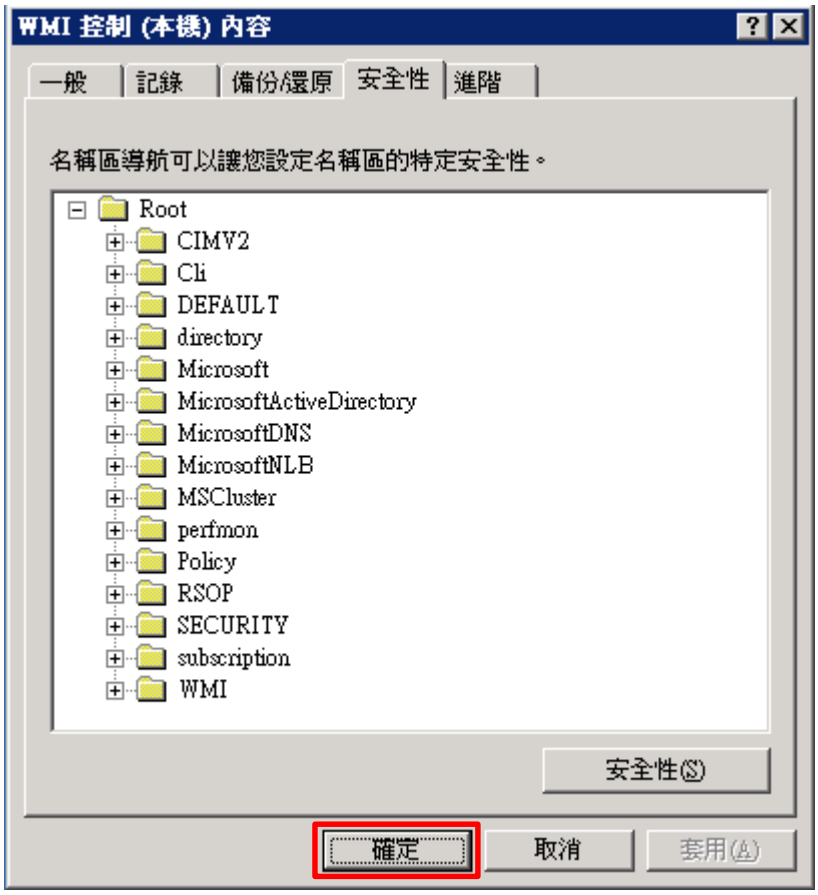


(7) 設定使用者權限

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

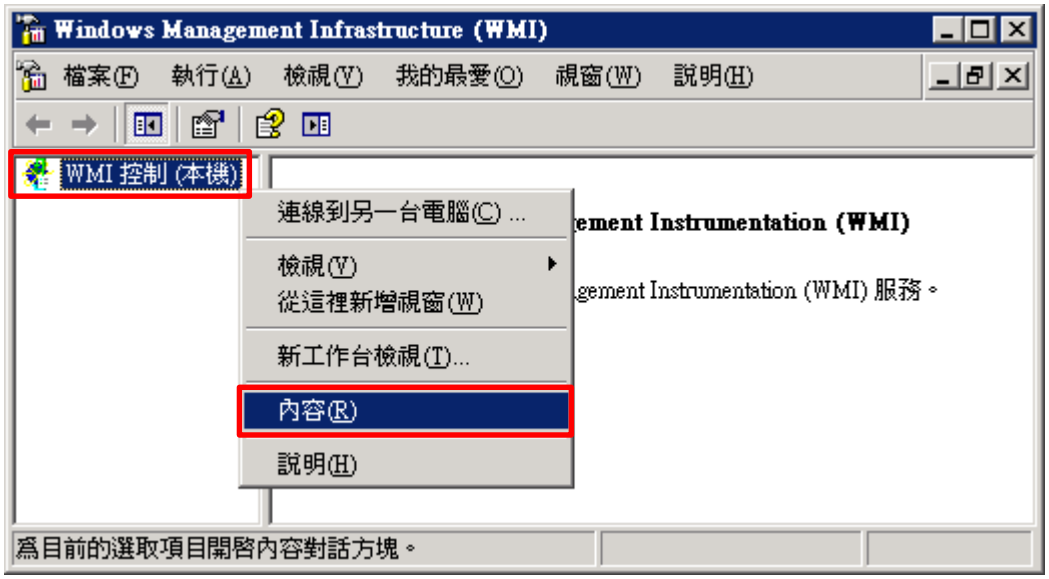
(1) 開啟 [命令提示字元]

(2) 開啟 WMI 控制

```
C:\> wmimgmt.msc
```

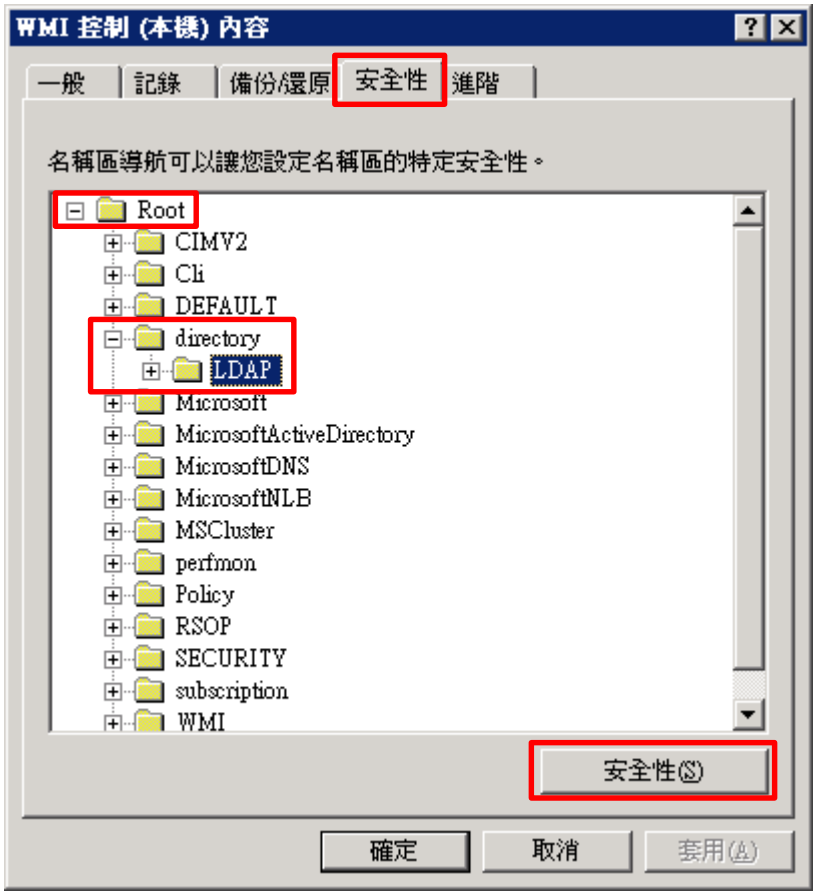
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



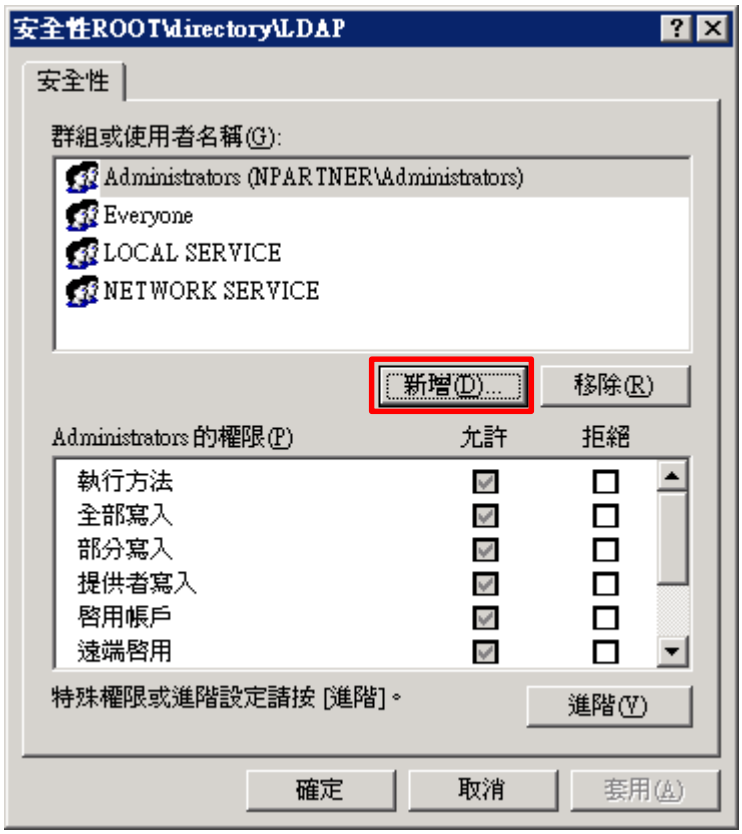
(4) 編輯 LDAP 安全性

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



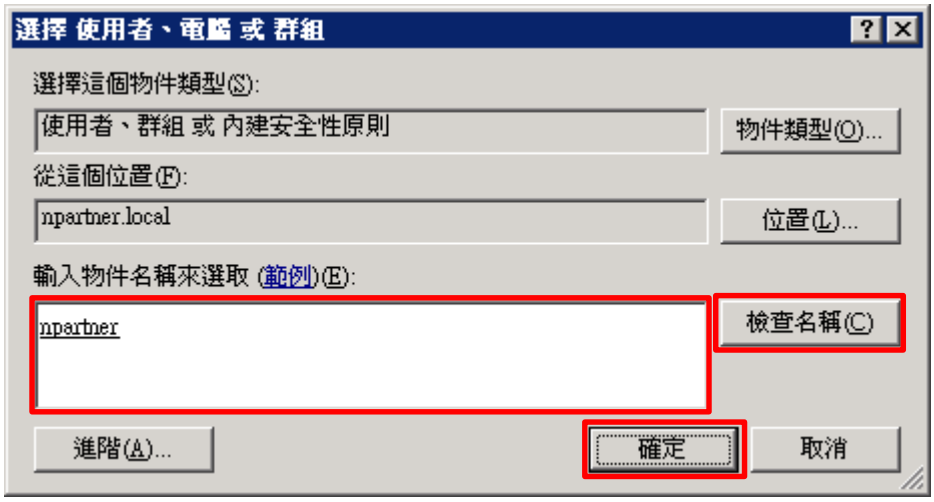
(5) 新增 WMI 使用者權限

按 [新增]



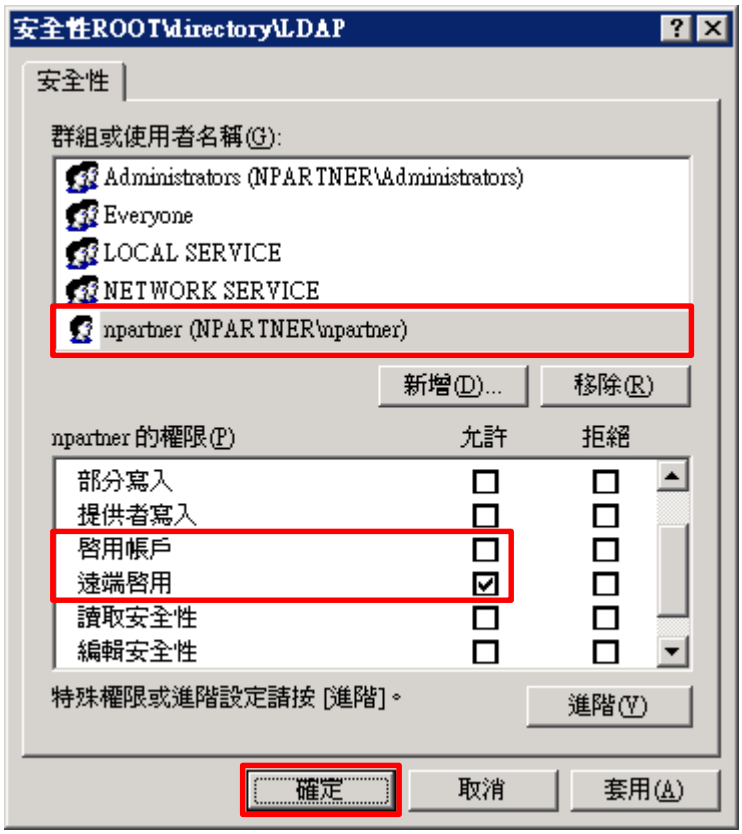
(6) 輸入使用者

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

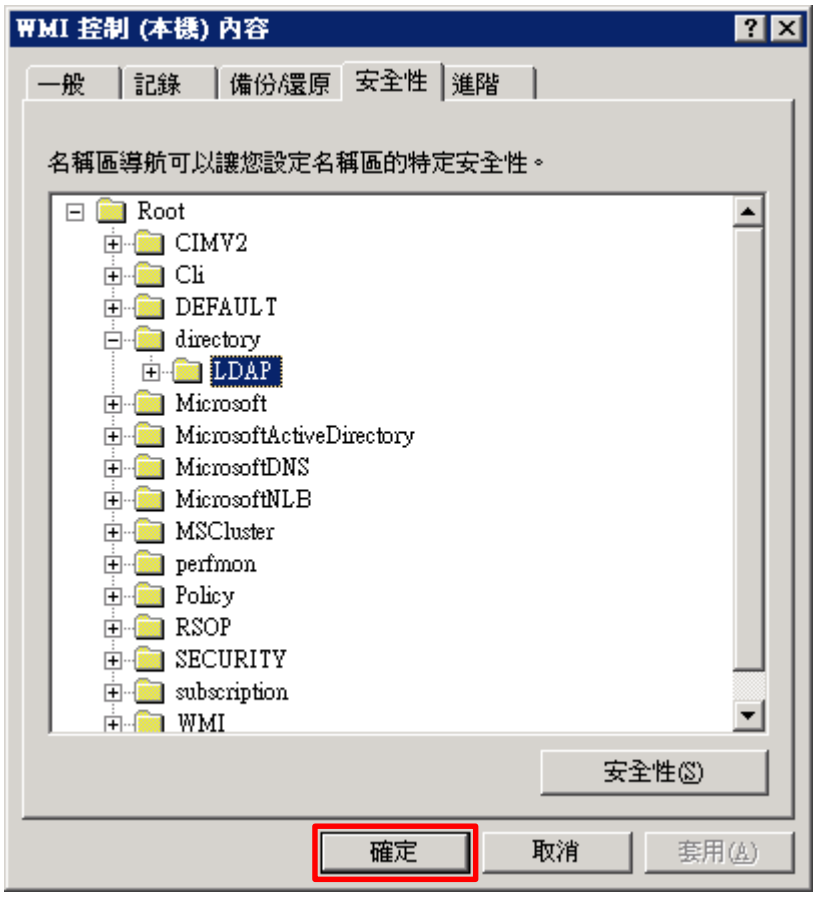


(7) 設定使用者權限

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]



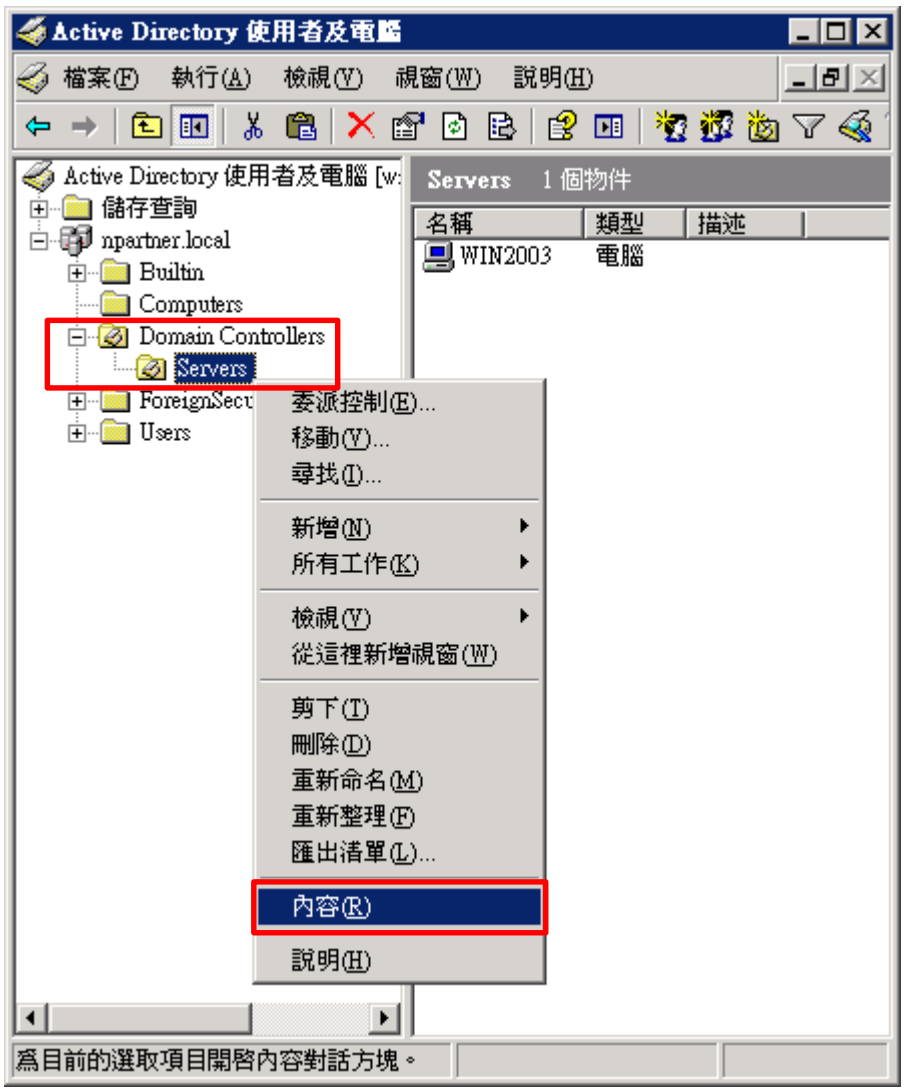
2.3.4 設定 Event log 讀取權限

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

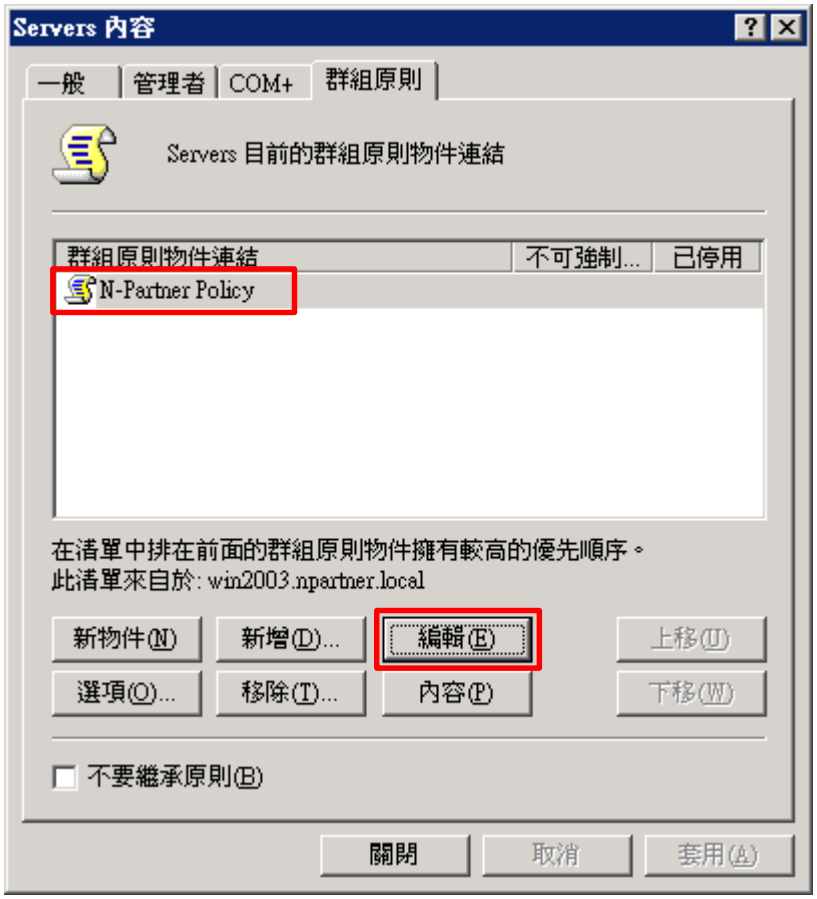
(2) Domain Controllers 的 Servers 組織單位，點選內容

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



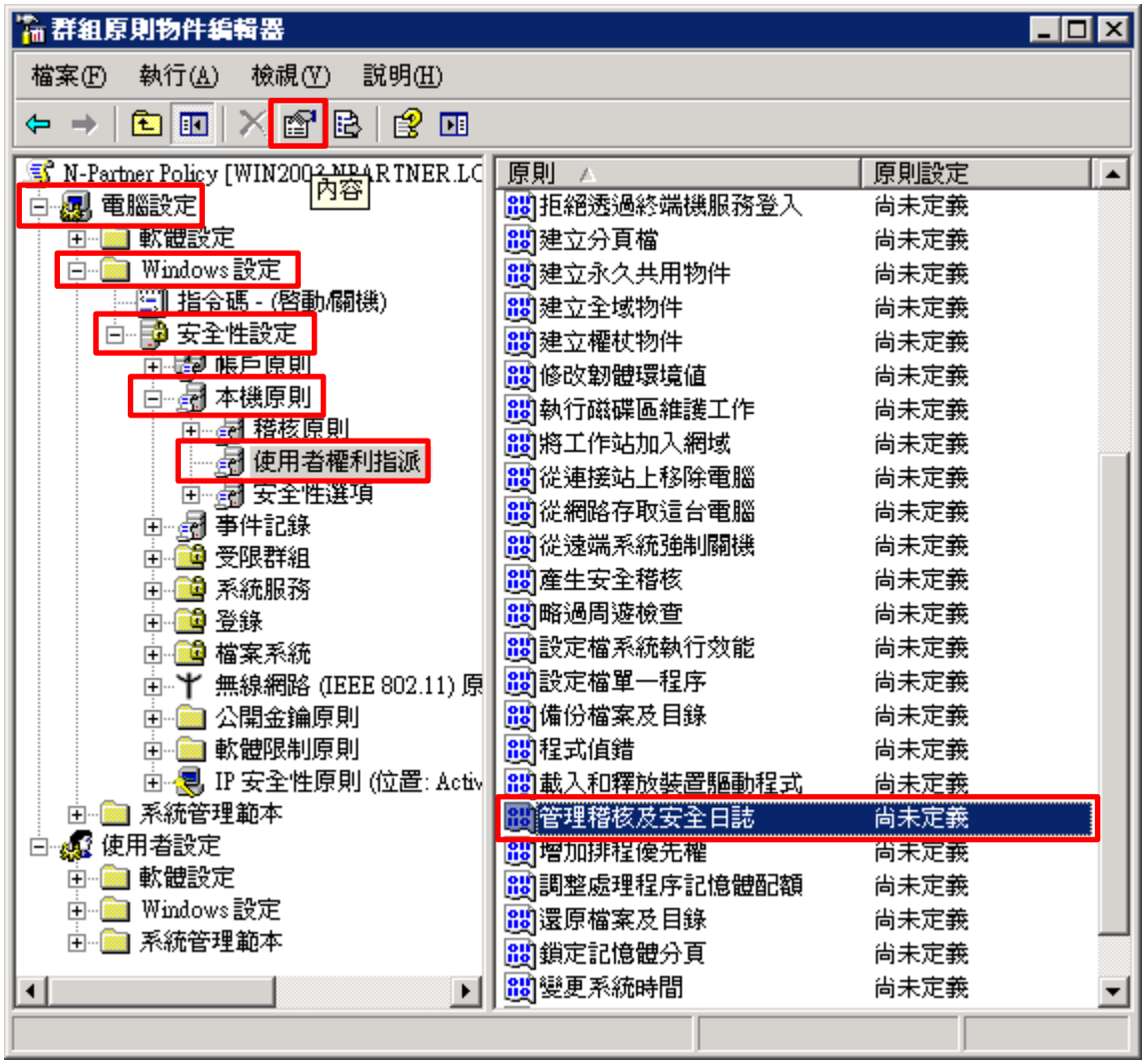
(3) 編輯群組原則物件

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



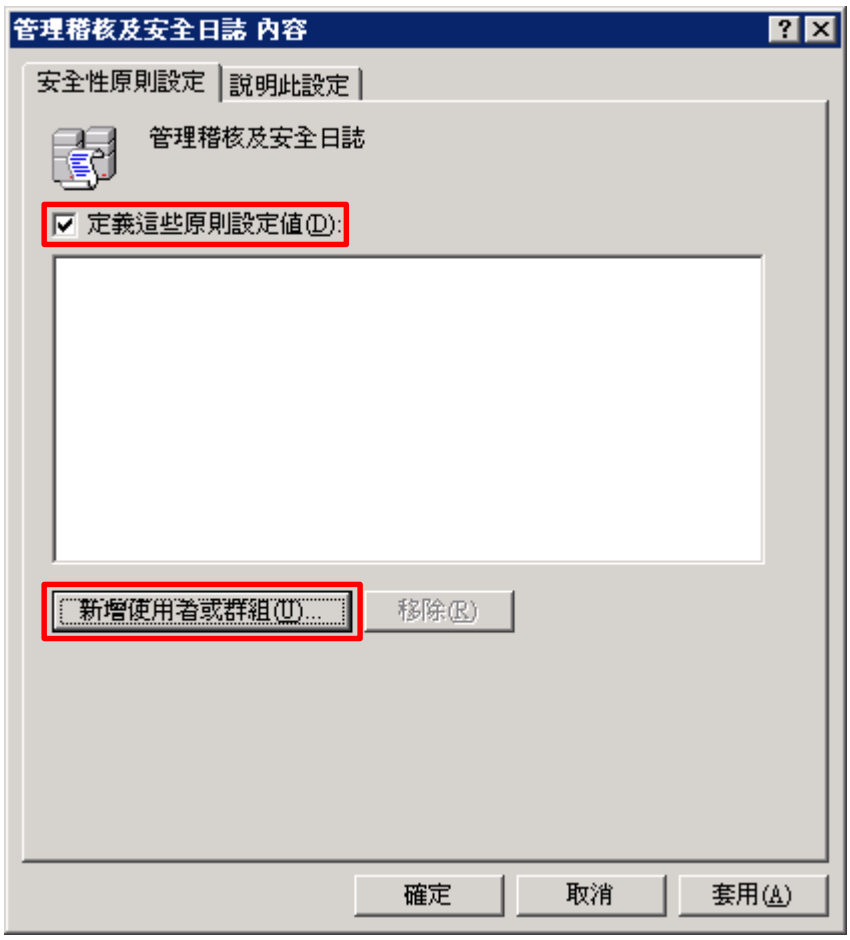
(4) 設定記錄檔

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



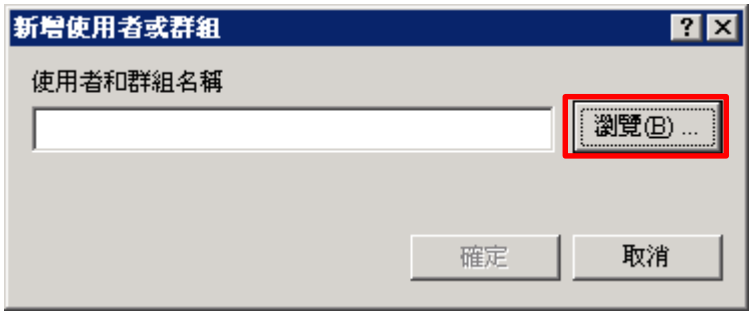
(5) 新增管理稽核使用者

勾選 [定義這些原則設定] -> 按 [新增使用者或群組...]



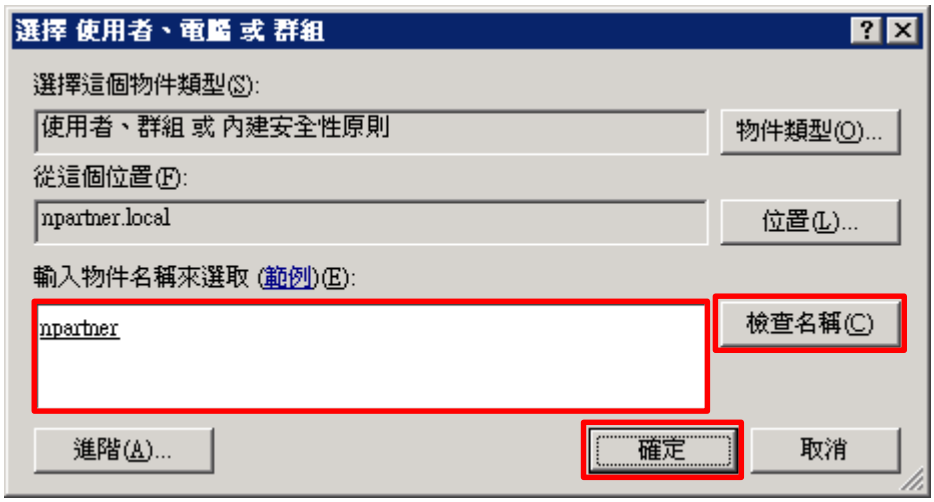
(6) 搜尋使用者

按 [瀏覽]



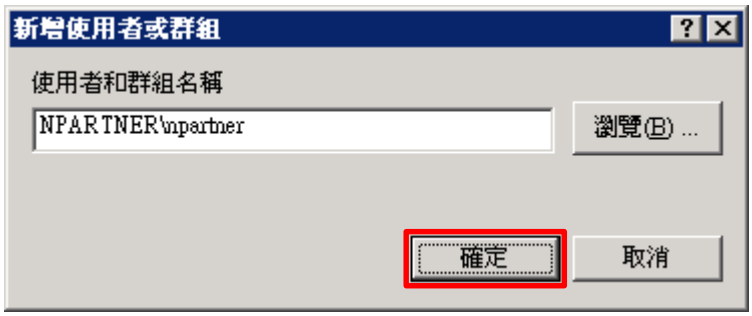
(7) 輸入使用者

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



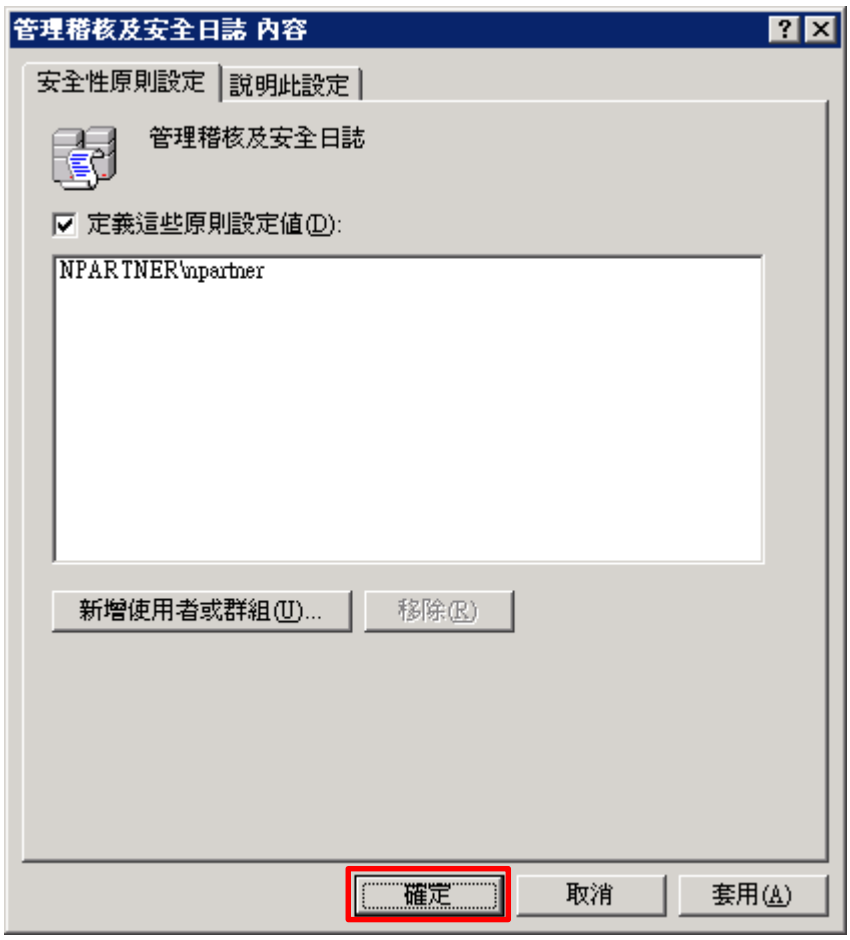
(8) 確定使用者

按 [確定]



(9) 確定設定記錄檔

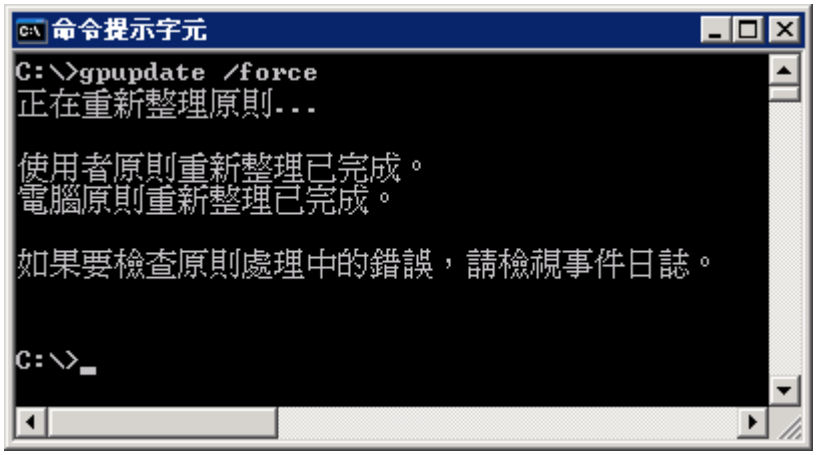
按 [確定]



(10) 開啟 [命令提示字元]

(11) 更新群組原則

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



2.3.5 重啟 WMI 服務

(1) 開啟 [Windows PowerShell]

(2) 停用 WMI 服務

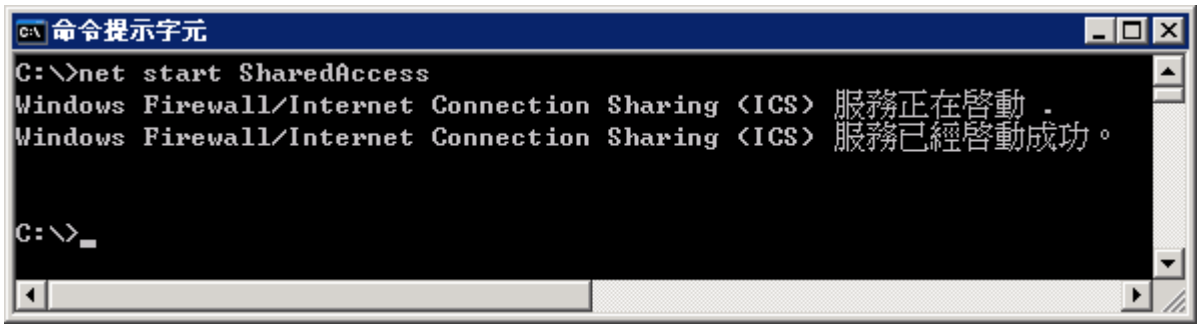
```
C:\> net stop winmgmt
```

(3) 啟用 WMI 服務

```
C:\> net start winmgmt
```

(4) 啟用 Firewall 服務

```
C:\> net start SharedAccess
```

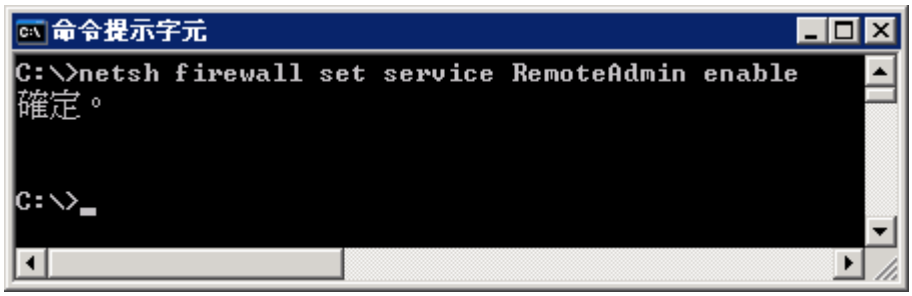


2.4 設定防火牆

(1) 開啟 [命令提示字元]

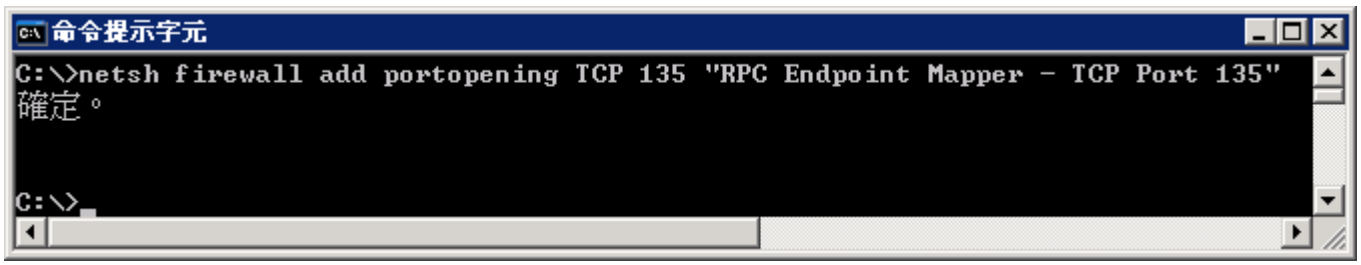
(2) 允許 WMI 通過防火牆

```
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
```

3. Windows 2008

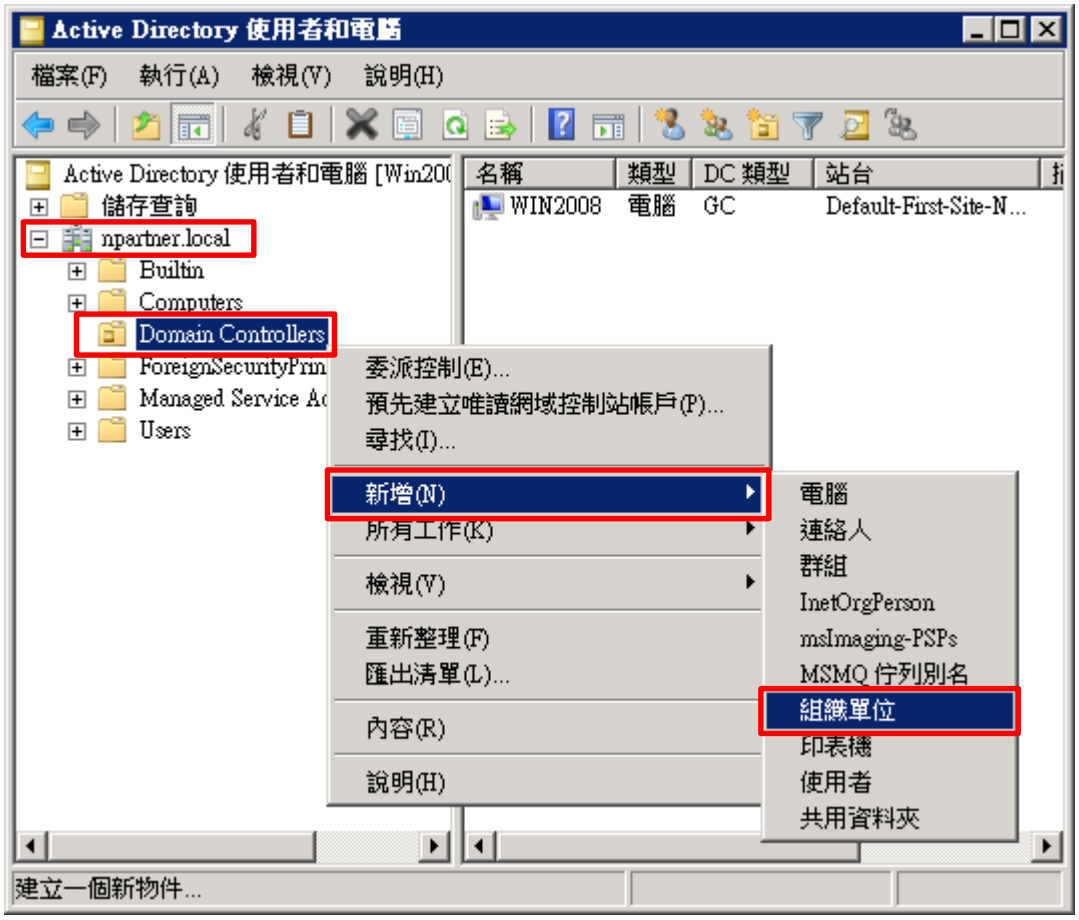
Windows 稽核原則設定 詳細說明請參考**前言**的稽核原則建議連結

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]

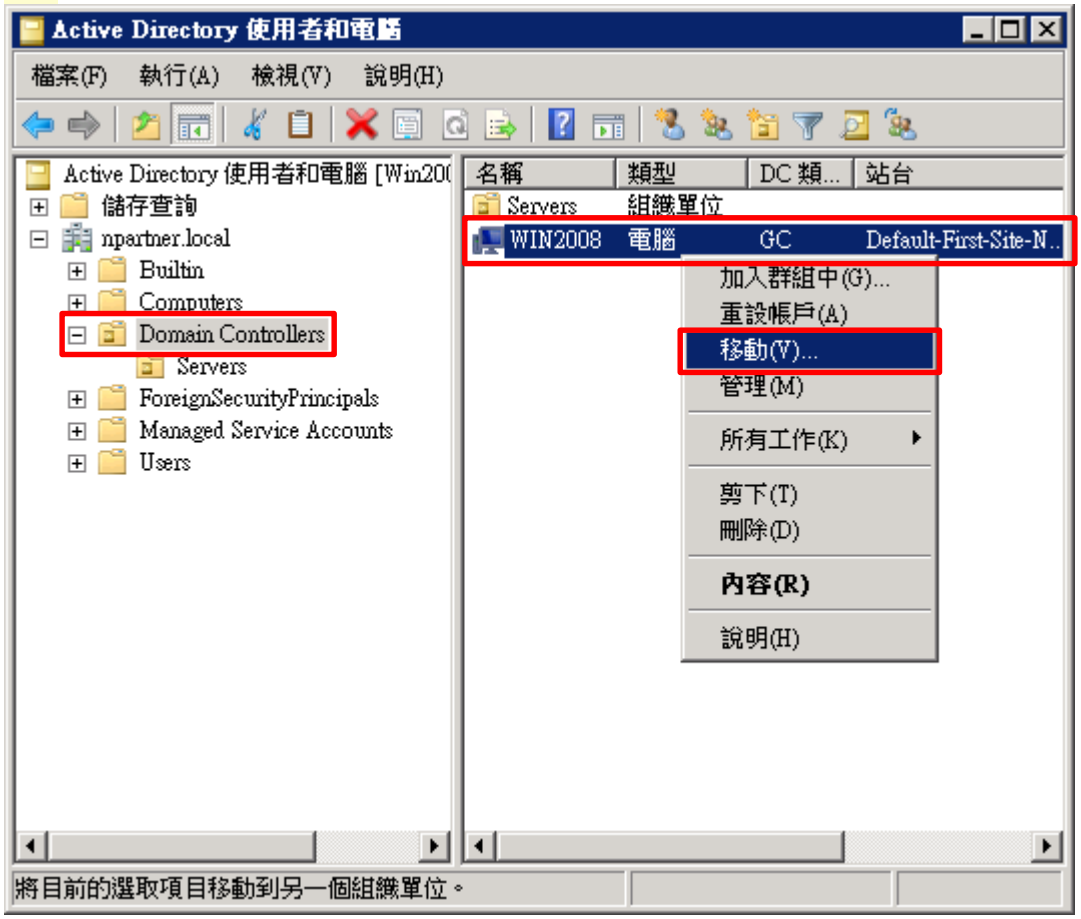


(3) 輸入組織單位名稱

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]

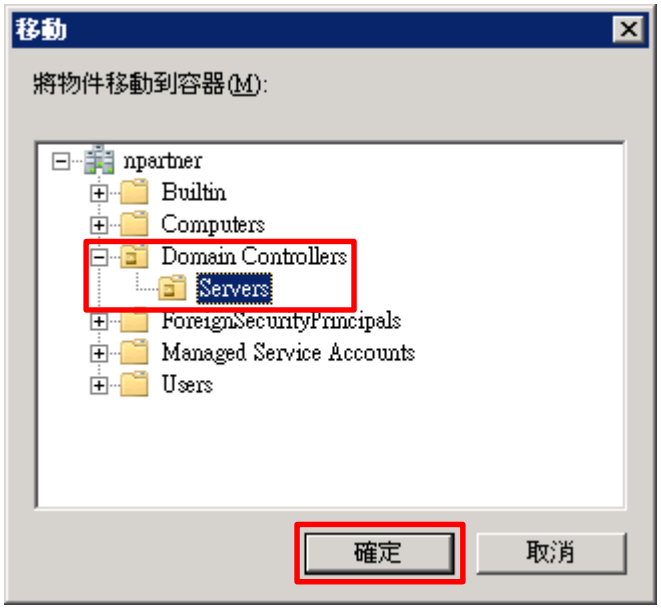
(4) 移動伺服器至新的組織單位

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]



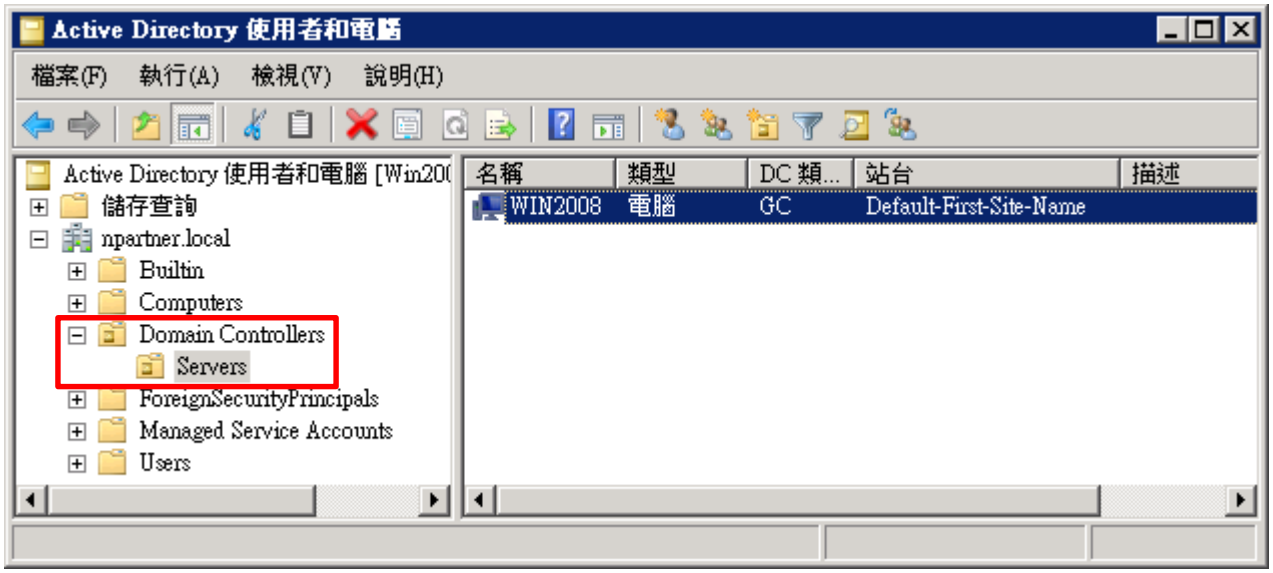
(5) 選擇組織單位

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



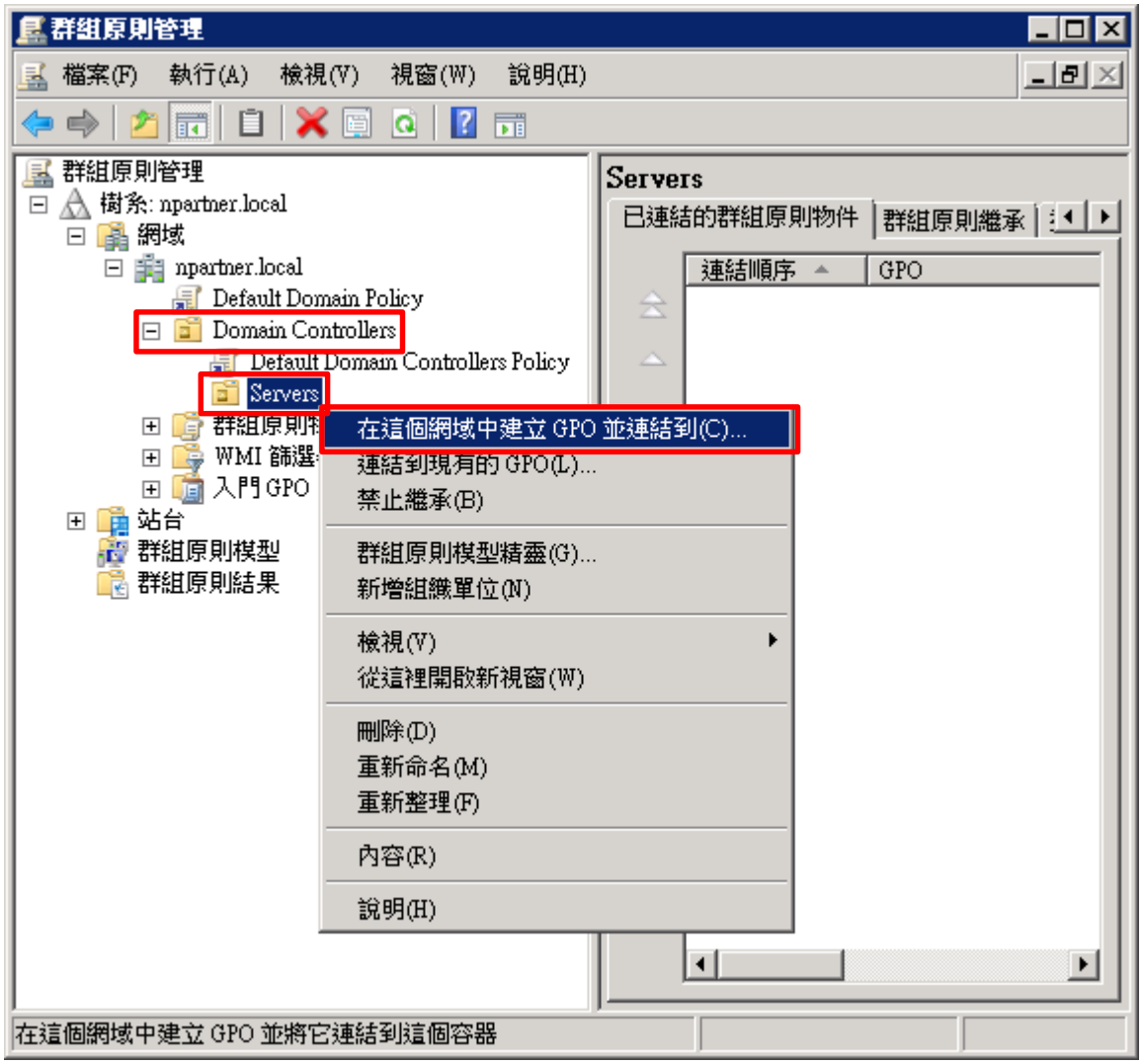
3.2 群組原則設定

(1) 開啟群組原則管理

開啟 [群組原則管理]

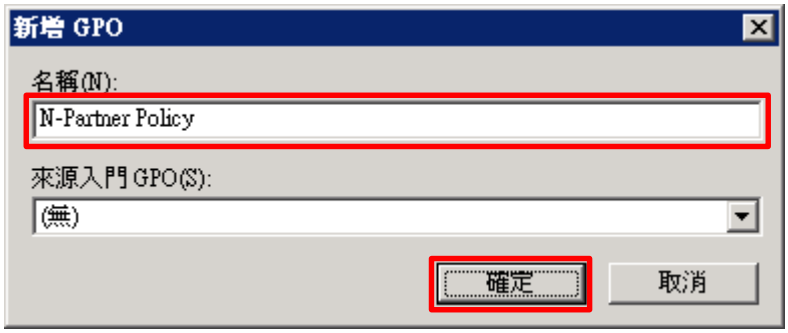
(2) 在 Servers 組織單位，新增群組原則物件

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...]



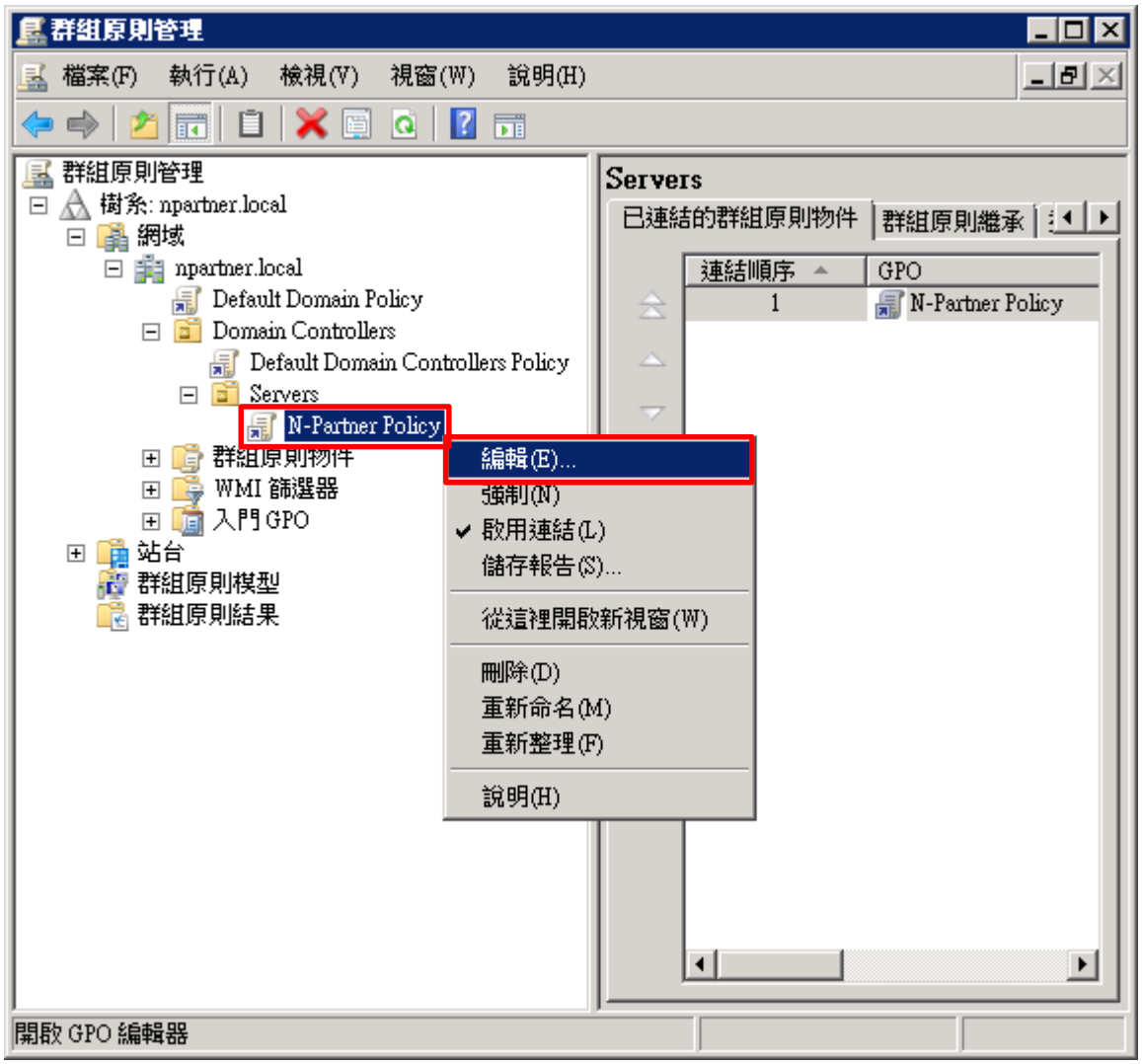
(3) 輸入群組原則物件名稱

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]



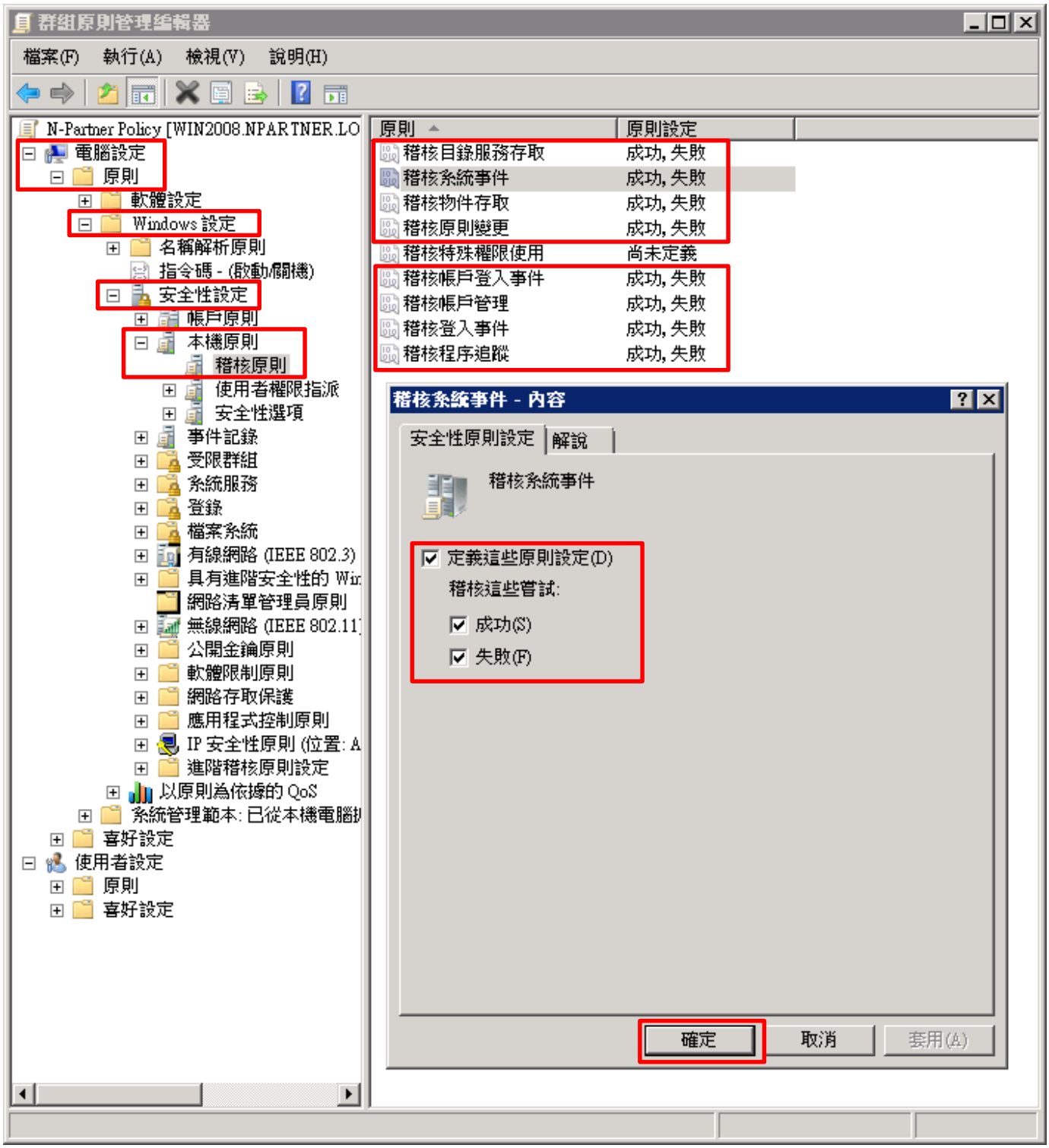
(4) 編輯群組原則物件

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



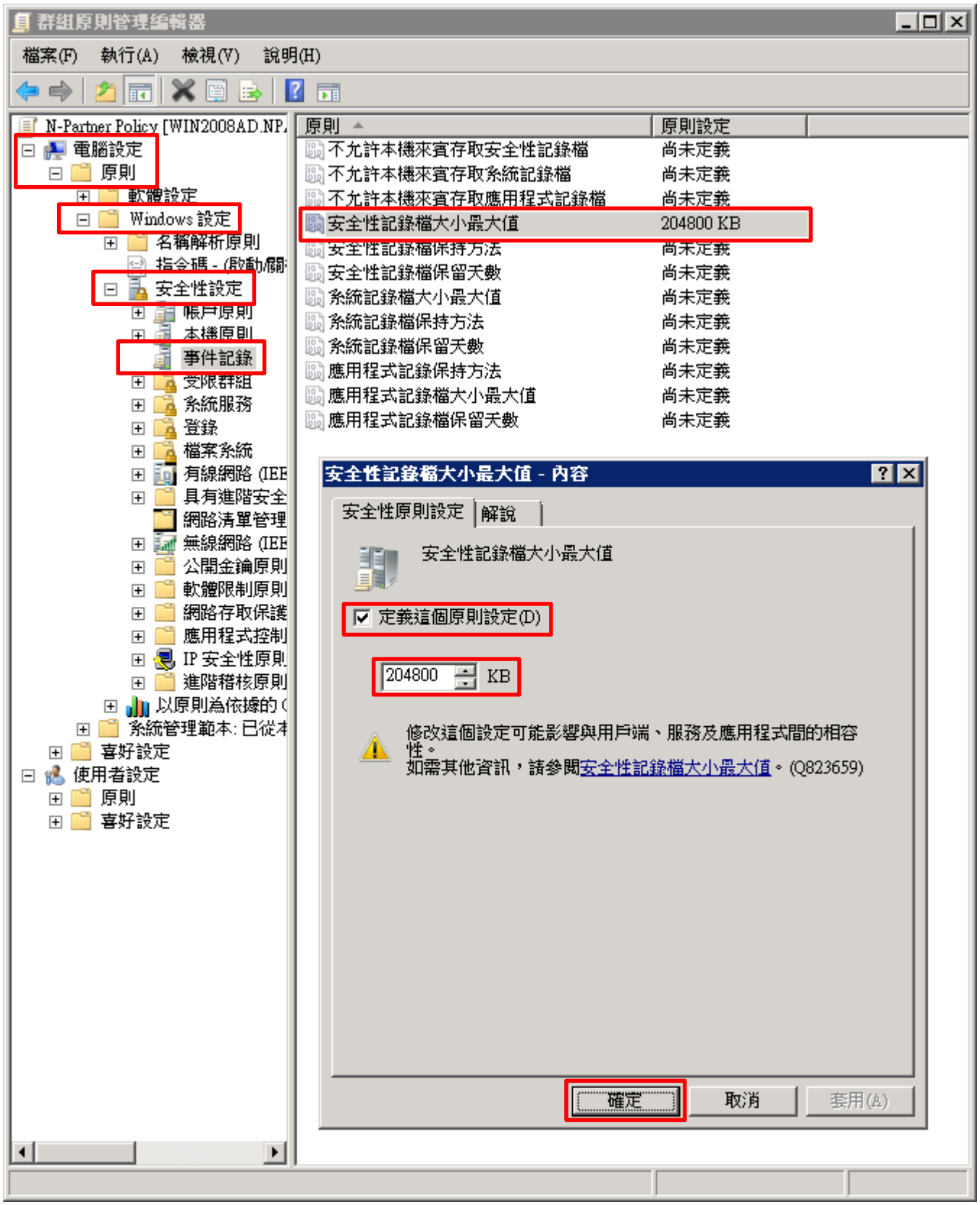
(5) 本機原則：稽核原則

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]



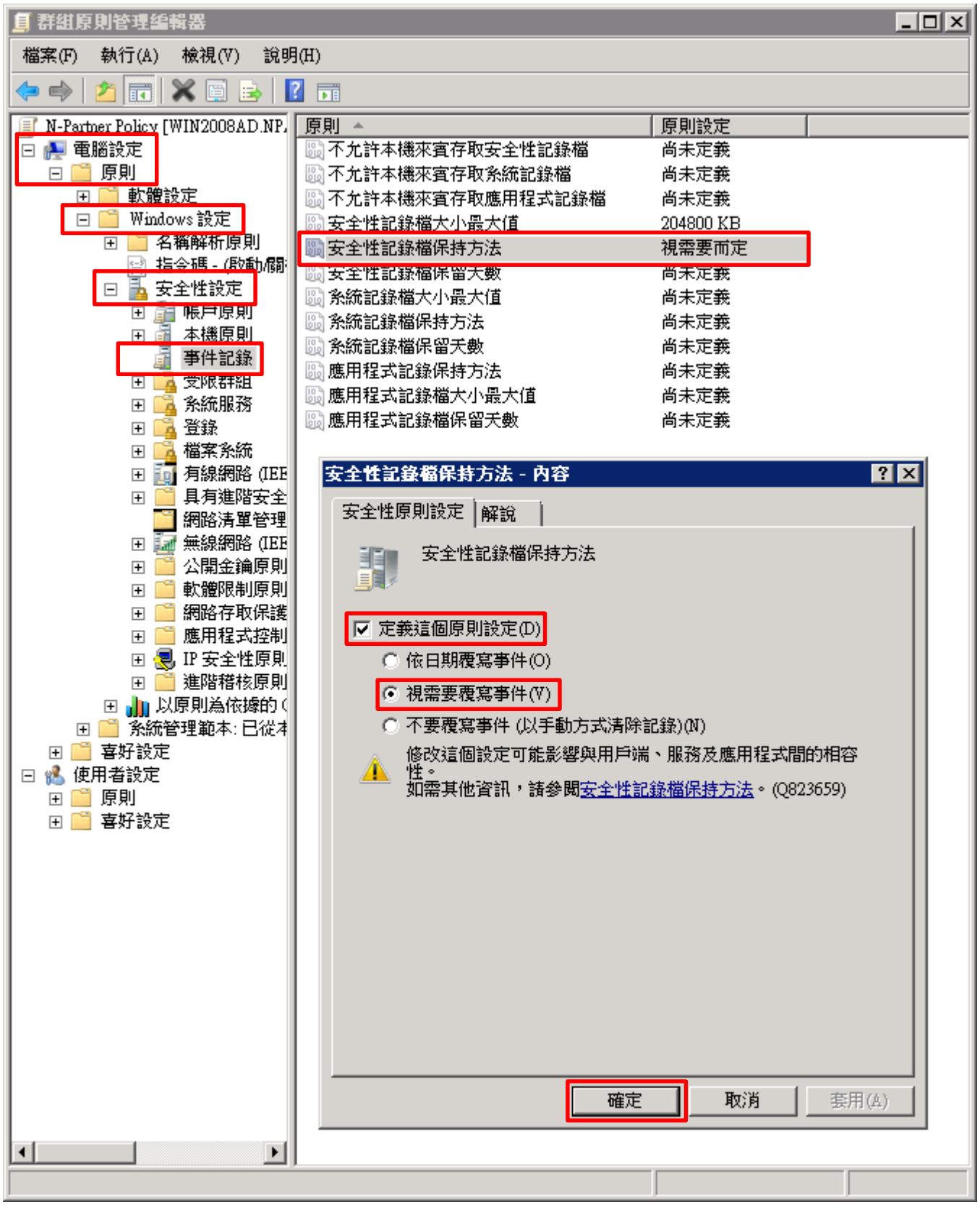
(6) 事件記錄：安全性記錄檔大小最大值

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]



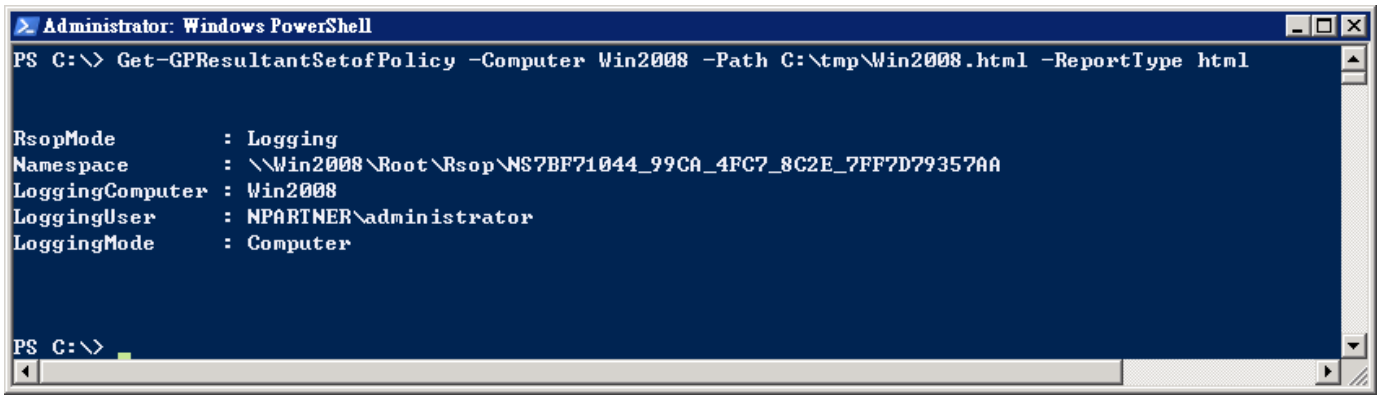
(8) 開啟 Windows PowerShell

(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

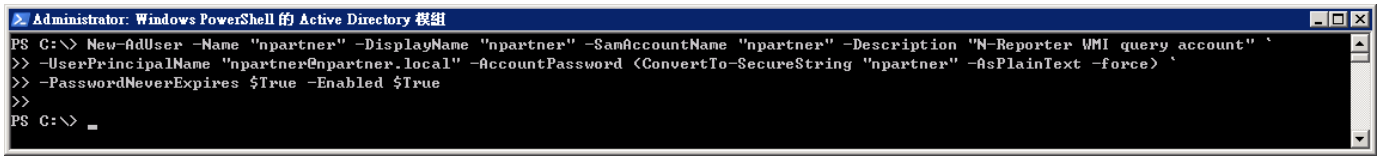
3.3 新增非管理帳號

3.3.1 新增使用者

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

(2) 新增帳號

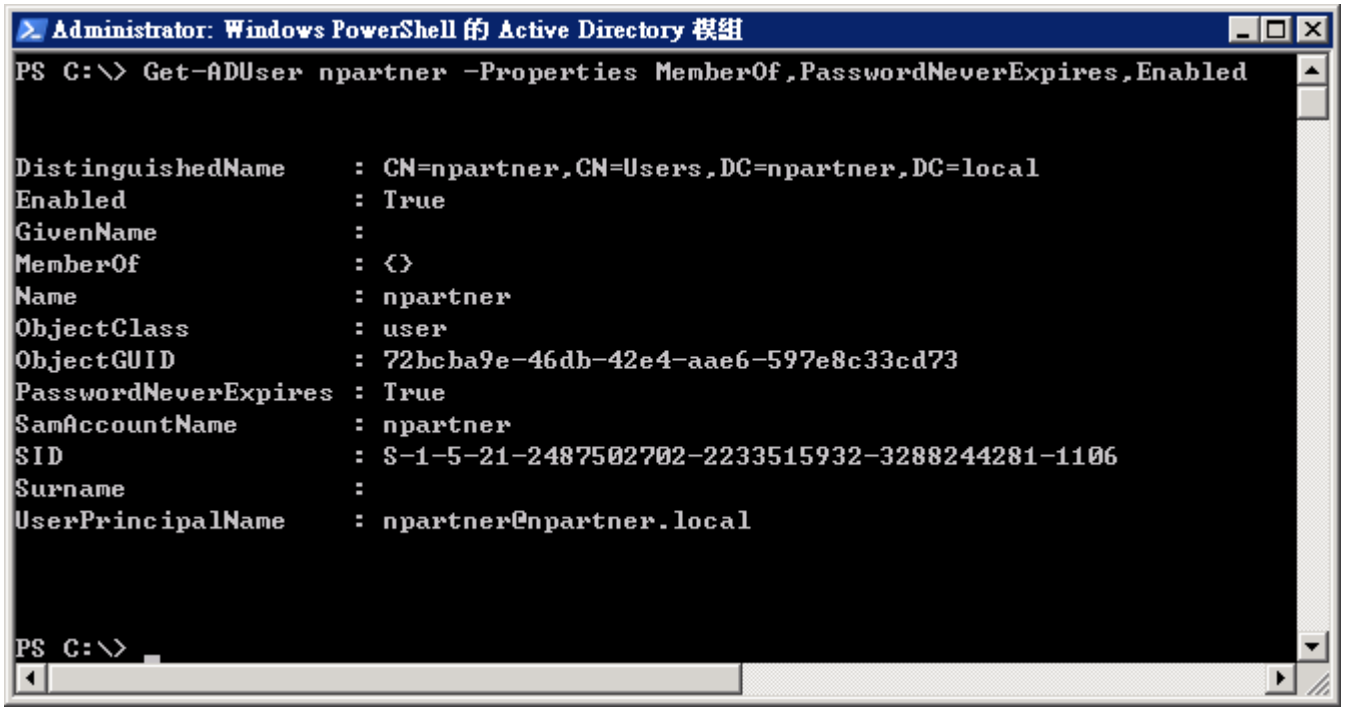
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" `
>> -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True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



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
```

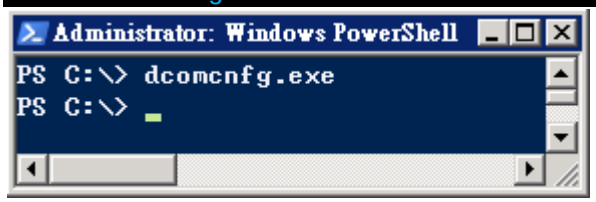


3.3.2 設定 DCOM 權限

(1) 開啟 [Windows PowerShell]

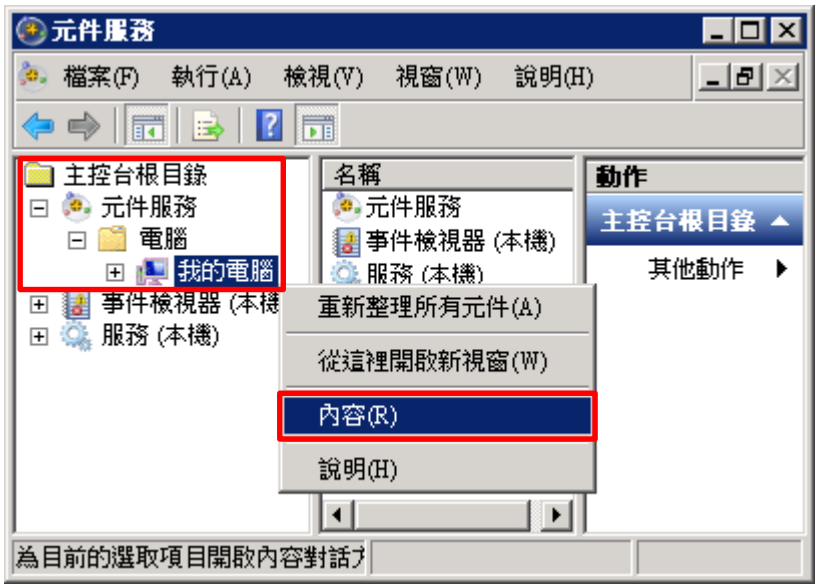
(2) 開啟元件服務

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



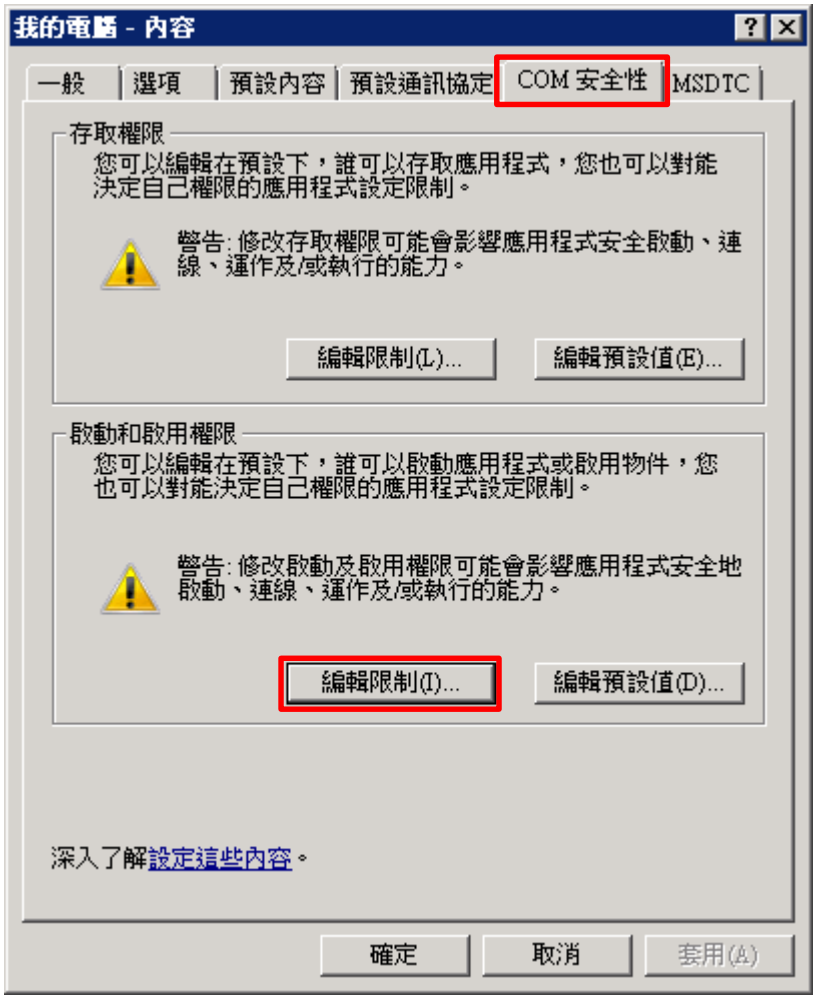
(3) 編輯電腦內容

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]



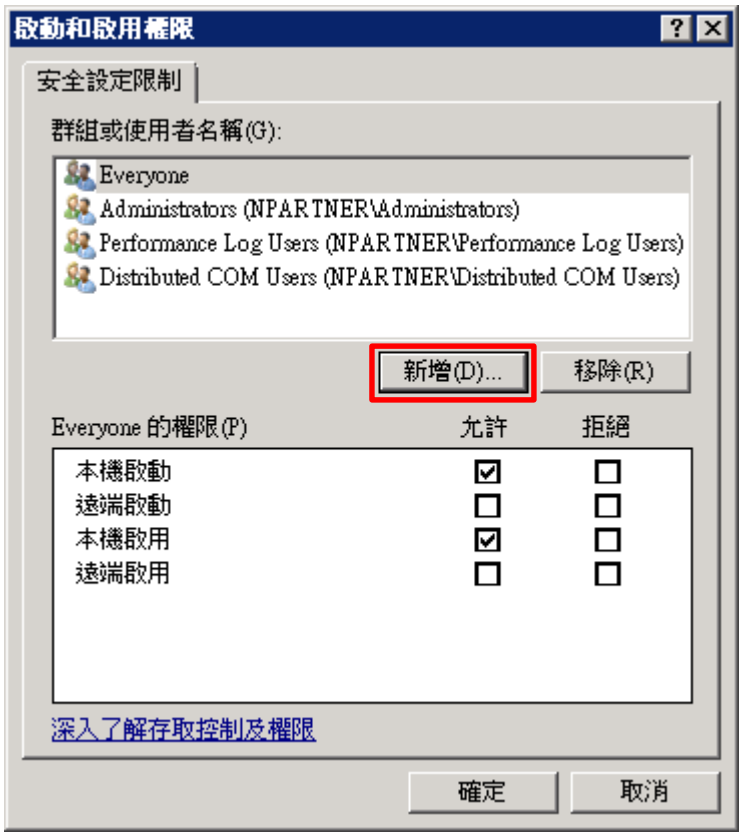
(4) 啟用權限

點選 [COM 安全性] 頁面 -> 啟動和啟用權限，按 [編輯限制]



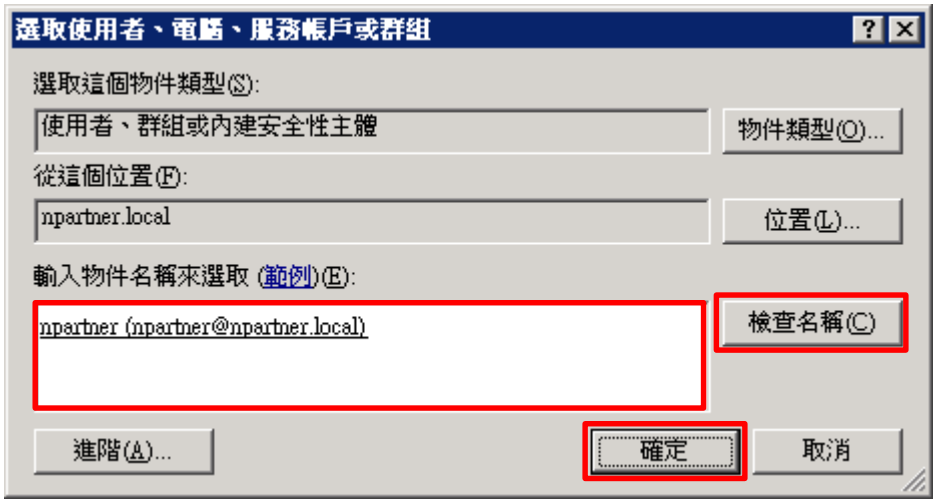
(5) 新增 DCOM 使用者權限

點選 [新增]



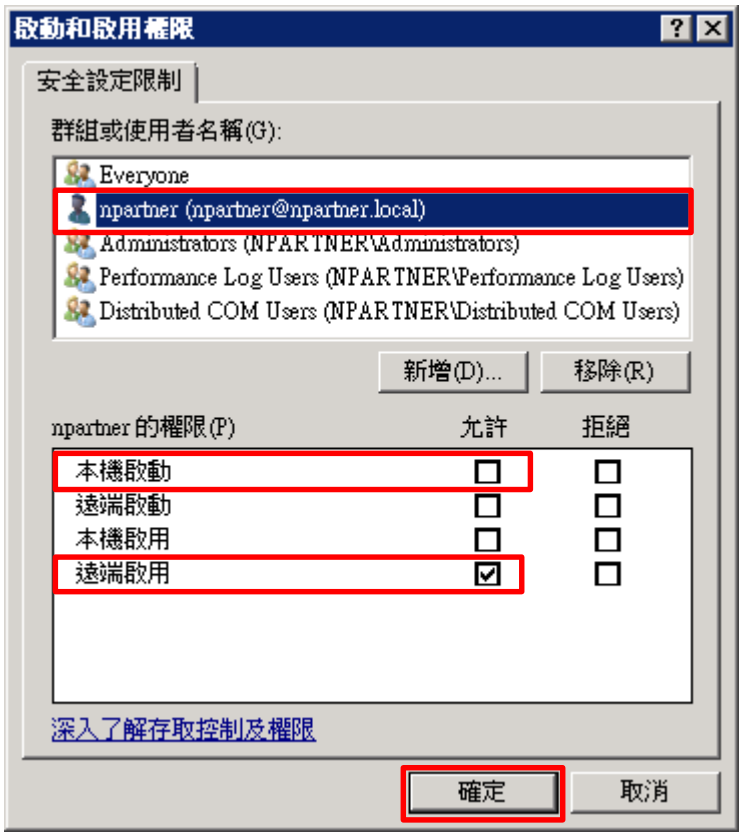
(6) 輸入使用者

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

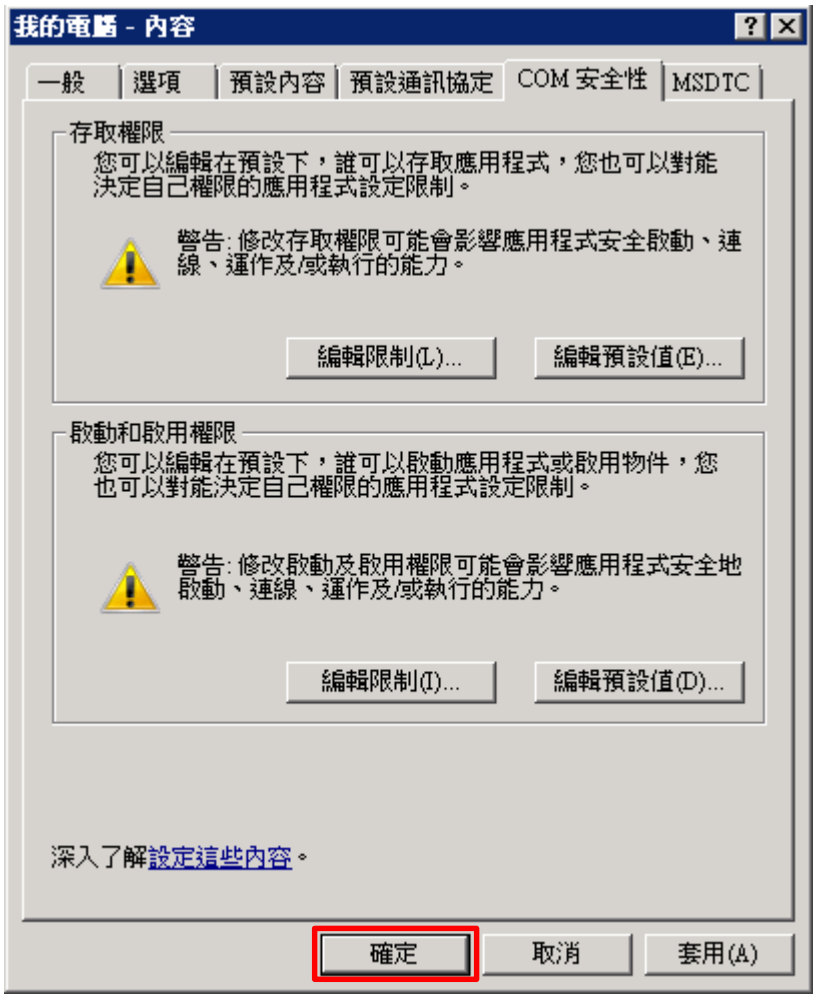


(7) 設定使用者權限

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]



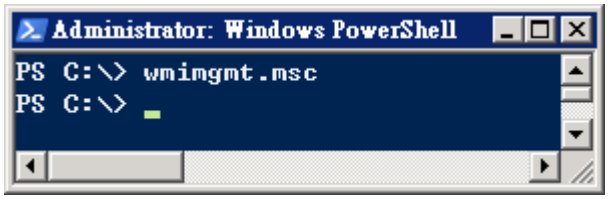
3.3.3 設定 WMI 權限

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:\> wmimgmt.msc
```

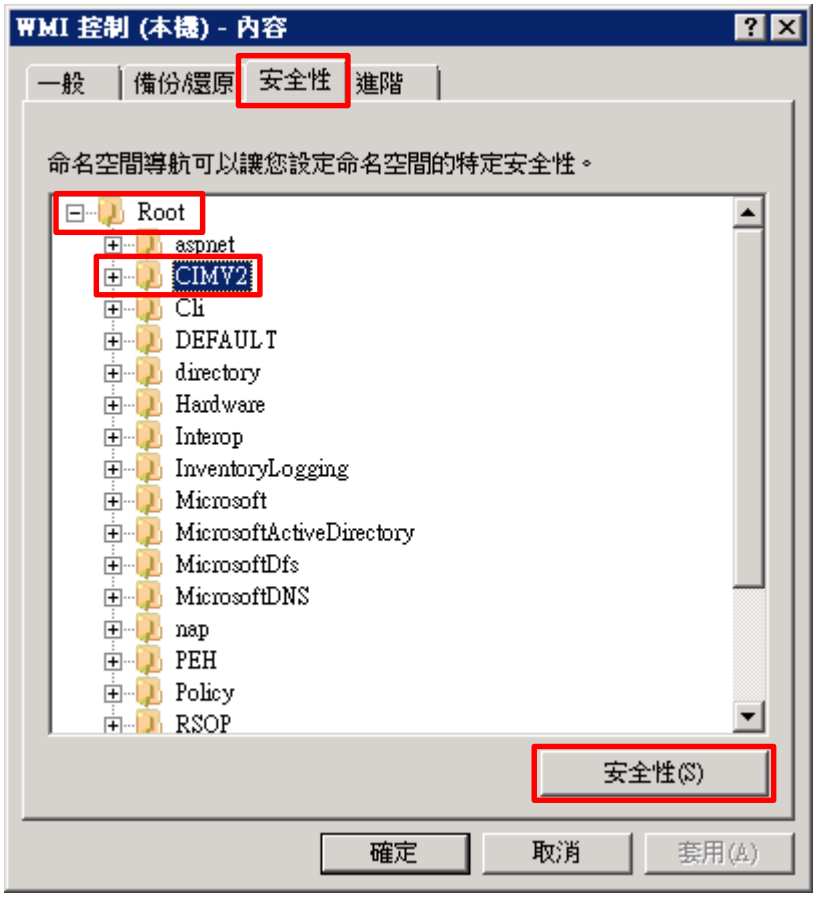


(3) 編輯 WMI 控制

點選 [WMI 控制 (本機)] -> 按  [內容]

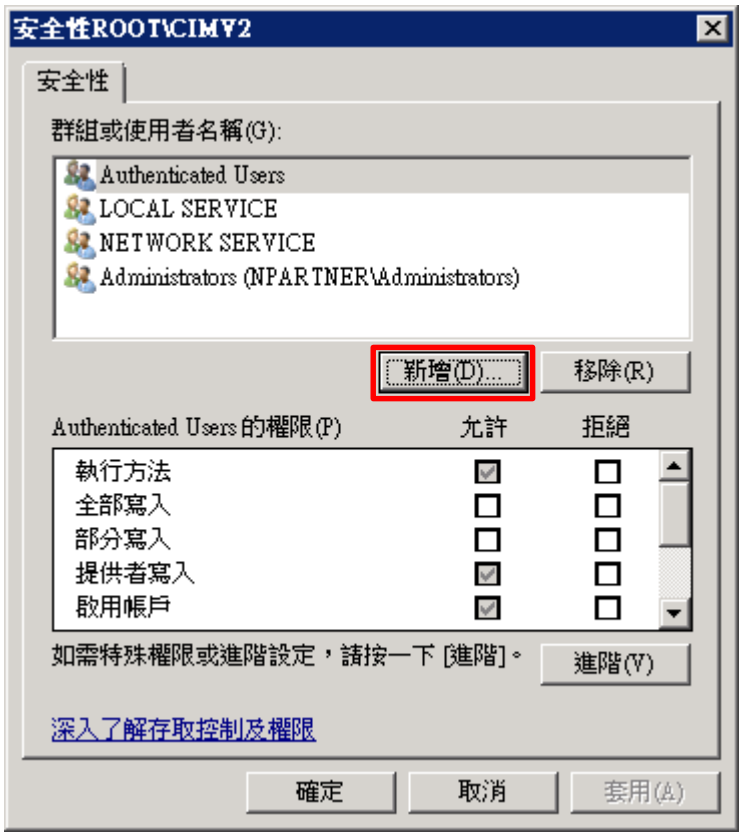
(4) 編輯 CIMV2 安全性

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



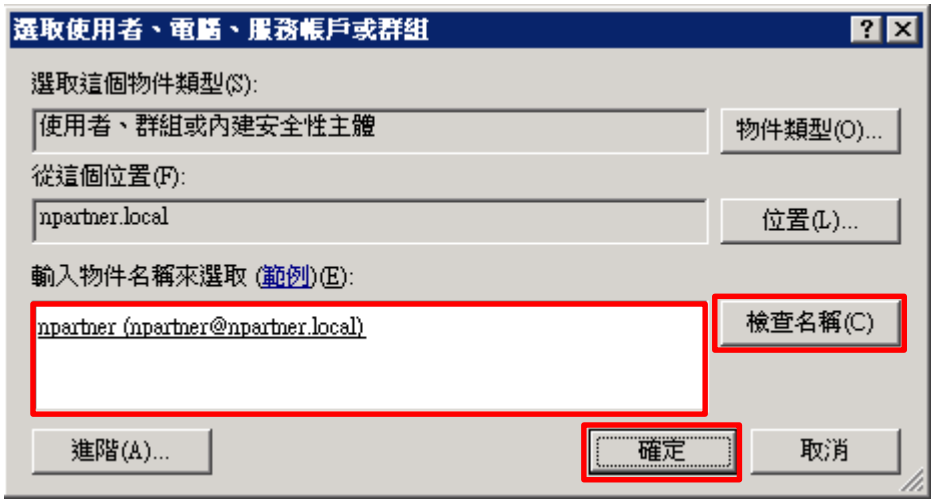
(5) 新增 WMI 使用者權限

按 [新增]



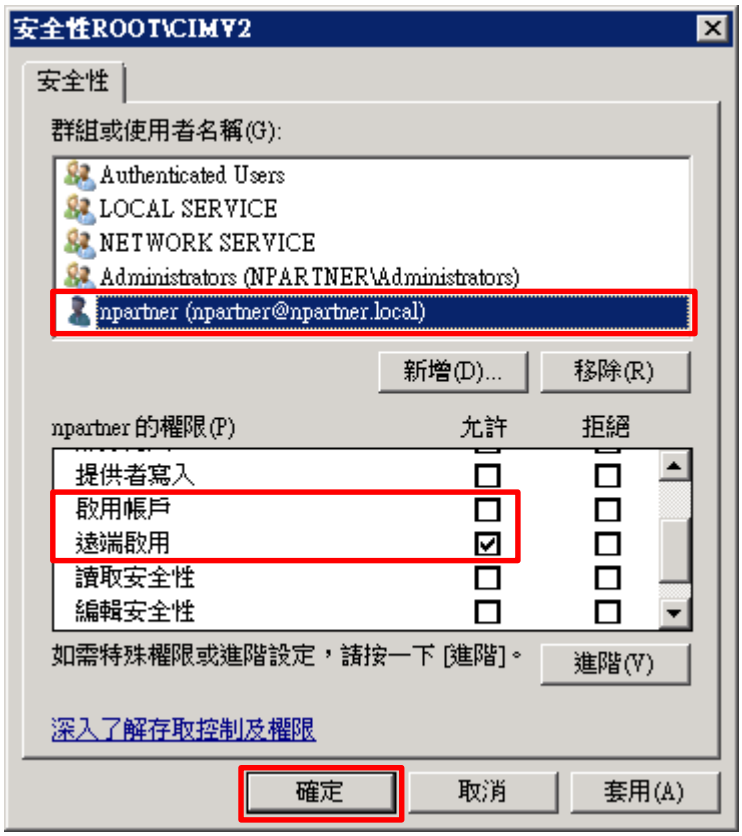
(6) 輸入使用者

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

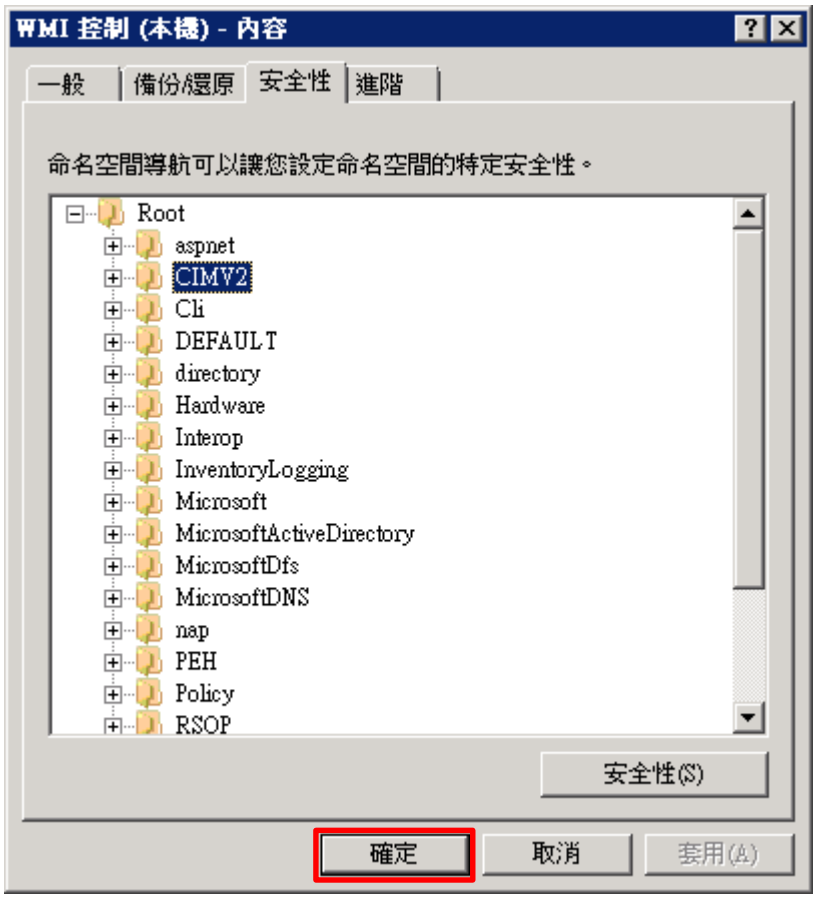


(7) 設定使用者權限

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]

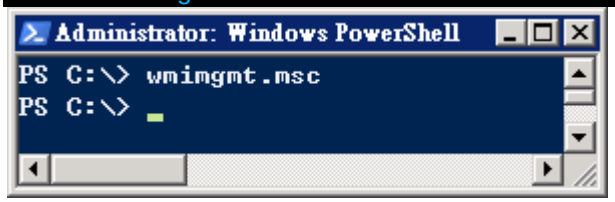


3.3.3.2 設定讀取使用者資料權限

(1) 開啟 [Windows PowerShell]

(2) 開啟元件服務

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

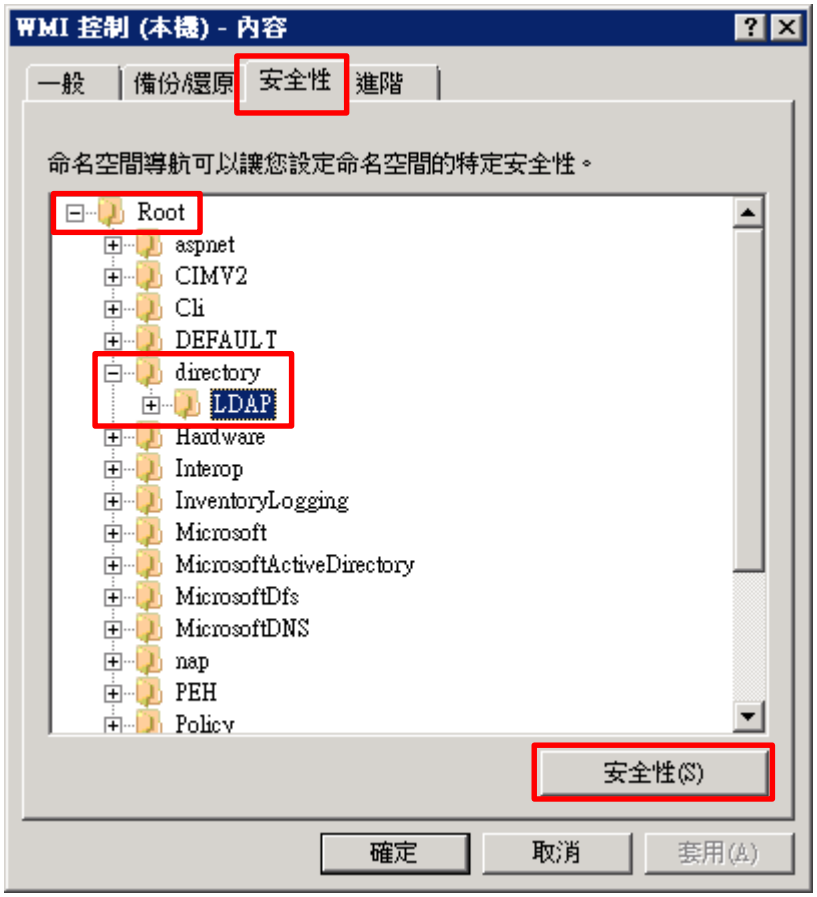


(3) 編輯 WMI 控制

點選 [WMI 控制 (本機)] -> 按  [內容]

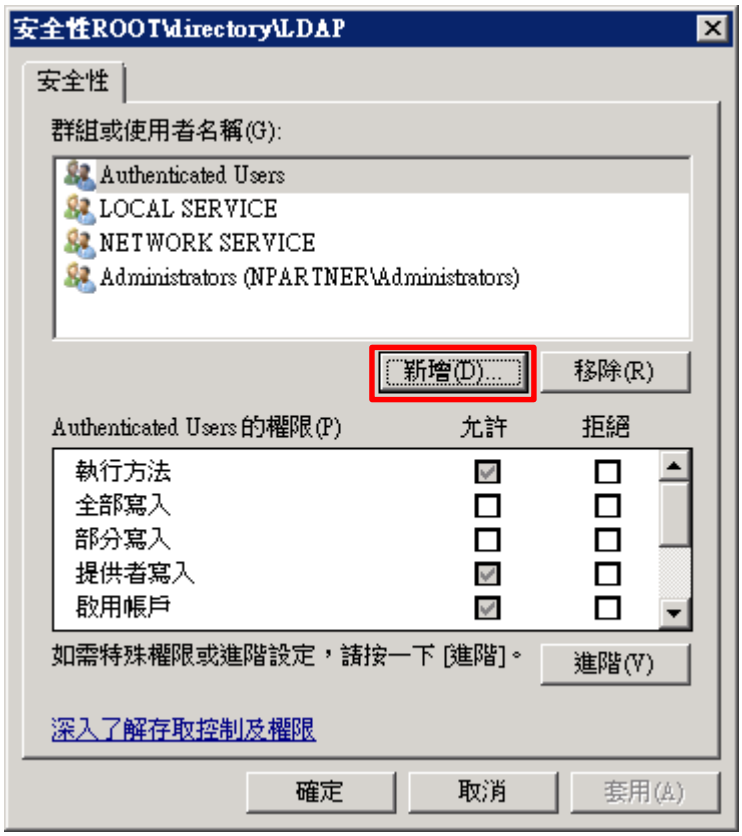
(4) 編輯 LDAP 安全性

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



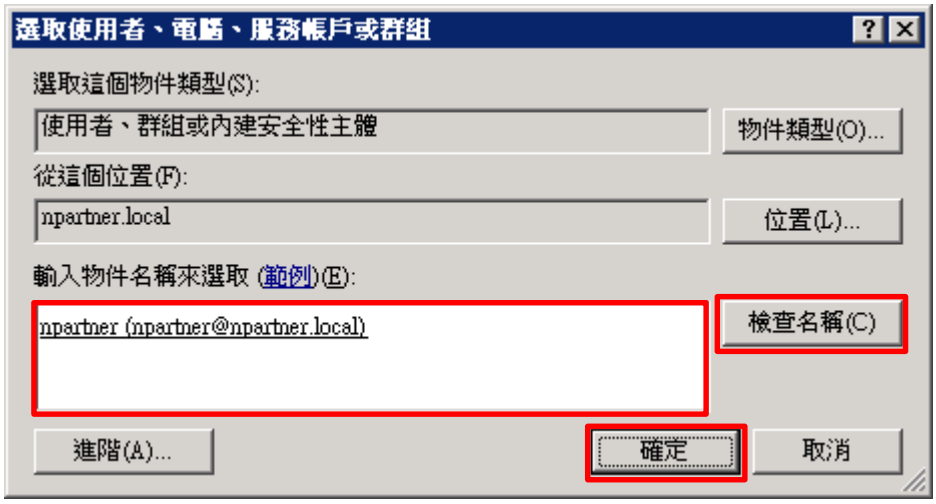
(5) 新增 WMI 使用者權限

按 [新增]



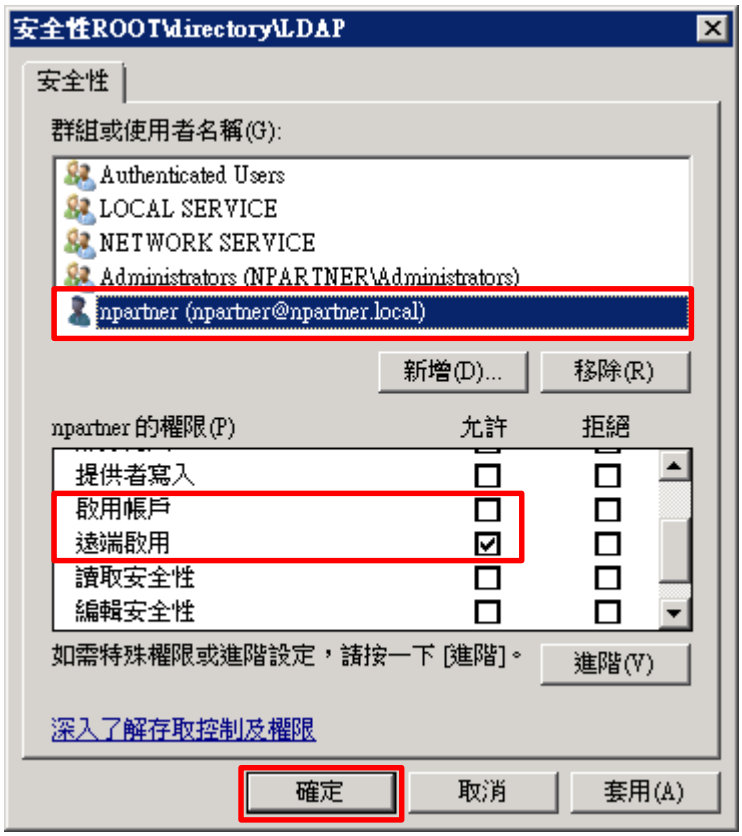
(6) 輸入使用者

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

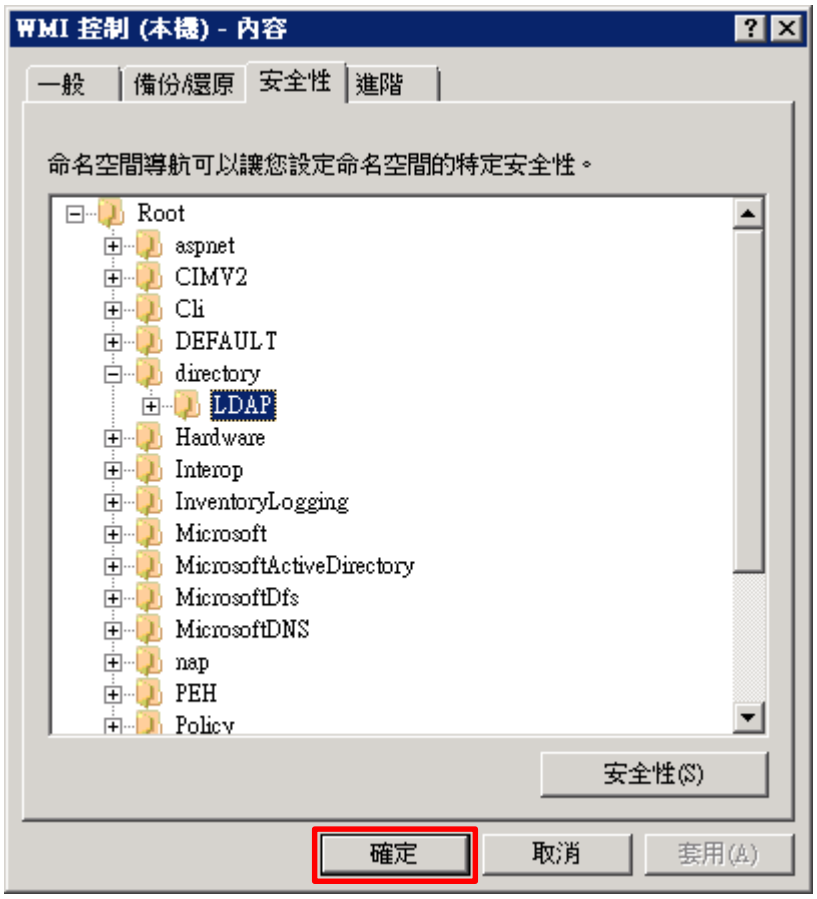


(7) 設定使用者權限

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]



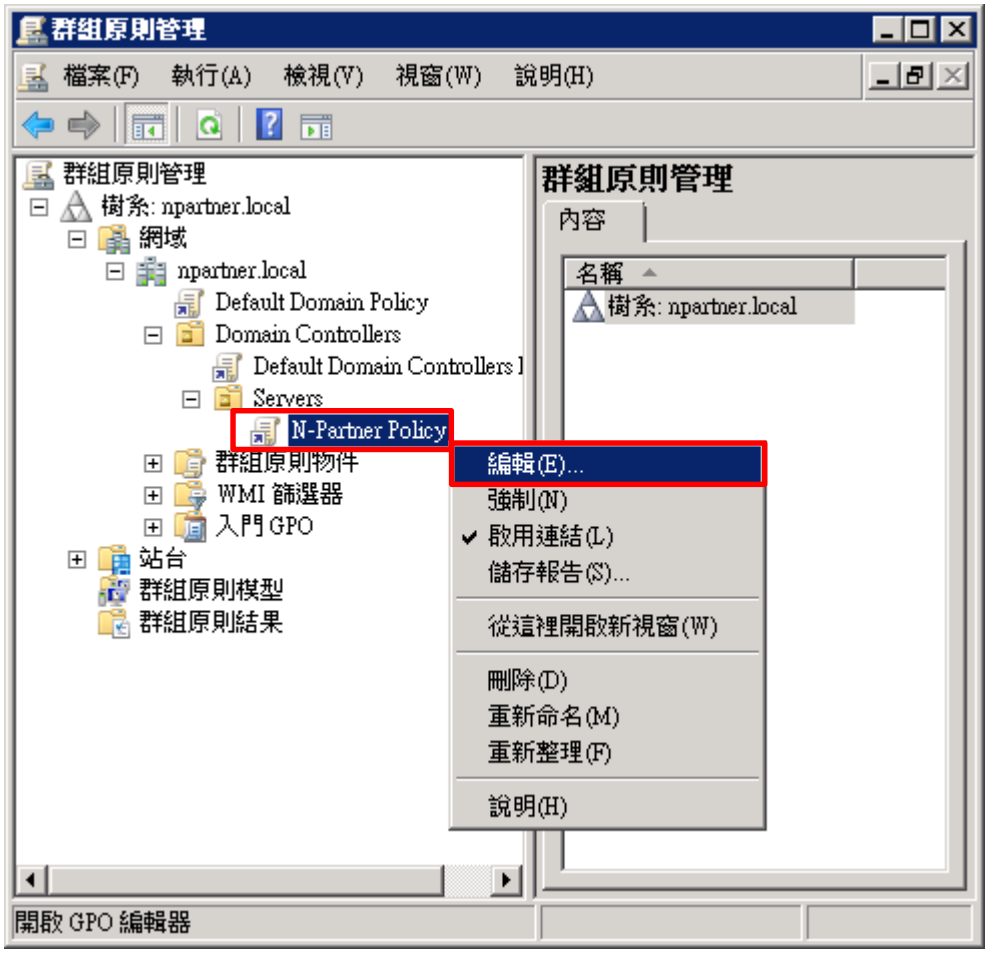
3.3.4 設定 Event log 讀取權限

(1) 開啟群組原則管理

開啟 [群組原則管理]

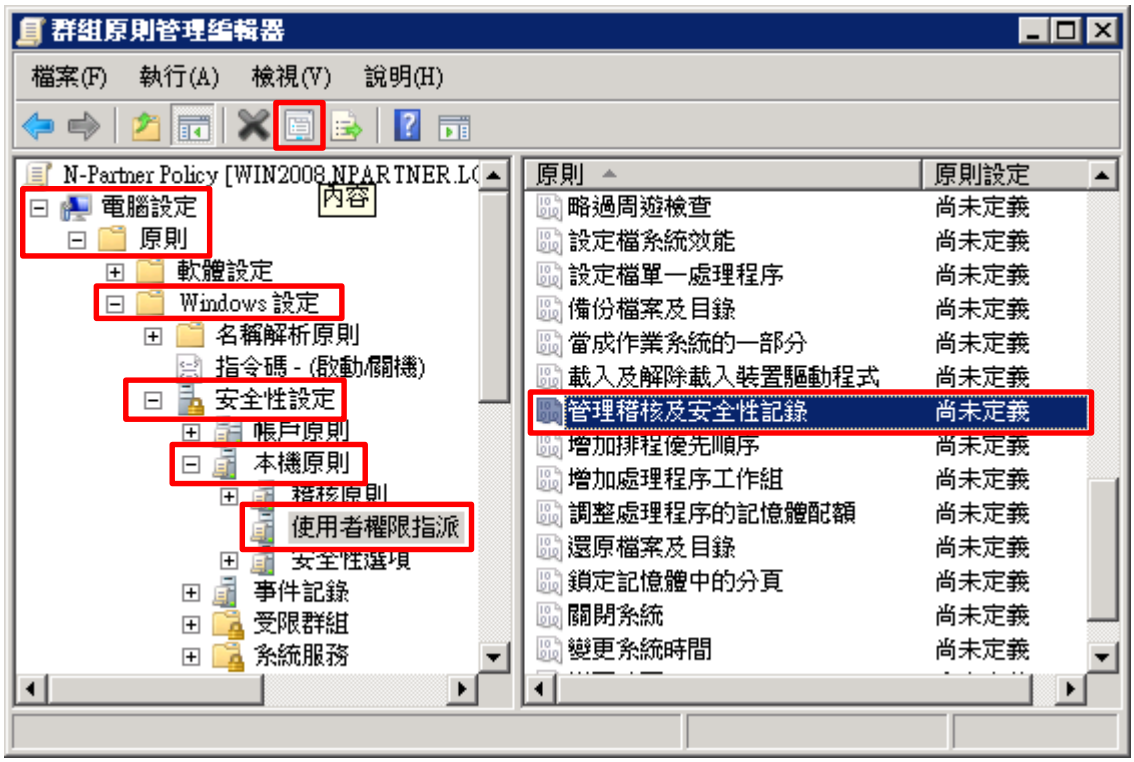
(2) 編輯群組原則物件

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



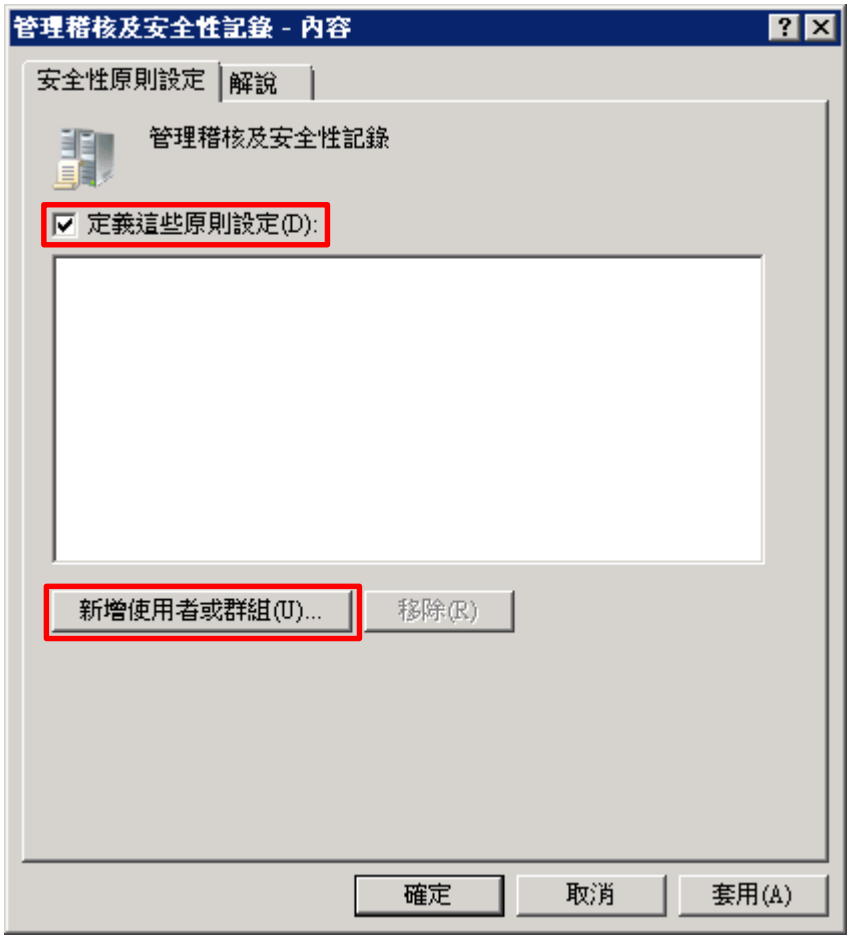
(3) 設定記錄檔

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



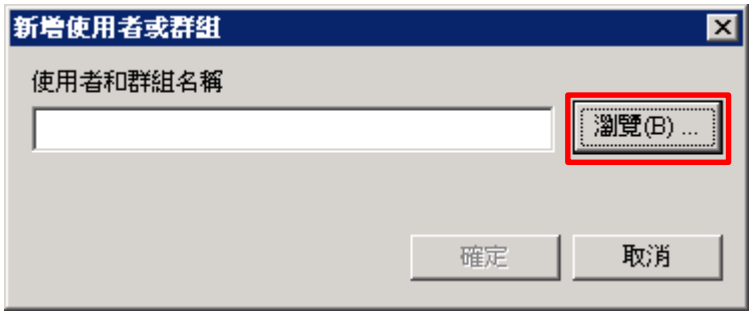
(4) 新增管理稽核使用者

勾選 [定義這些原則設定] -> 按 [新增使用者或群組...]



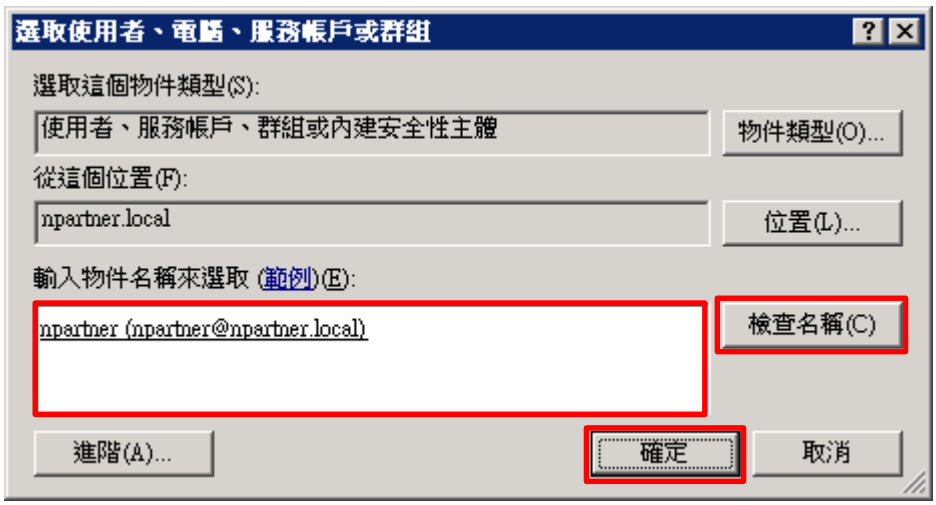
(5) 搜尋使用者

按 [瀏覽]



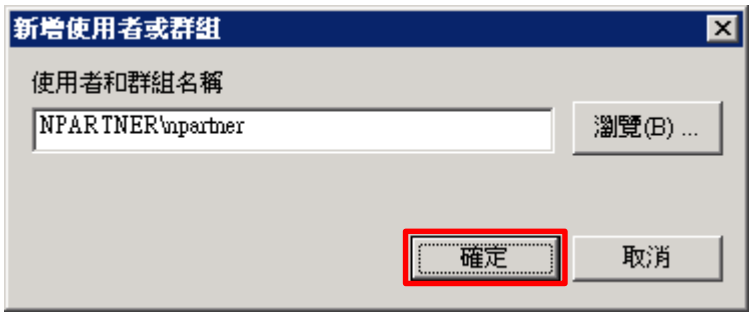
(6) 輸入使用者

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



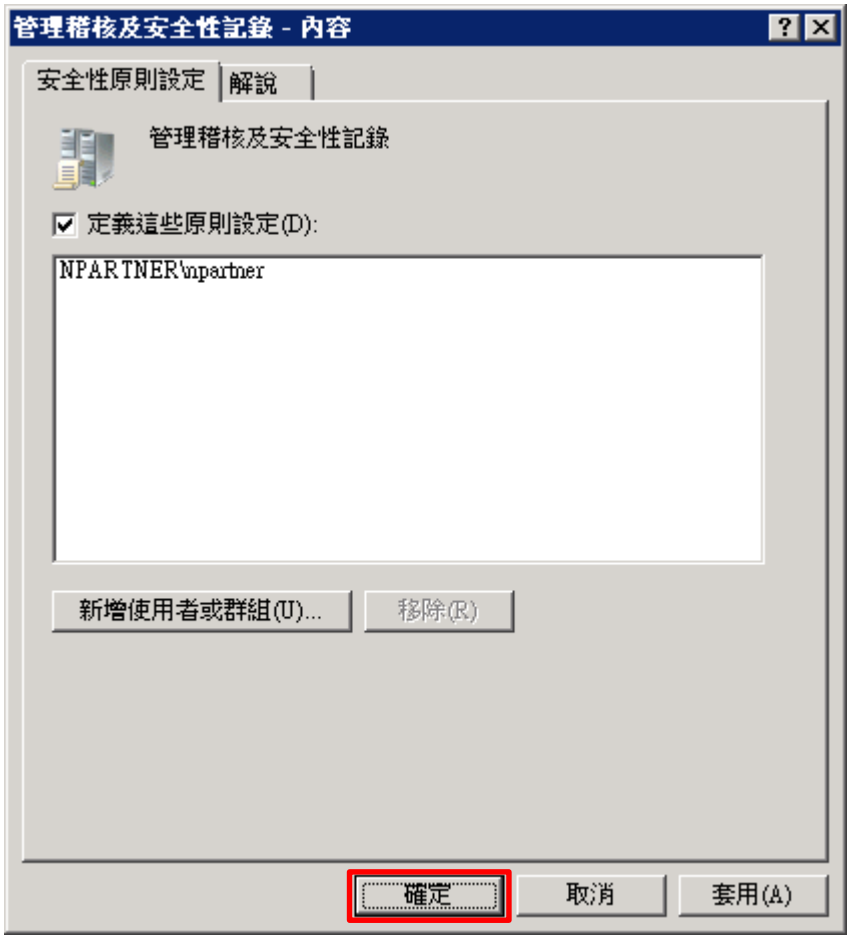
(7) 確定使用者

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

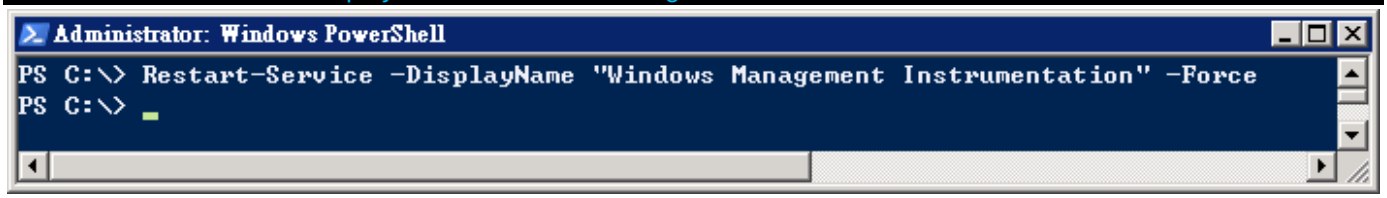
```
PS C:\> gpupdate /force
```

3.3.5 重啟 WMI 服務

(1) 開啟 [Windows PowerShell]

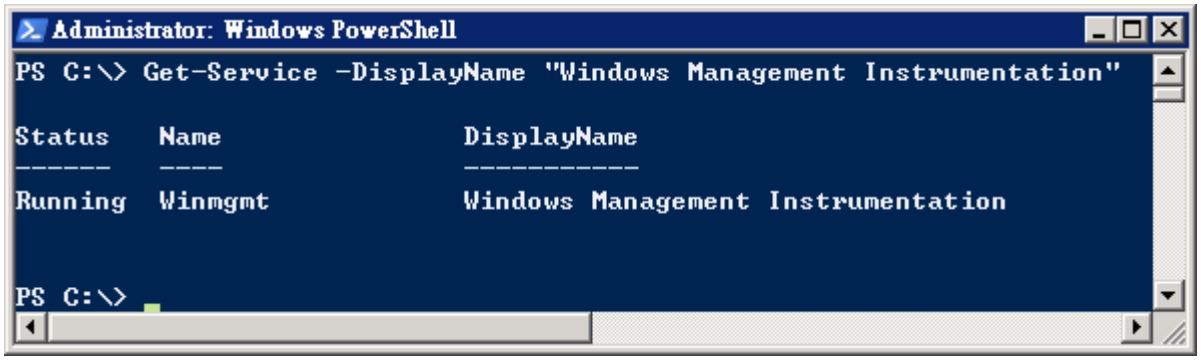
(2) 重啟 WMI 服務

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



(3) 查看 WMI 服務

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

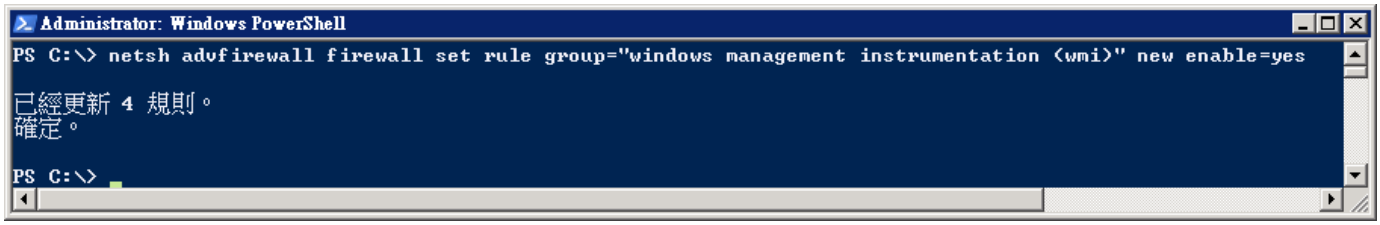


3.4 設定防火牆

(1) 開啟 [Windows PowerShell]

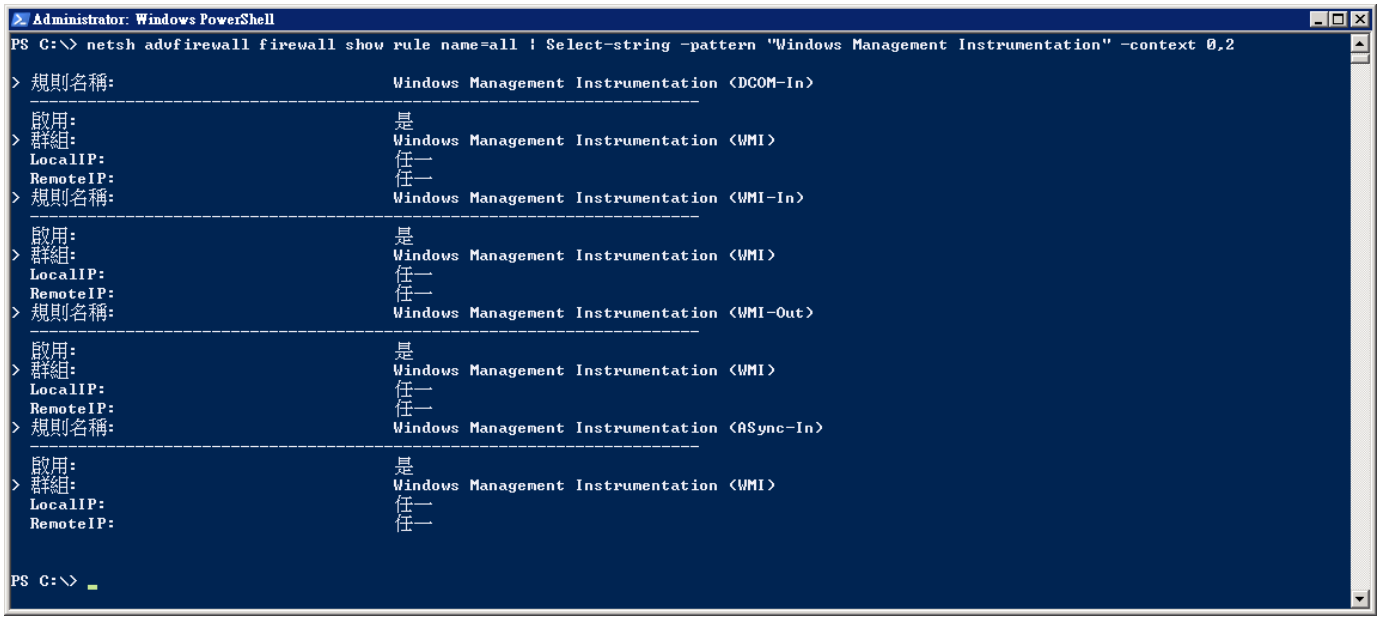
(2) 允許 WMI 通過防火牆

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



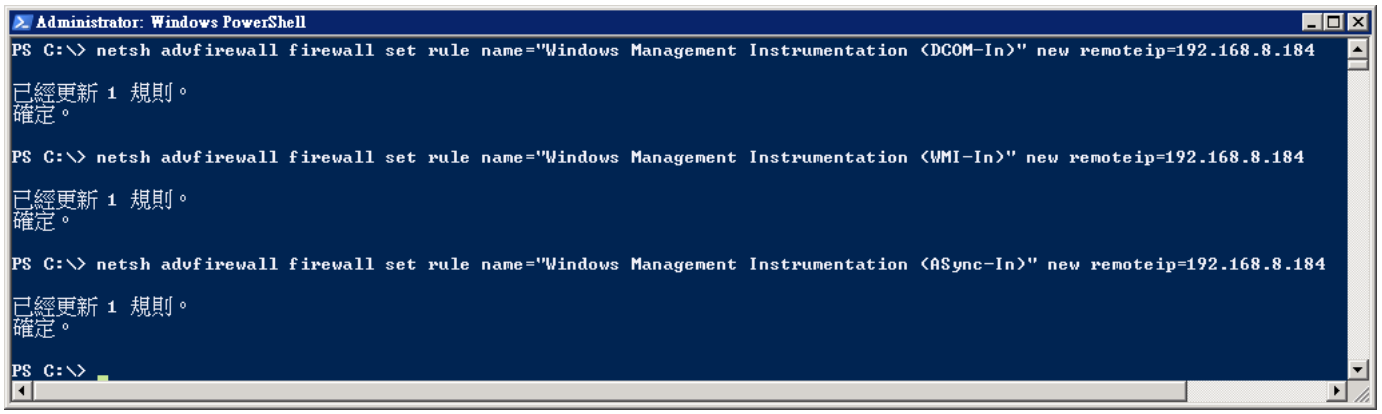
(3) 查看防火牆 WMI 啟用狀態

```
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

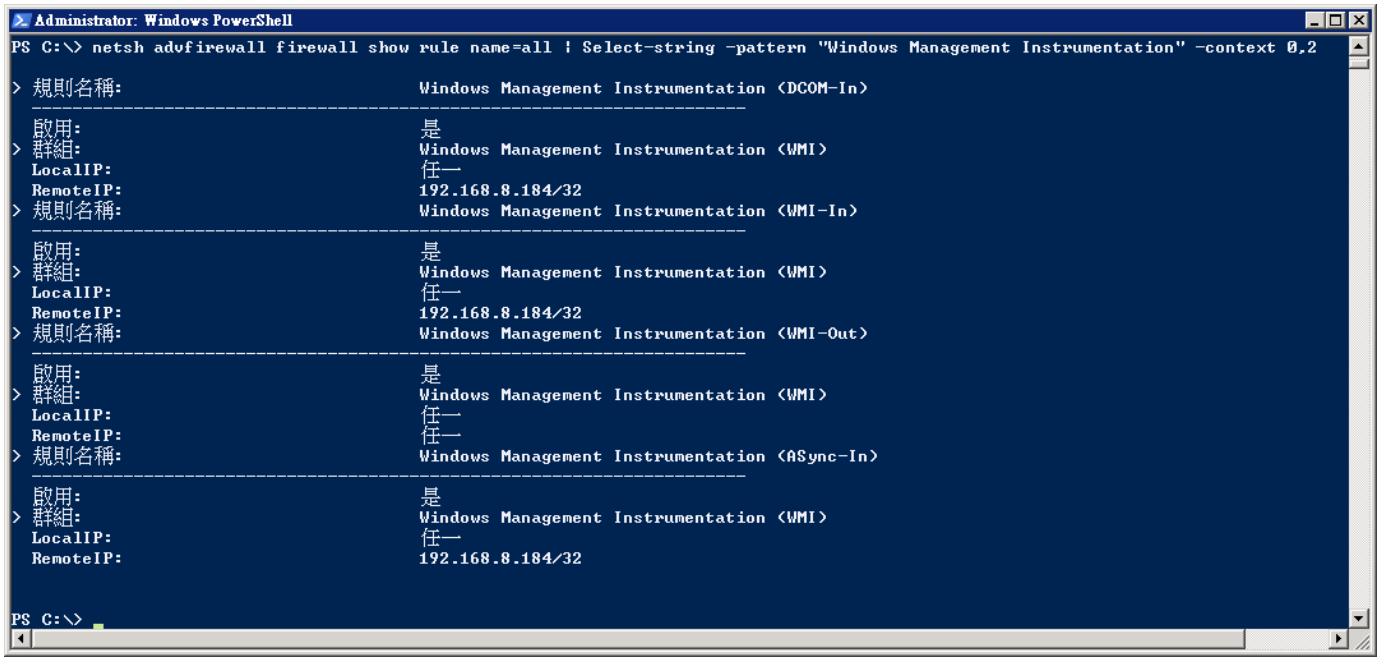
```
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (DCOM-In)" new remoteip=192.168.8.184
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (WMI-In)" new remoteip=192.168.8.184
PS C:\> netsh advfirewall firewall set rule name="Windows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



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
```



4. Windows 2012

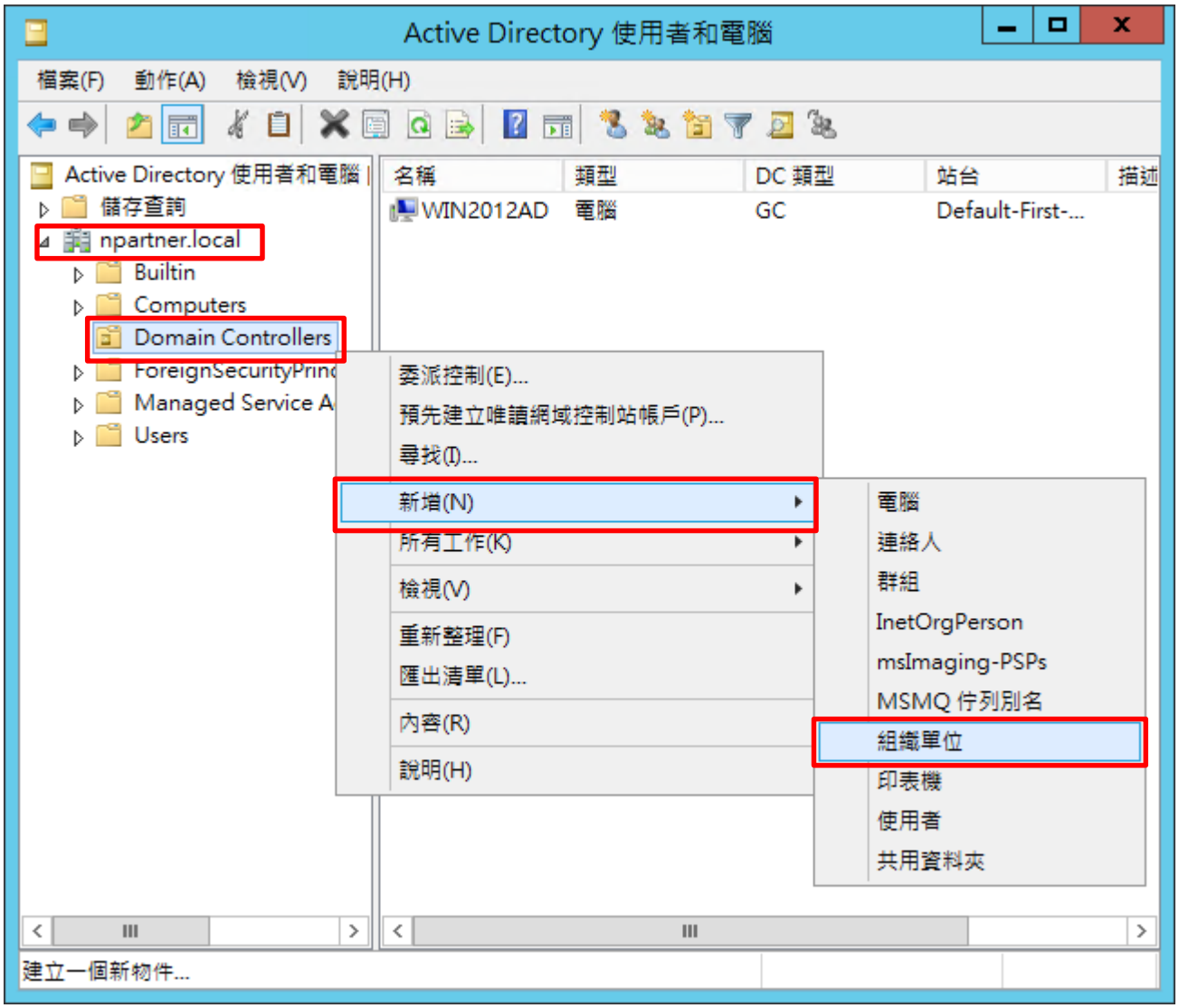
Windows 稽核原則設定 詳細說明請參考前言的稽核原則建議連結

4.1 組織單位設定

(1) 開啟 [Active Directory 使用者和電腦]

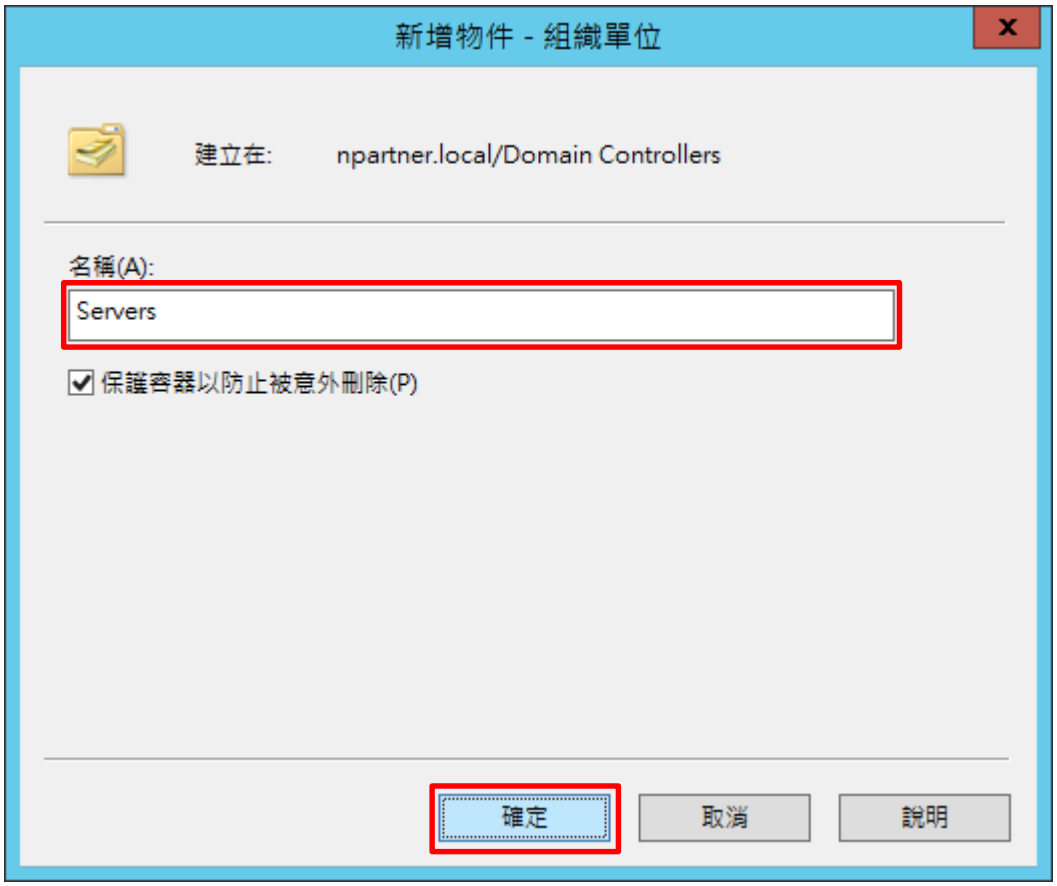
(2) 新增組織單位

[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]



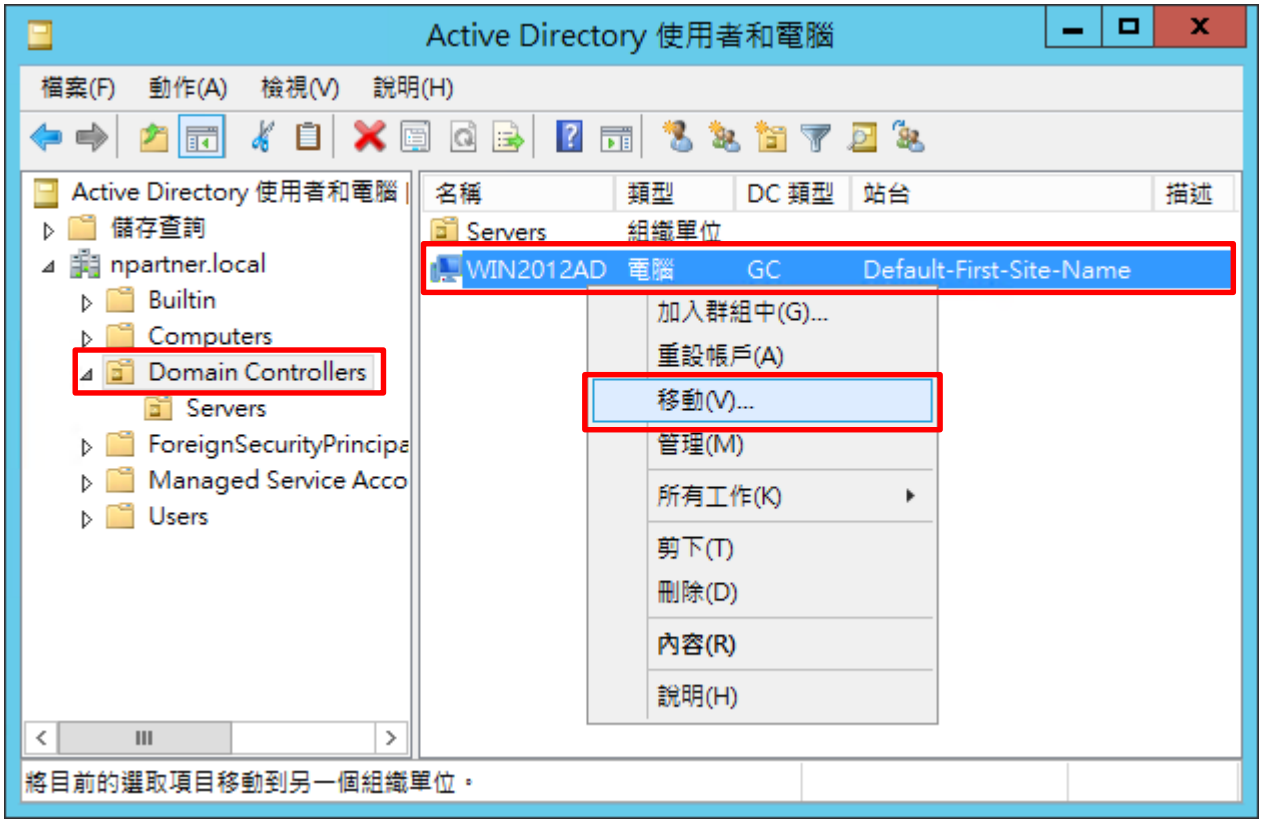
(3) 輸入組織單位名稱

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]



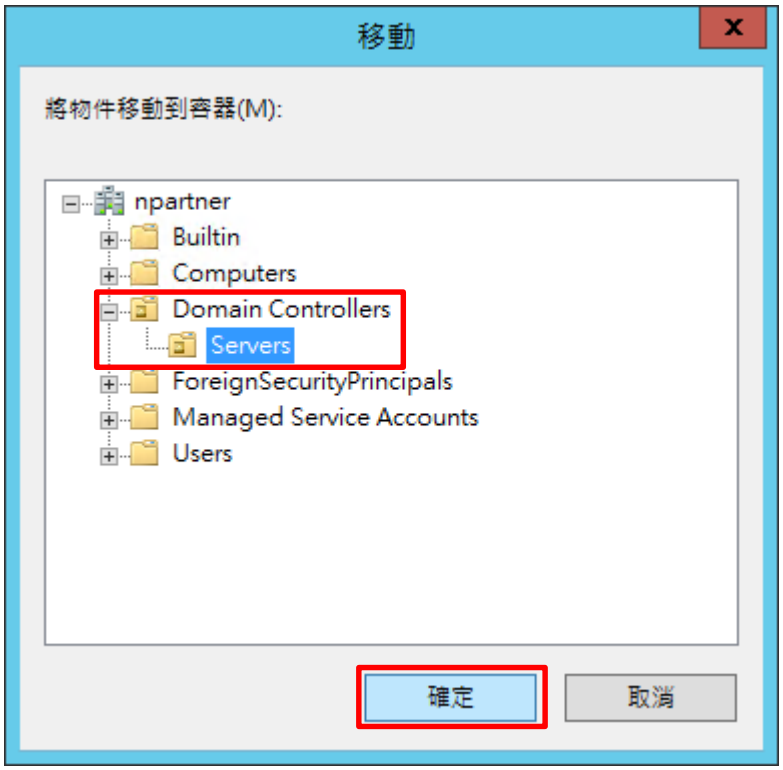
(4) 移動伺服器至新的組織單位

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]



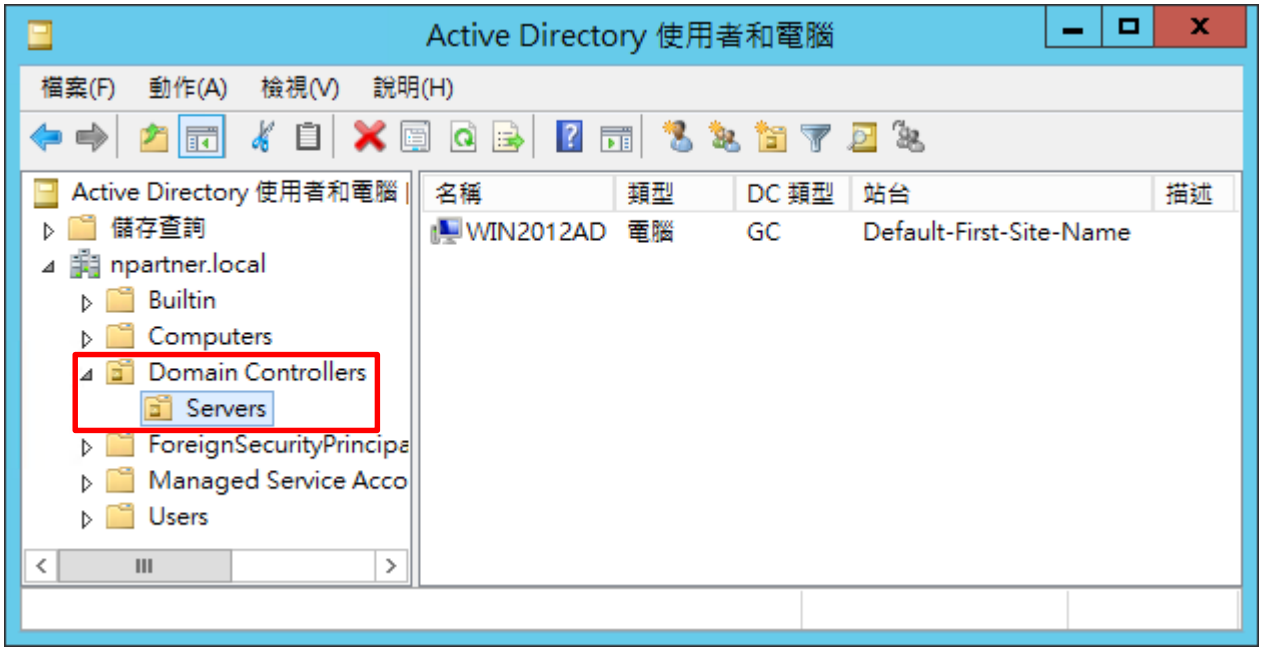
(5) 選擇組織單位

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

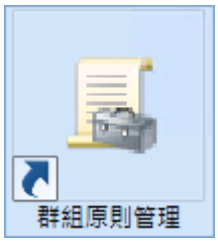
展開 [Domain Controllers] 的 [Servers] 組織單位，確認 [Win2012AD] 伺服器已移動



4.2 群組原則設定

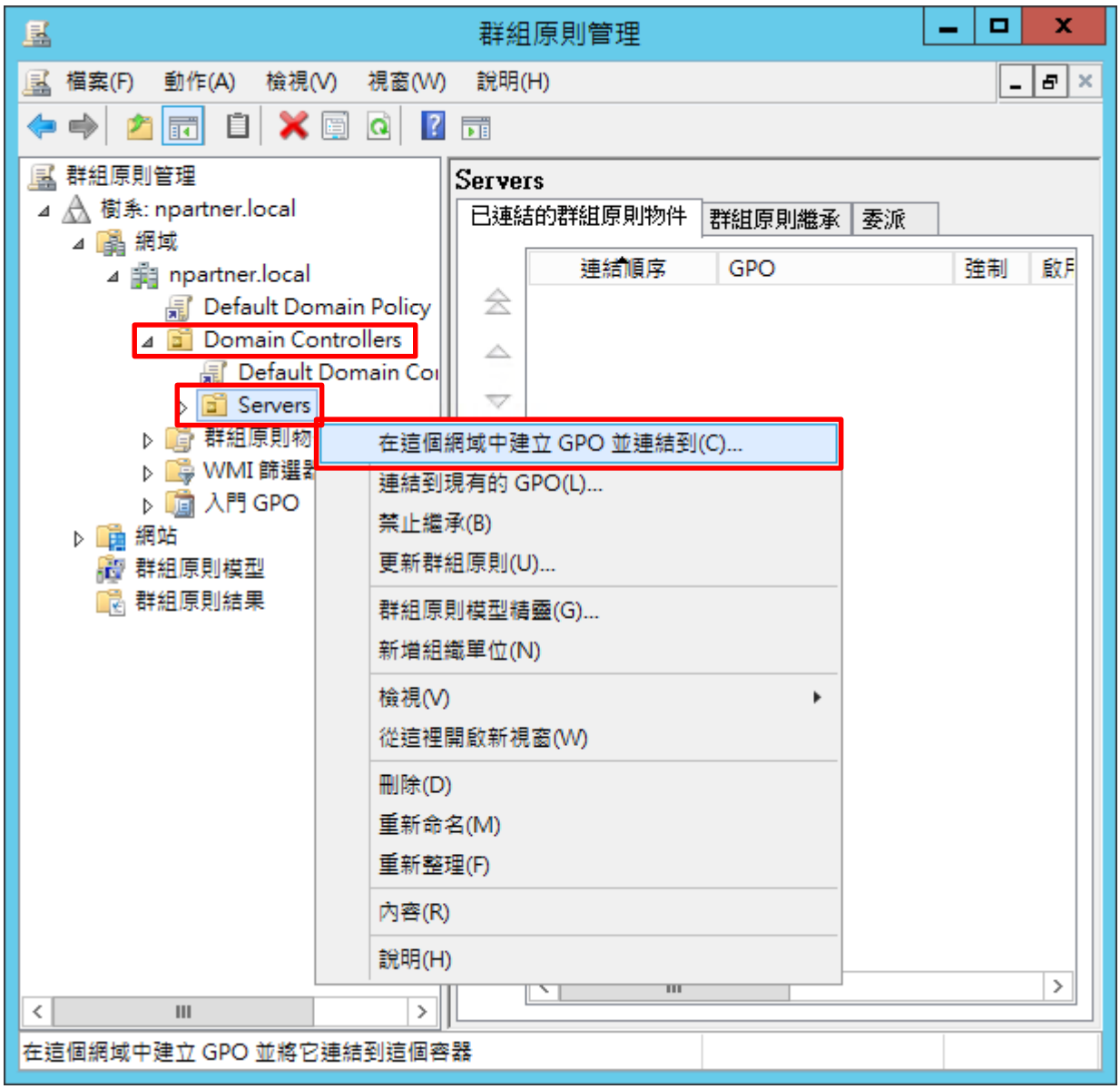
(1) 開啟群組原則管理

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

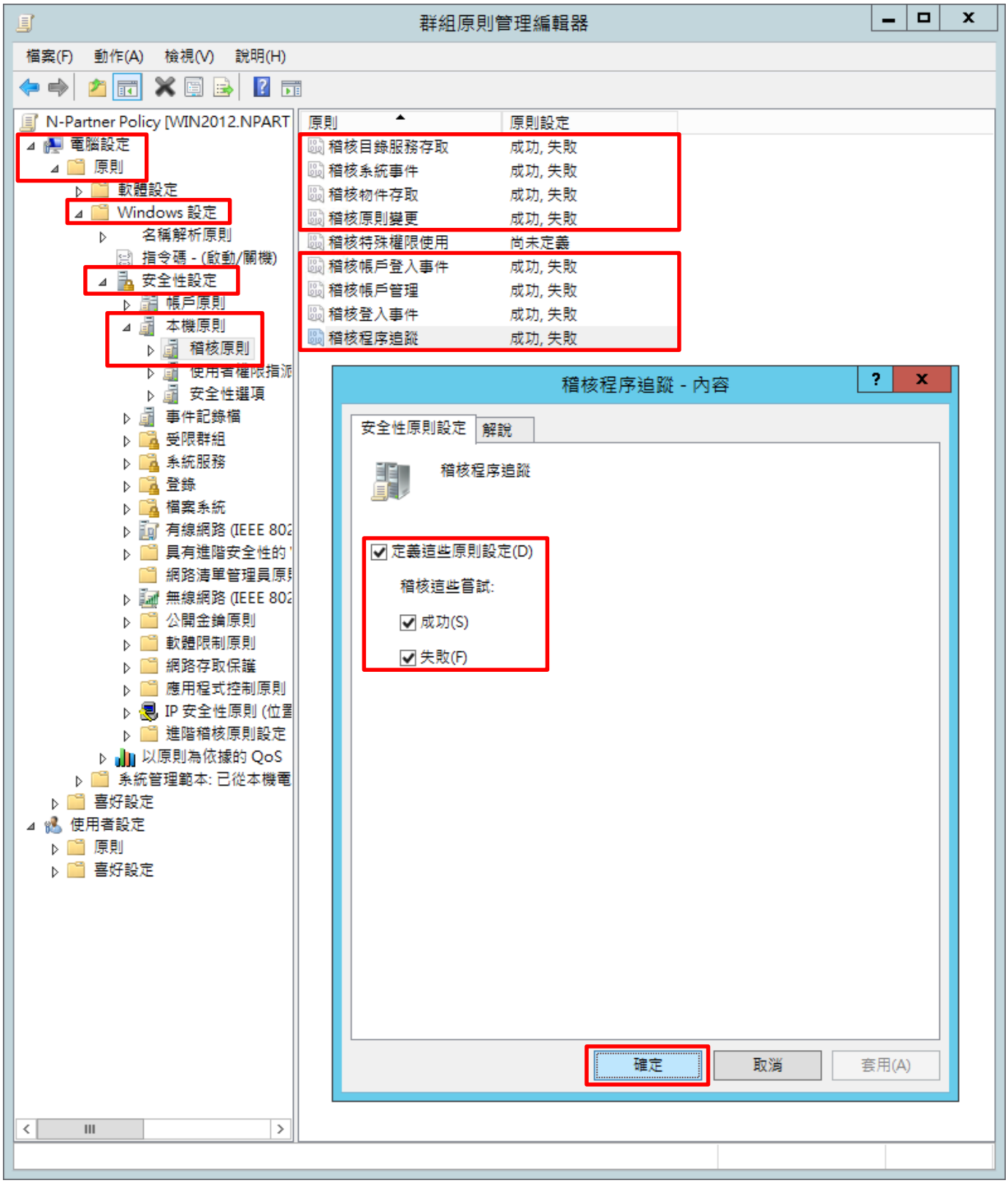
輸入群組原則物件名稱: N-Partner Policy 註：請依客戶環境建立群組物件名稱 -> 按 [確定]

(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]

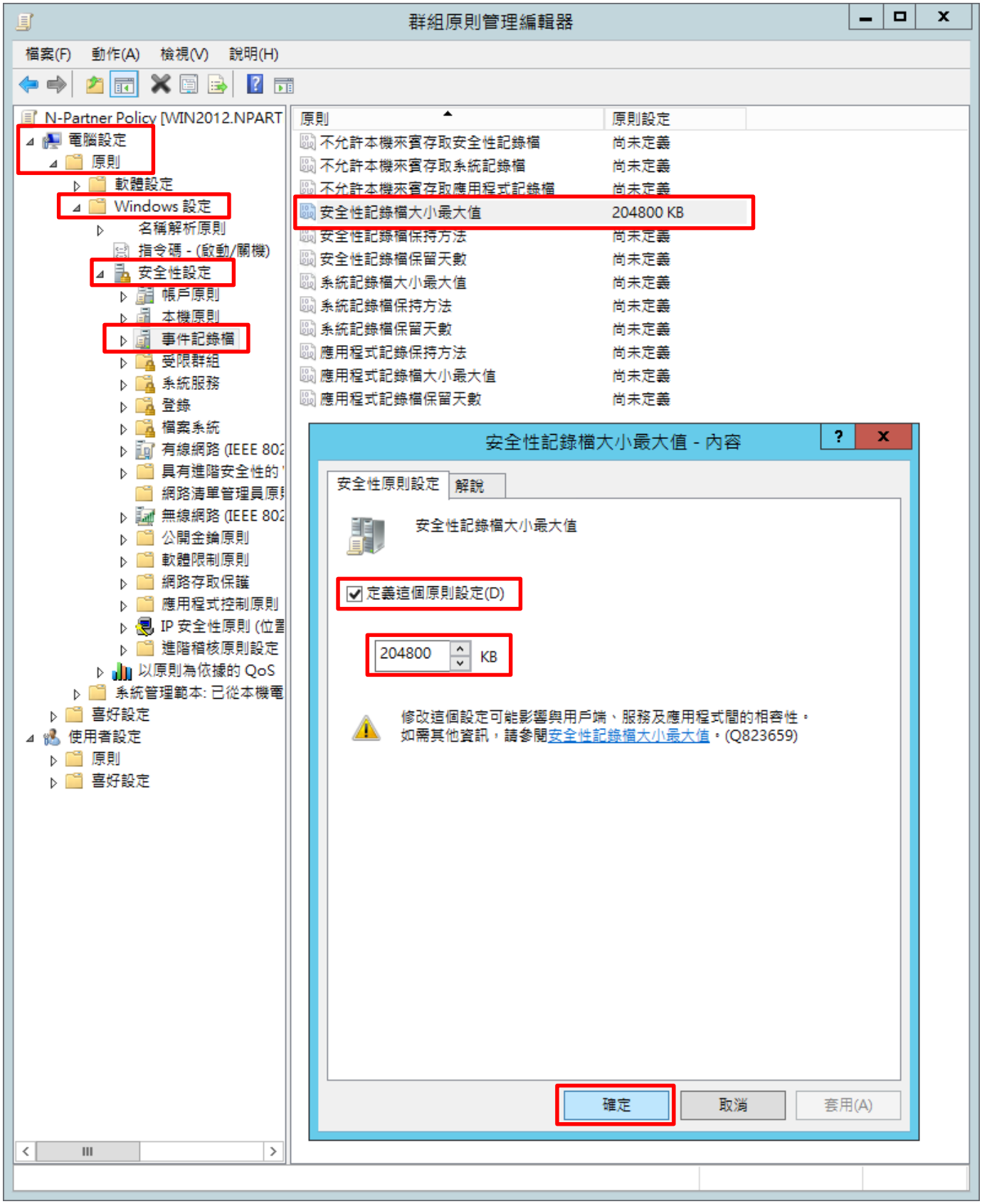
(5) 本機原則：稽核原則

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]



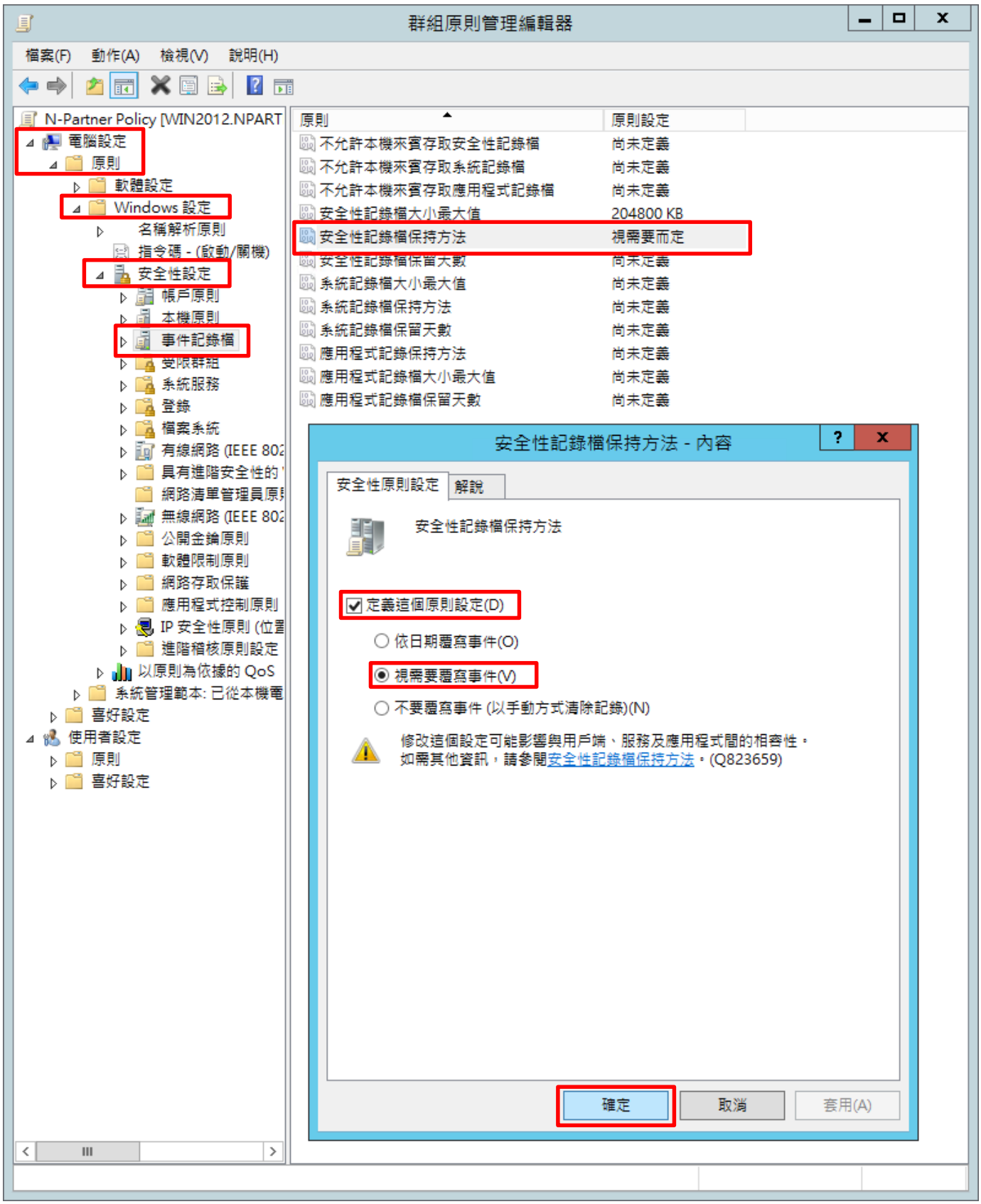
(6) 事件記錄：安全性記錄檔大小最大值

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

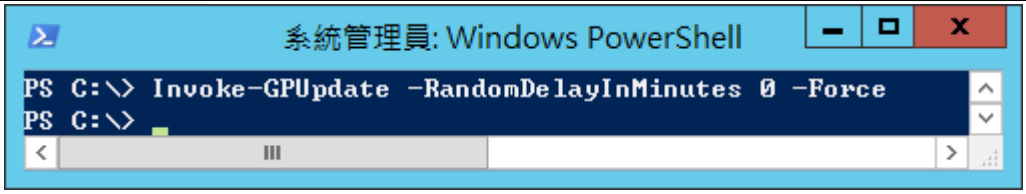
展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔保持方法] 項目 -> 勾選 [定義這個原則設定] -> 點選 [視需要覆寫事件] -> 按 [確定]



(8) 開啟 [Windows PowerShell]

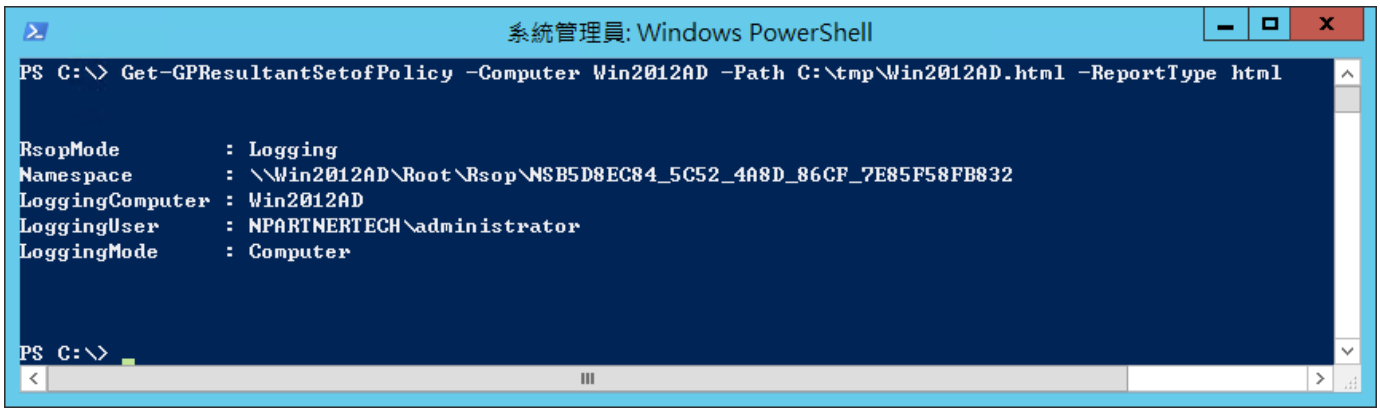
(9) 更新群組原則

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



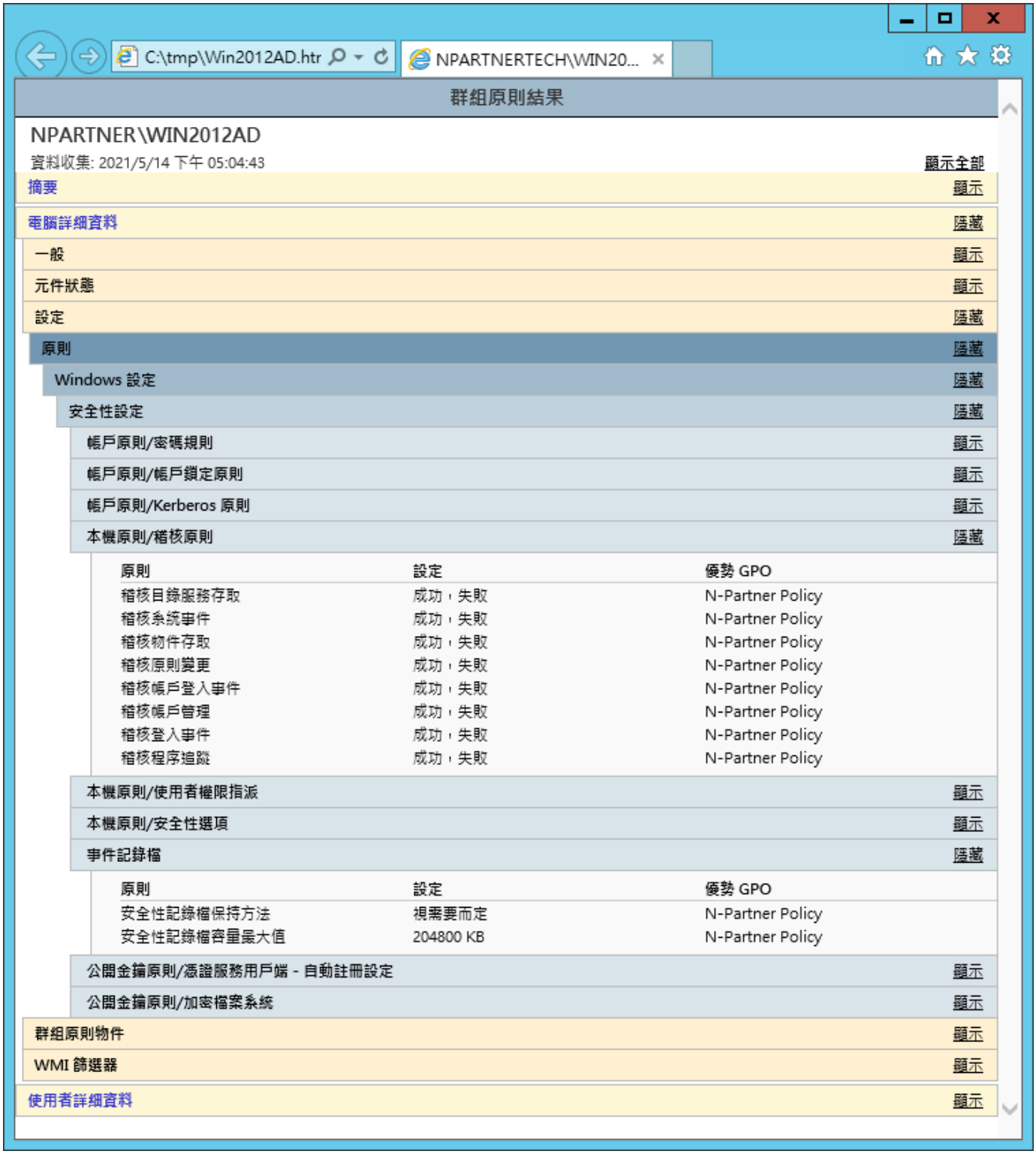
(10) 產生伺服器群組原則報表

```
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



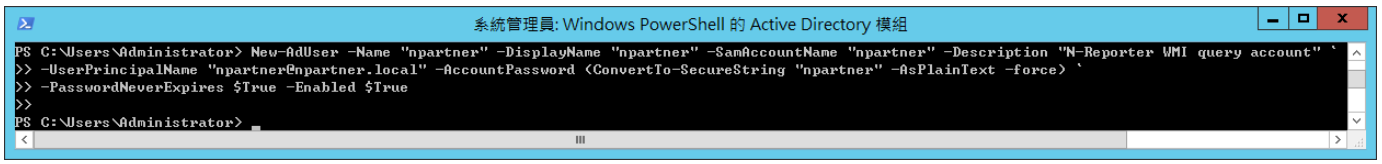
4.3 新增非管理帳號

4.3.1 新增使用者

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

(2) 新增帳號

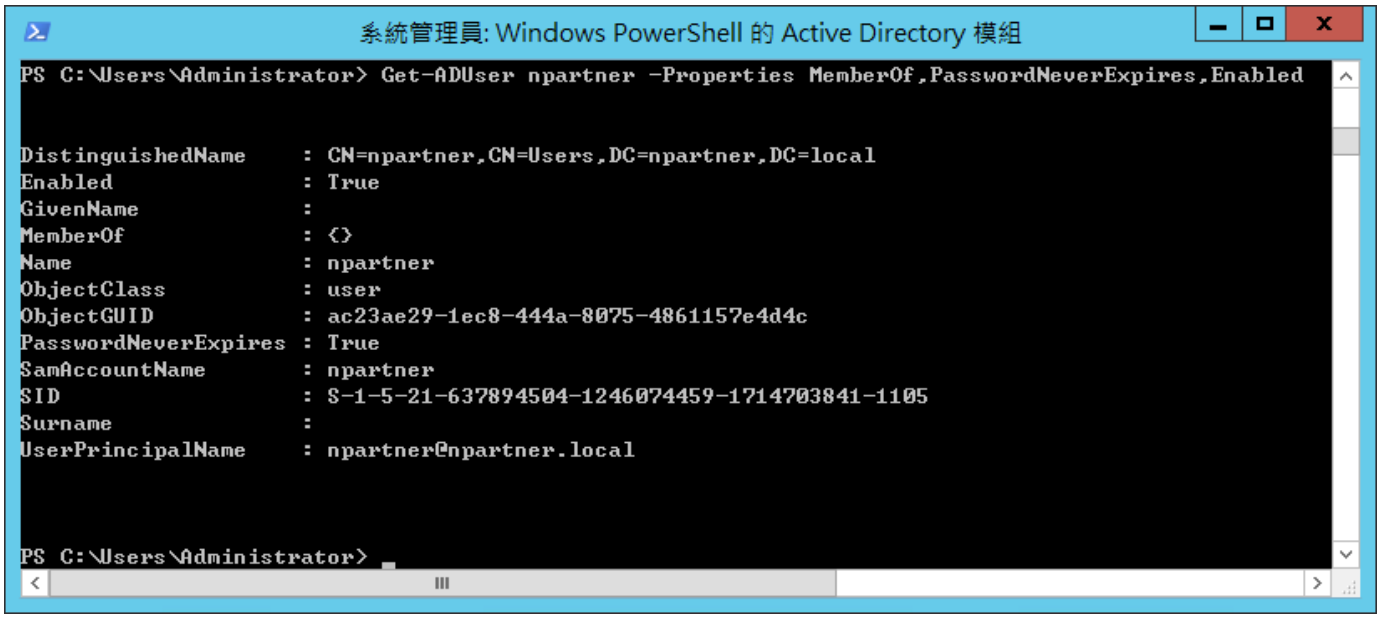
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" `
>> -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True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



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
```

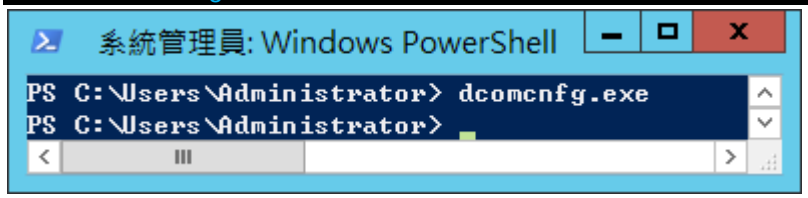


4.3.2 設定 DCOM 權限

(1) 開啟 [Windows PowerShell]

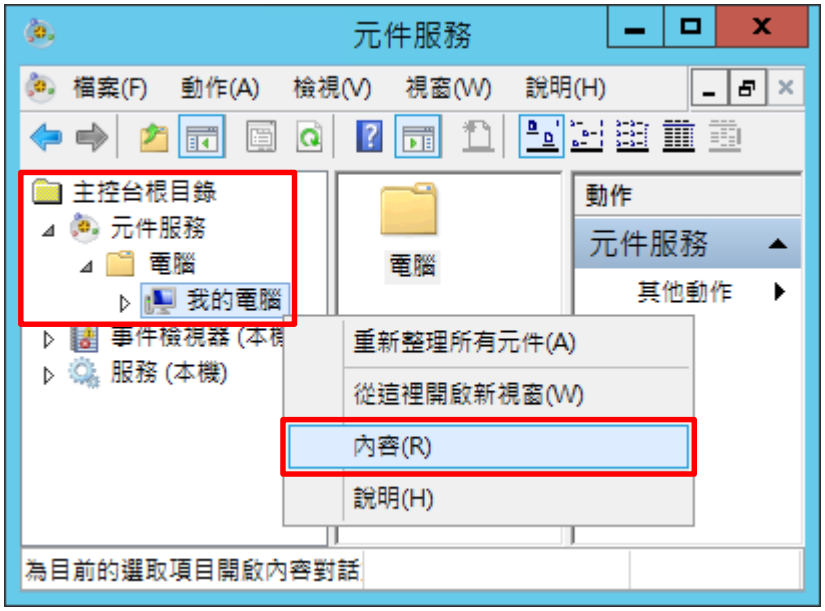
(2) 開啟元件服務

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



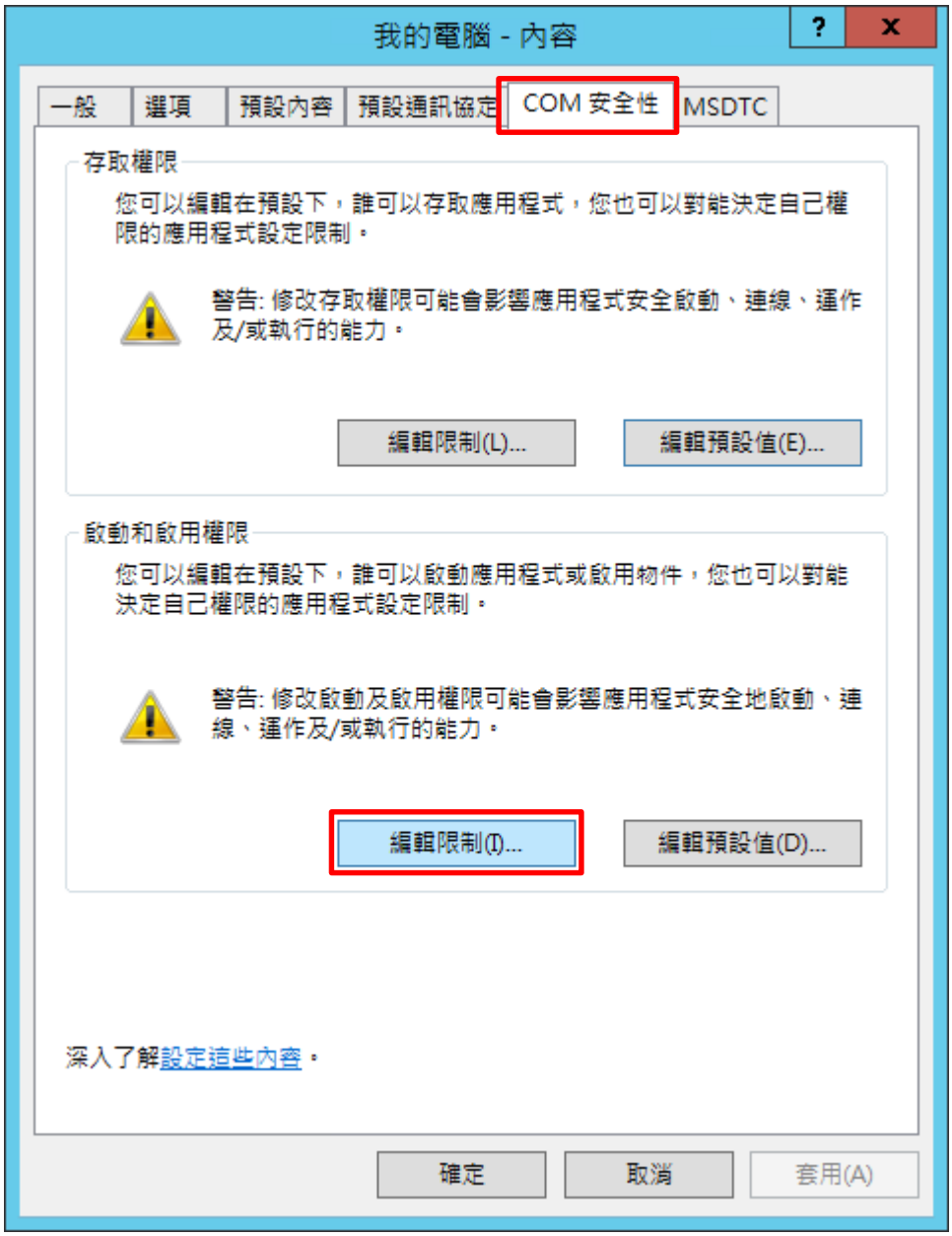
(3) 編輯電腦內容

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]



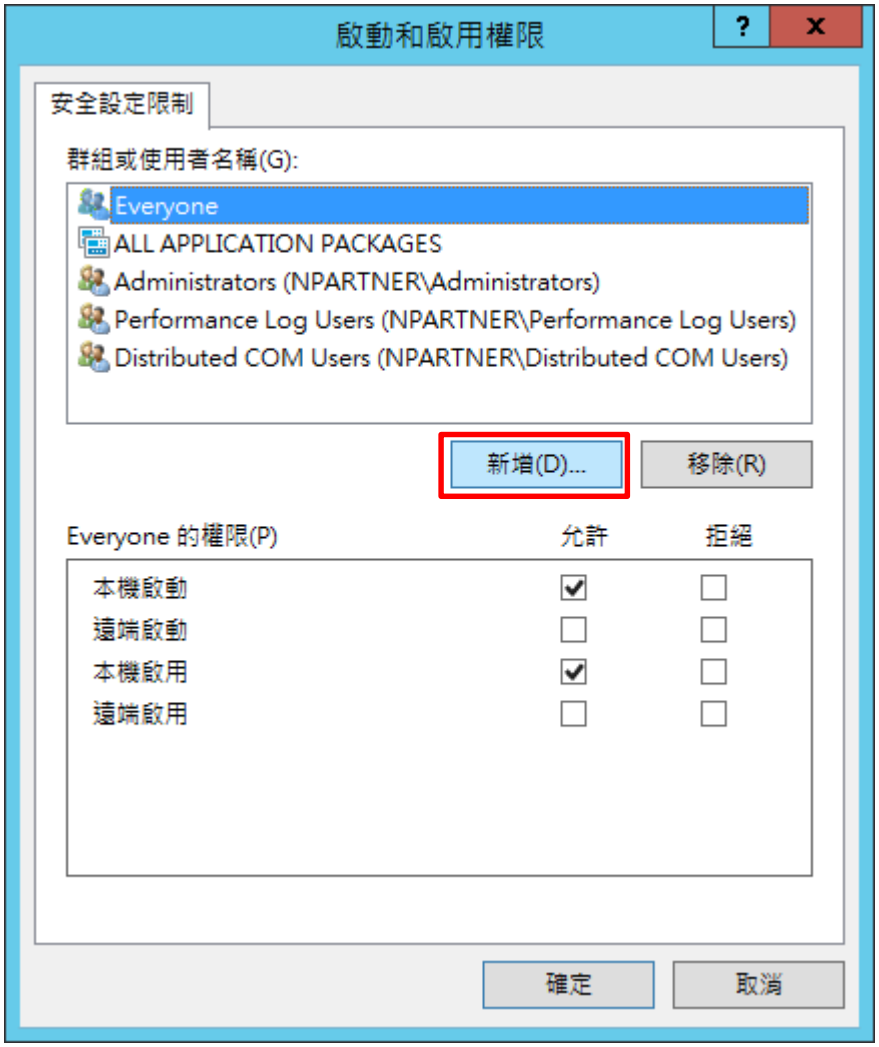
(4) 啟用權限

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]

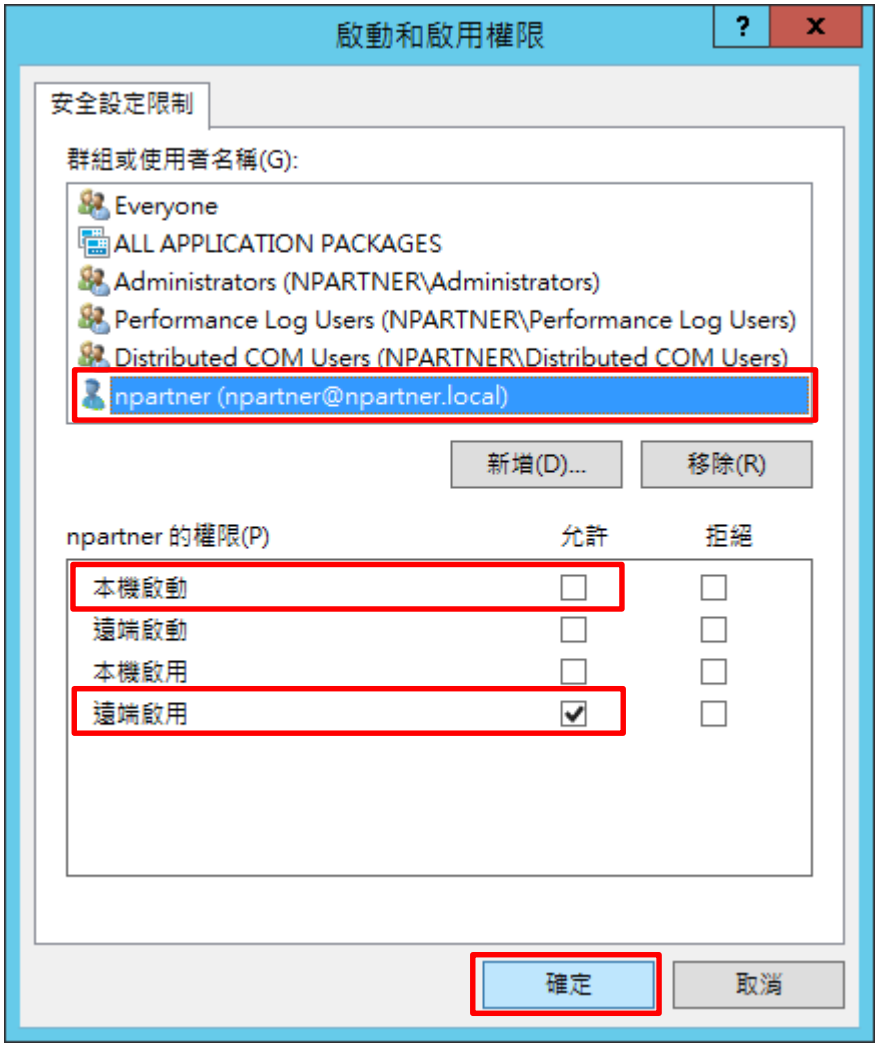


(6) 輸入使用者

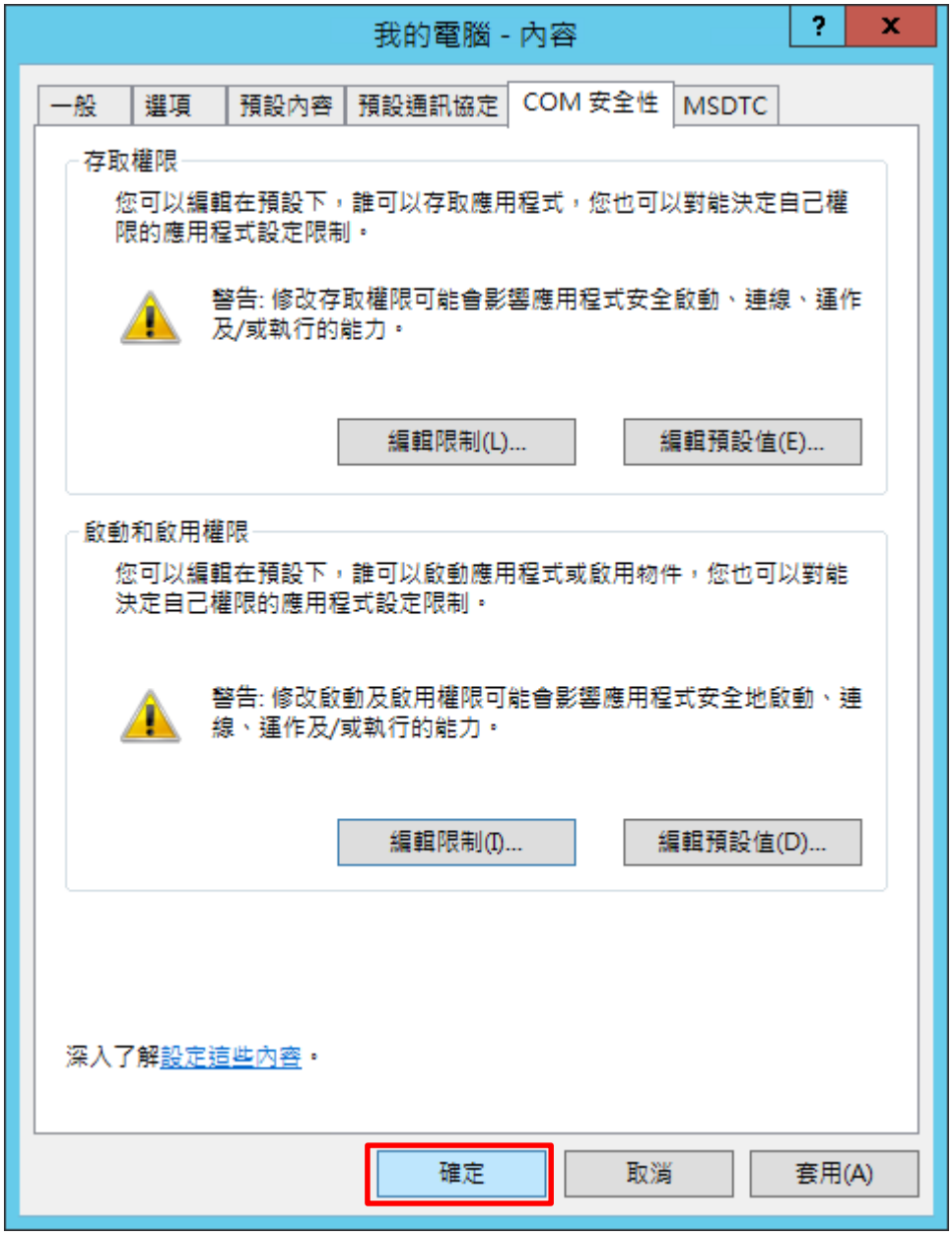
輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

(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]



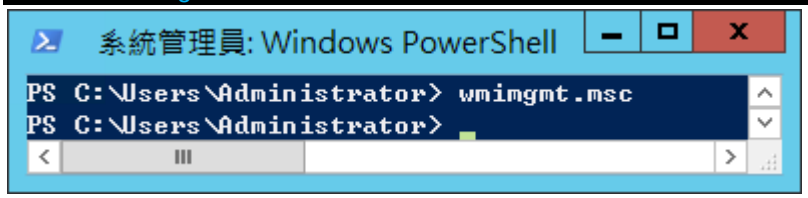
4.3.3 設定 WMI 權限

4.3.3.1 設定事件日誌權限

(1) 開啟 [Windows PowerShell]

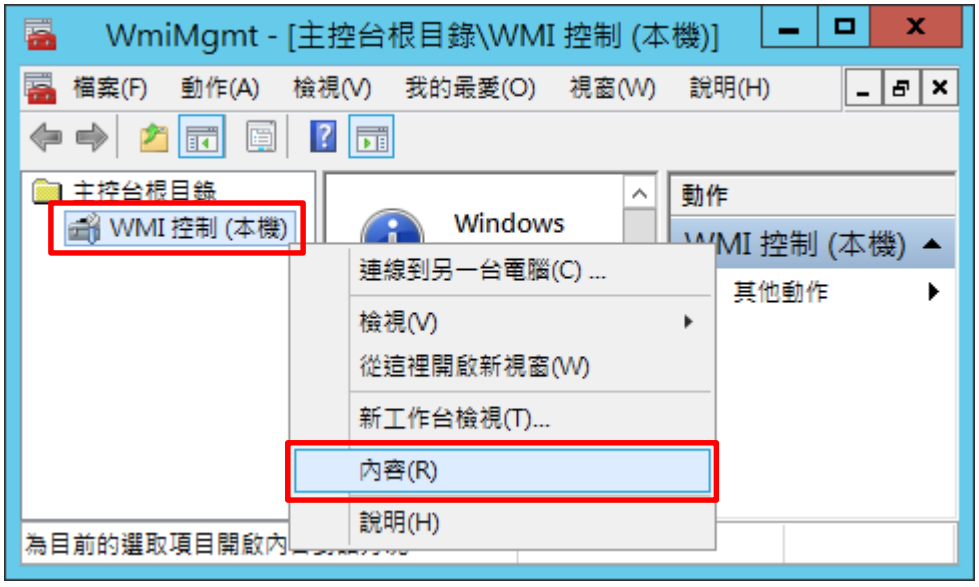
(2) 開啟元件服務

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



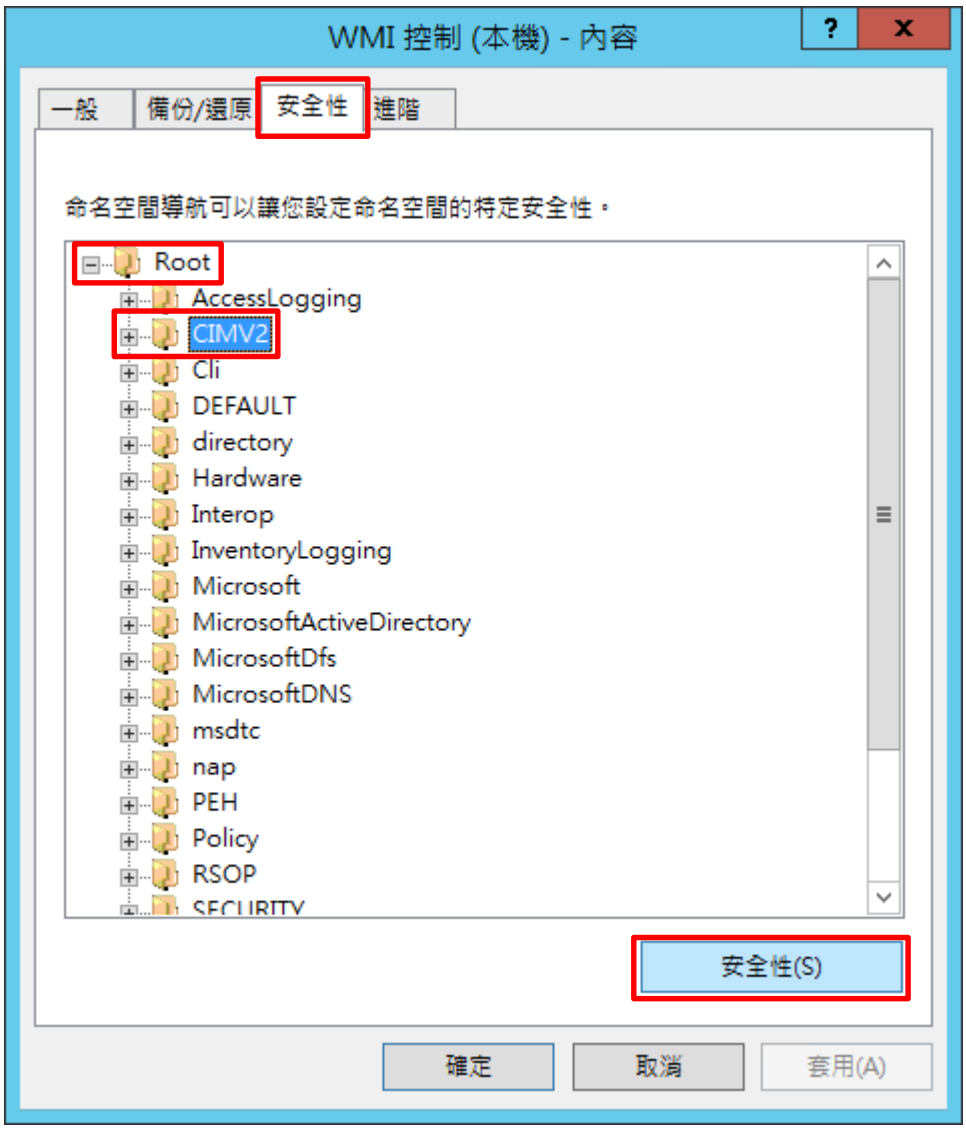
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



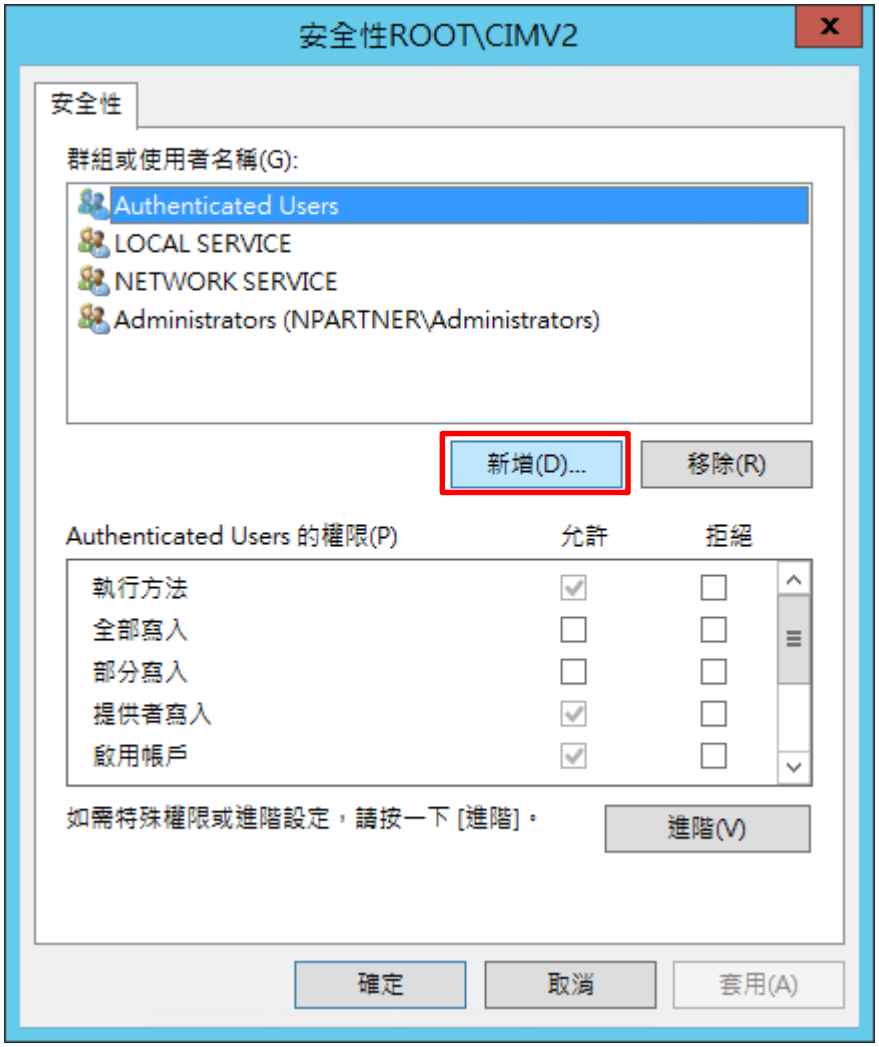
(4) 編輯 CIMV2 安全性

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]

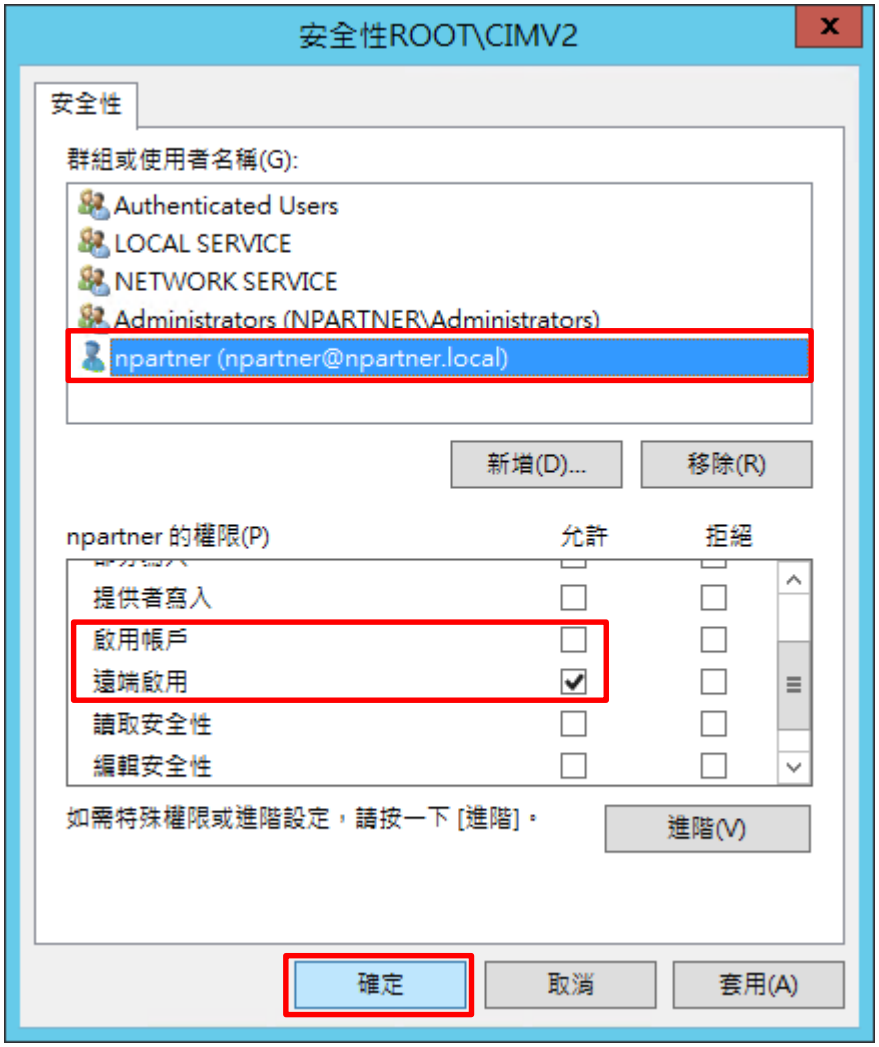


(6) 輸入使用者

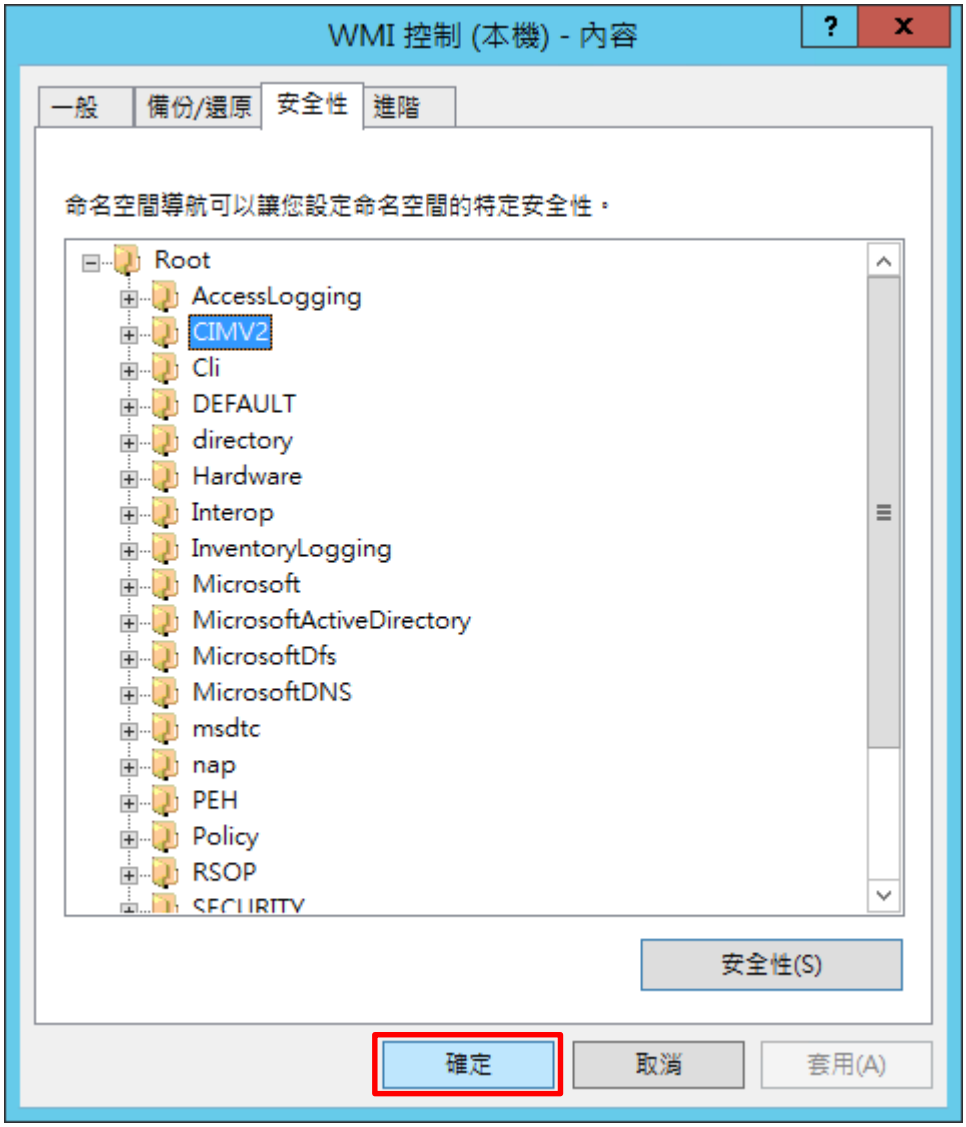
輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

(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]

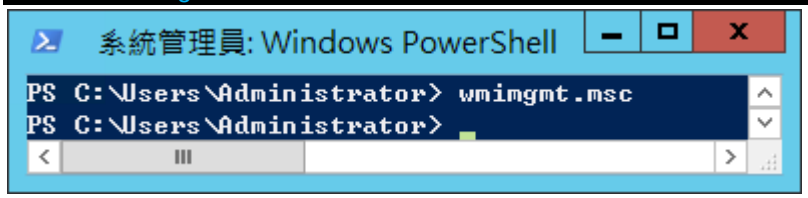


4.3.3.2 設定讀取使用者資料權限

(1) 開啟 [Windows PowerShell]

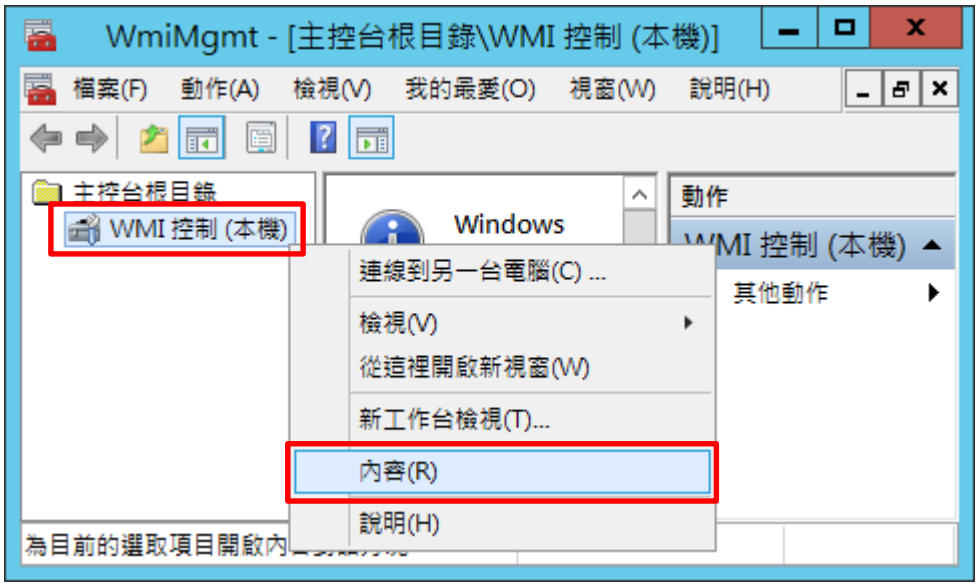
(2) 開啟元件服務

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



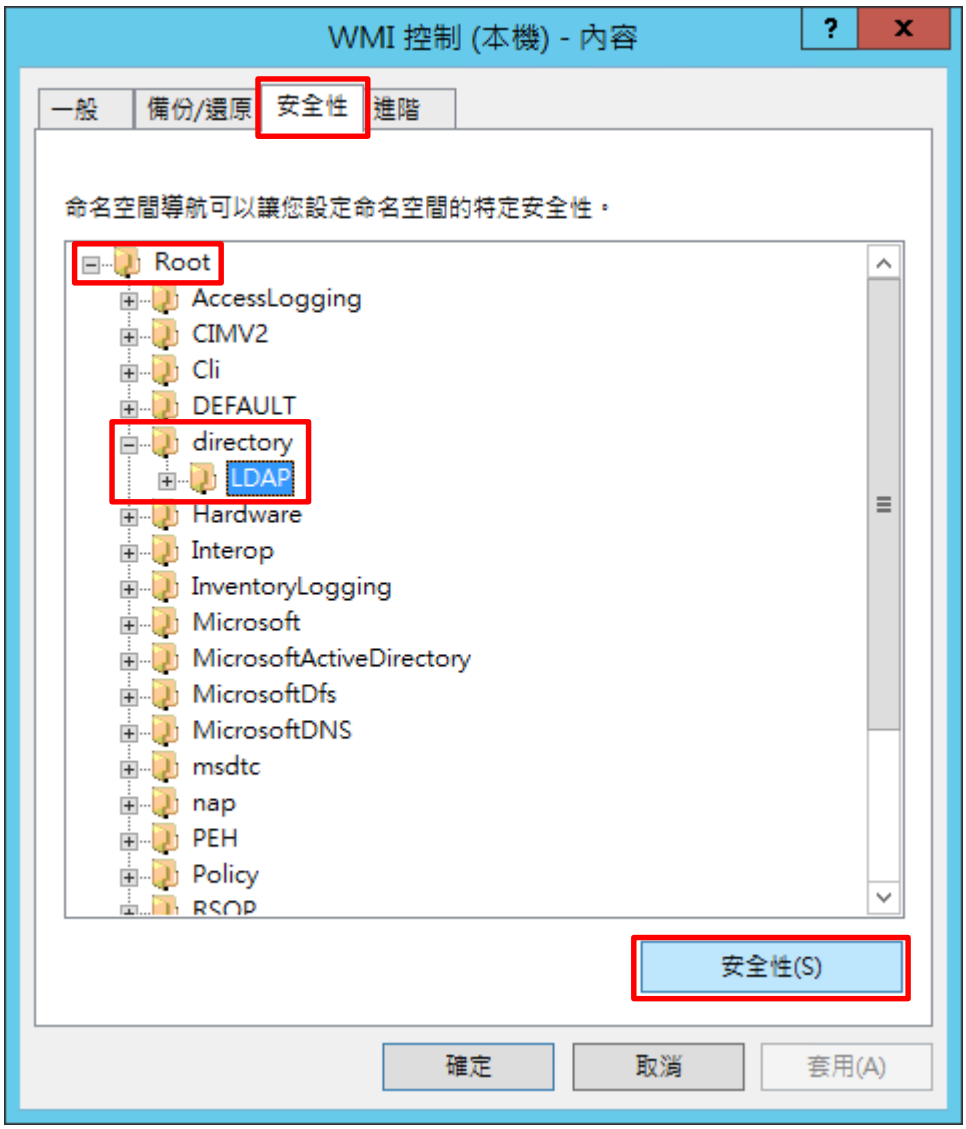
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



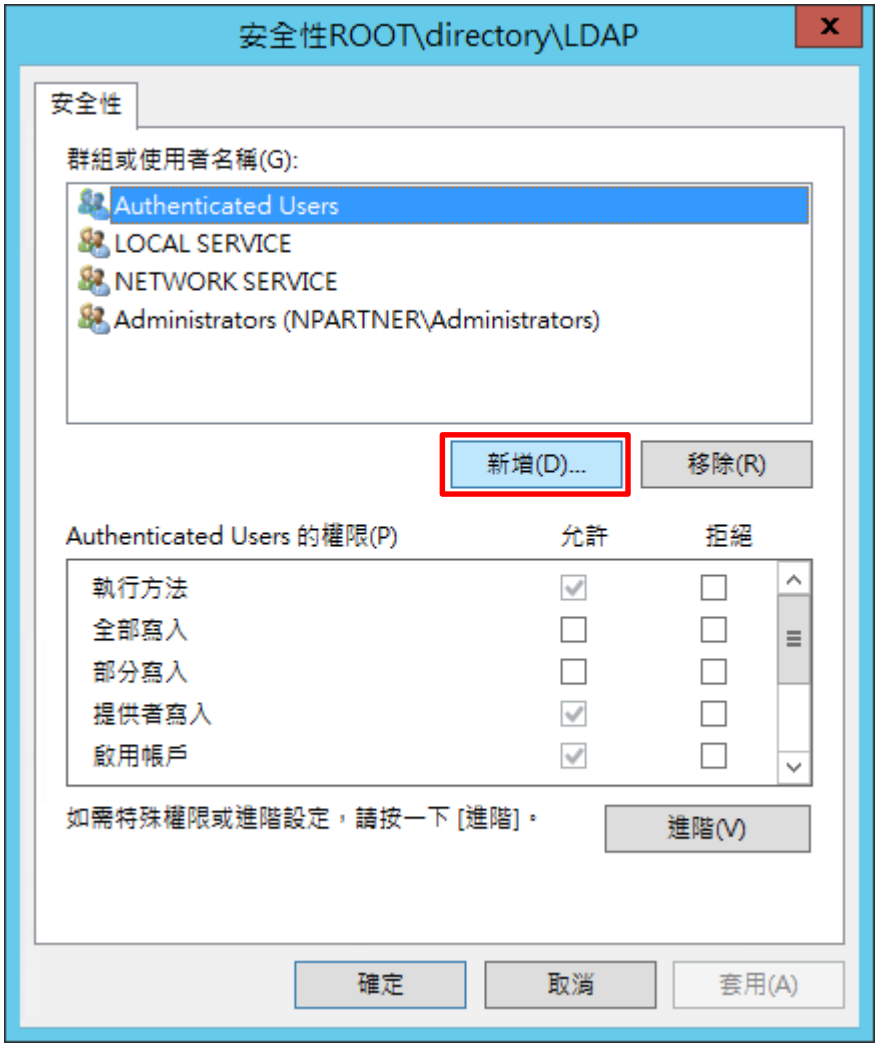
(4) 編輯 LDAP 安全性

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]

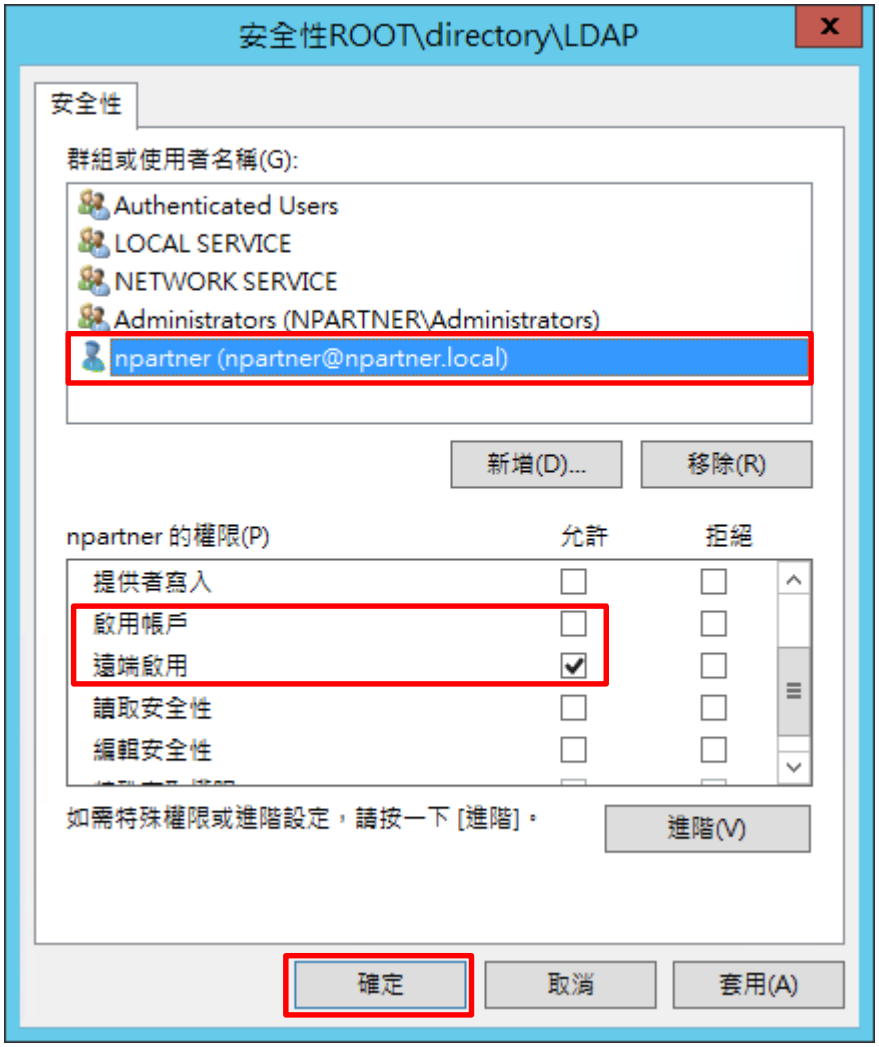


(6) 輸入使用者

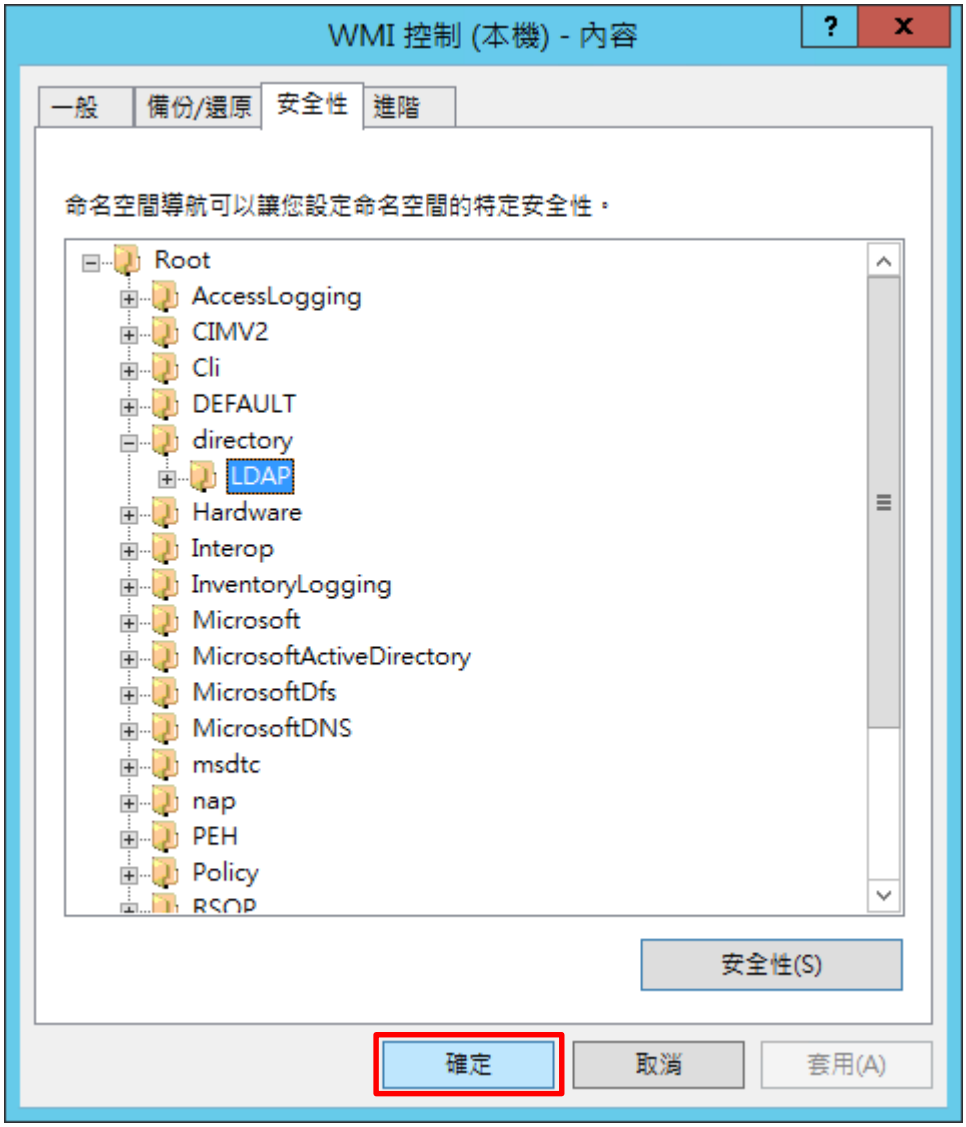
輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

(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]



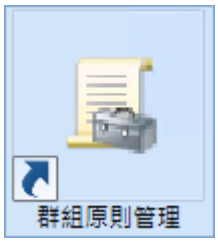
(8) 按 [確定]



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]

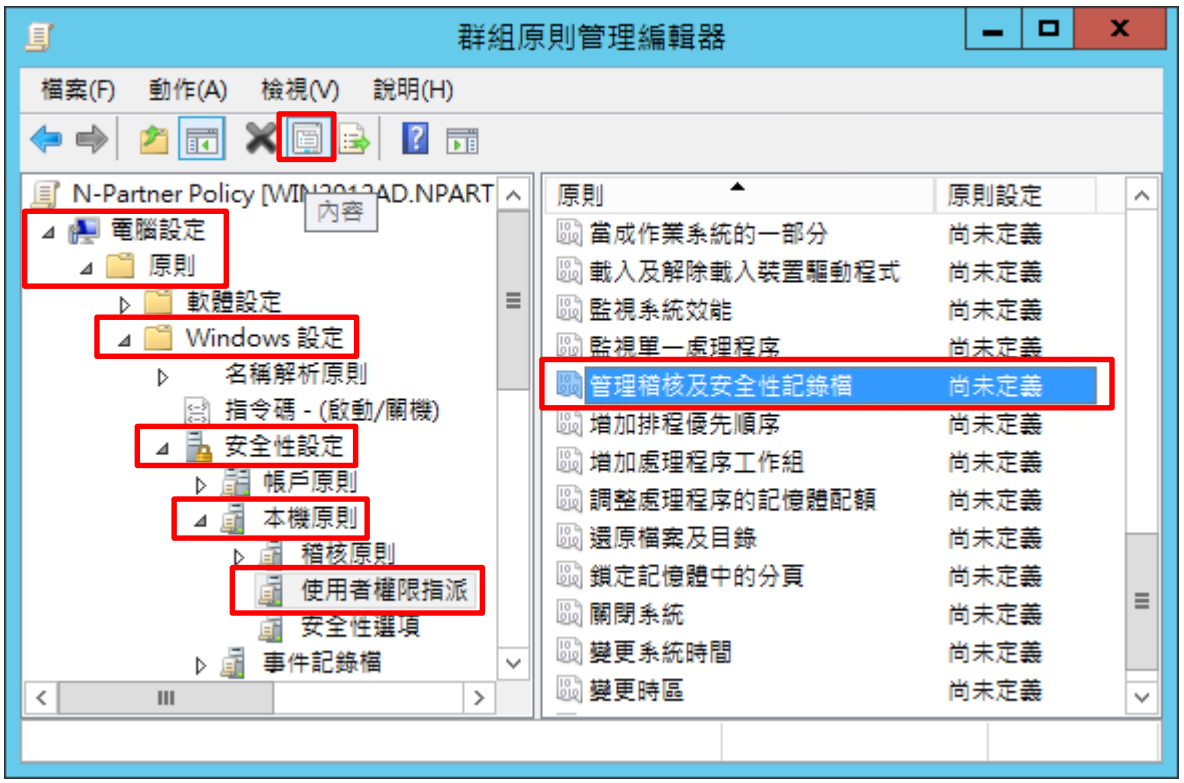


(2) 編輯群組原則物件

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

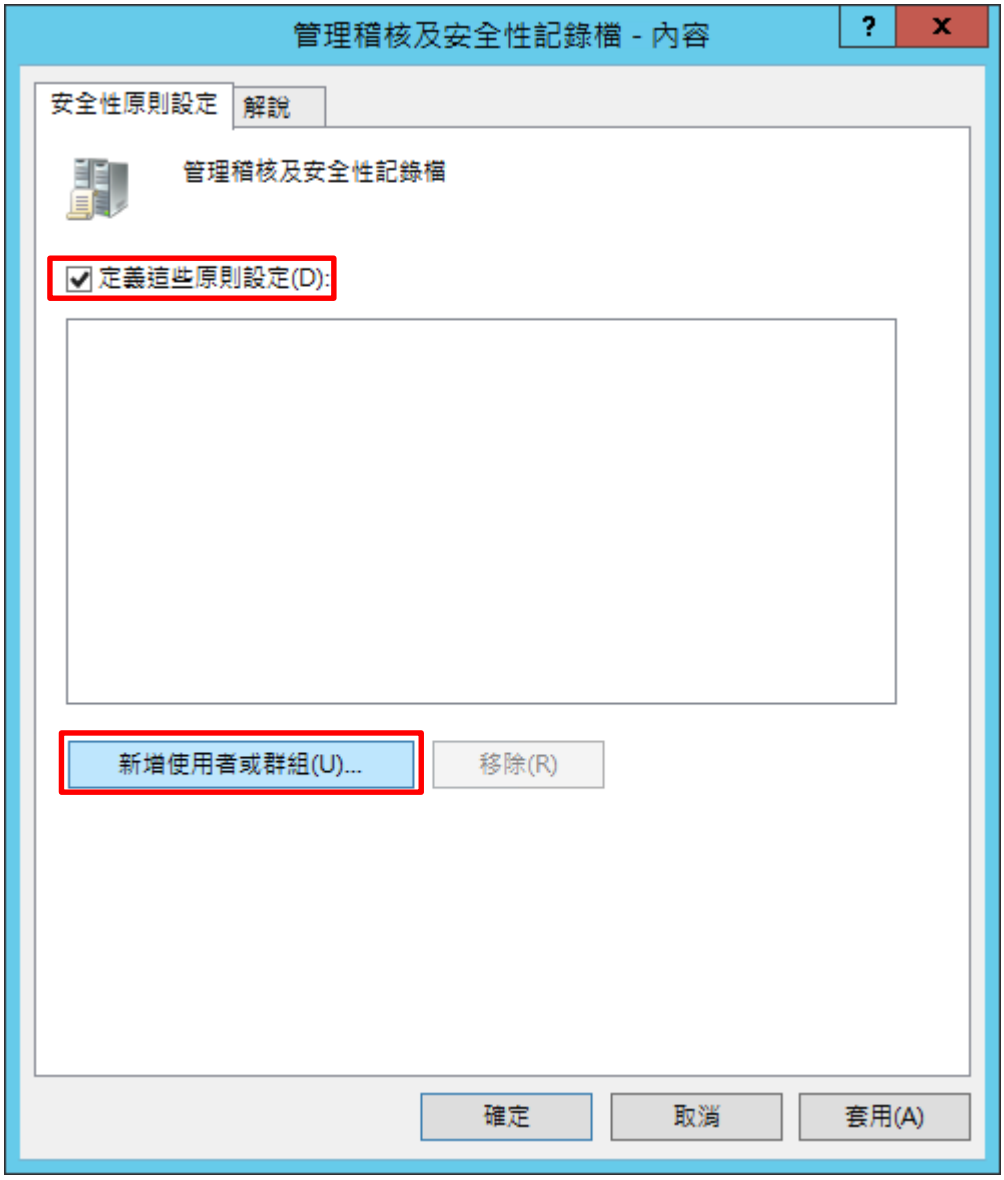
(3) 設定記錄檔

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 [管理稽核及安全性記錄檔] 項目 -> 點選  內容



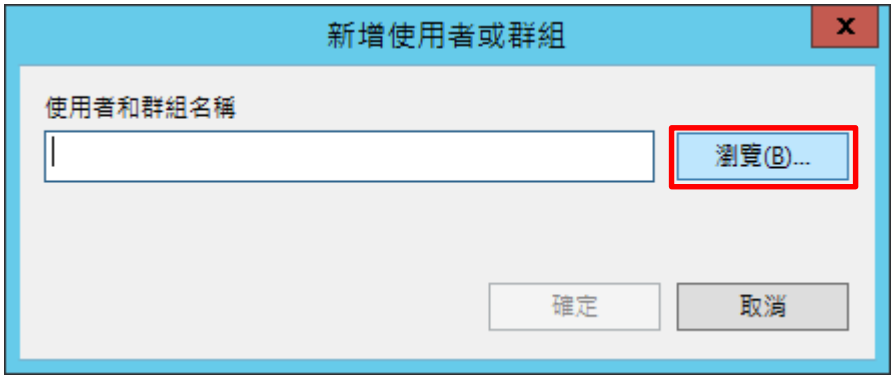
(4) 新增管理稽核使用者

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

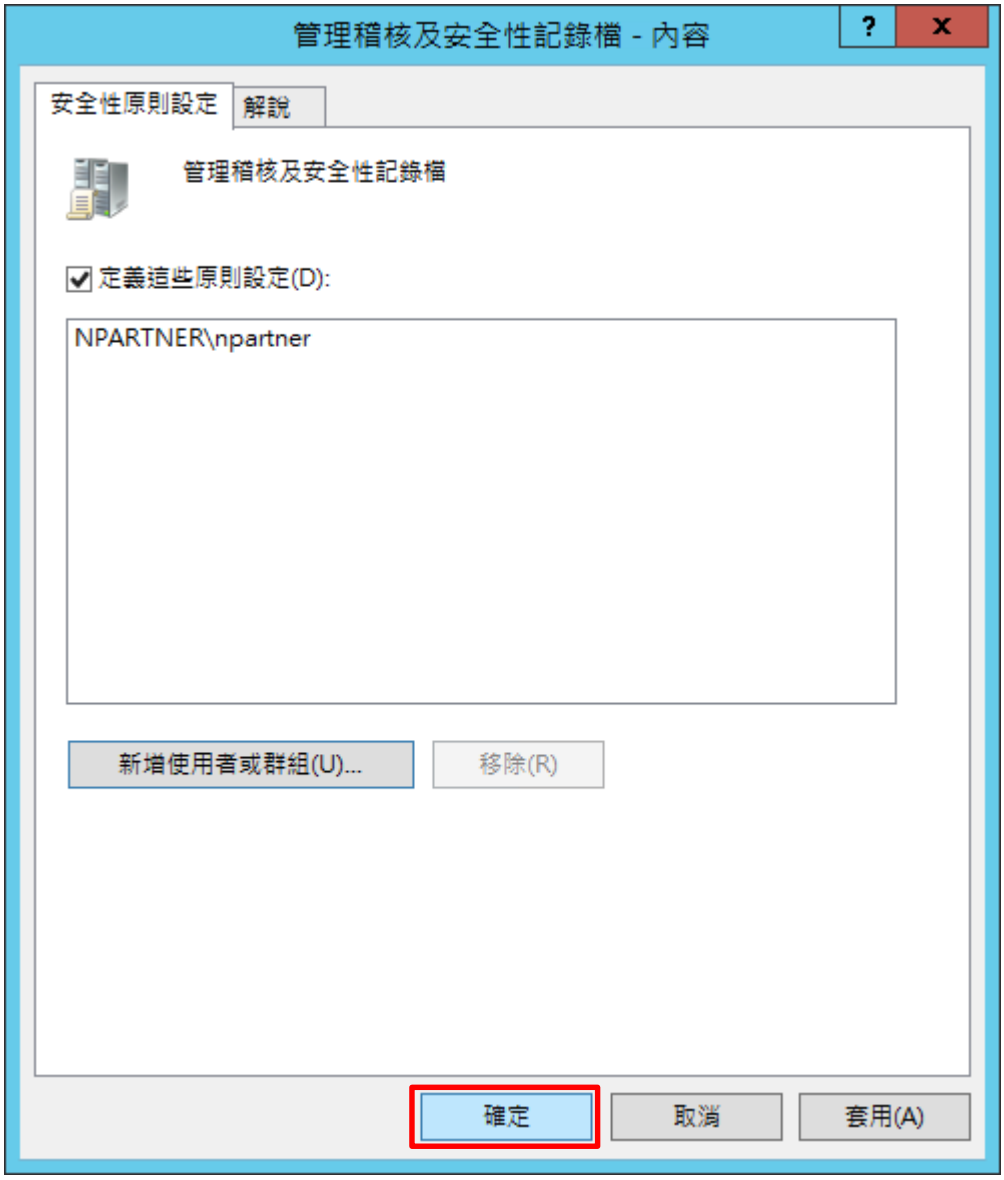
輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

(7) 確定使用者

按 [確定]

(8) 確定設定記錄檔

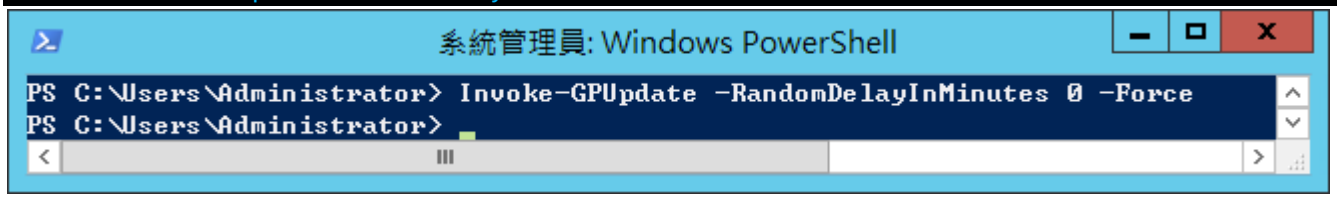
按 [確定]



(9) 開啟 [Windows PowerShell]

(10) 更新群組原則

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

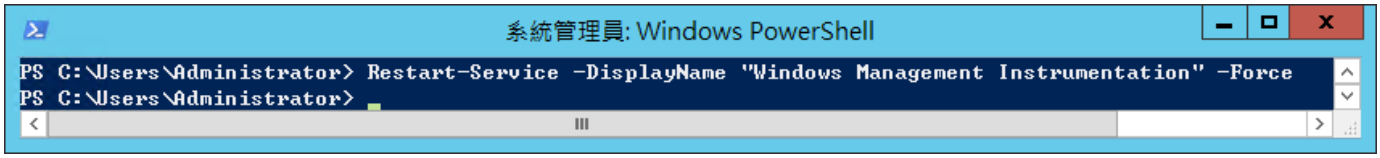


4.3.5 重啟 WMI 服務

(1) 開啟 [Windows PowerShell]

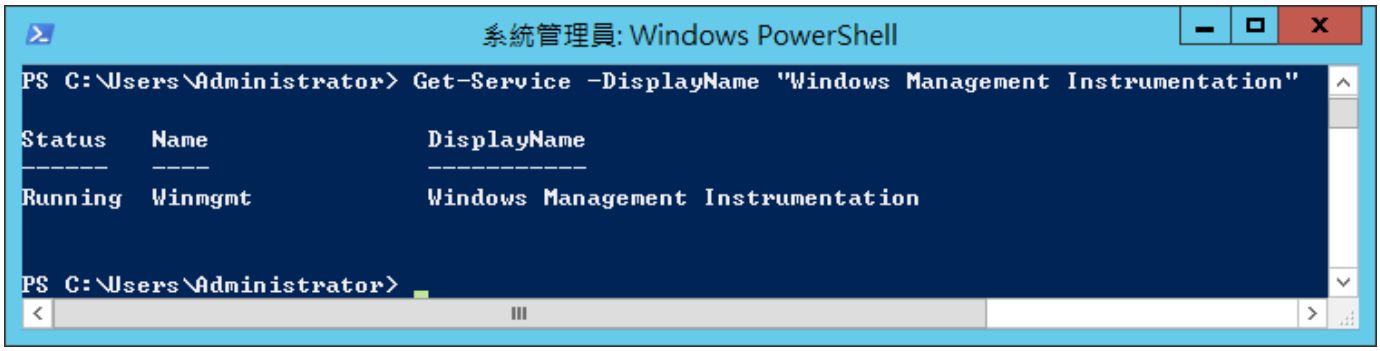
(2) 重啟 WMI 服務

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



(3) 查看 WMI 服務

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

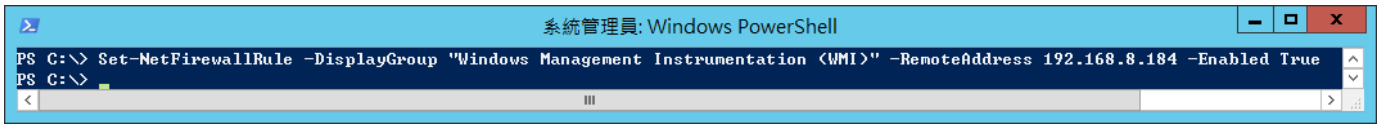


4.4 設定防火牆

(1) 開啟 [Windows PowerShell]

(2) 設定防火牆，只允許 N-Reporter IP query WMI

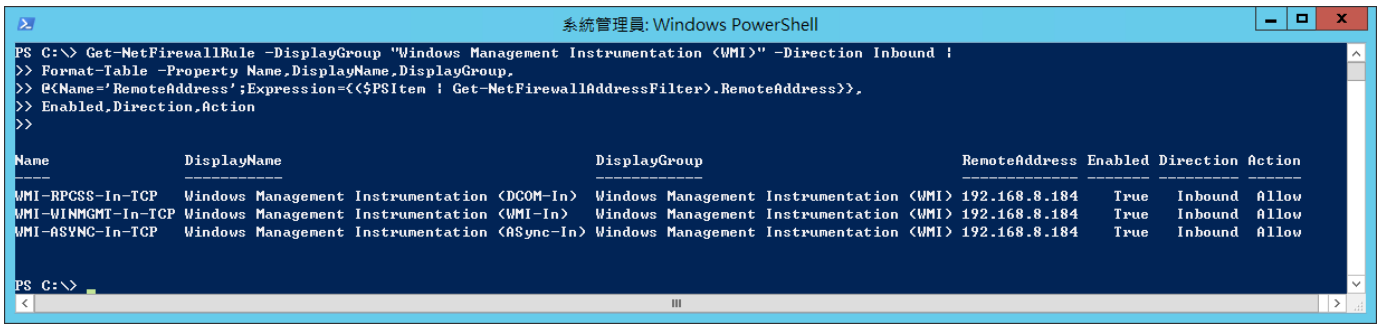
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress
192.168.8.184 -Enabled True
```



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
```

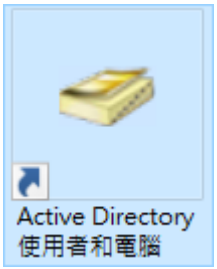


5. Windows 2016

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

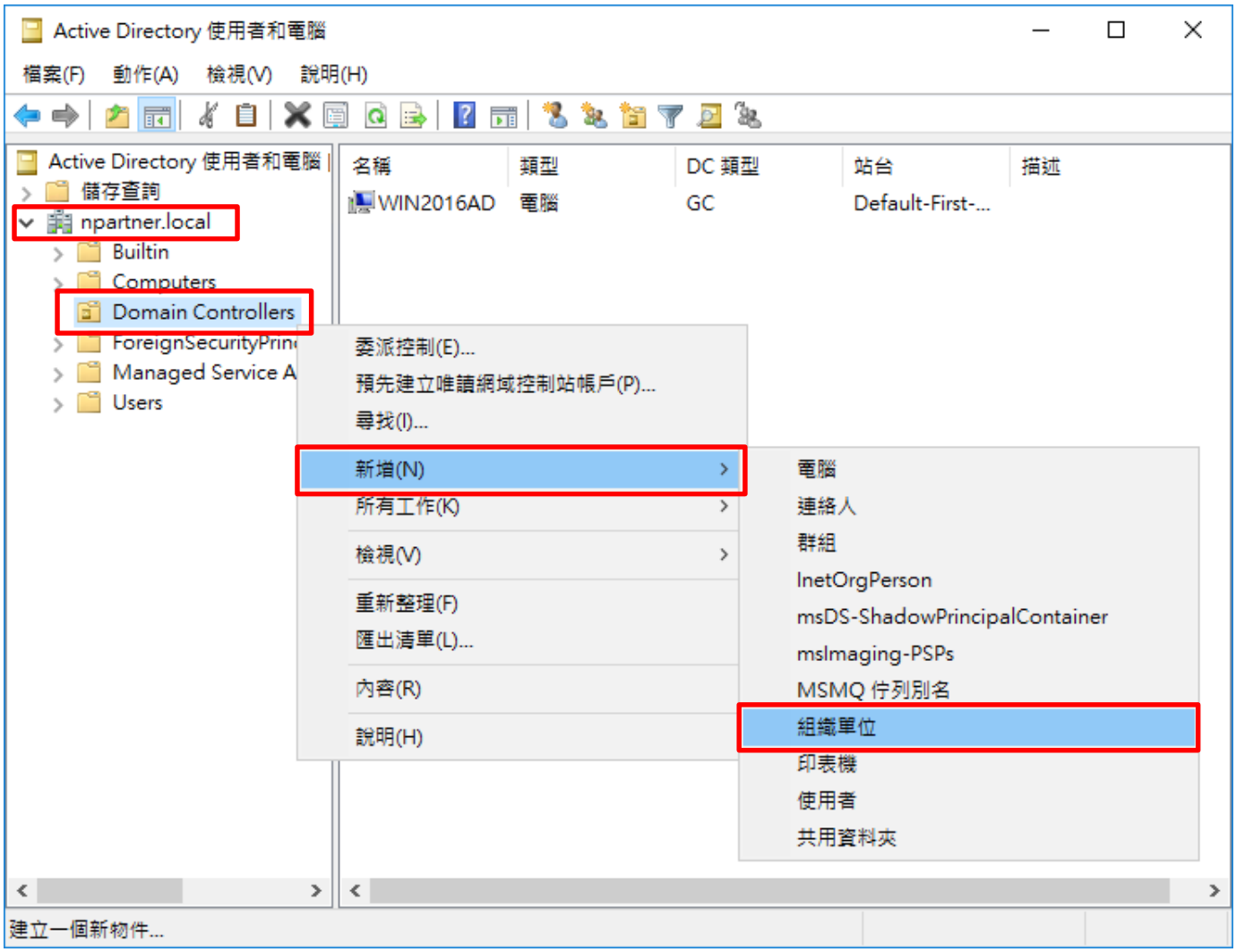
5.1 組織單位設定

(1) 開啟 [Active Directory 使用者和電腦]



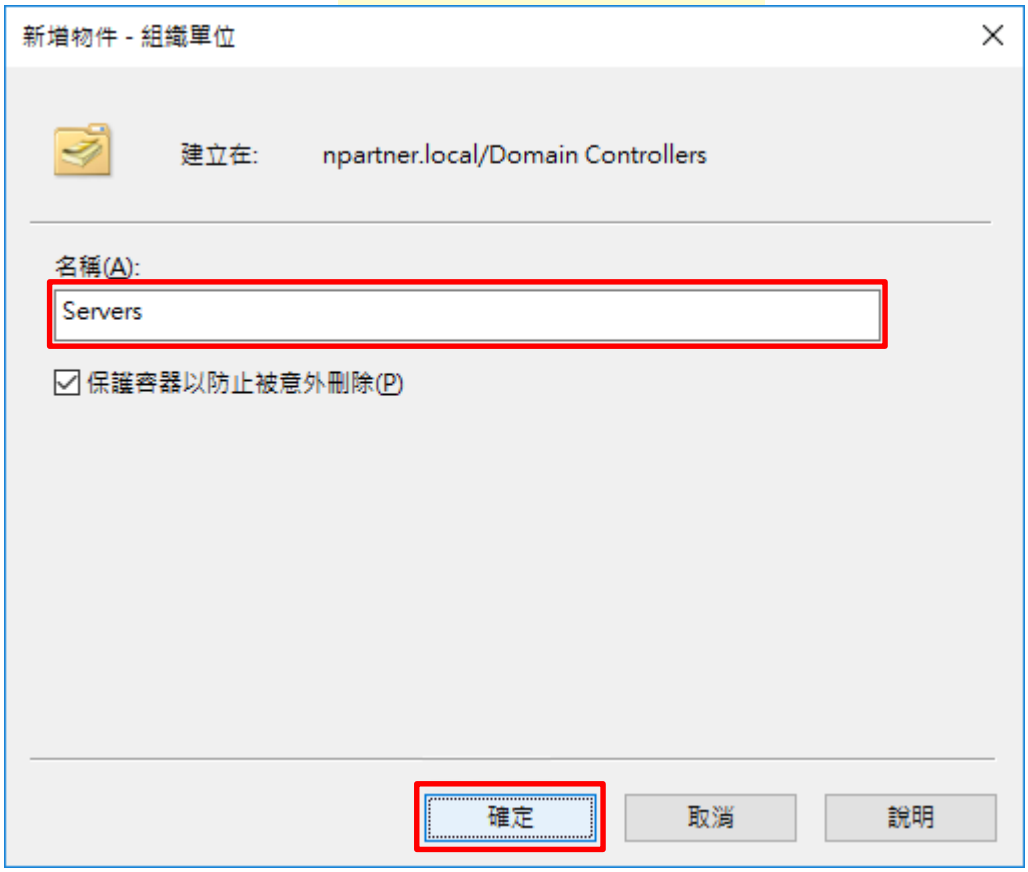
(2) 新增組織單位

[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]



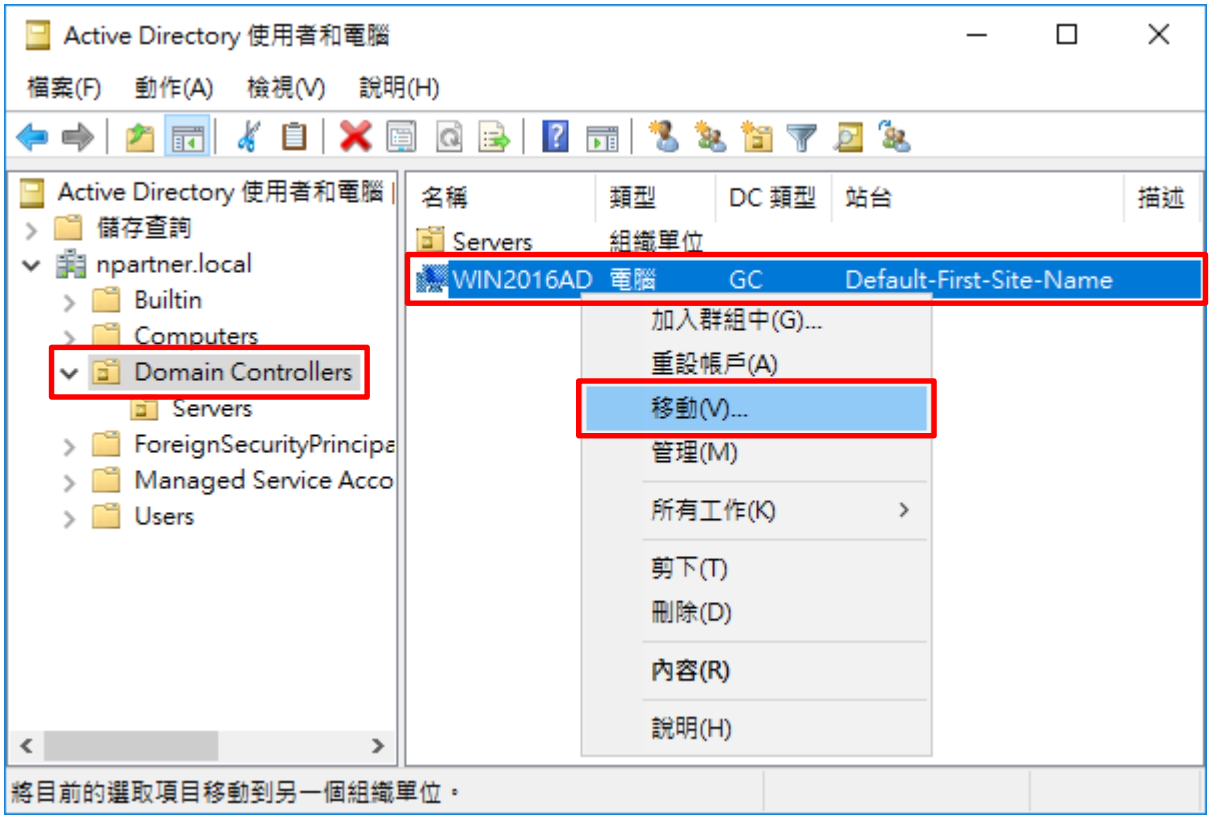
(3) 輸入組織單位名稱

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]



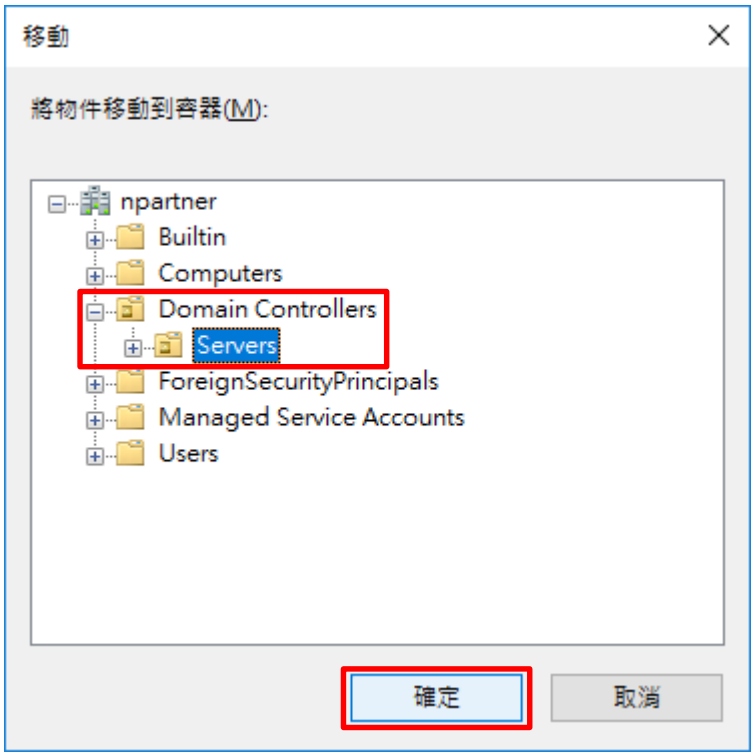
(4) 移動伺服器至新的組織單位

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]



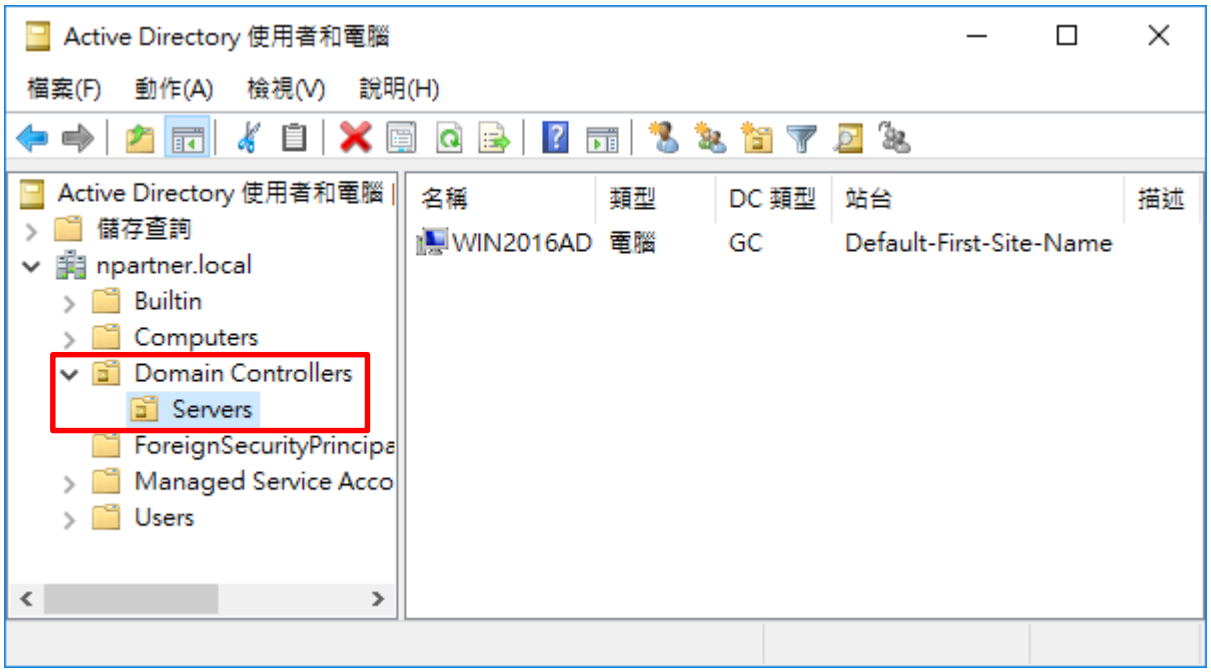
(5) 選擇組織單位

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

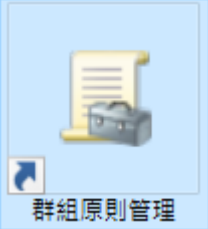
展開 [Domain Controllers] 的 [Servers] 組織單位，確認 [Win2016AD] 伺服器已移動



5.2 群組原則設定

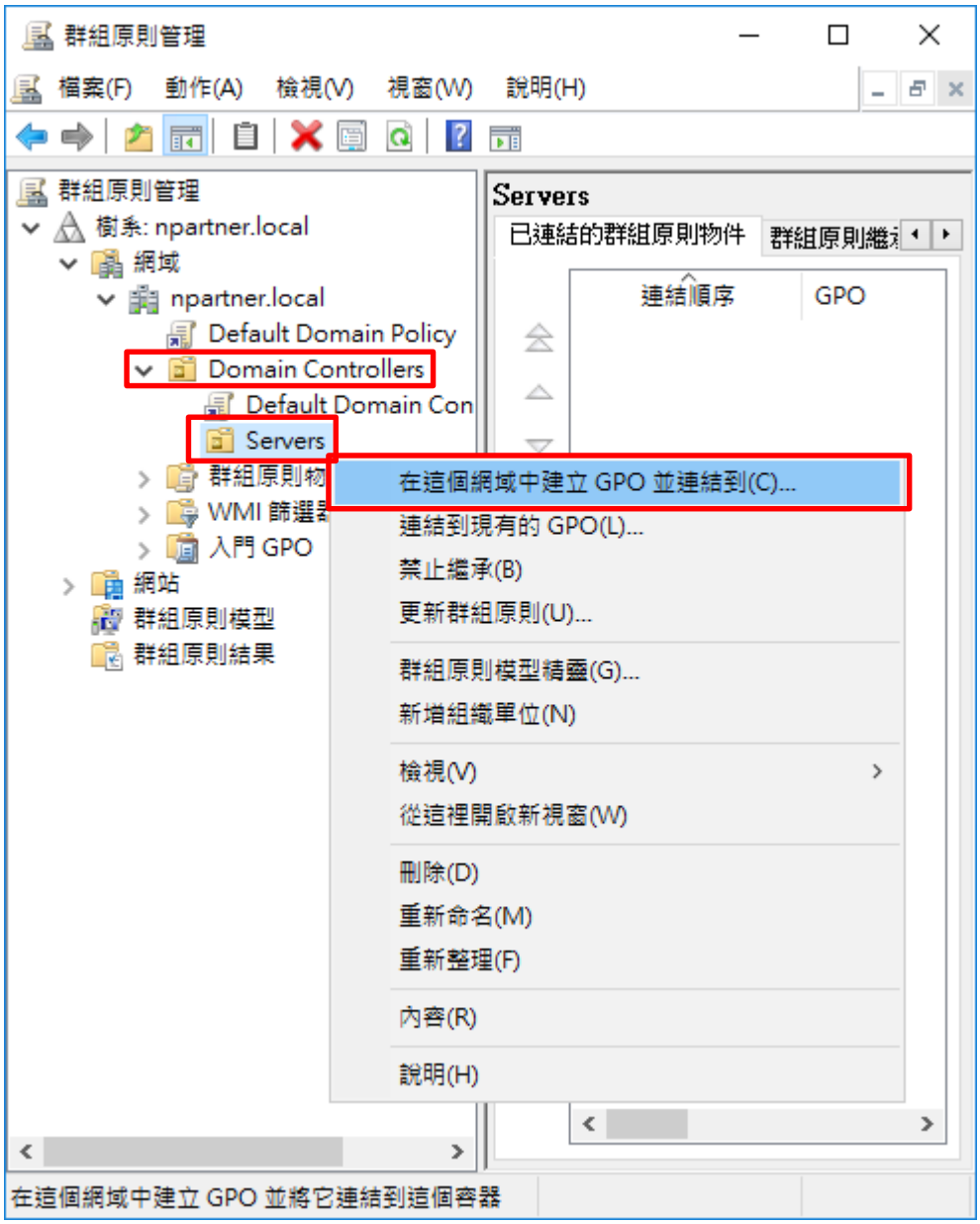
(1) 開啟群組原則管理

開啟 [群組原則管理]



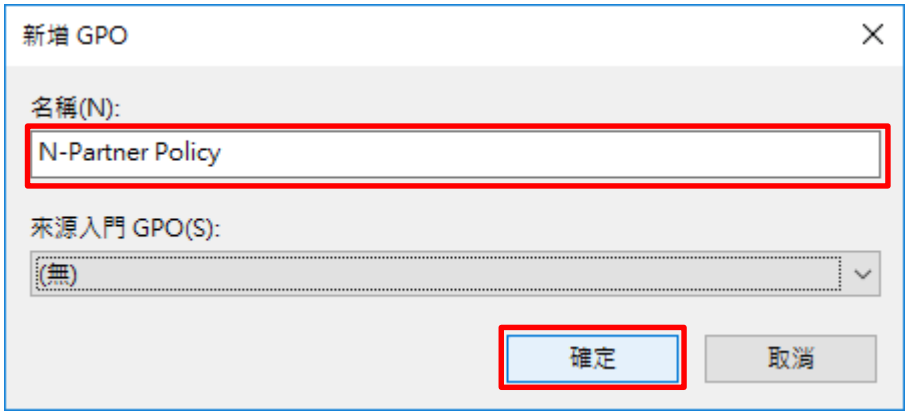
(2) 在 Servers 組織單位，新增群組原則物件

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...]



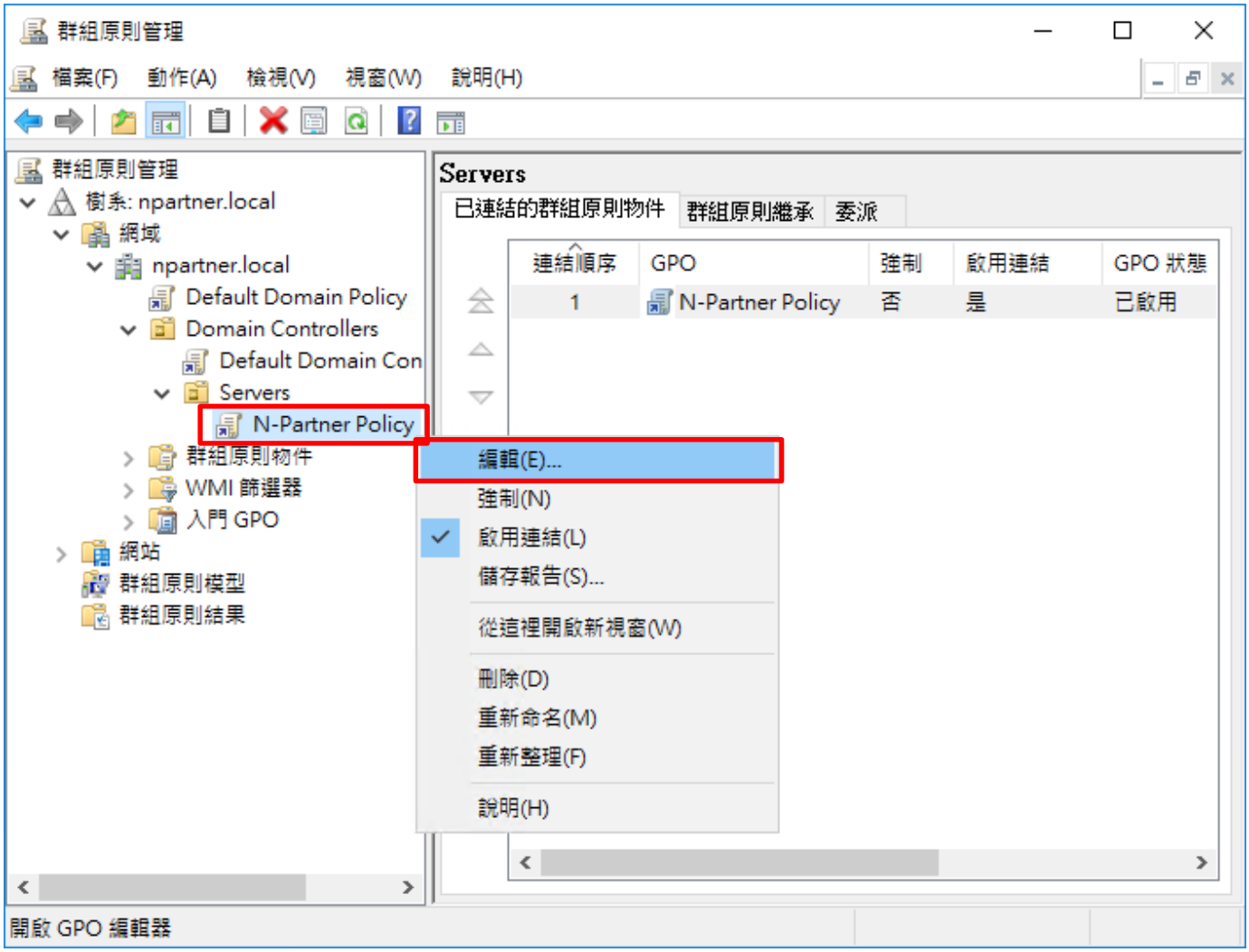
(3) 輸入群組原則物件名稱

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]



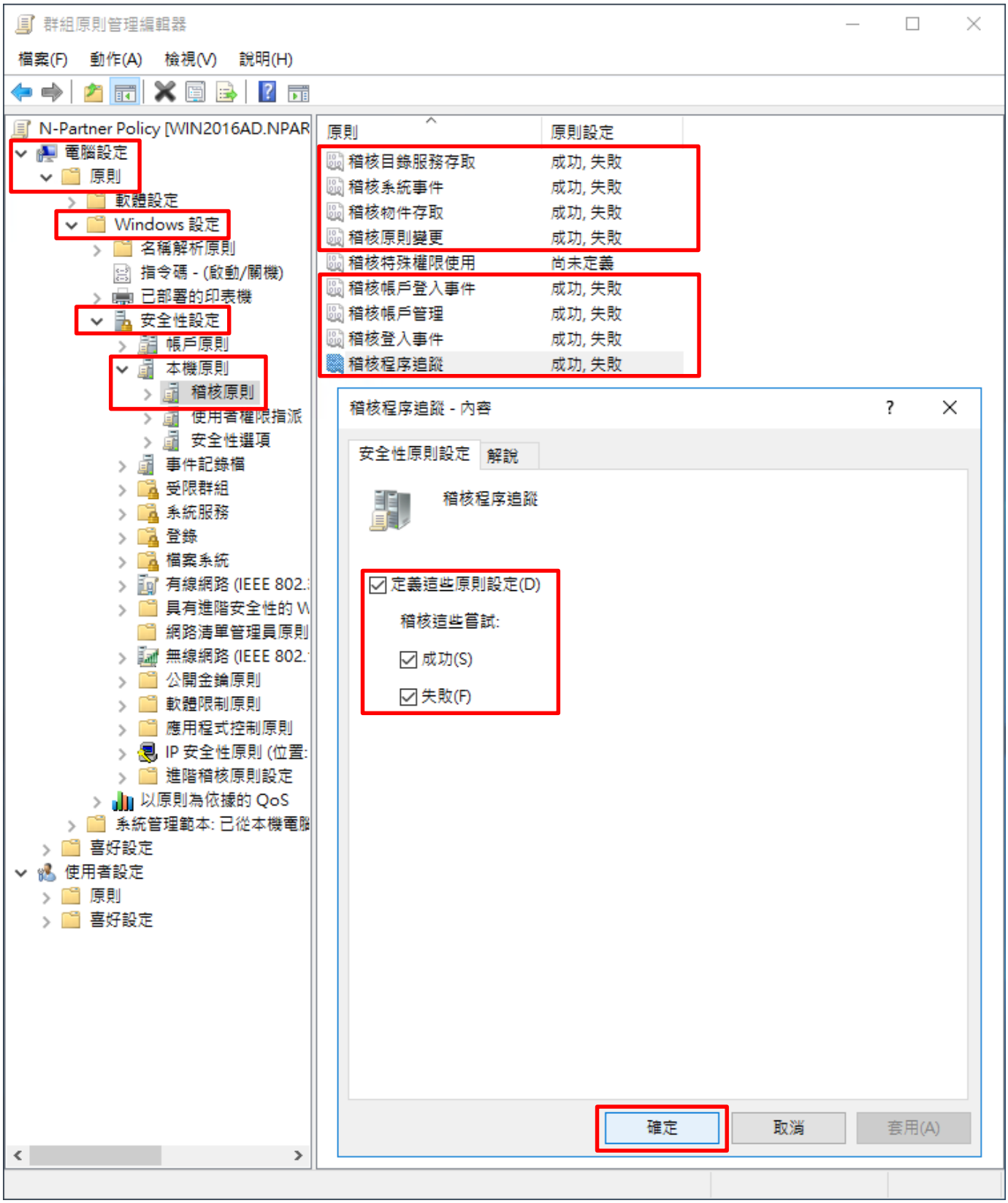
(4) 編輯群組原則物件

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



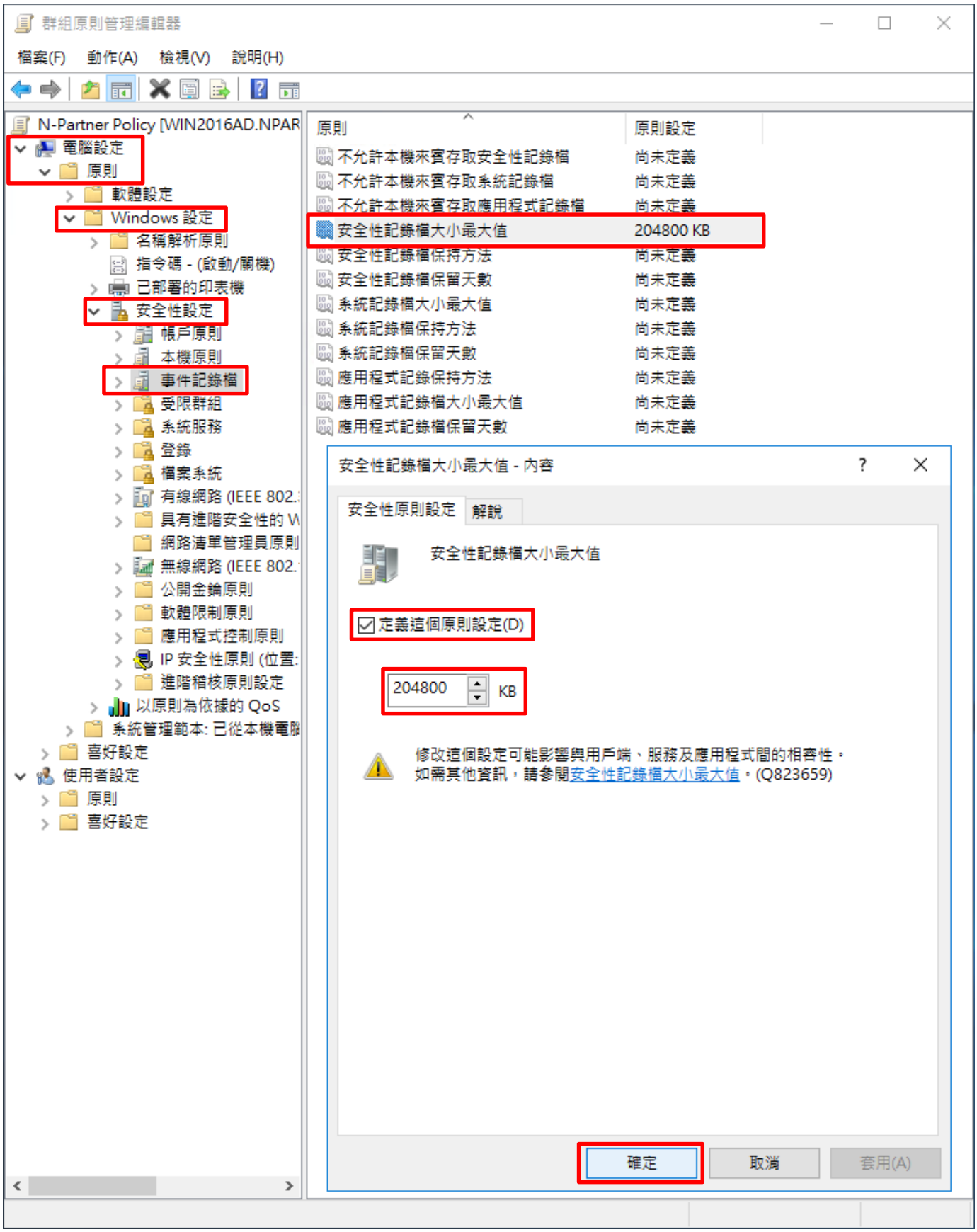
(5) 本機原則：稽核原則

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]



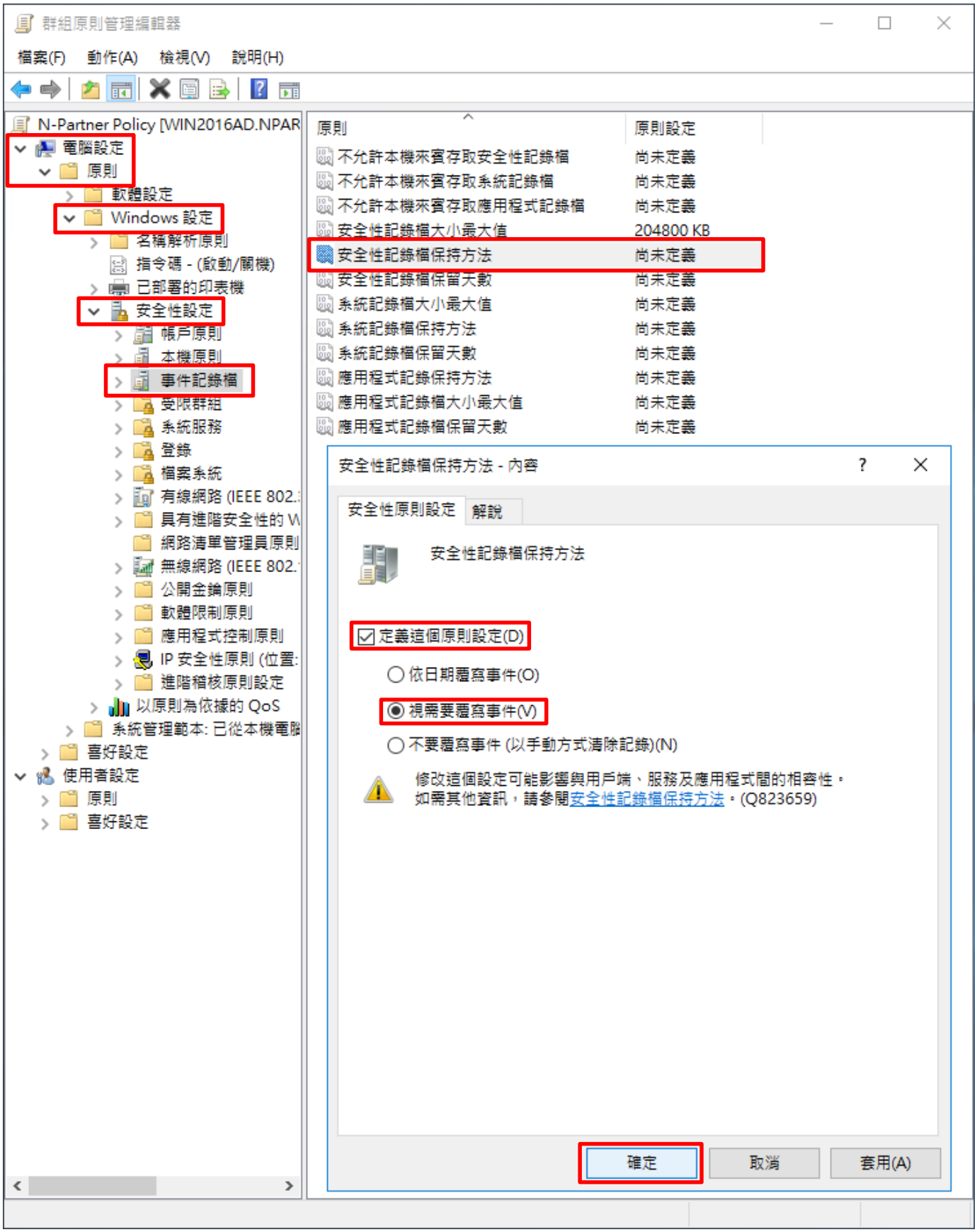
(6) 事件記錄：安全性記錄檔大小最大值

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]

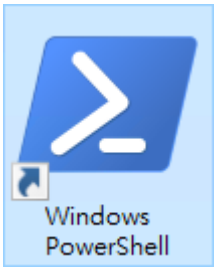


(7) 事件記錄：安全性記錄檔大小最大值

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]

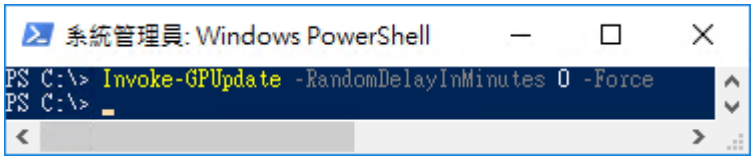


(8) 開啟 [Windows PowerShell]



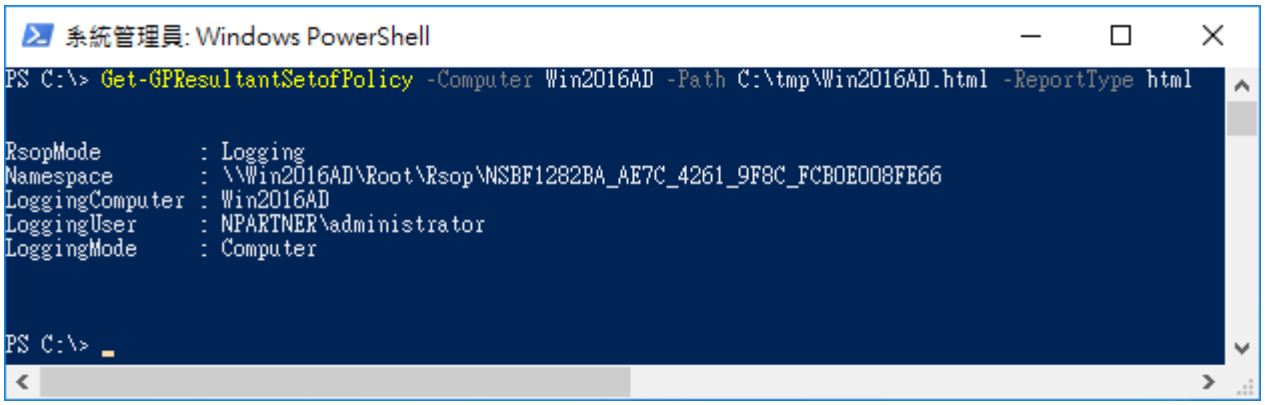
(9) 更新群組原則

```
PS C:\> Invoke-GPUpdate -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

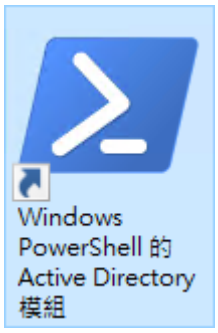
(11) 開啟報表，確認 Windows 2016 AD 伺服器，套用 N-Partner Policy 群組原則

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]



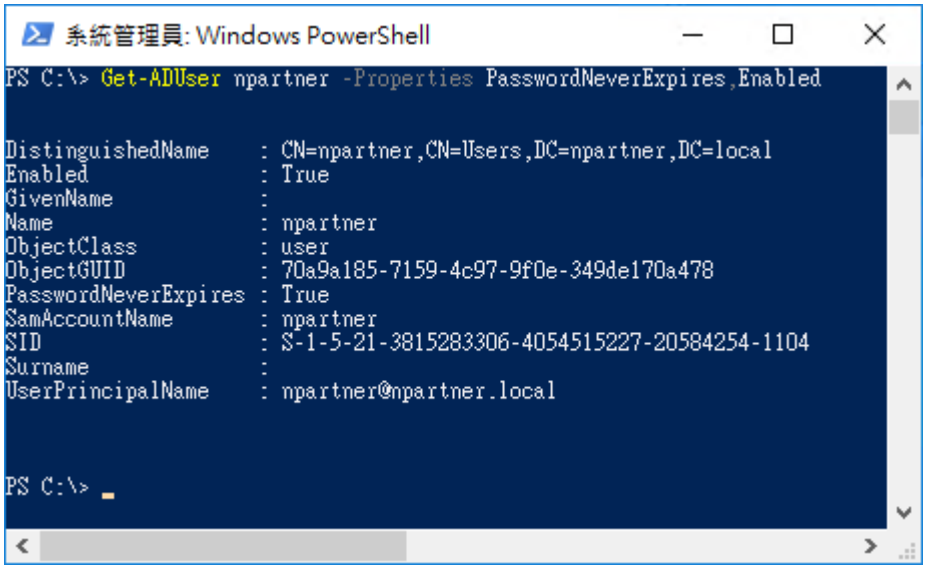
(2) 新增帳號

```
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
```

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
```

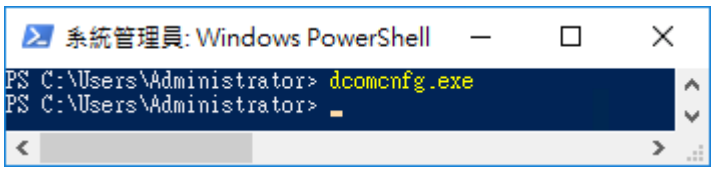


5.3.2 設定 DCOM 權限

(1) 開啟 [Windows PowerShell]

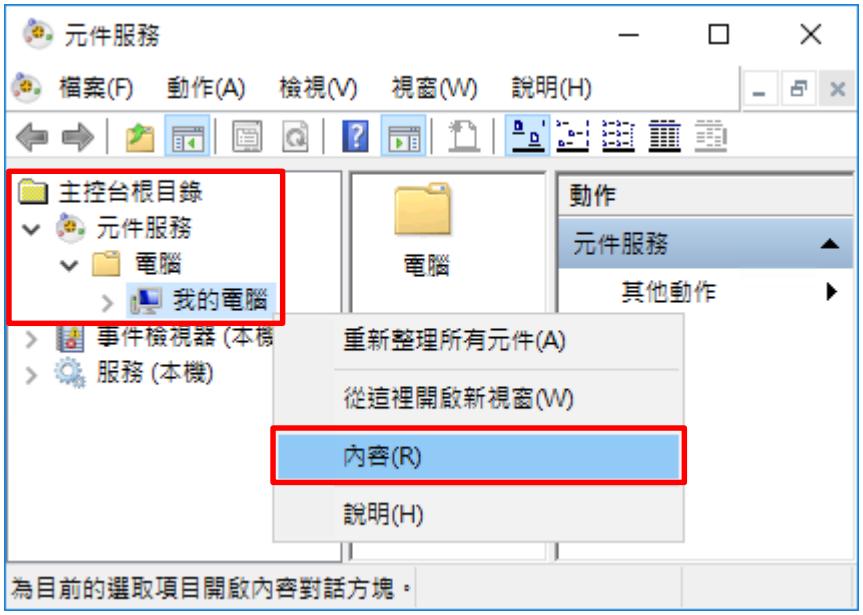
(2) 開啟元件服務

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



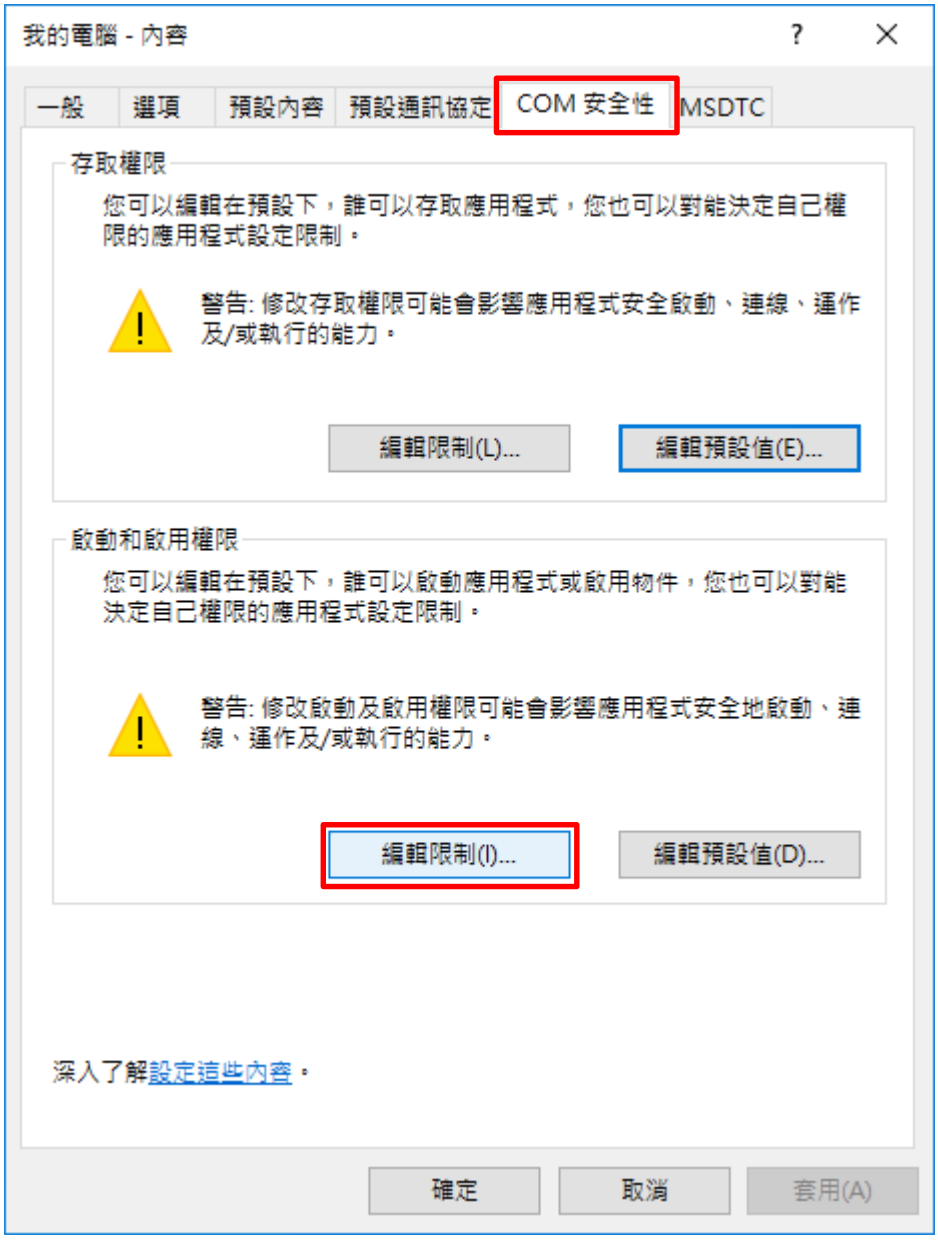
(3) 編輯電腦內容

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]



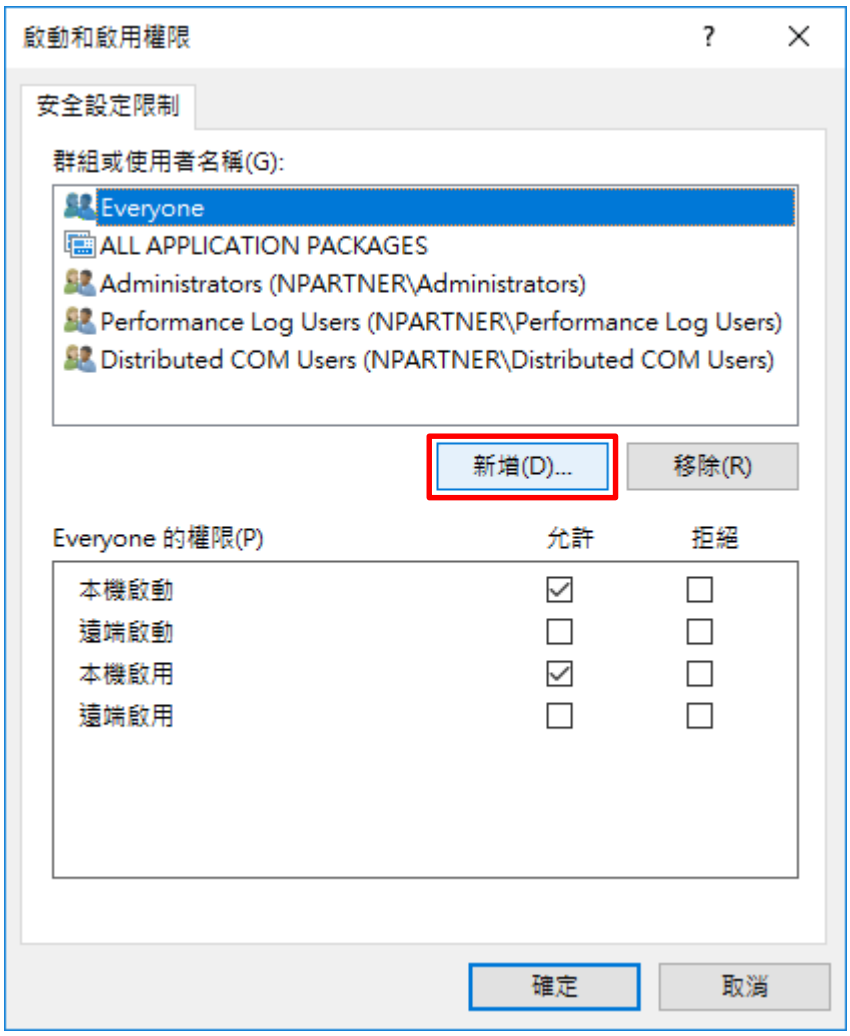
(4) 啟用權限

點選 [COM 安全性] 頁面 -> 啟動和啟用權限，按 [編輯限制]



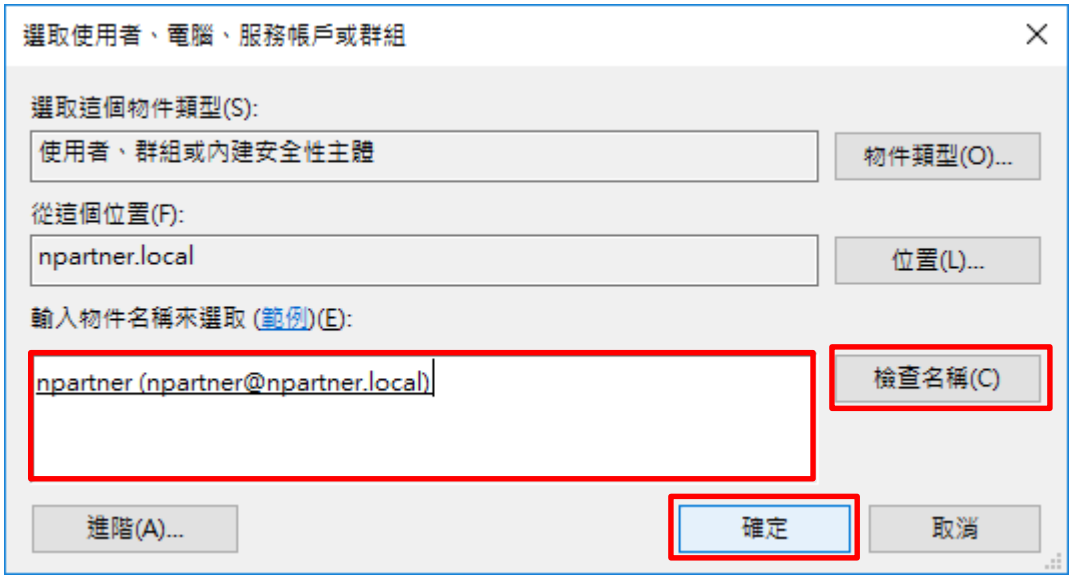
(5) 新增 DCOM 使用者權限

點選 [新增]



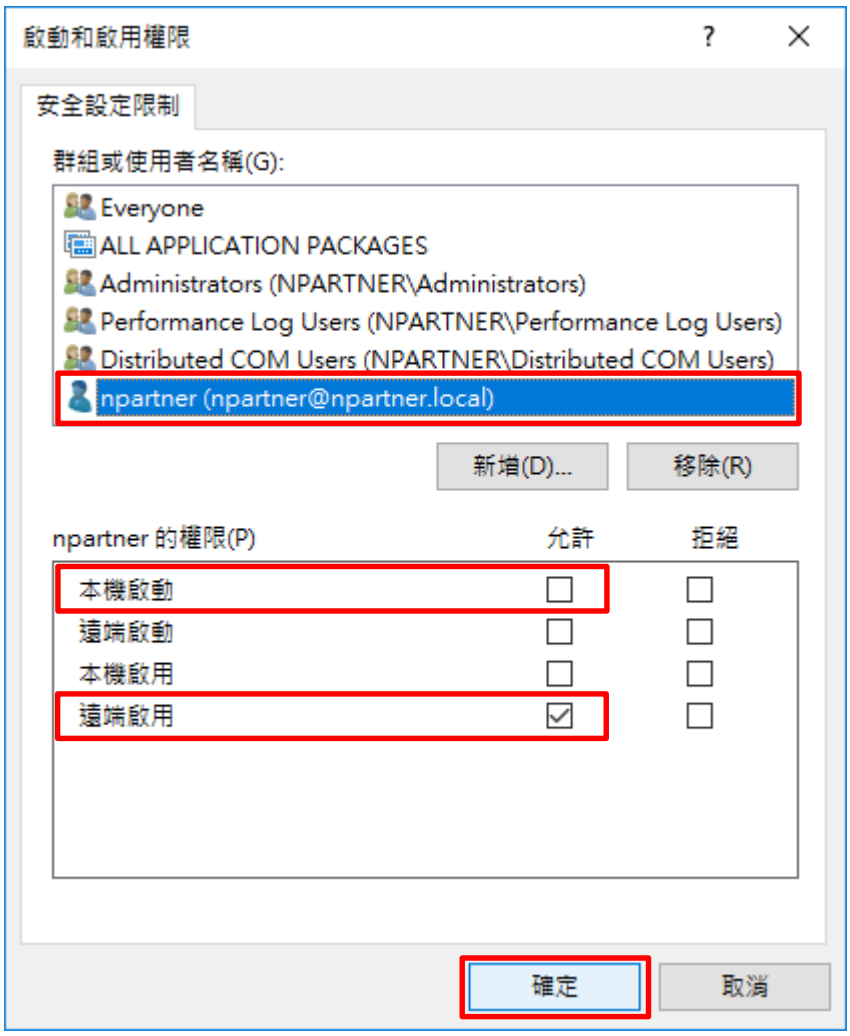
(6) 輸入使用者

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]

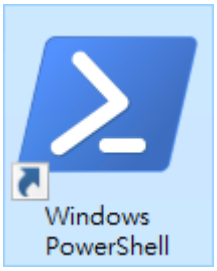


(8) 按 [確定]

5.3.3 設定 WMI 權限

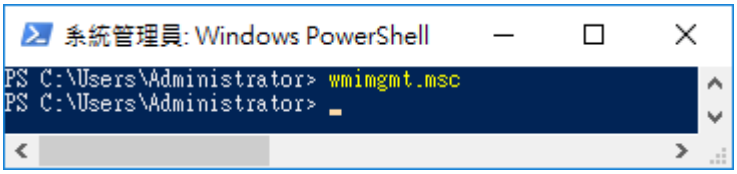
5.3.3.1 設定事件日誌權限

(1) 開啟 [Windows PowerShell]



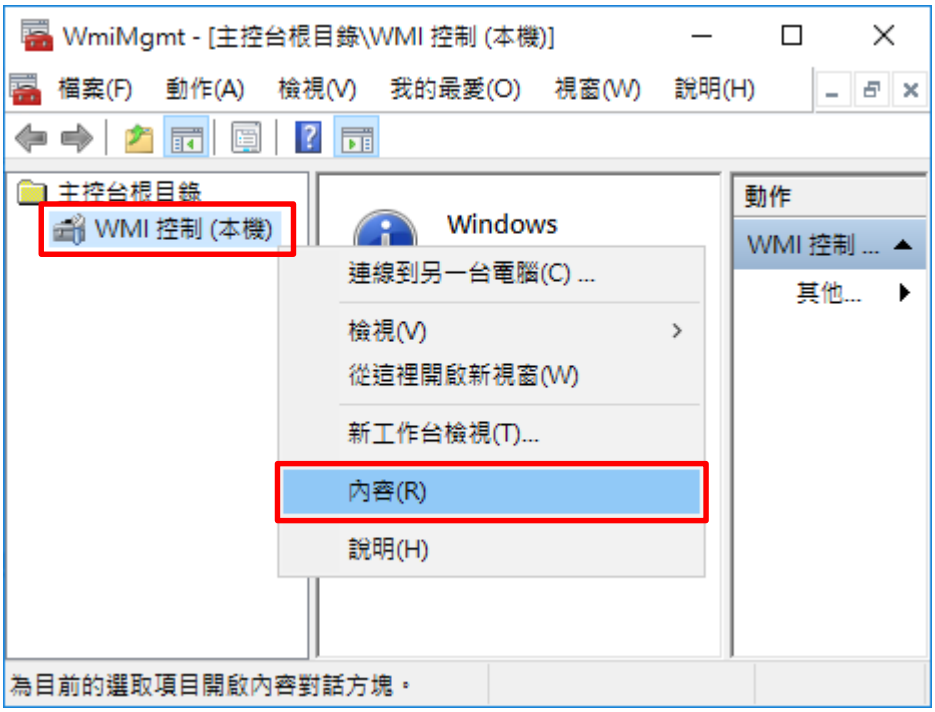
(2) 開啟元件服務

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



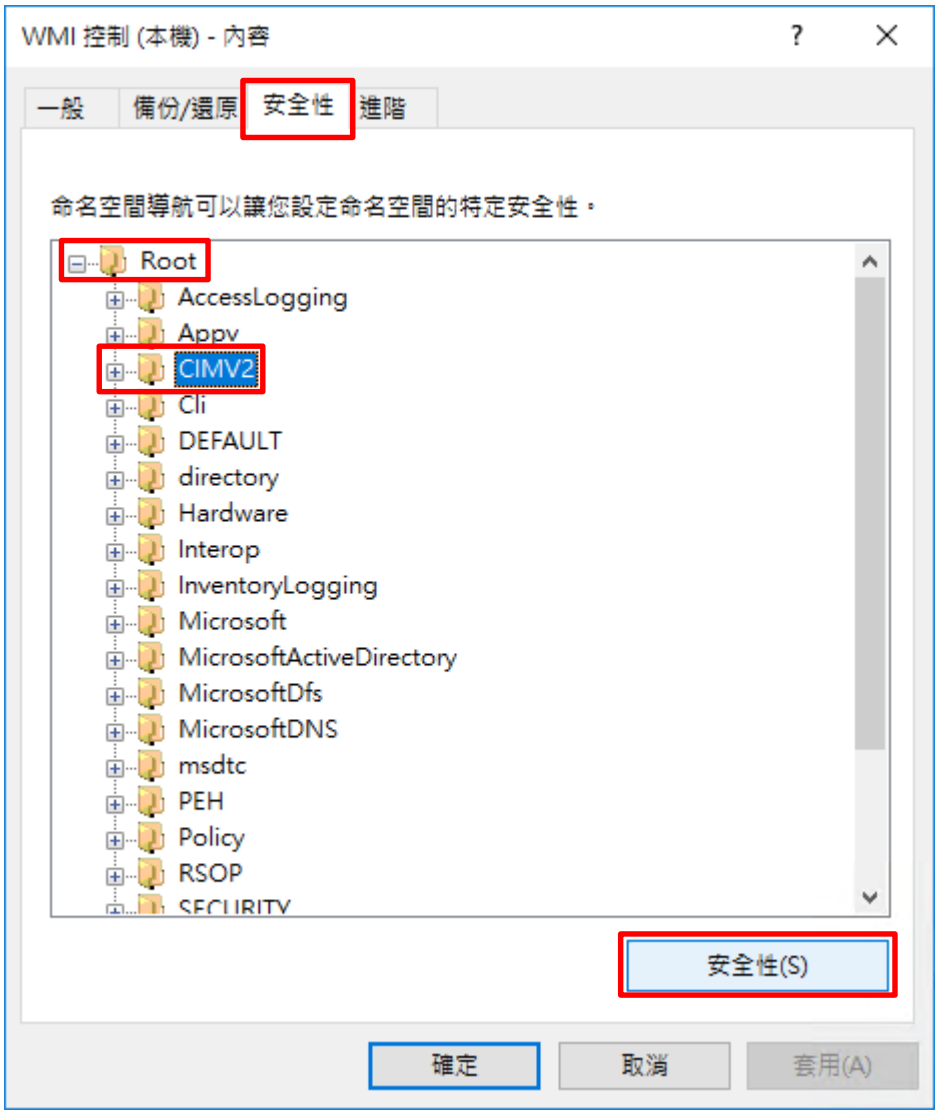
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



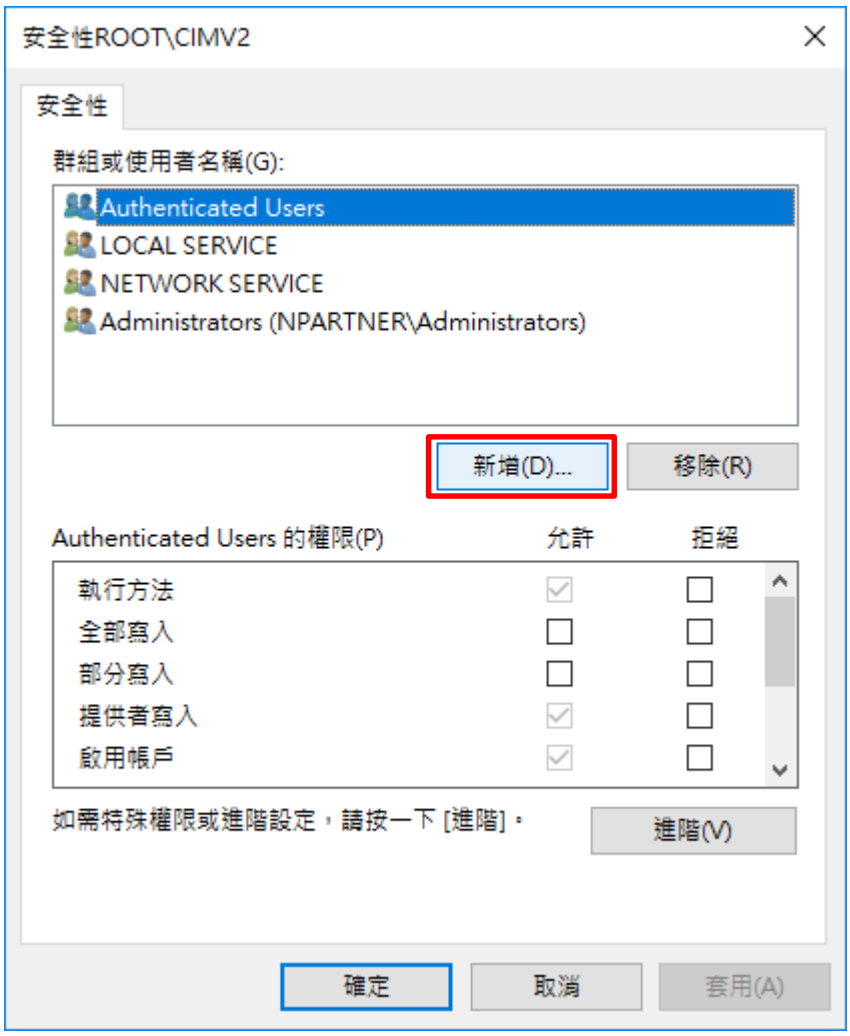
(4) 編輯 CIMV2 安全性

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



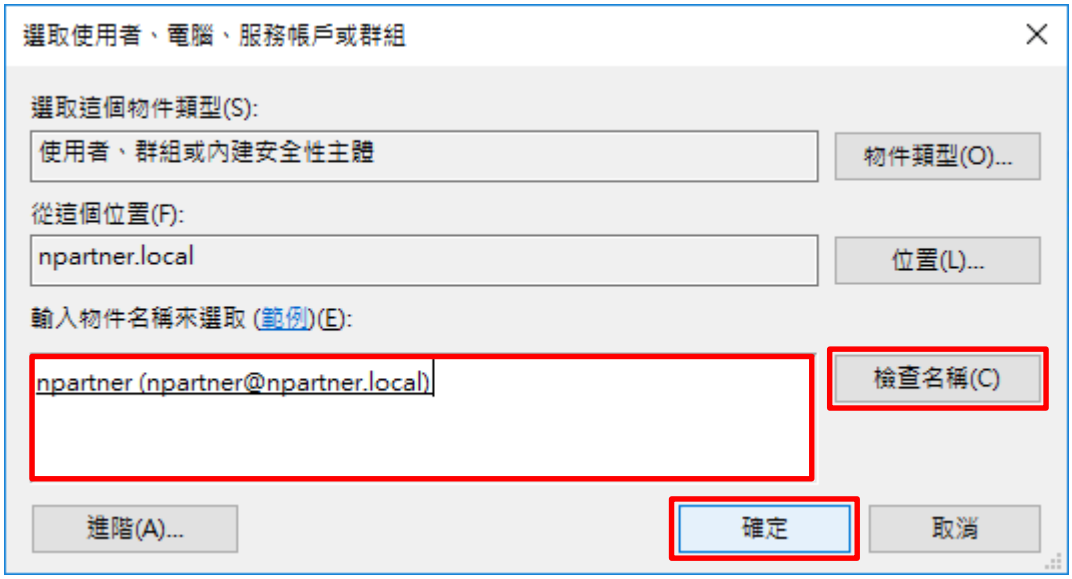
(5) 新增 WMI 使用者權限

按 [新增]



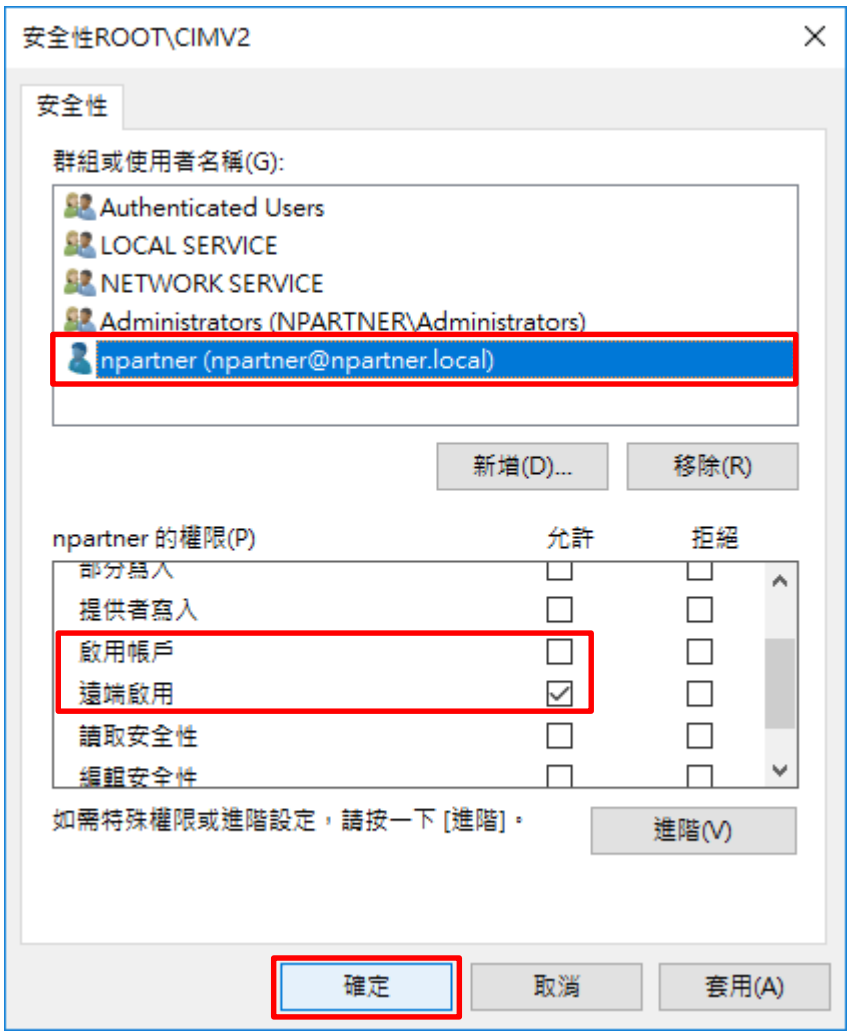
(6) 輸入使用者

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

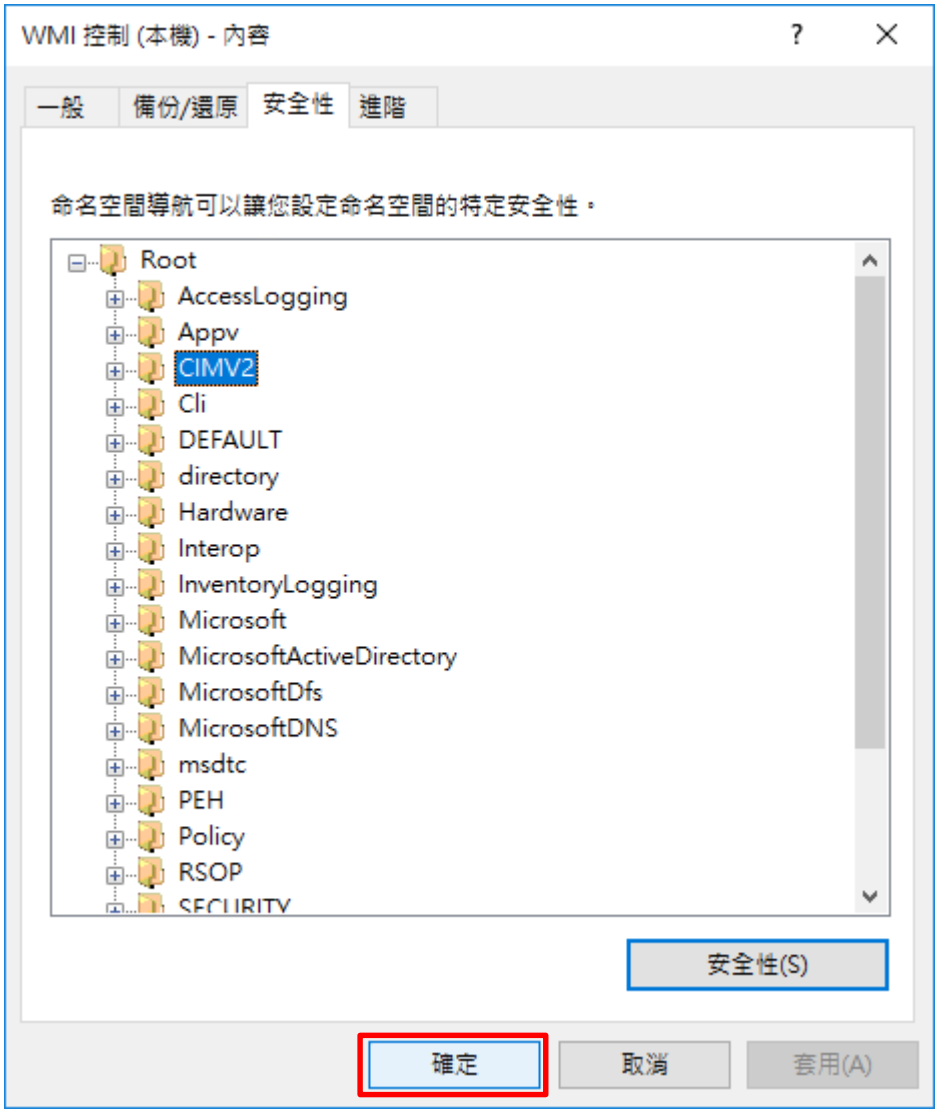


(7) 設定使用者權限

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]

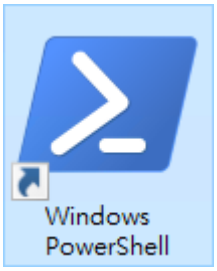


(8) 按 [確定]



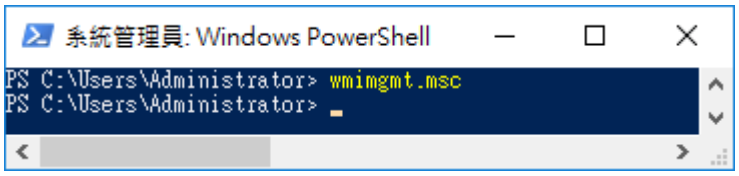
5.3.3.2 設定讀取使用者資料權限

(1) 開啟 [Windows PowerShell]



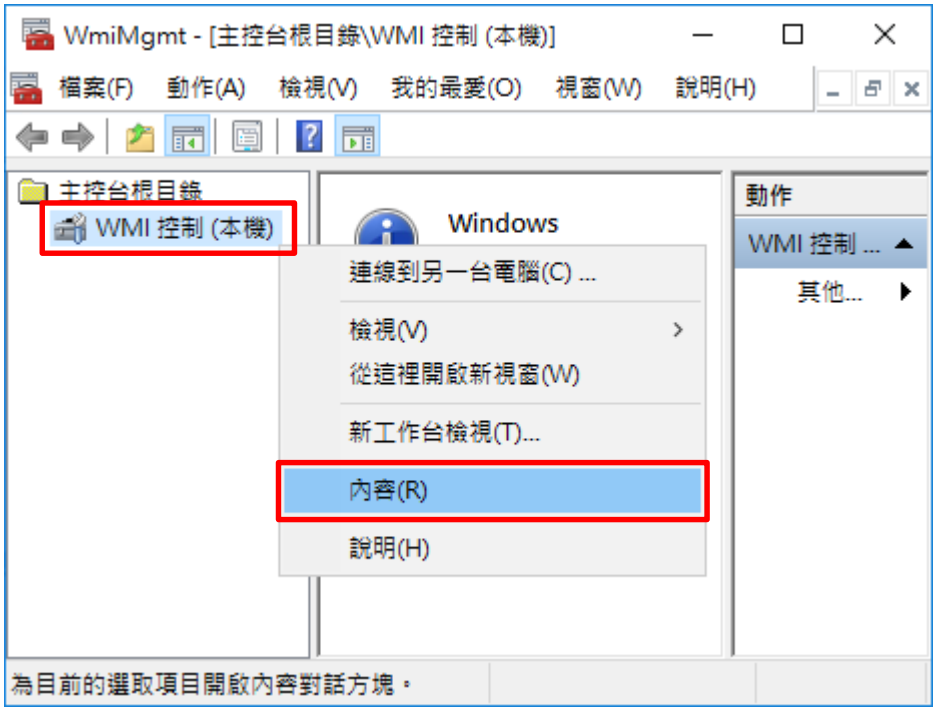
(2) 開啟元件服務

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



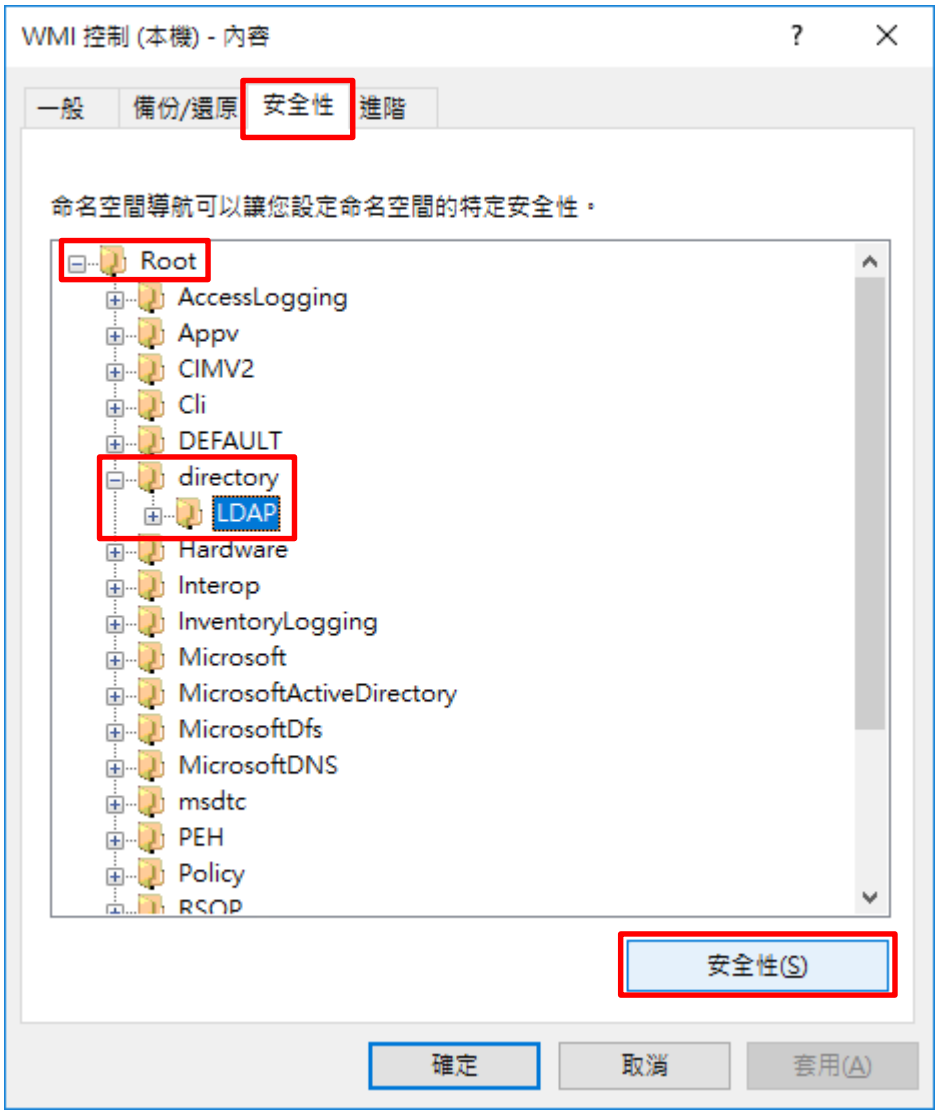
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



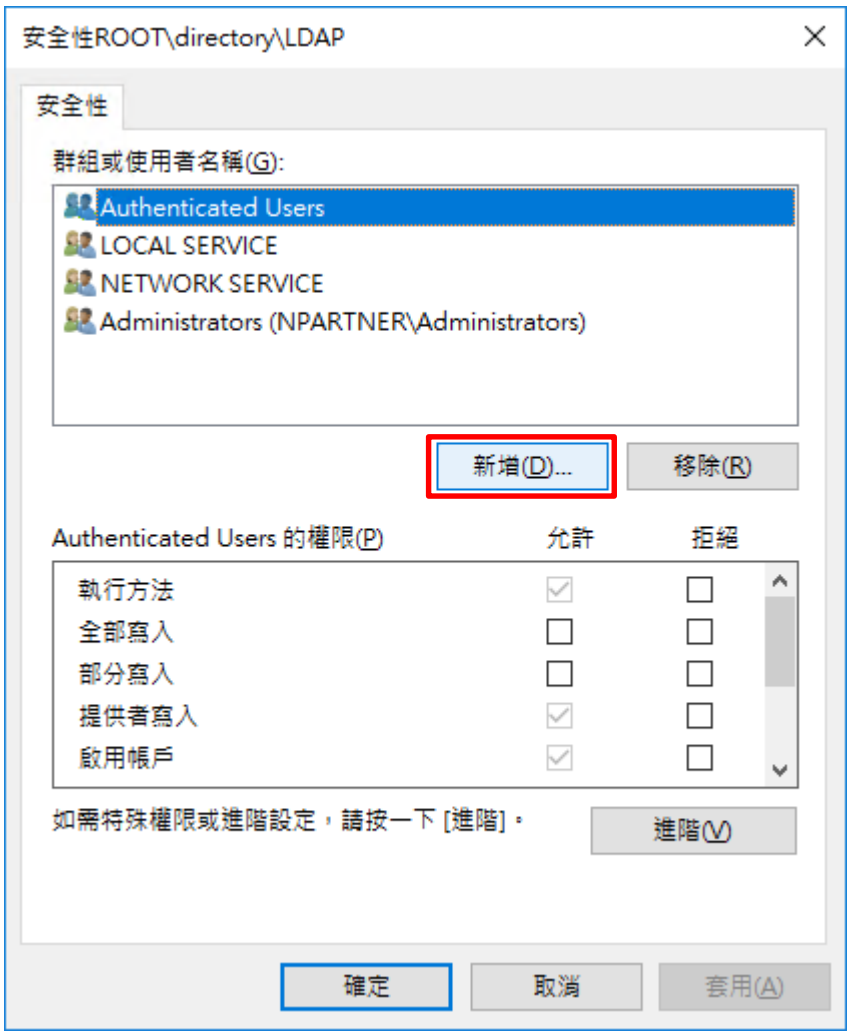
(4) 編輯 LDAP 安全性

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



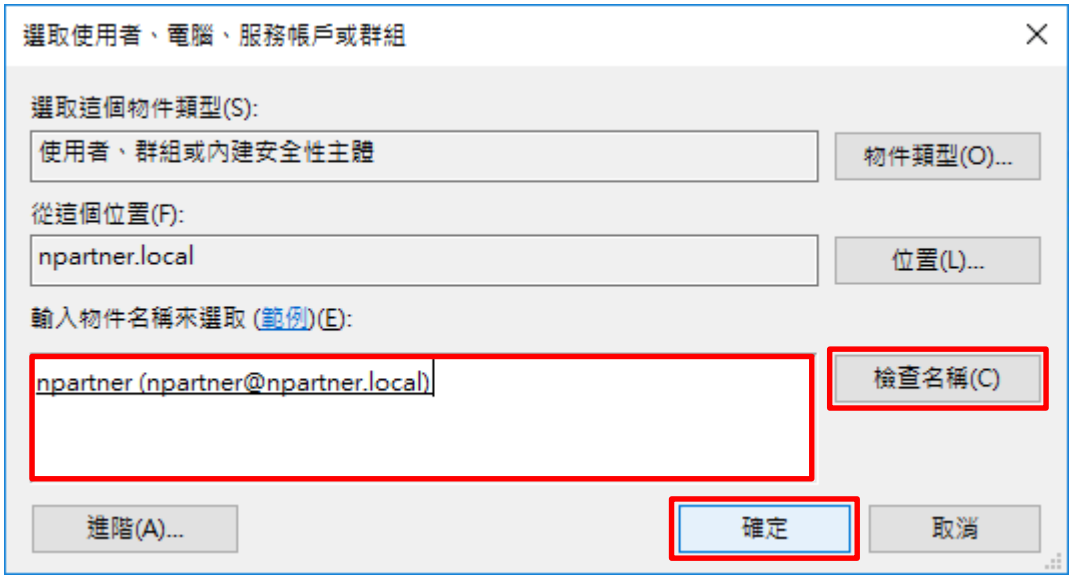
(5) 新增 WMI 使用者權限

按 [新增]



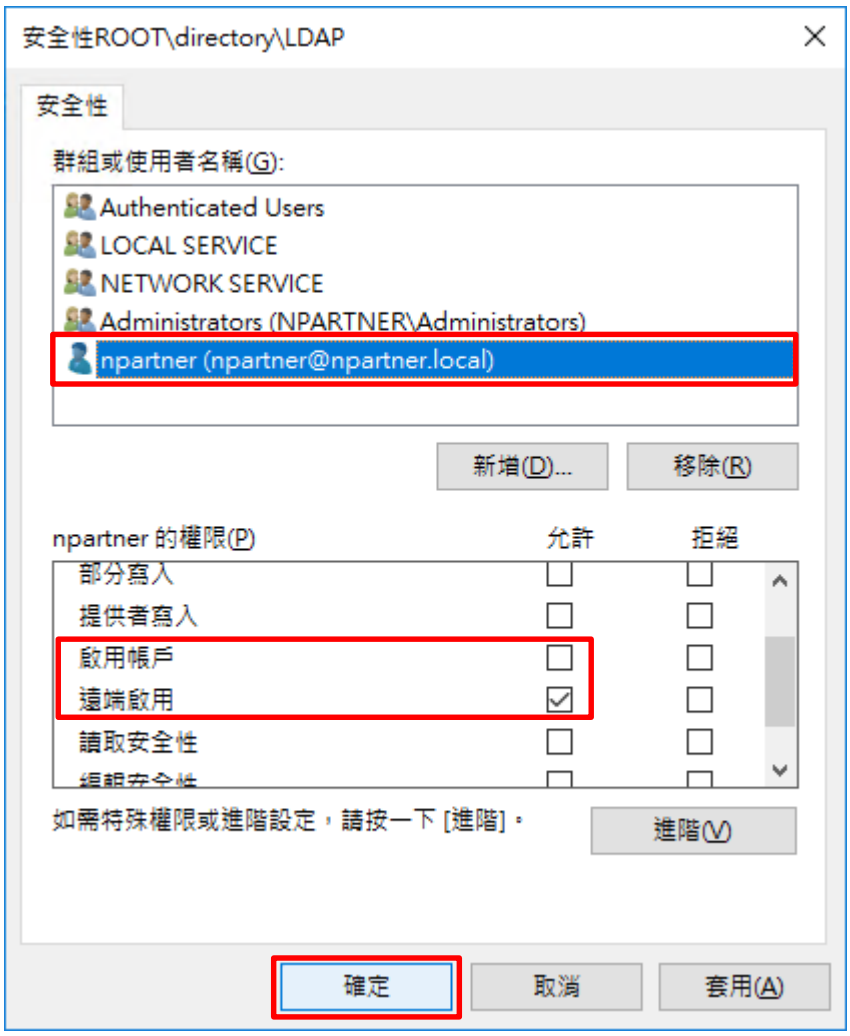
(6) 輸入使用者

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

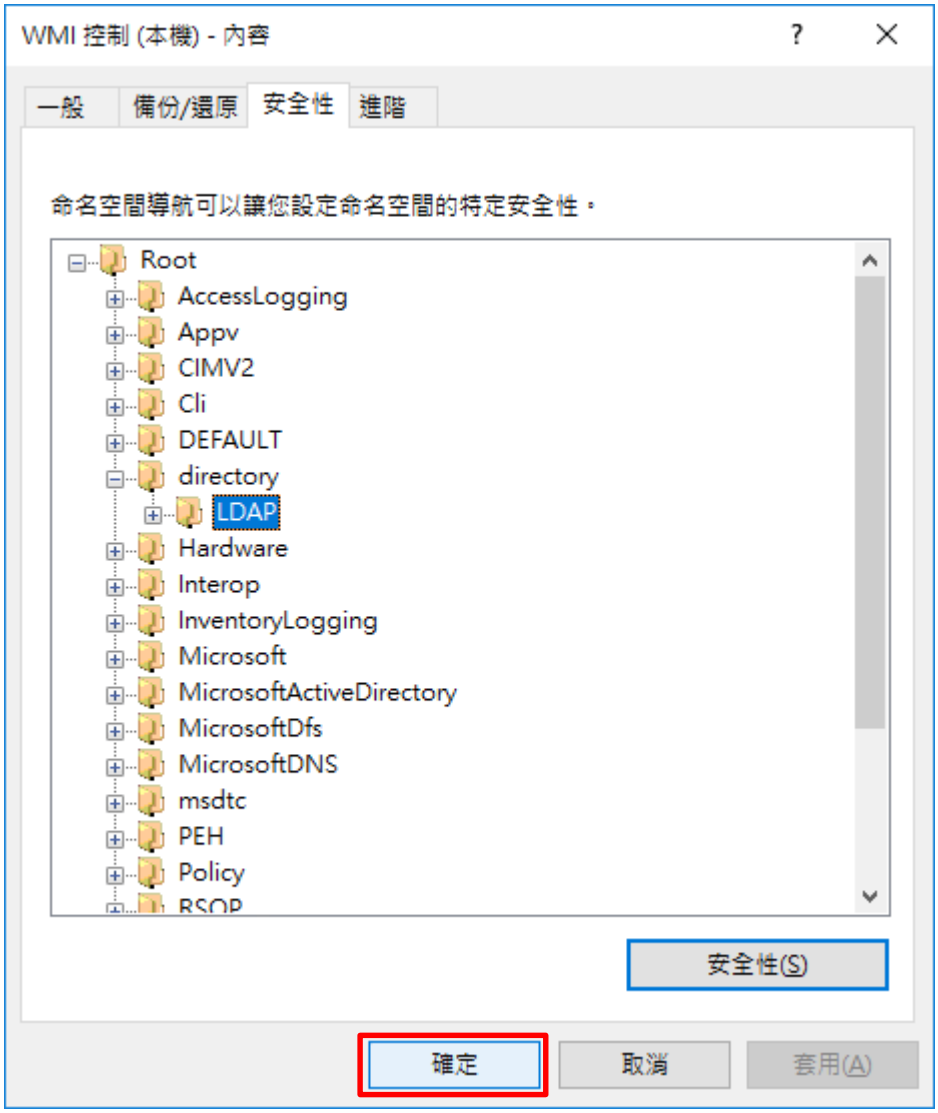


(7) 設定使用者權限

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]

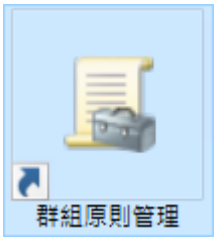


(8) 按 [確定]



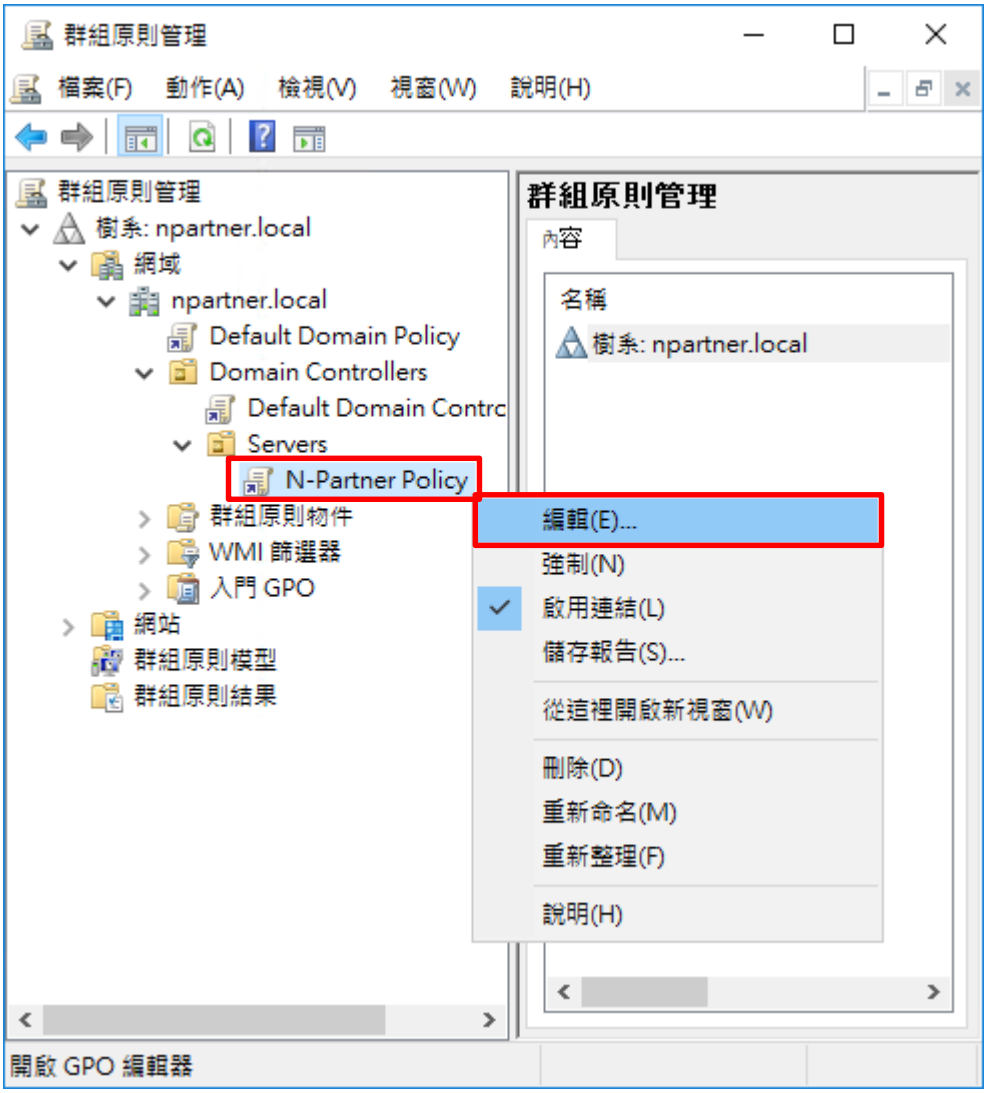
5.3.4 設定 Event log 讀取權限

(1) 開啟 [群組原則管理]



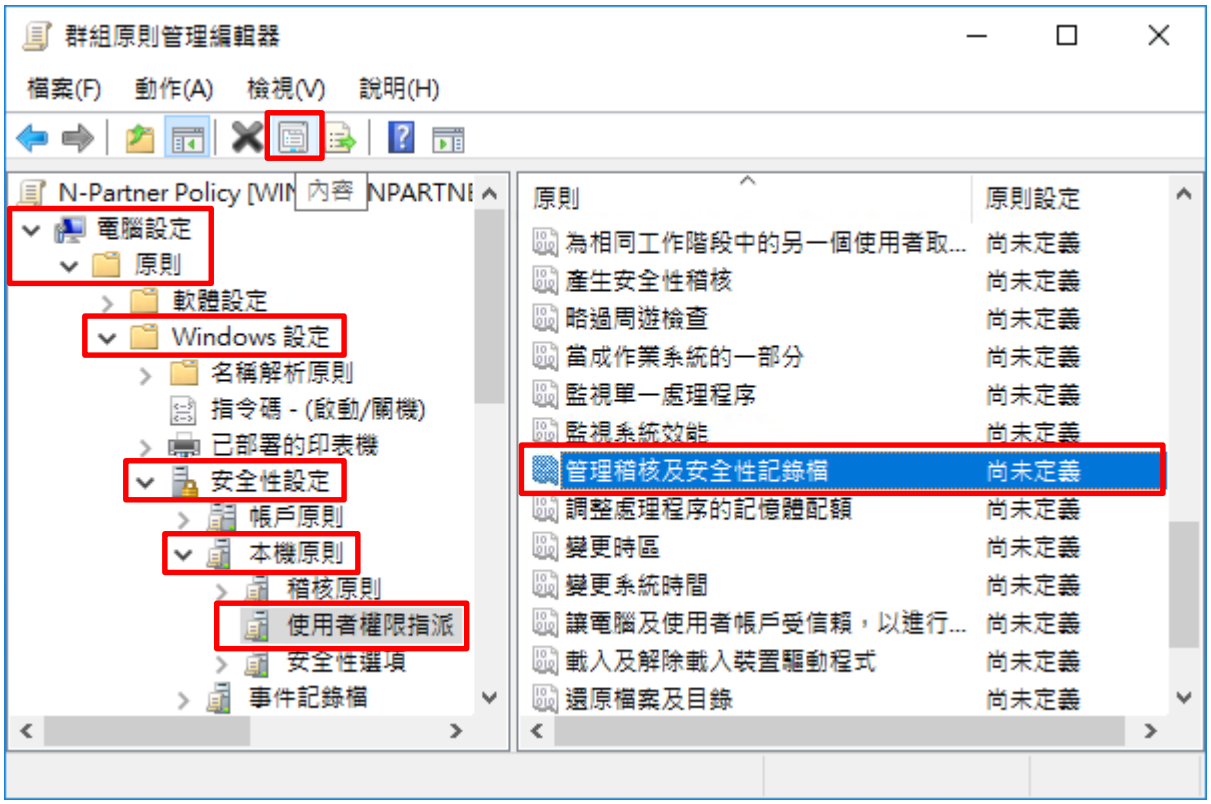
(2) 編輯群組原則物件

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 [管理稽核及安全性記錄檔] 項目 -> 點選  內容

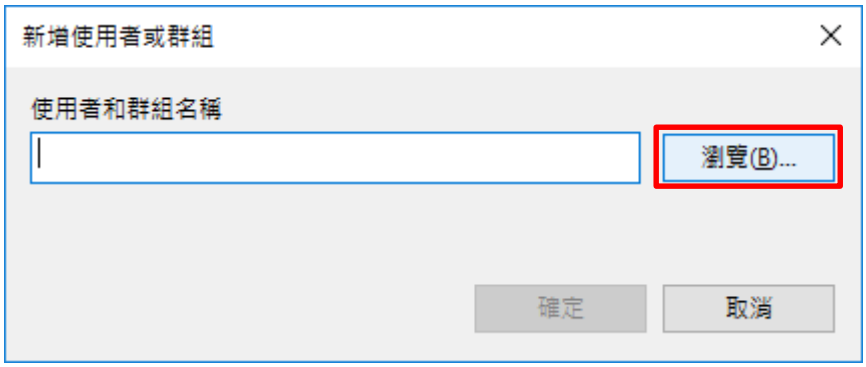


(4) 新增管理稽核使用者

勾選 [定義這些原則設定] -> 按 [新增使用者或群組...]

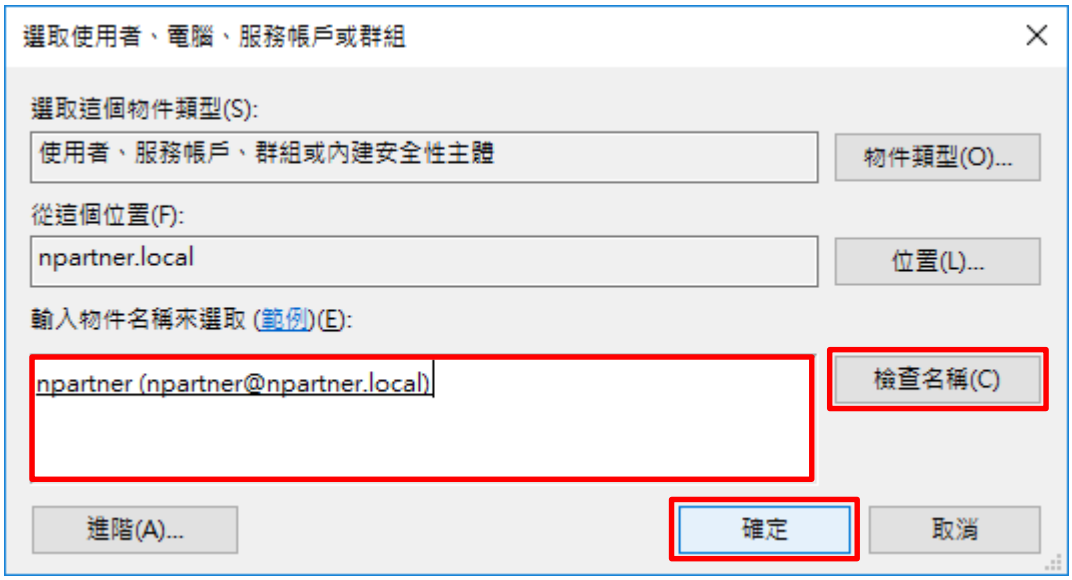
(5) 搜尋使用者

按 [瀏覽]



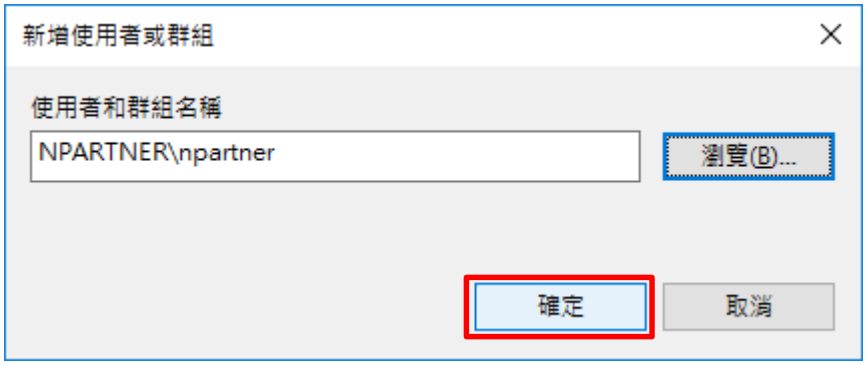
(6) 輸入使用者

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



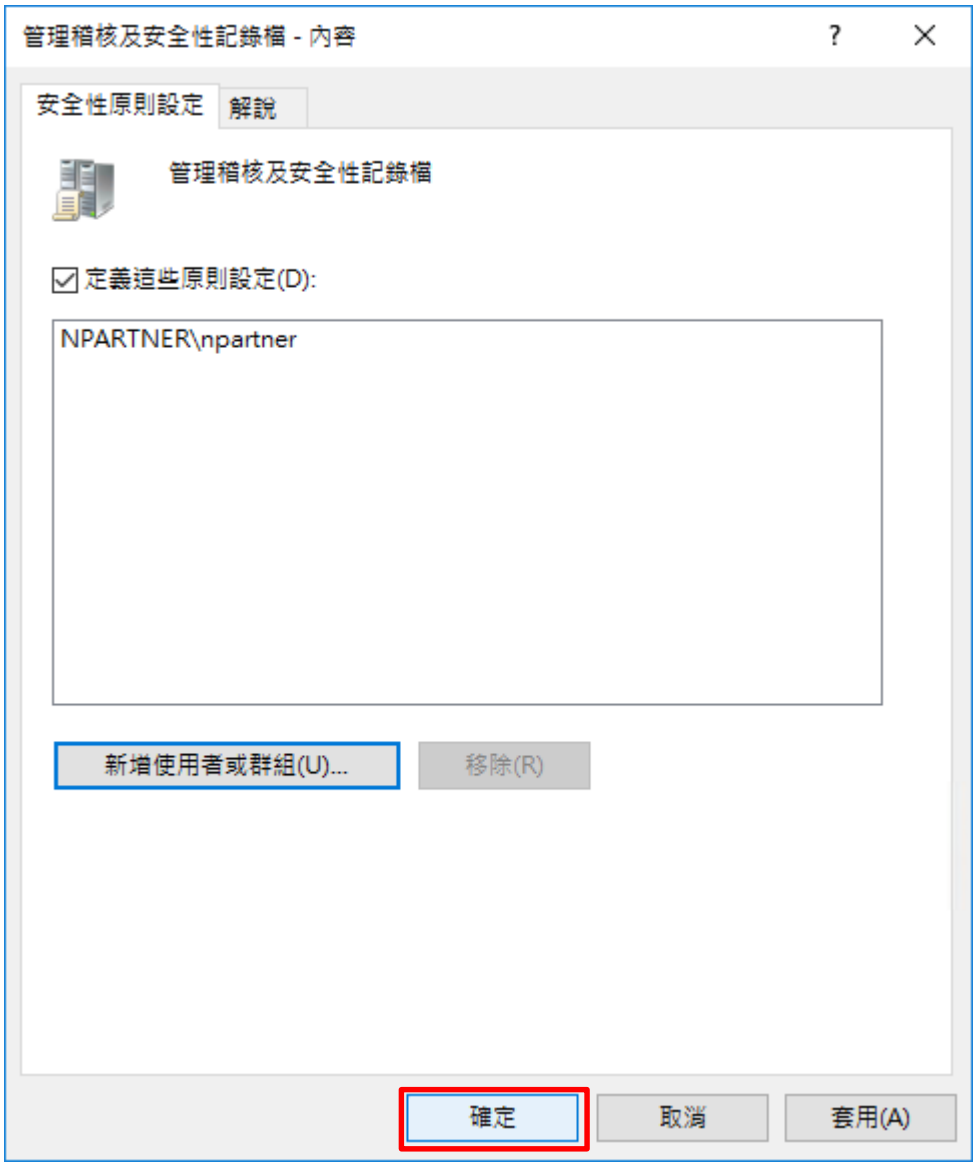
(7) 確定使用者

按 [確定]



(8) 確定設定記錄檔

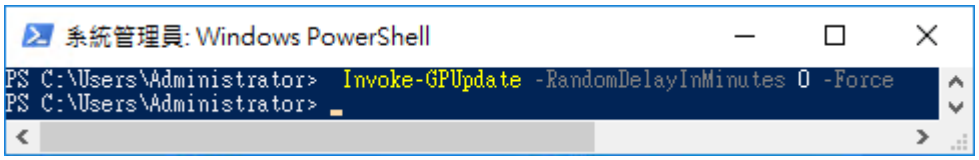
按 [確定]



(9) 開啟 [Windows PowerShell]

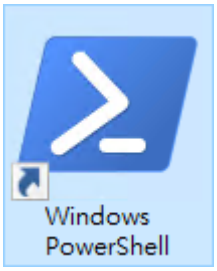
(10) 更新群組原則

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



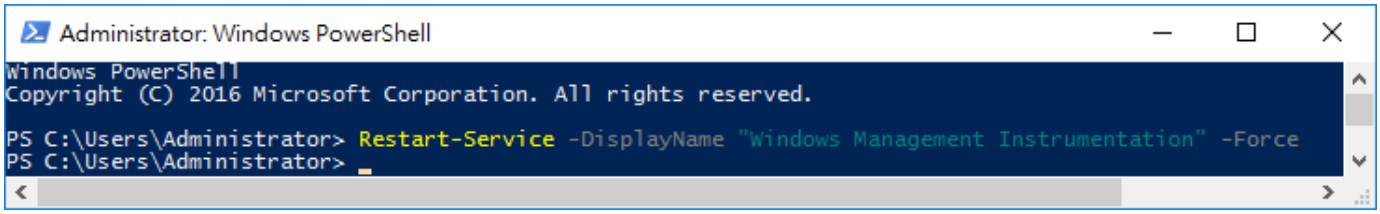
5.3.5 重啟 WMI 服務

(1) 開啟 [Windows PowerShell]



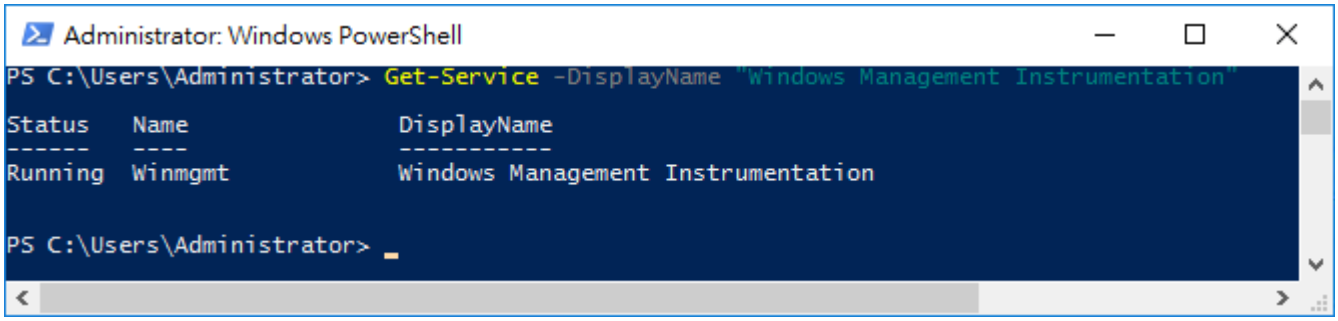
(2) 重啟 WMI 服務

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



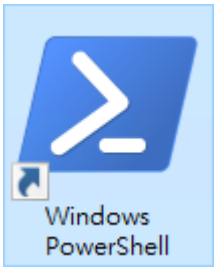
(3) 查看 WMI 服務

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



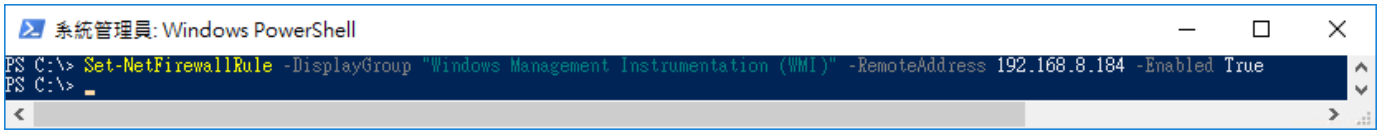
5.4 設定防火牆

(1) 開啟 [Windows PowerShell]



(2) 設定防火牆，只允許 N-Reporter IP query WMI

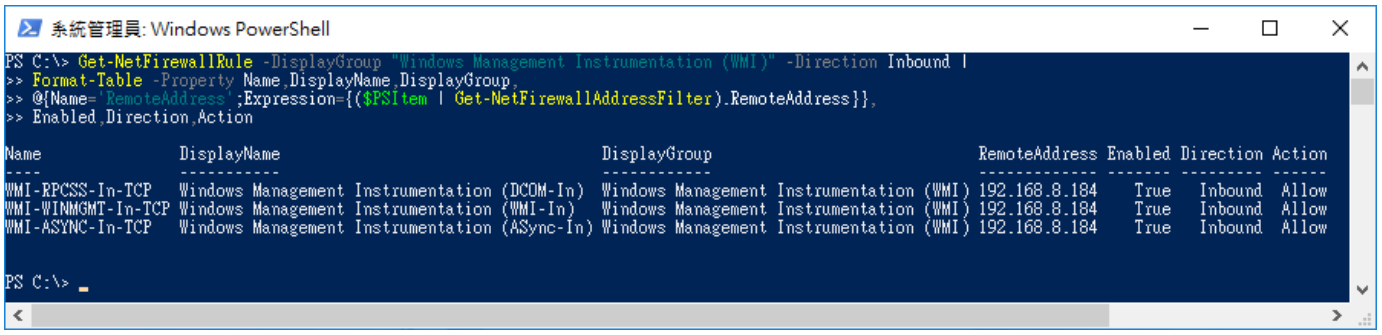
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress
192.168.8.184 -Enabled True
```



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
```

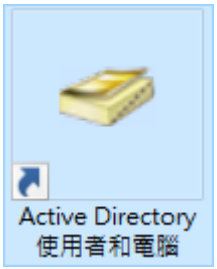


6. Windows 2019

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

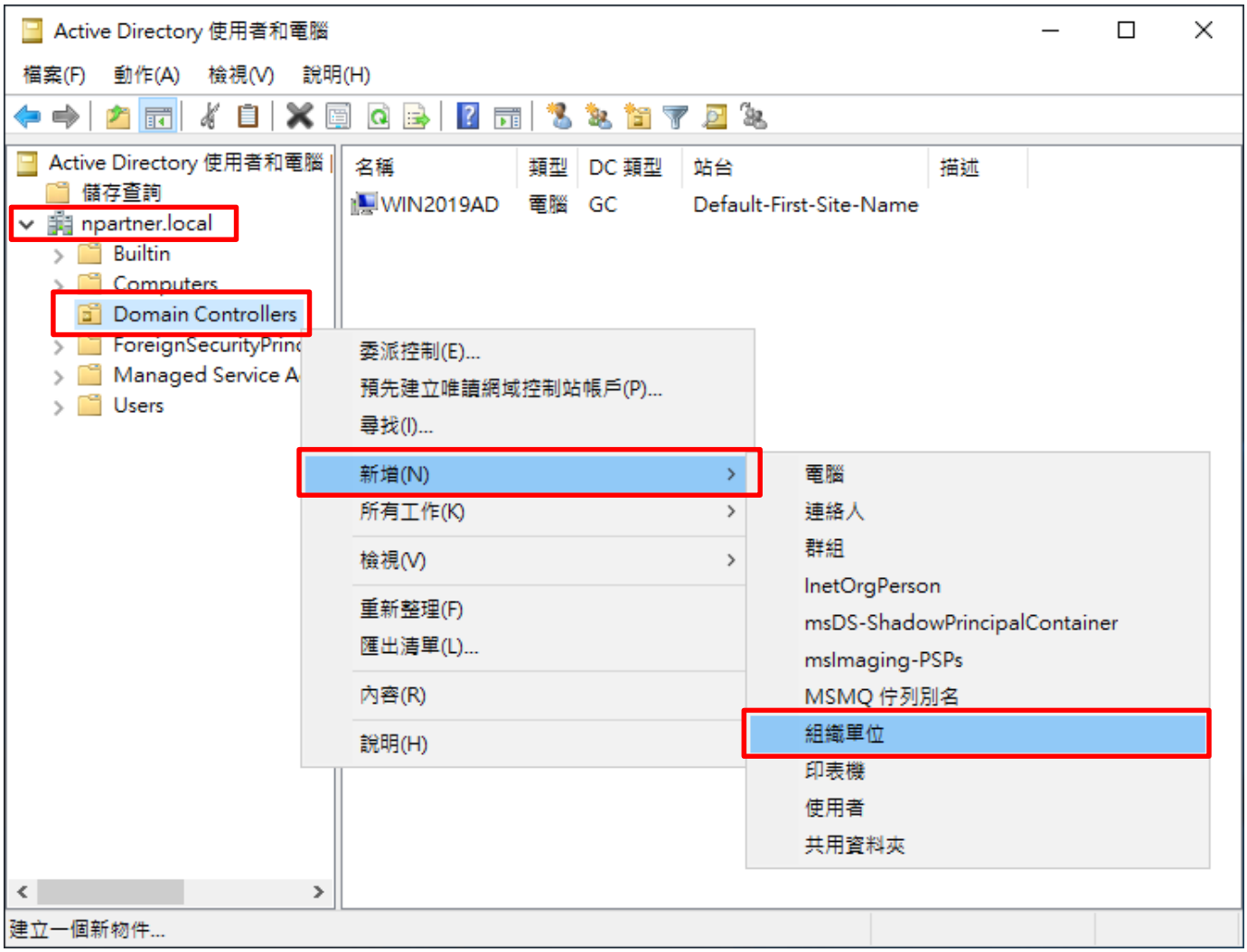
6.1 組織單位設定

(1) 開啟 [Active Directory 使用者和電腦]



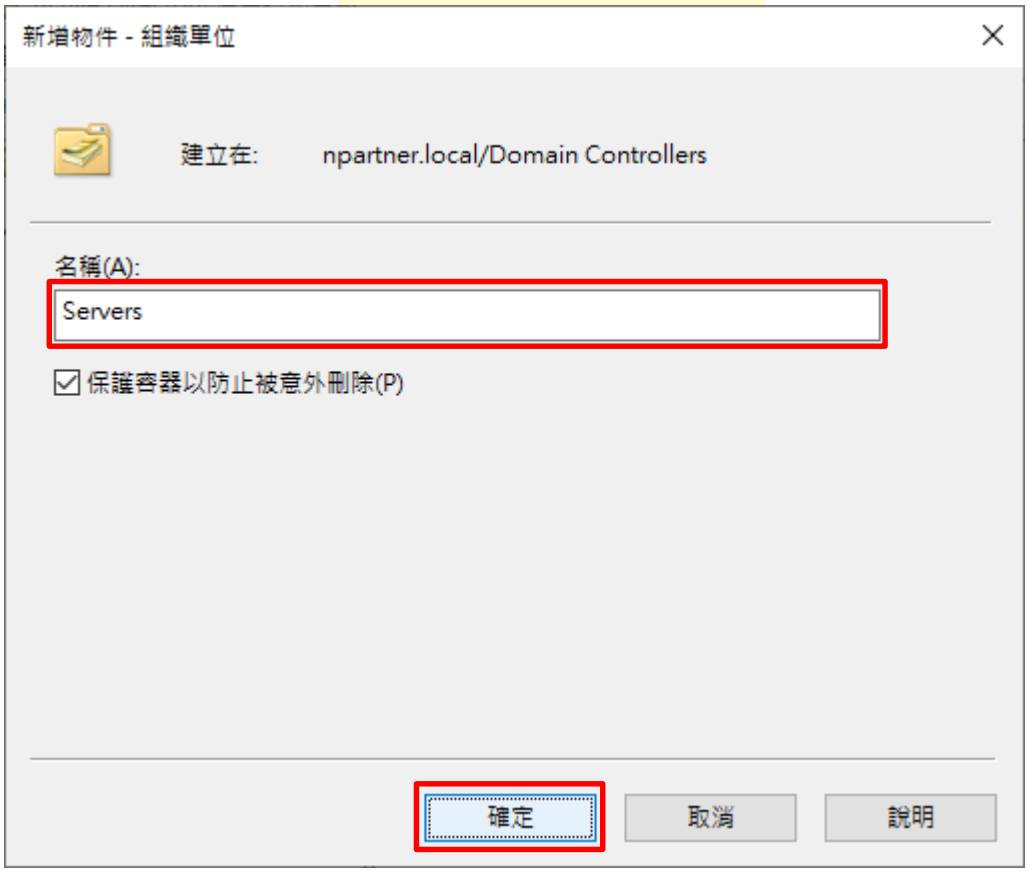
(2) 新增組織單位

[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]



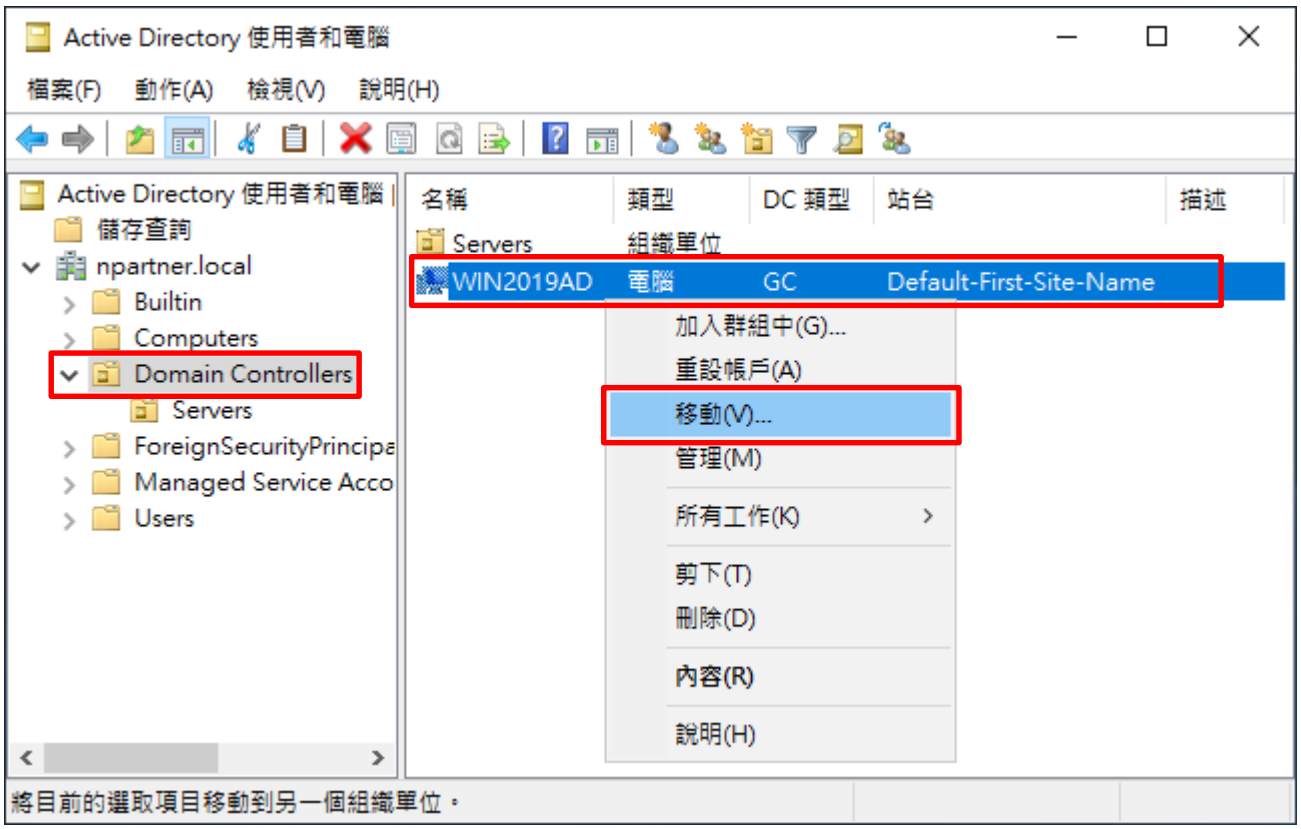
(3) 輸入組織單位名稱

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]



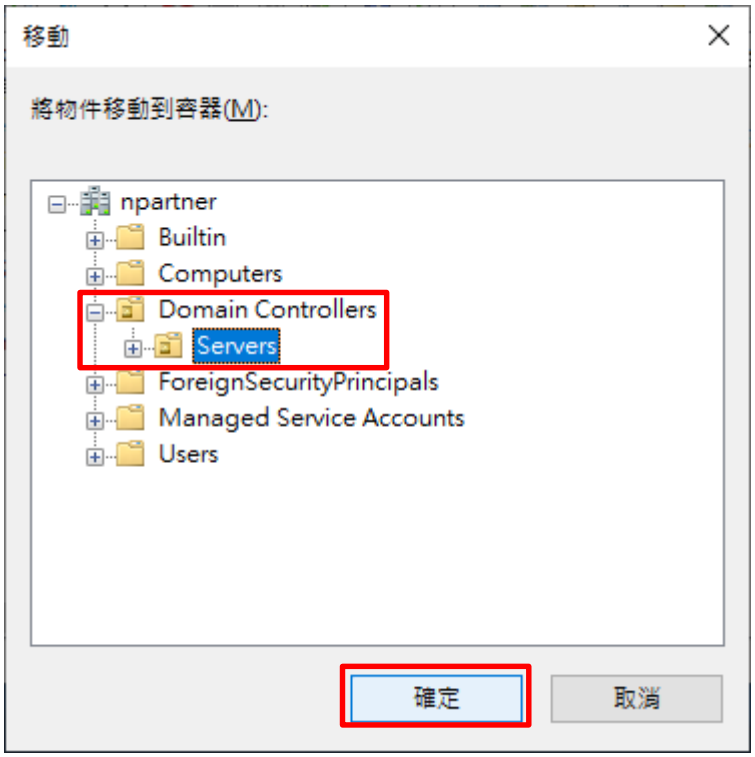
(4) 移動伺服器至新的組織單位

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]



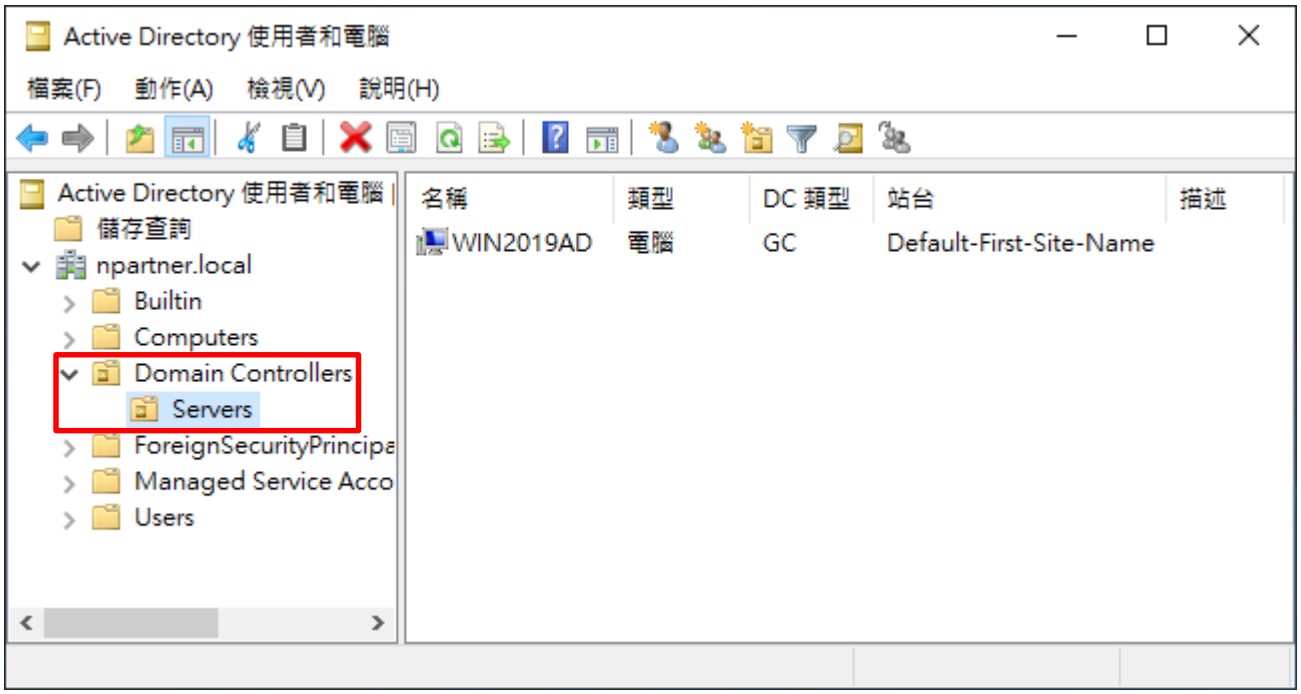
(5) 選擇組織單位

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



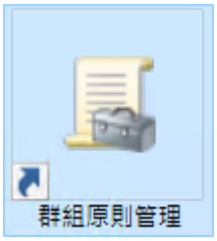
(6) 確認伺服器已移動至新的組織單位

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



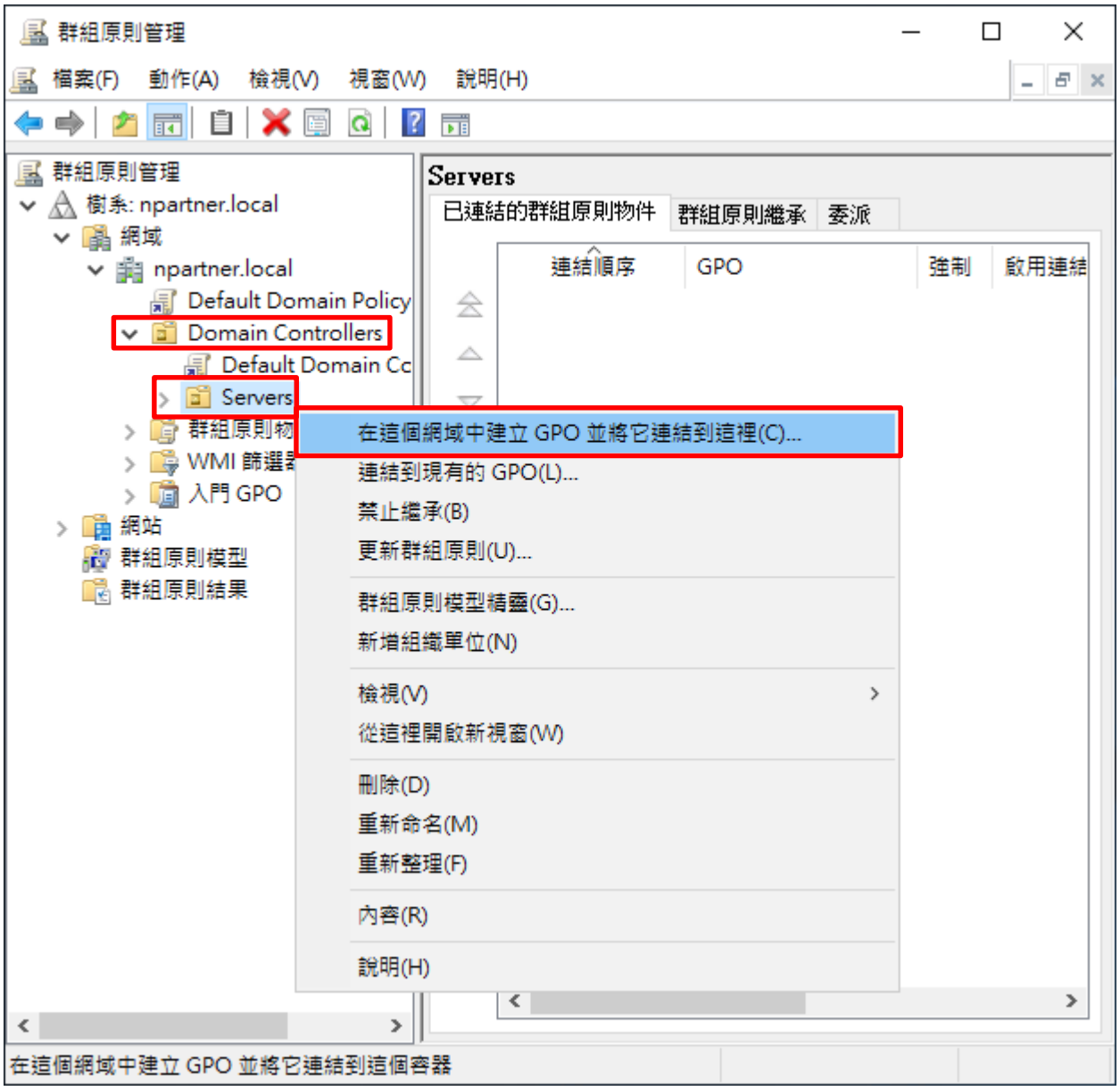
6.2 群組原則設定

(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...]

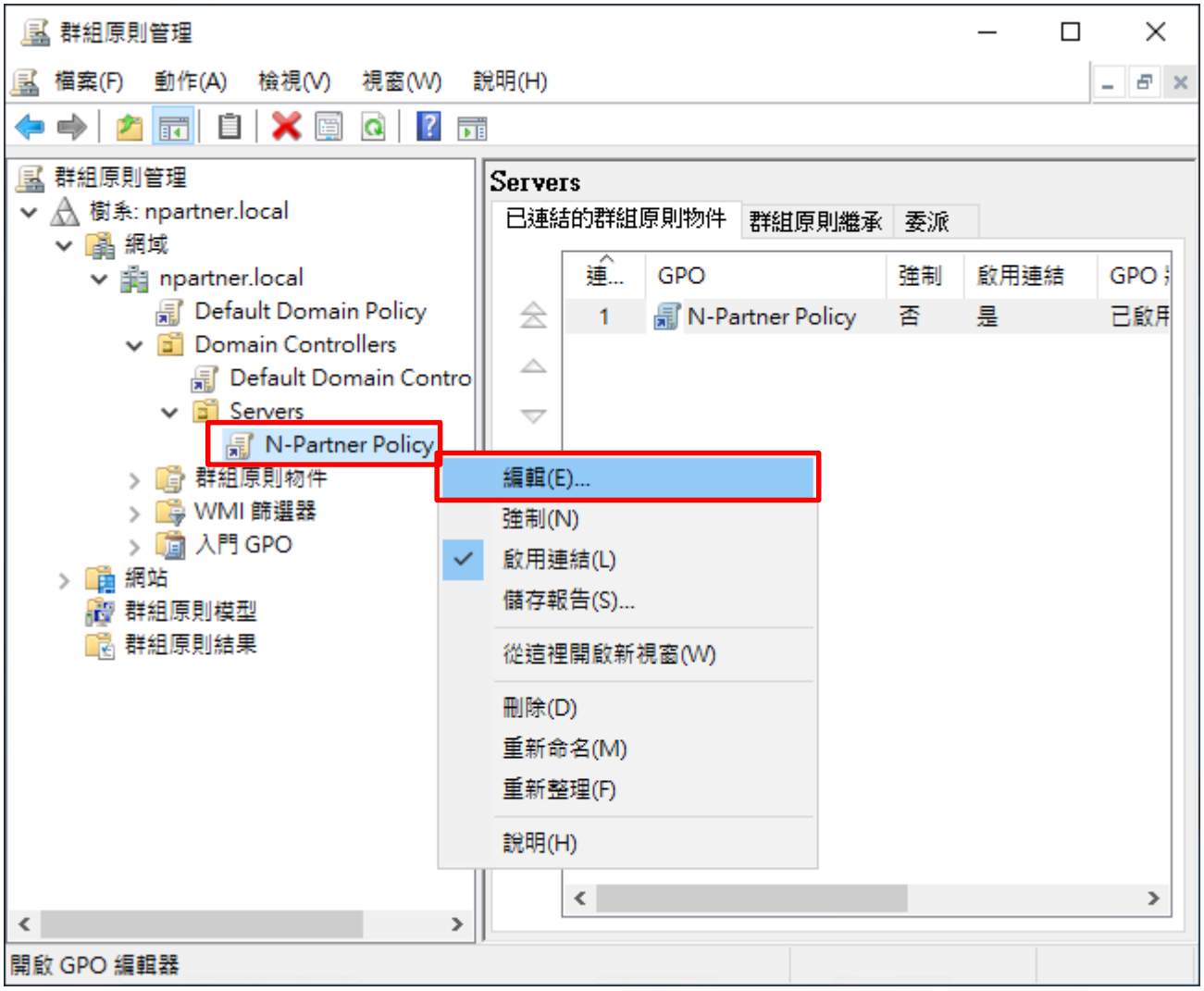


(3) 輸入群組原則物件名稱

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]

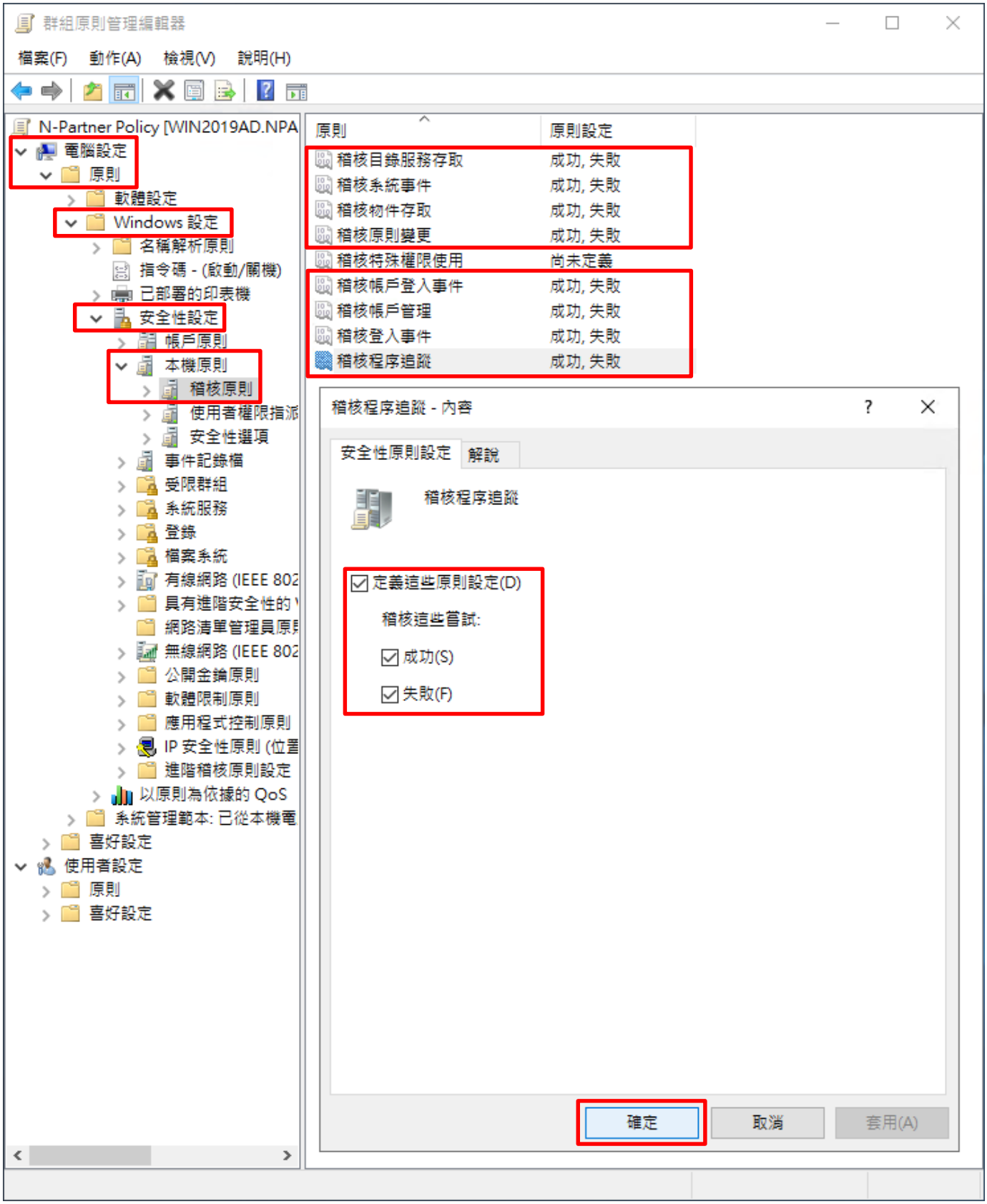
(4) 編輯群組原則物件

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



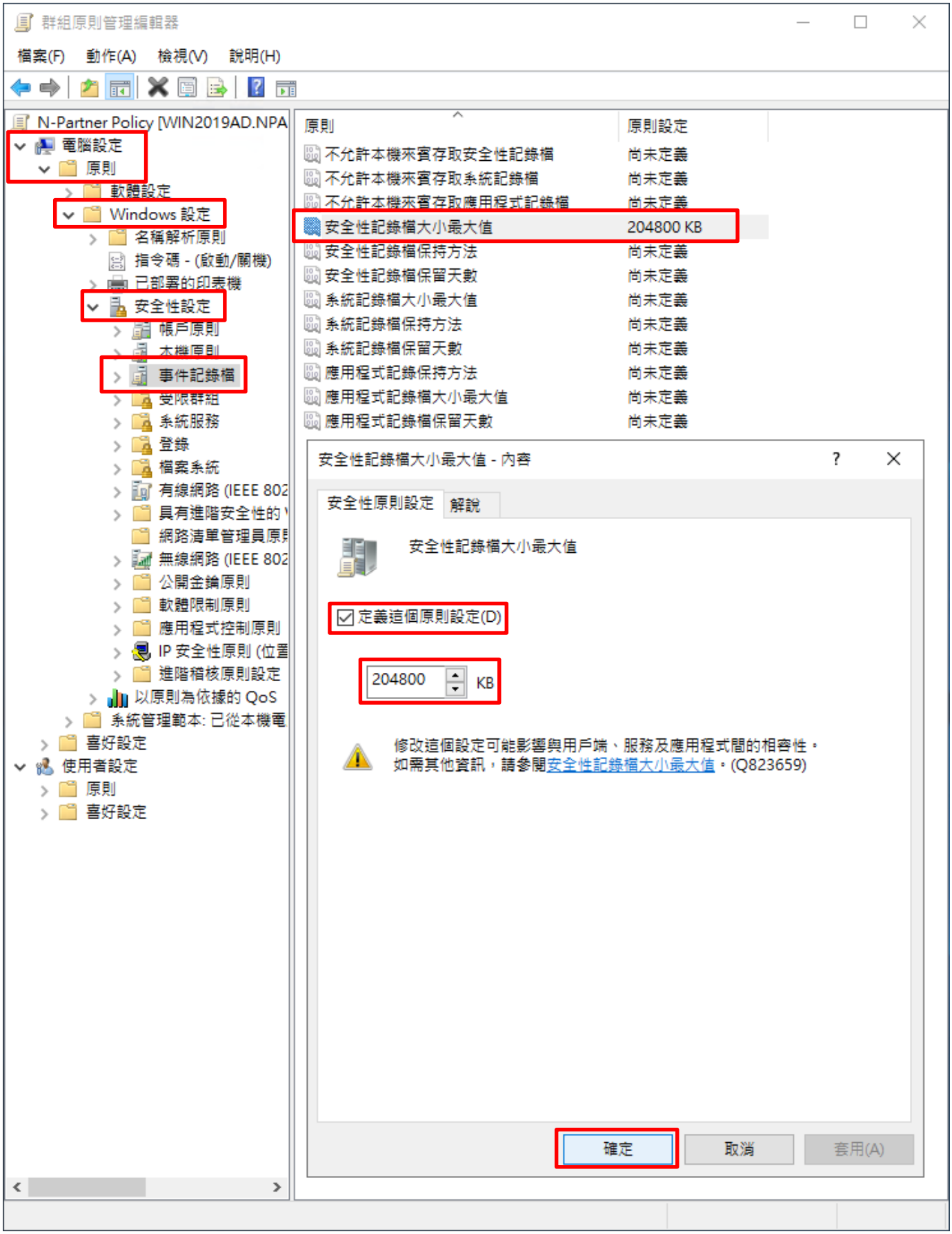
(5) 本機原則：稽核原則

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]



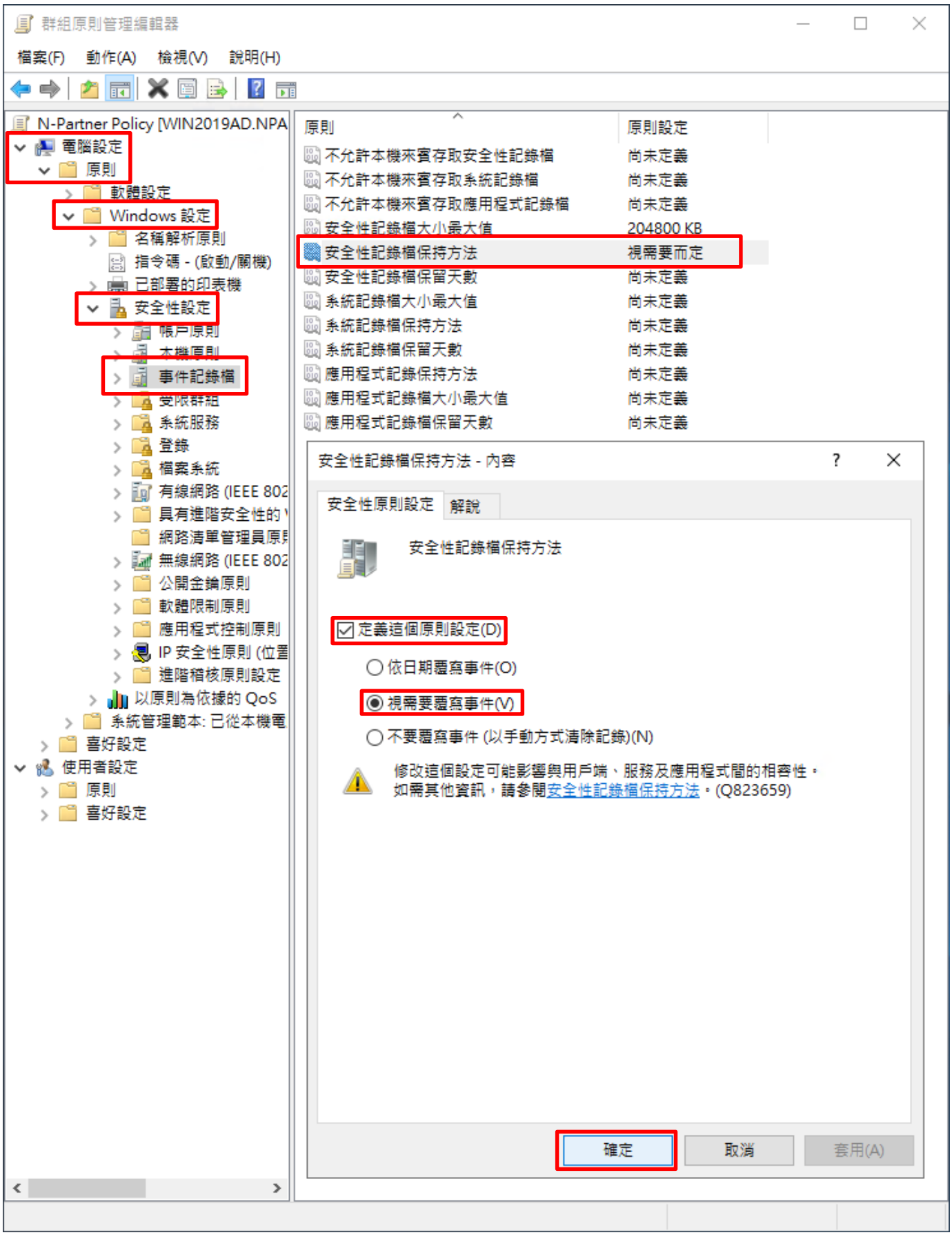
(6) 事件記錄：安全性記錄檔大小最大值

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]



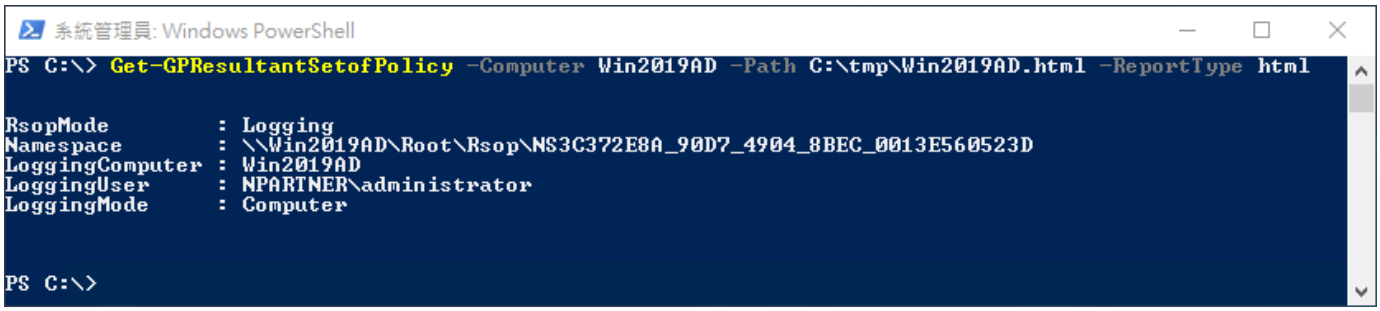
(8) 開啟 [Windows PowerShell]

(9) 更新群組原則

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

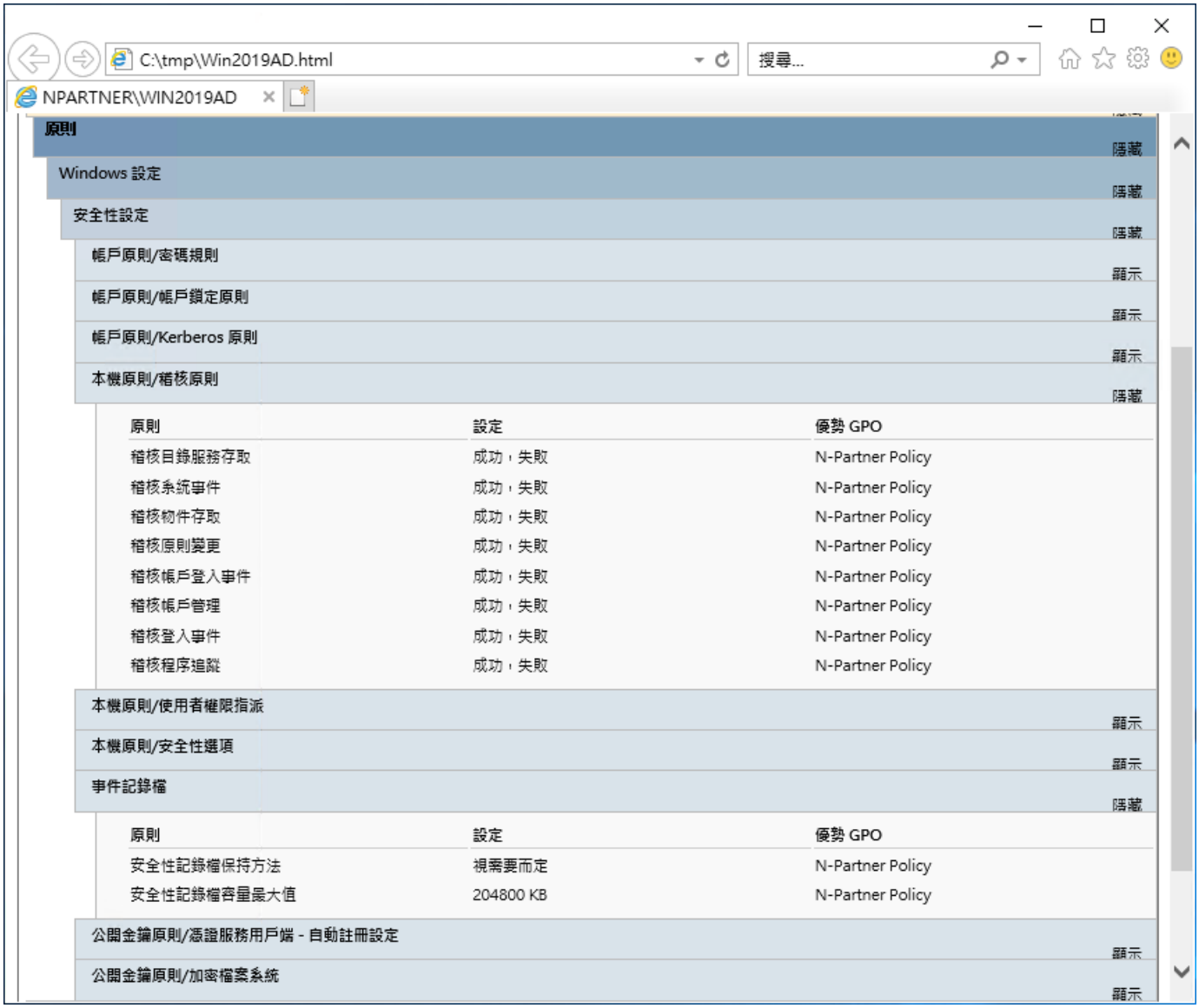
(10) 產生伺服器群組原則報表

```
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

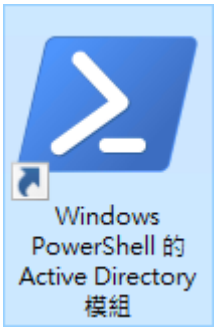
(11) 開啟報表，確認 Windows 2019 AD 伺服器，套用 N-Partner Policy 群組原則



6.3 新增非管理帳號

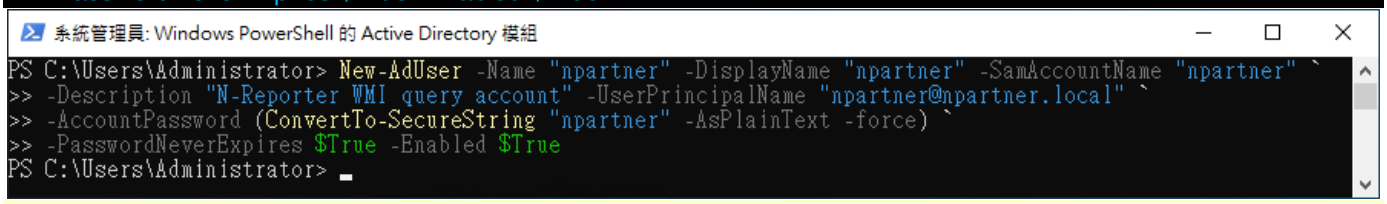
6.3.1 新增使用者

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



(2) 新增帳號

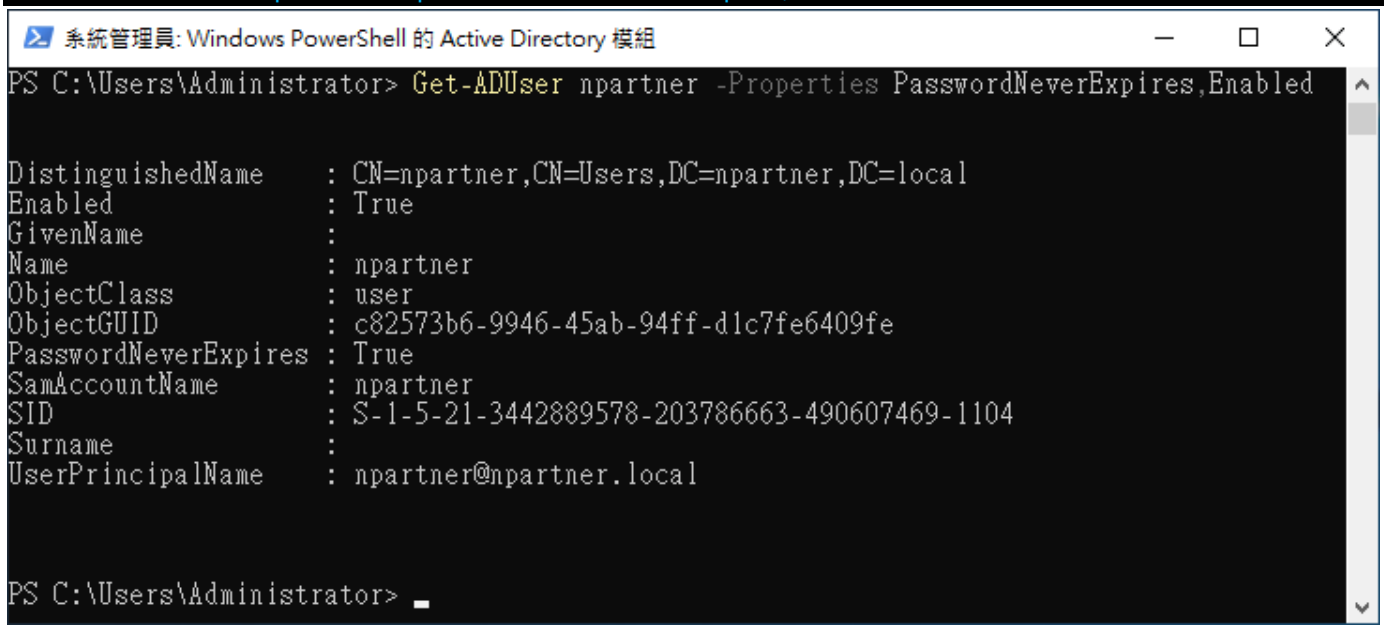
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled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

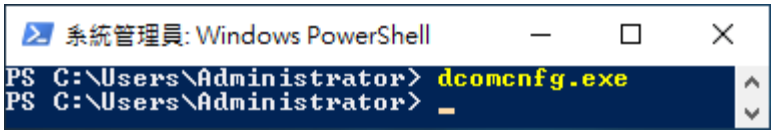


6.3.2 設定 DCOM 權限

(1) 開啟 [Windows PowerShell]

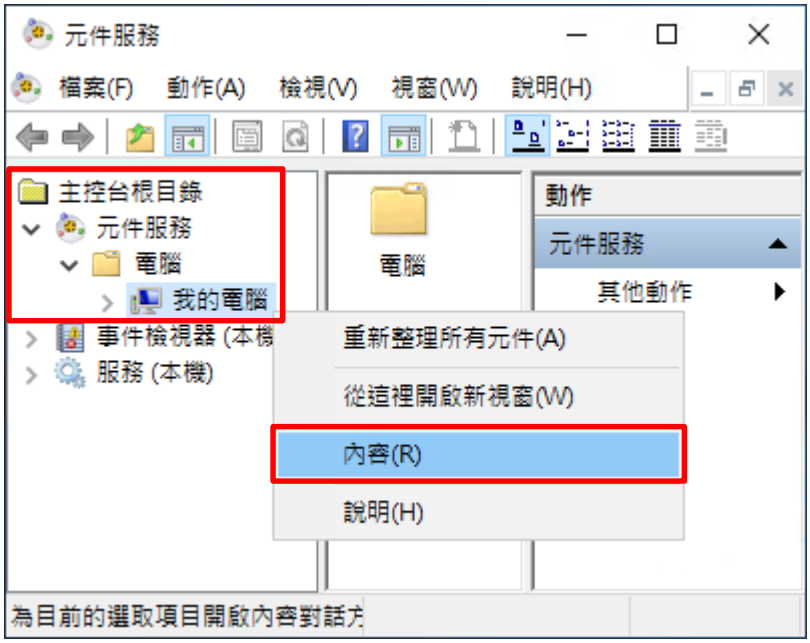
(2) 開啟元件服務

```
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]

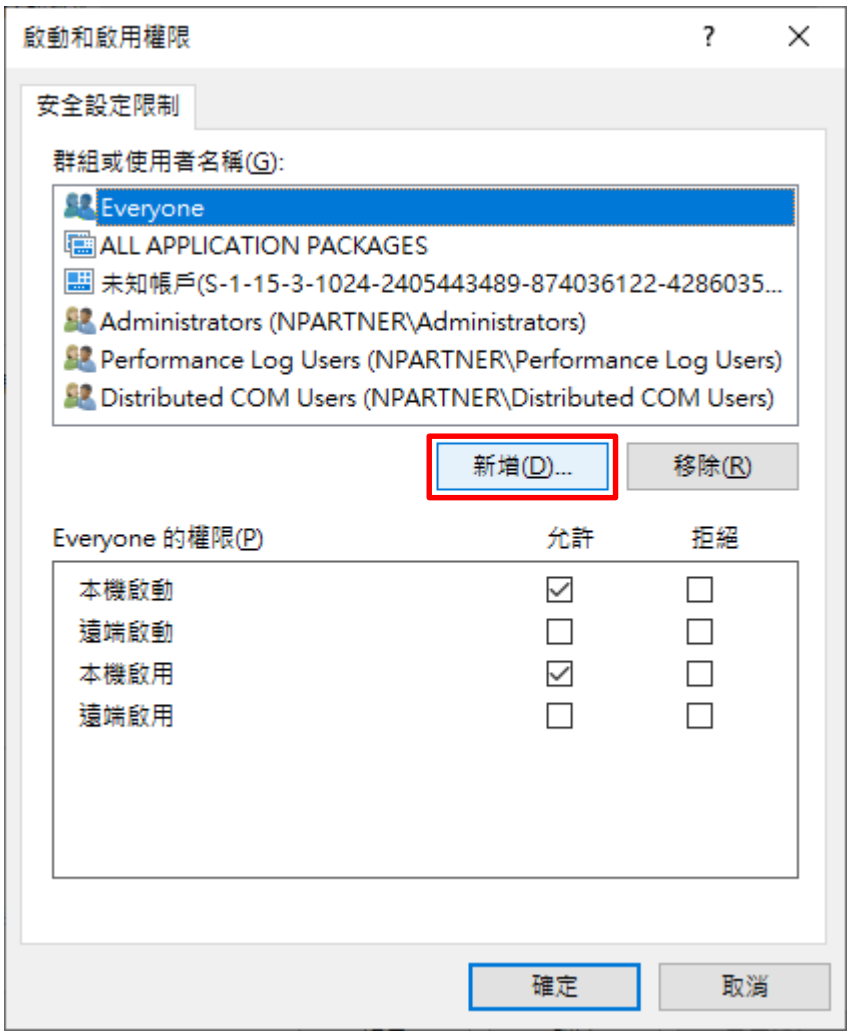


(4) 啟用權限

點選 [COM 安全性] 頁面 -> 啟動和啟用權限，按 [編輯限制]

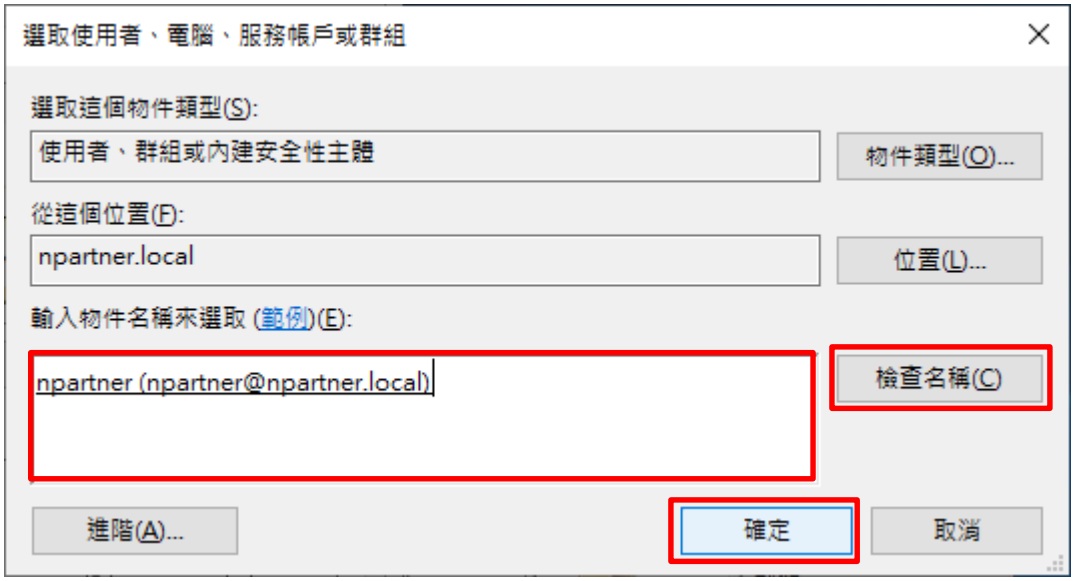
(5) 新增 DCOM 使用者權限

點選 [新增]



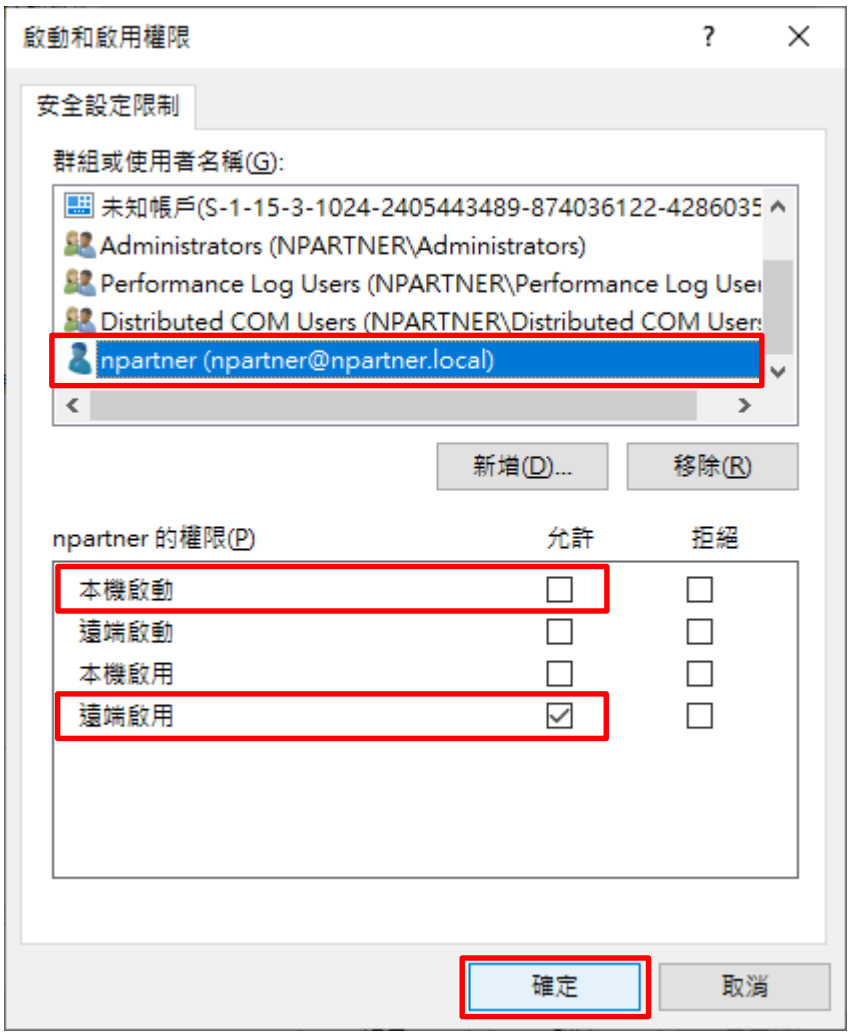
(6) 輸入使用者

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]

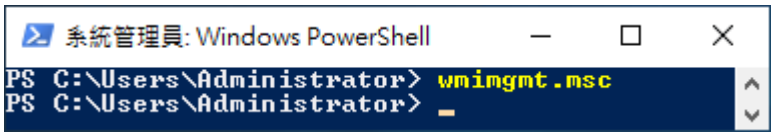
6.3.3 設定 WMI 權限

6.3.3.1 設定事件日誌權限

(1) 開啟 [Windows PowerShell]

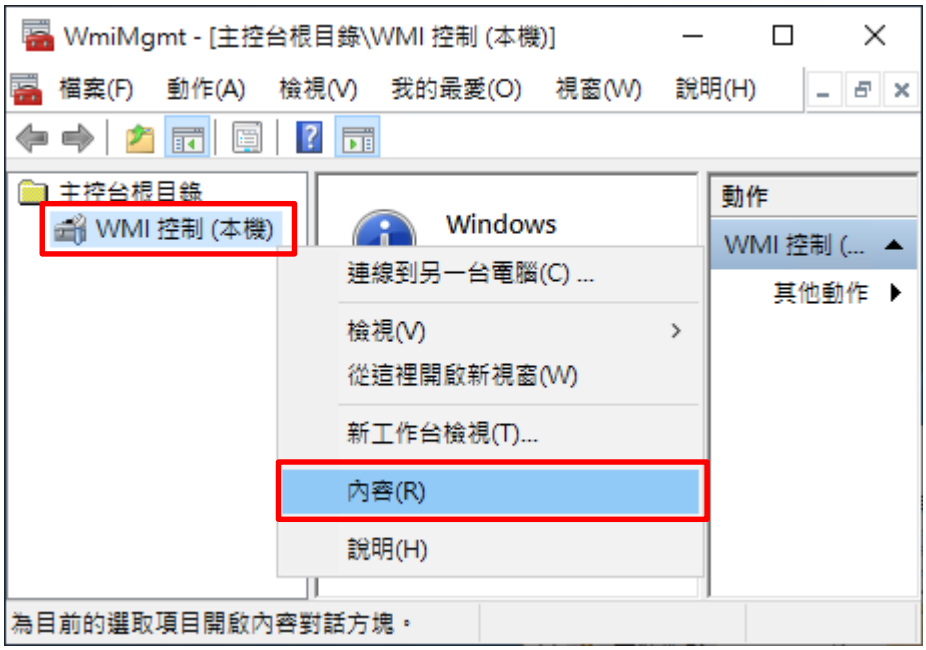
(2) 開啟元件服務

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



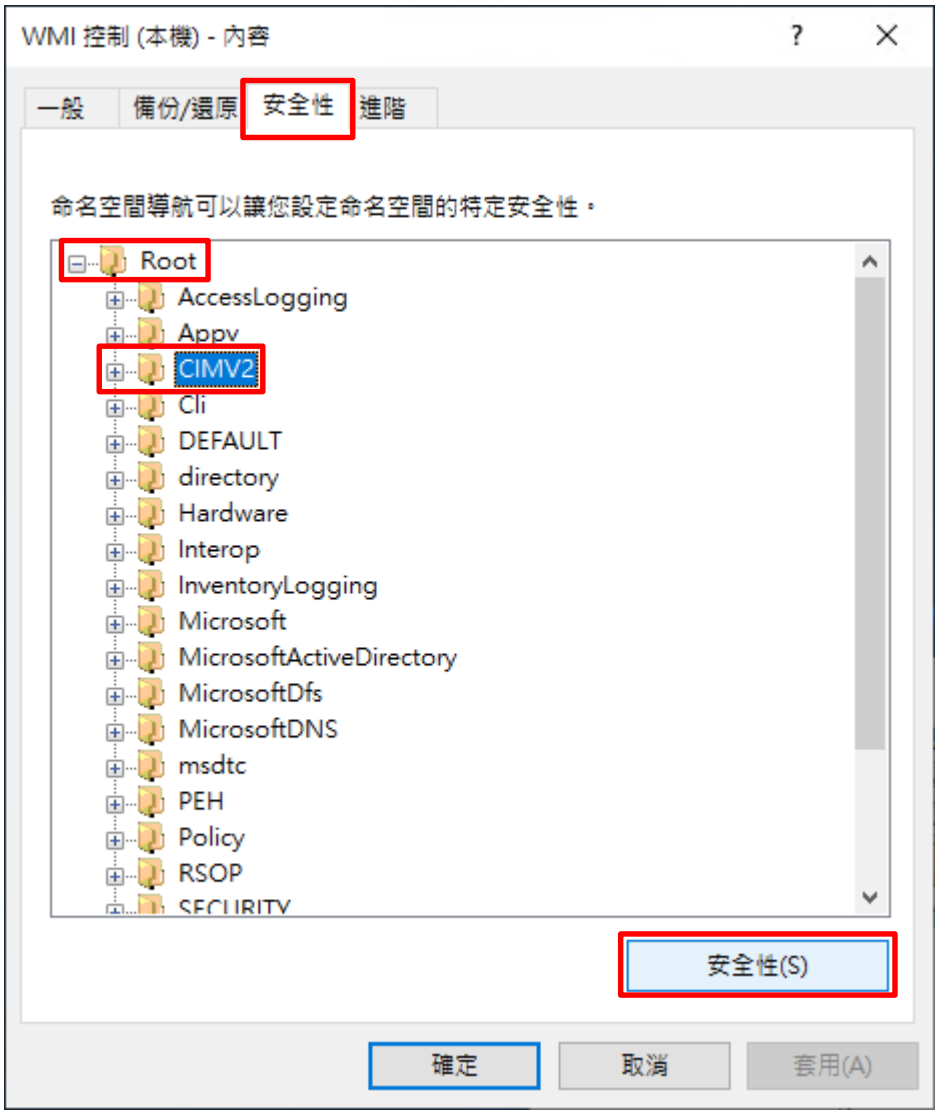
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



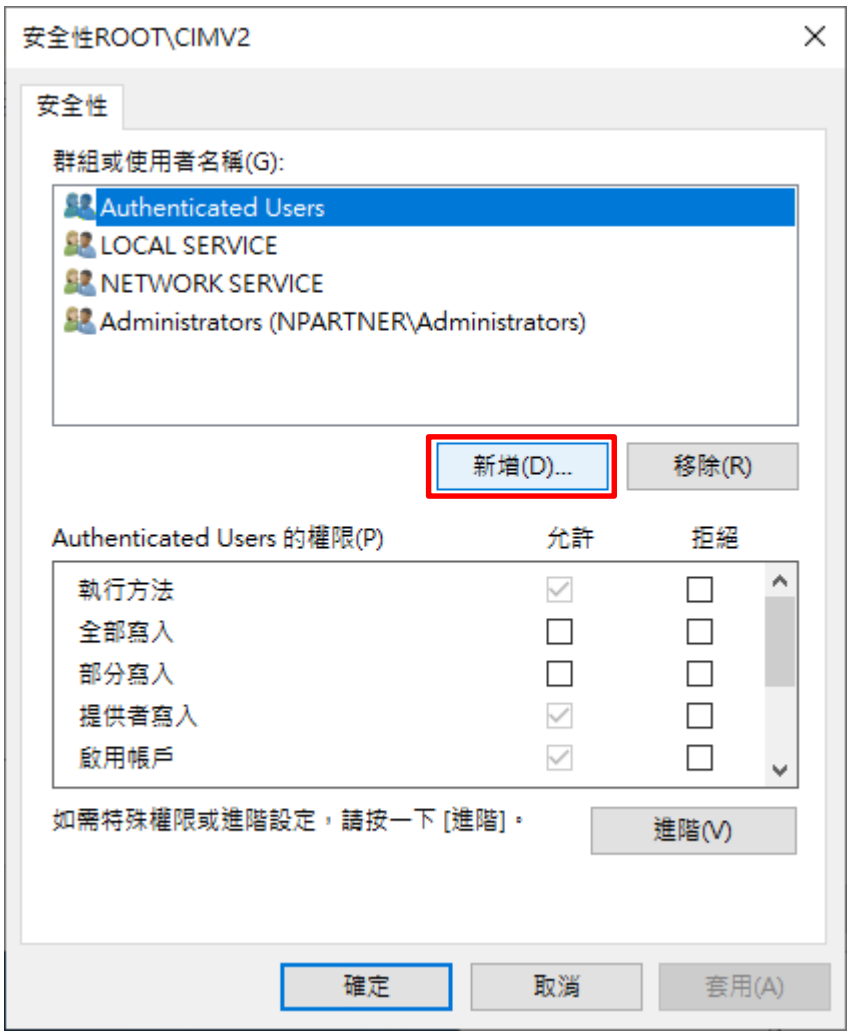
(4) 編輯 CIMV2 安全性

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]

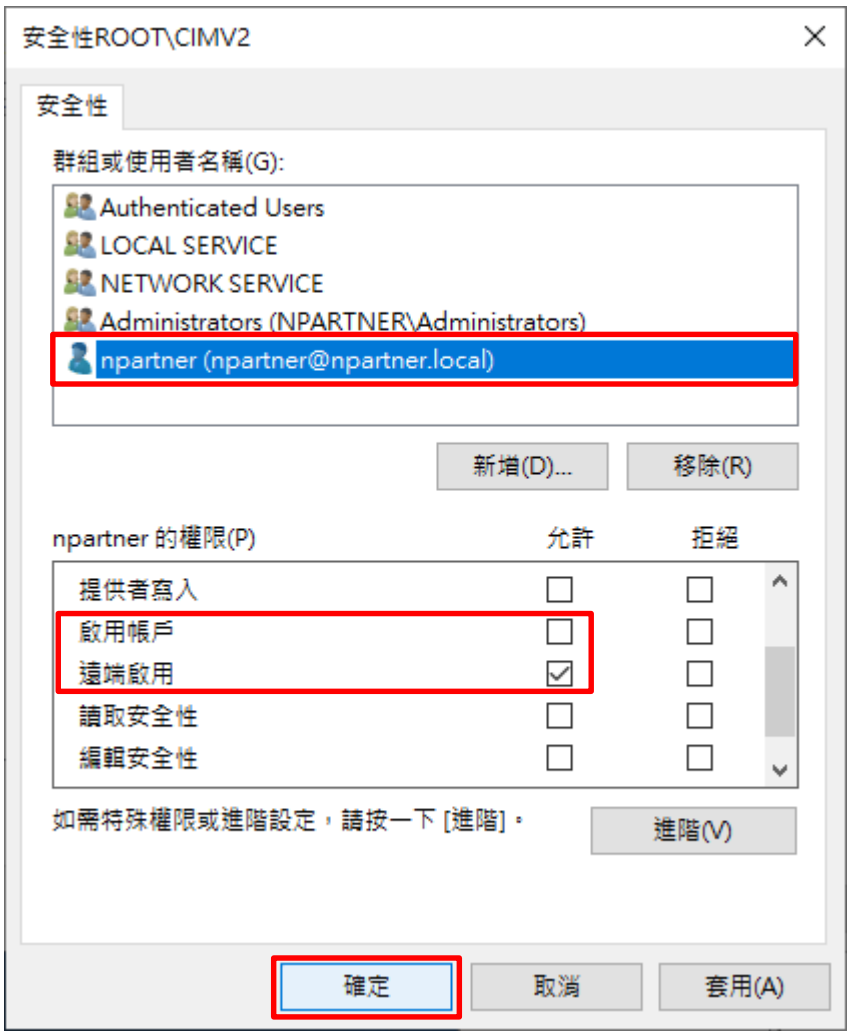


(6) 輸入使用者

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

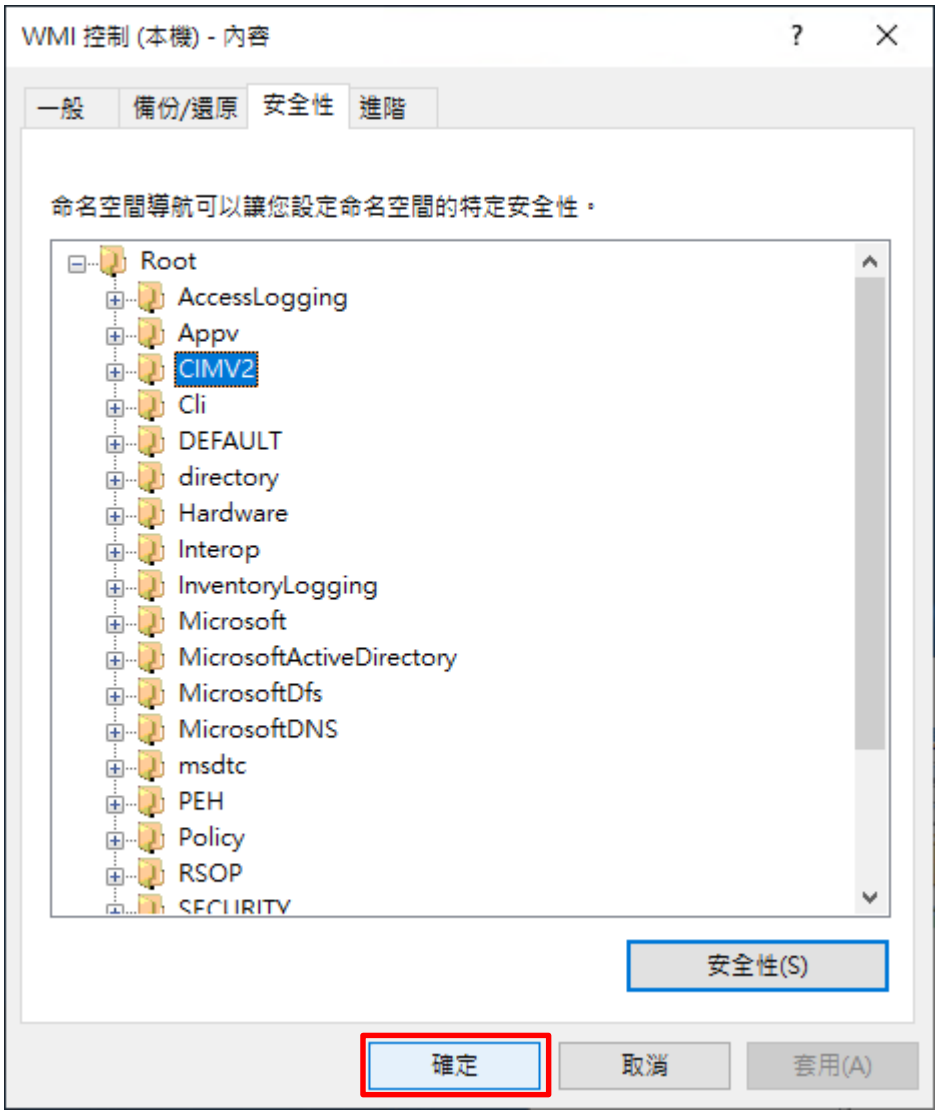
(7) 設定使用者權限

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]

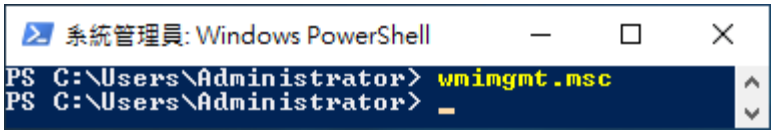


6.3.3.2 設定讀取使用者資料權限

(1) 開啟 [Windows PowerShell]

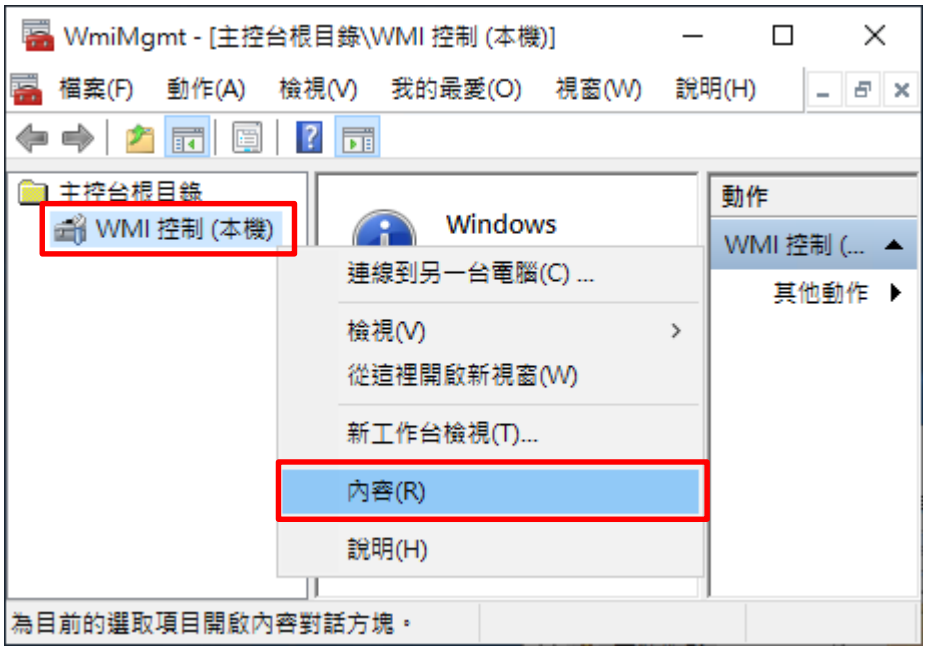
(2) 開啟元件服務

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



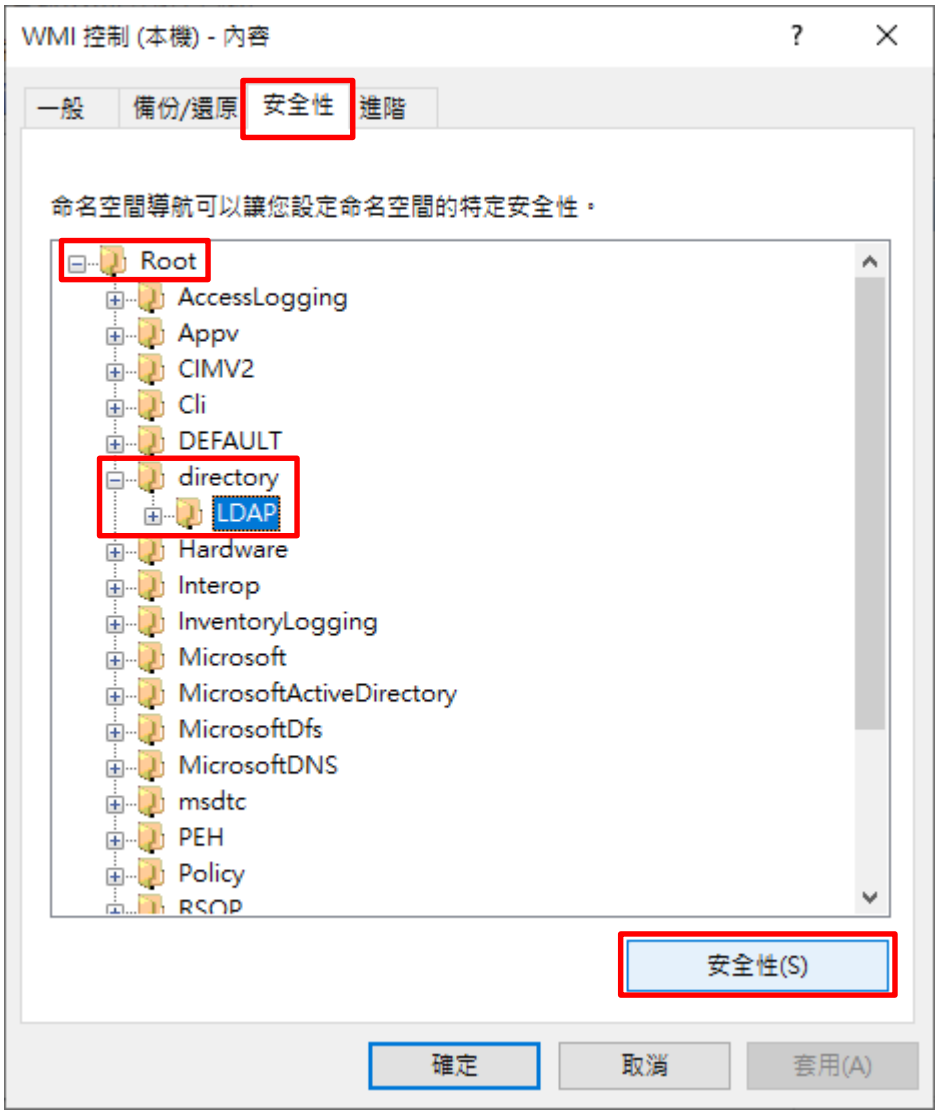
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



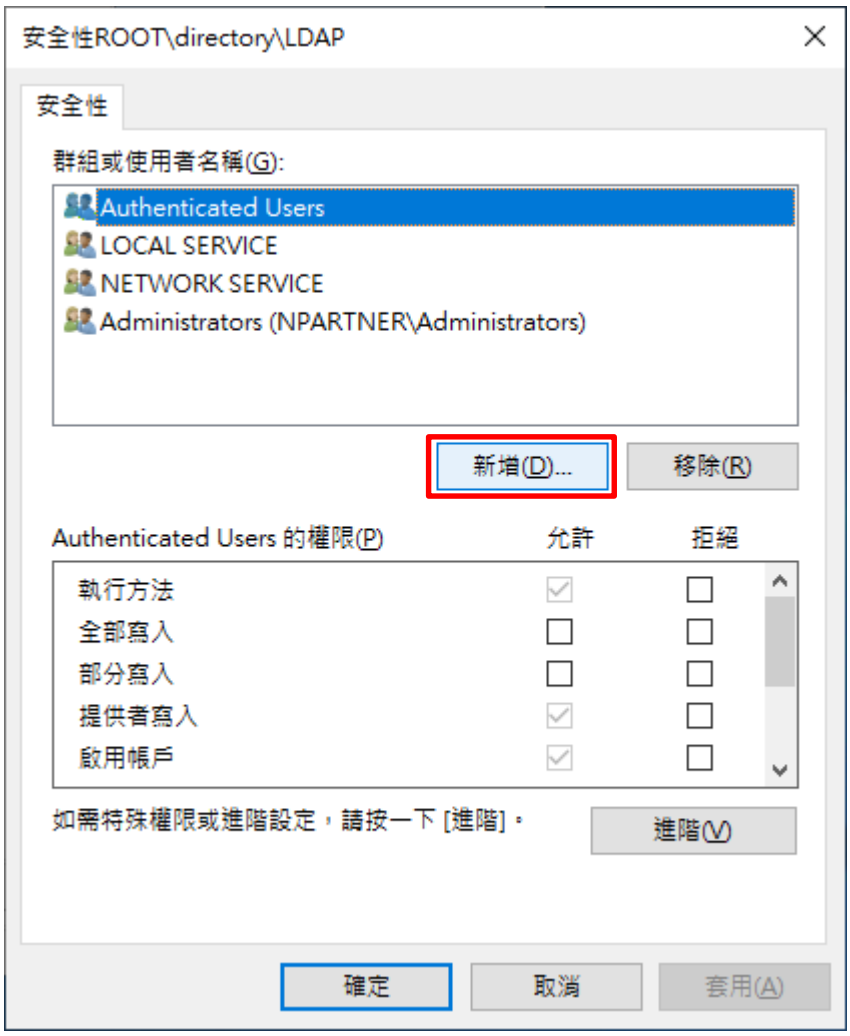
(4) 編輯 LDAP 安全性

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]

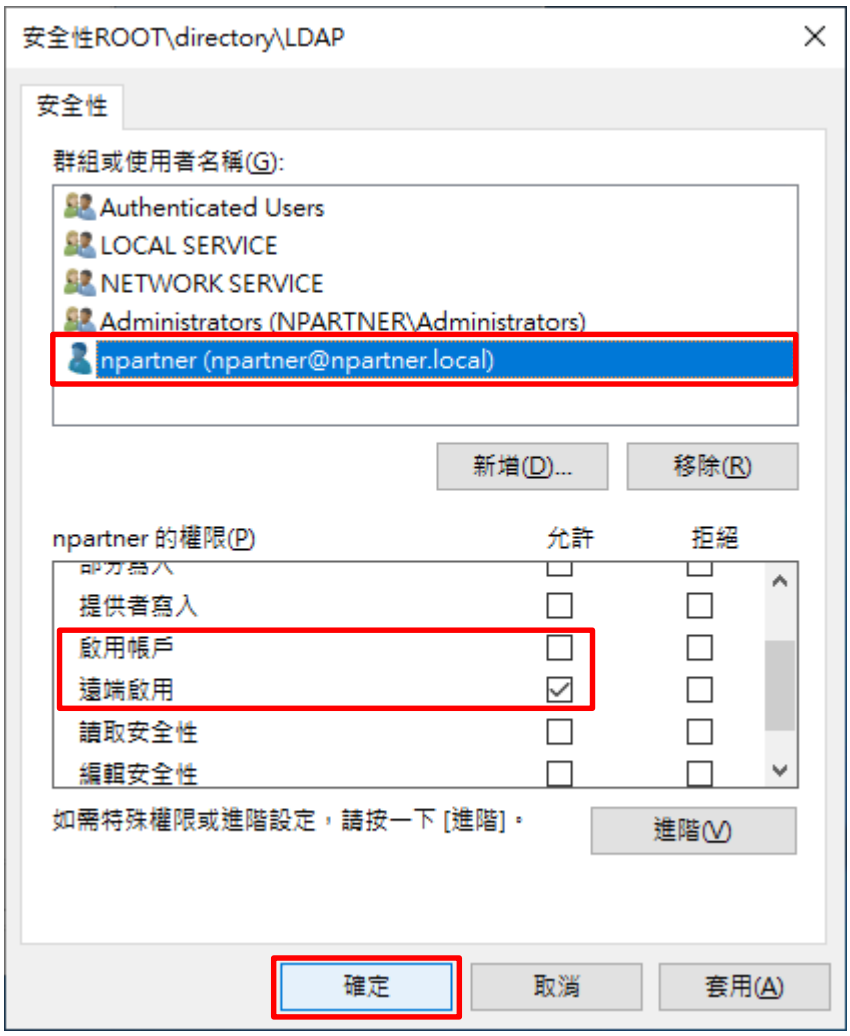


(6) 輸入使用者

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

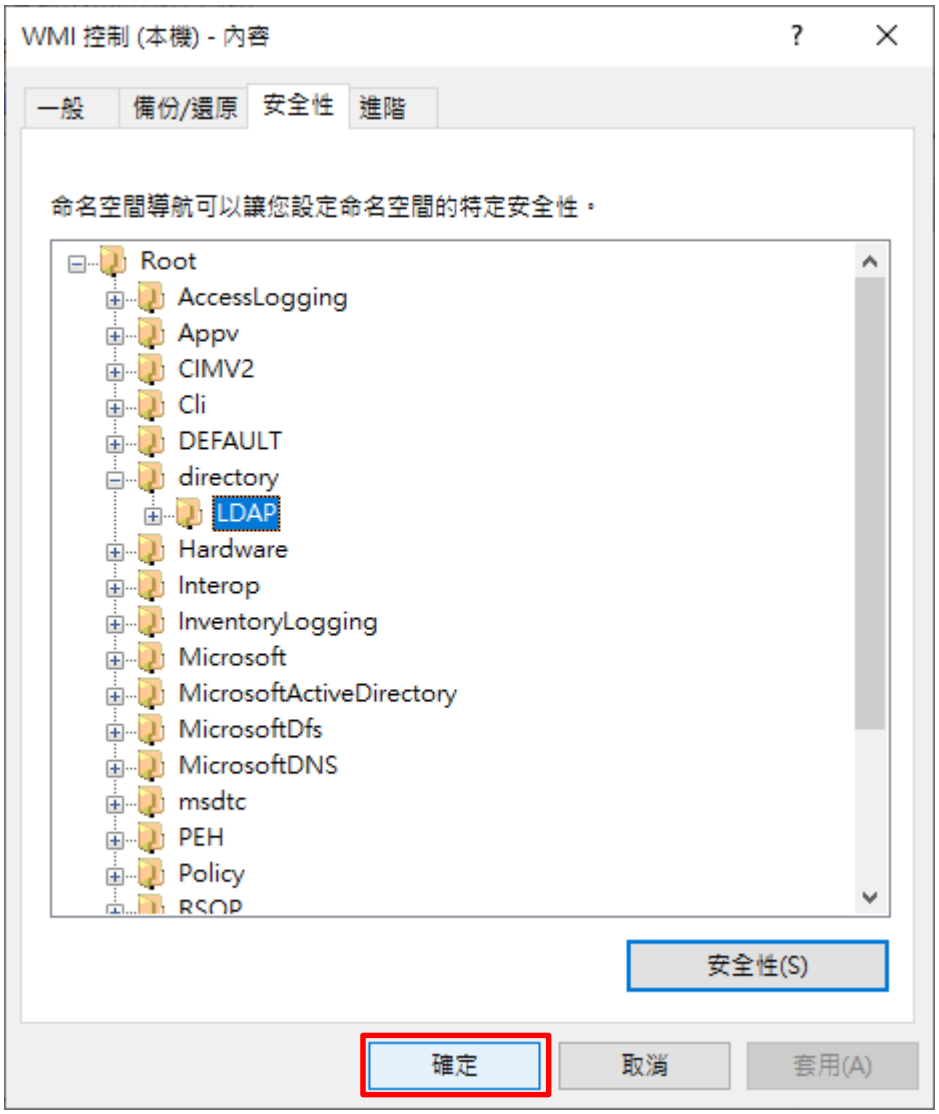
(7) 設定使用者權限

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) 確定使用者權限

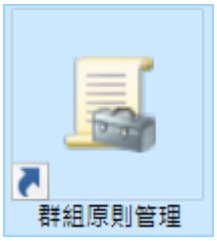
按 [確定]



6.3.4 設定 Event log 讀取權限

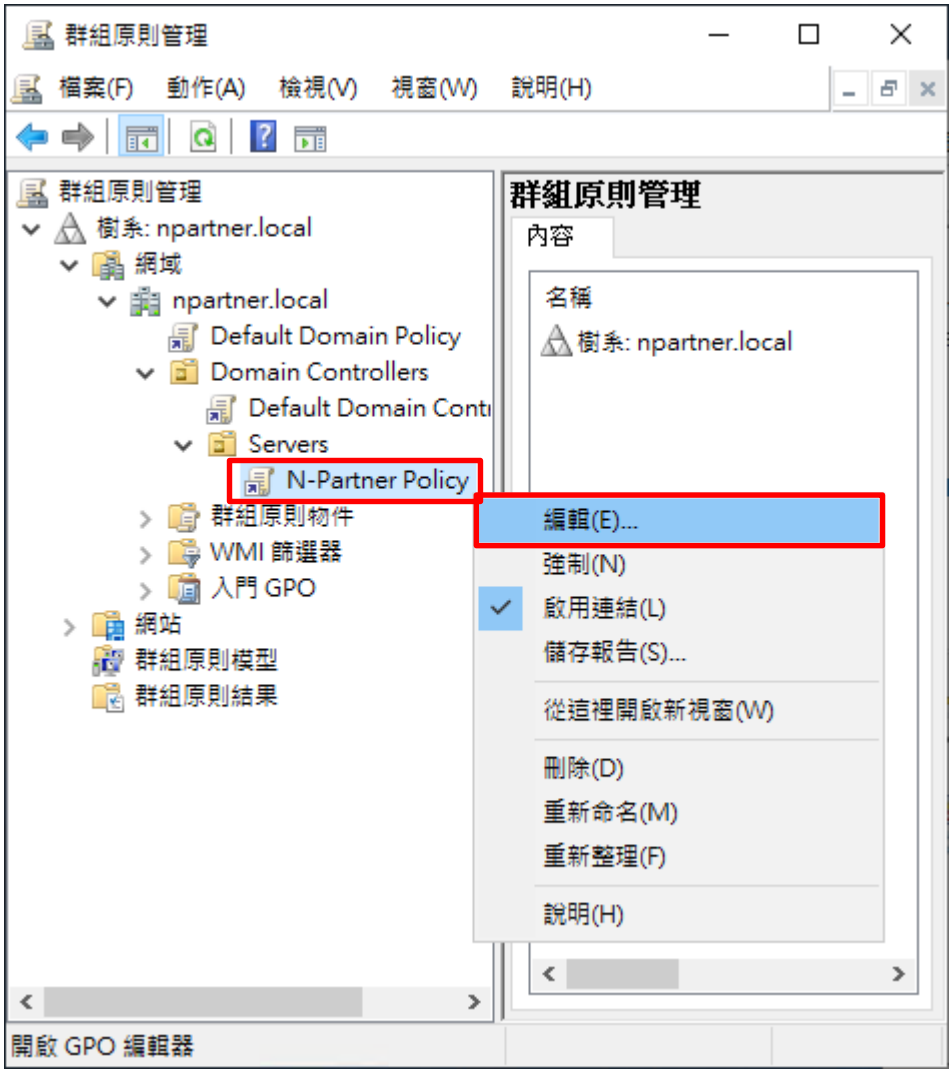
(1) 開啟群組原則管理

開啟 [群組原則管理]



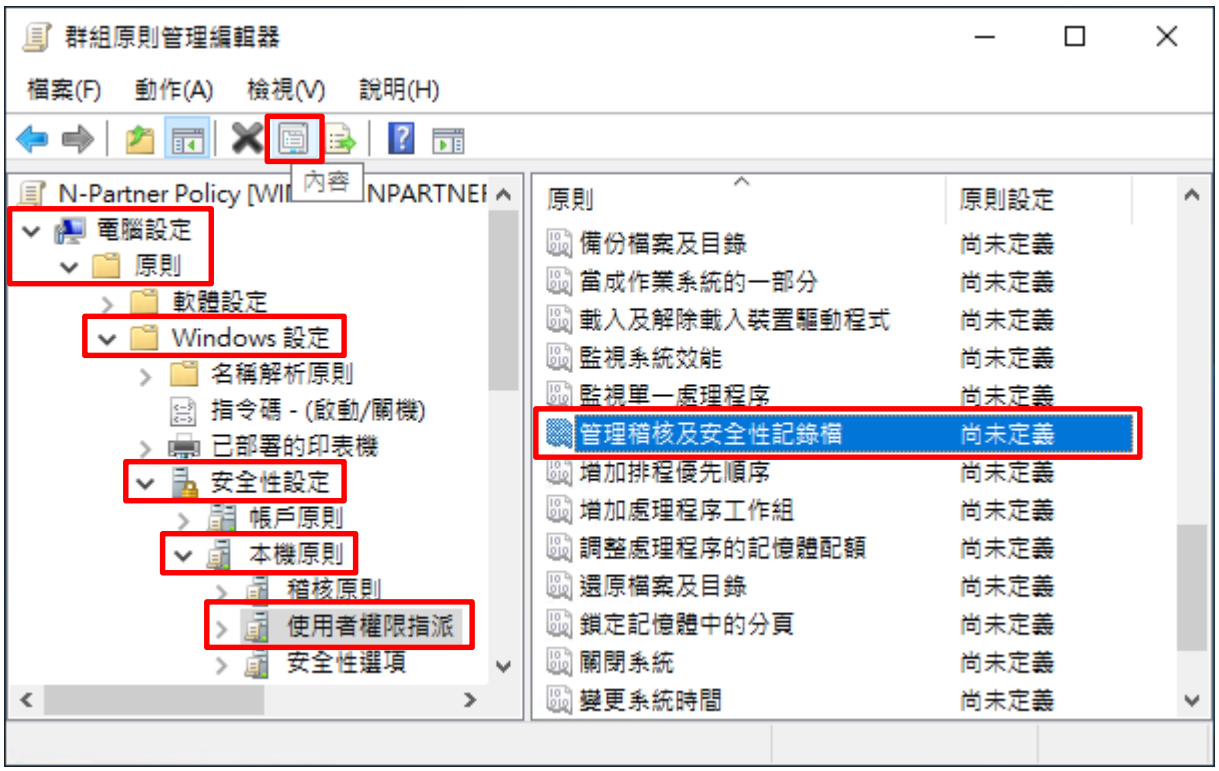
(2) 編輯群組原則物件

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 [管理稽核及安全性記錄檔] 項目 -> 點選  內容

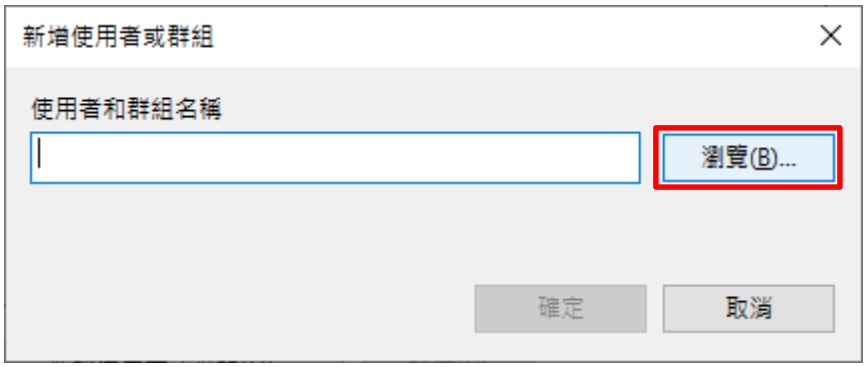


(4) 新增管理稽核使用者

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

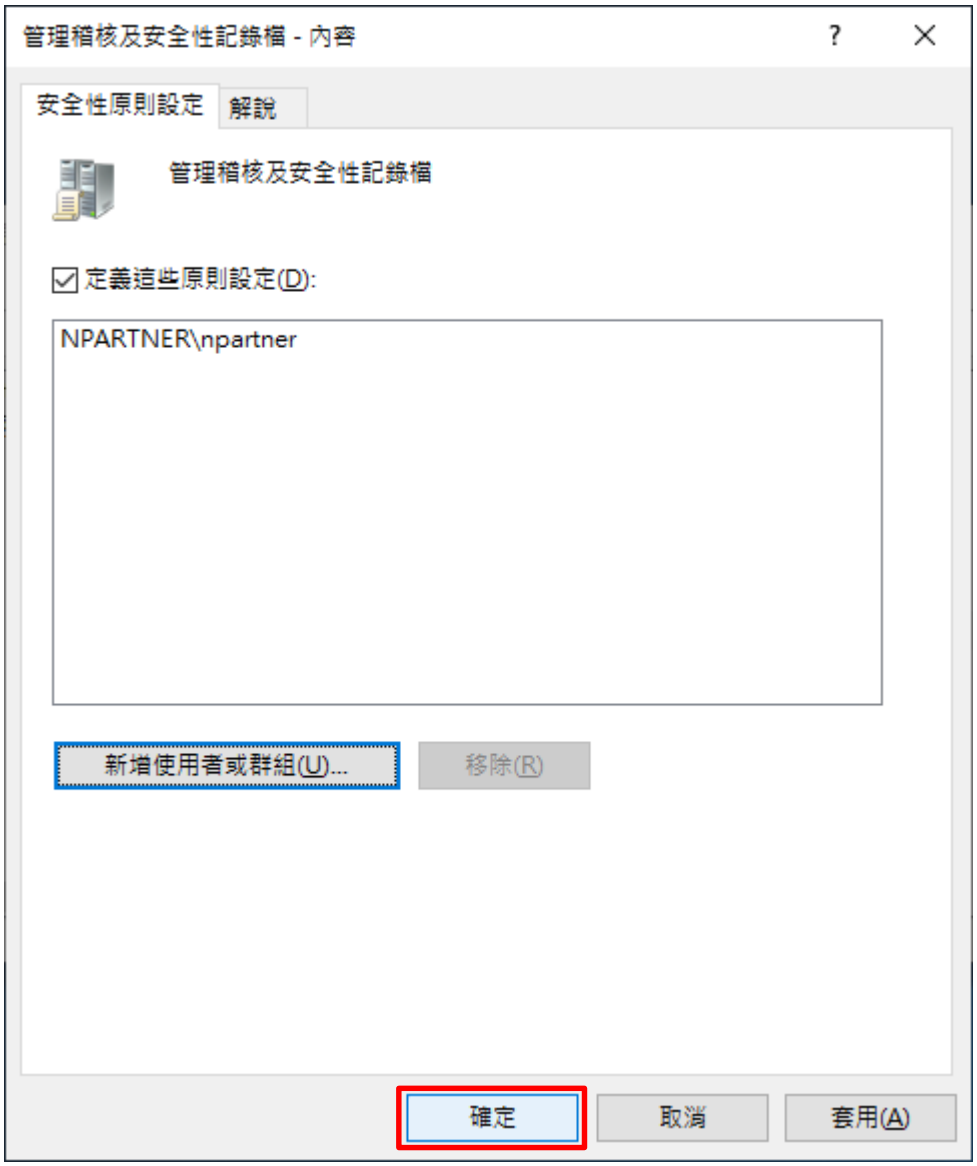
輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

(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:\> Invoke-GPUpdate -RandomDelayInMinutes 0 -Force
```

6.3.5 重啟 WMI 服務

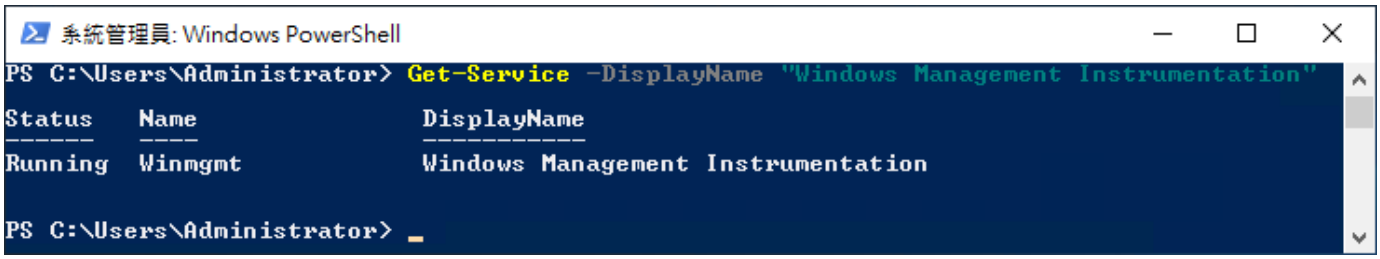
(1) 開啟 [Windows PowerShell]

(2) 重啟 WMI 服務

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

(3) 查看 WMI 服務

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

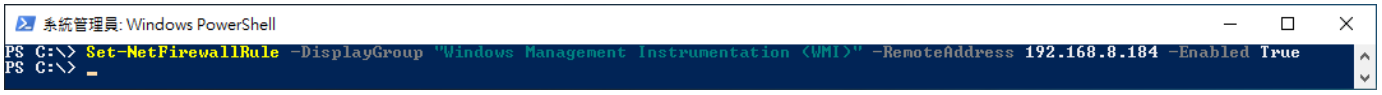


6.4 設定防火牆

(1) 開啟 [Windows PowerShell]

(2) 設定防火牆，只允許 N-Reporter IP query WMI

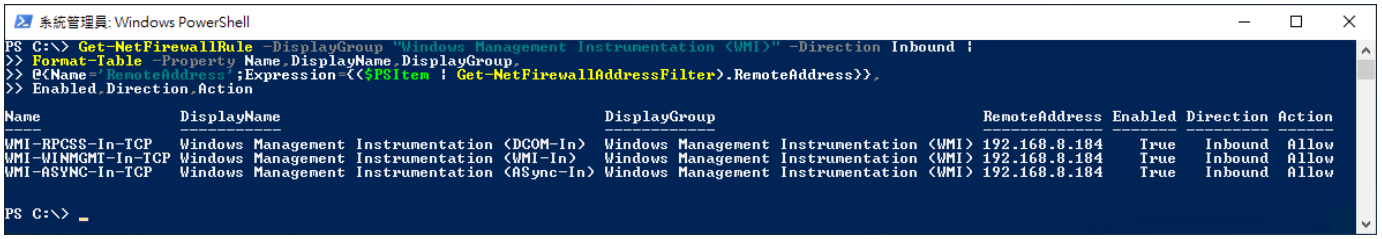
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress
192.168.8.184 -Enabled True
```



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

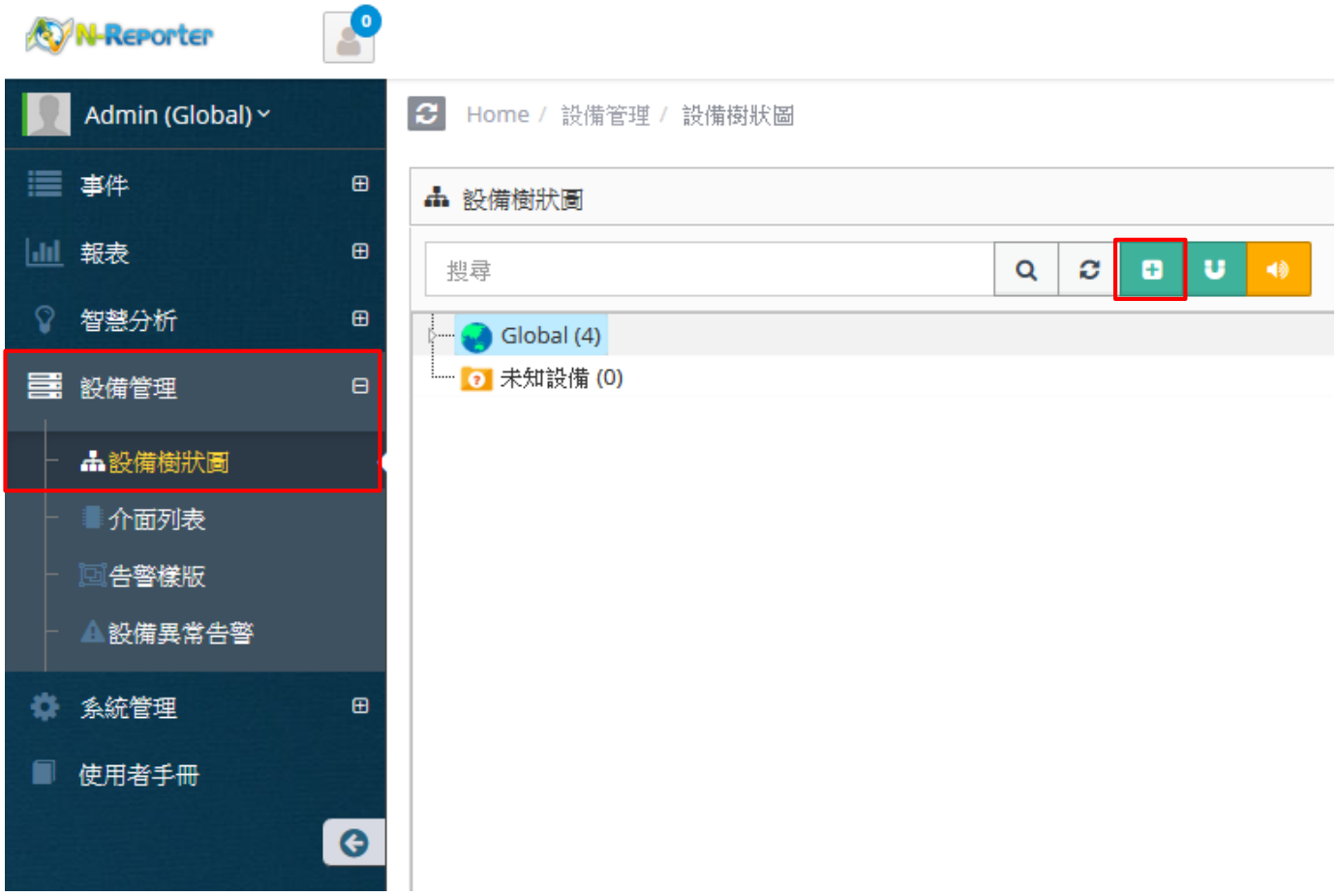
```
PS C:\> Get-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -Direction Inbound |
>> Format-Table -Property Name,DisplayName,DisplayGroup,
>> @{Name='RemoteAddress';Expression={($PSItem | Get-NetFirewallAddressFilter).RemoteAddress}},
>> Enabled,Direction,Action
```



7. N-Reporter

(1) 新增 Windows AD WMI 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]



7.1 Windows 2003 或之前版本作業系統

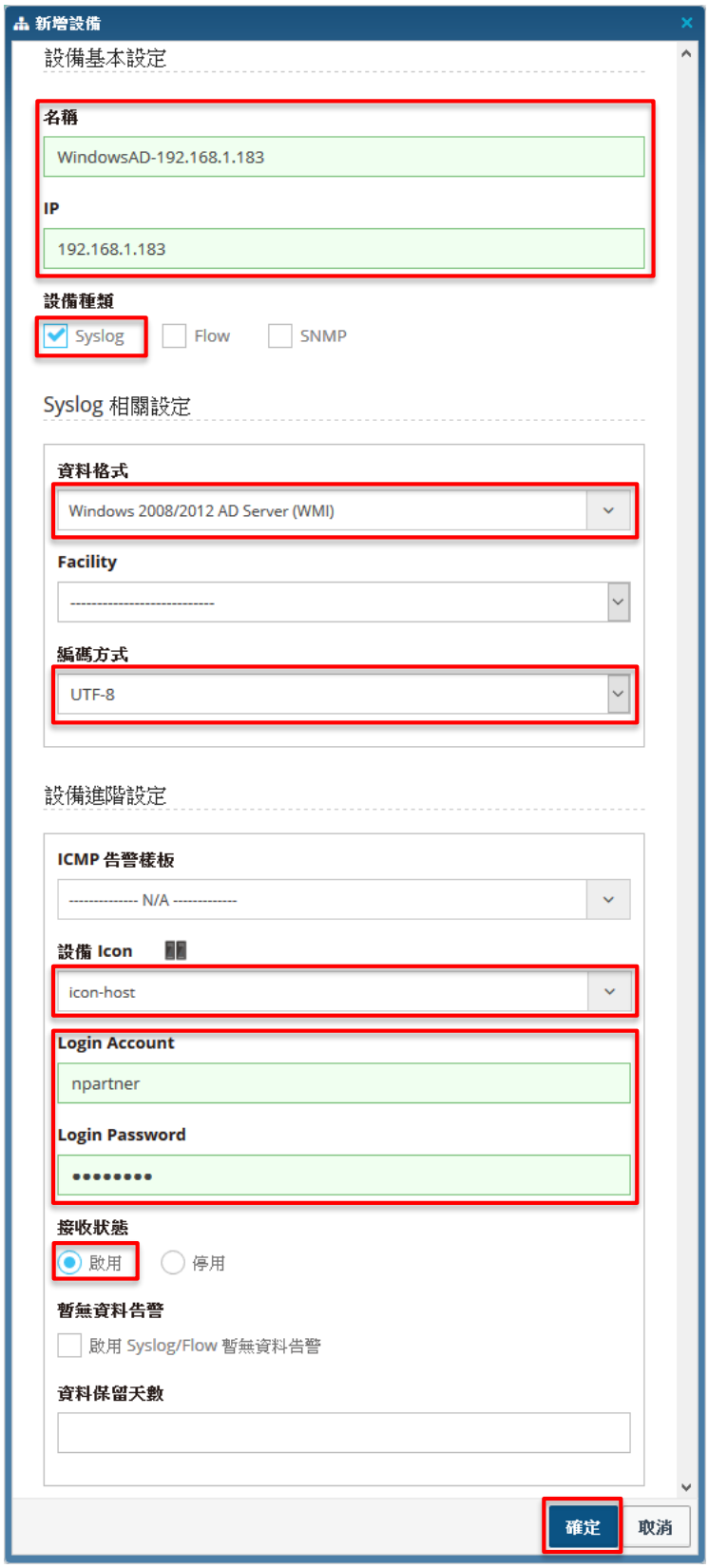
(2) 設定 Windows AD WMI 設備

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]

7.2 Windows 2008 或之後版本作業系統

(2) 設定 Windows AD WMI 設備

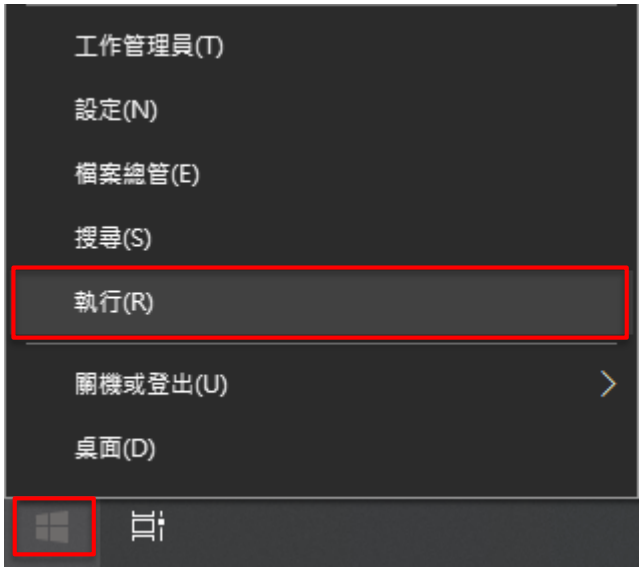
輸入名稱和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [Windows 2008/2012 AD Server (WMI)] 和編碼方式: [UTF-8] -> 選擇設備 Icon: [icon-host] -> 輸入 Windows AD 的 Login Account 和 Login Password -> 點選接收狀態: [啟用] -> 按 [確定]



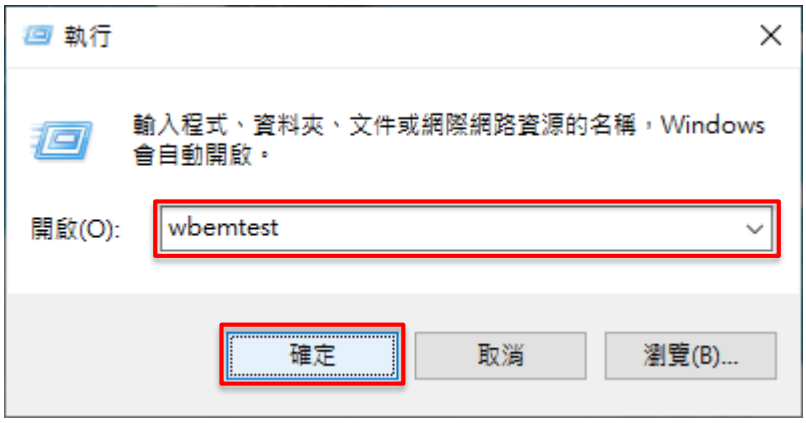
8. 問題排除

8.1 WMI Query Language 檢查

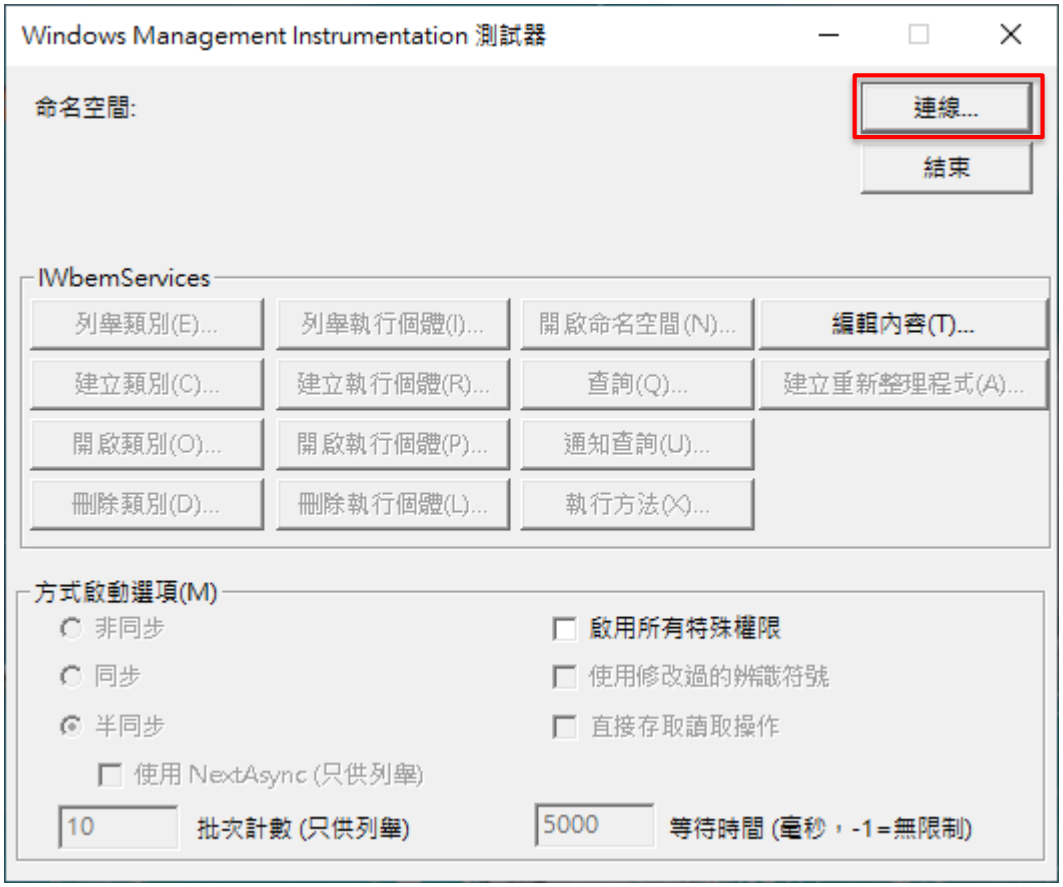
(1) 按  -> 點選 [執行]



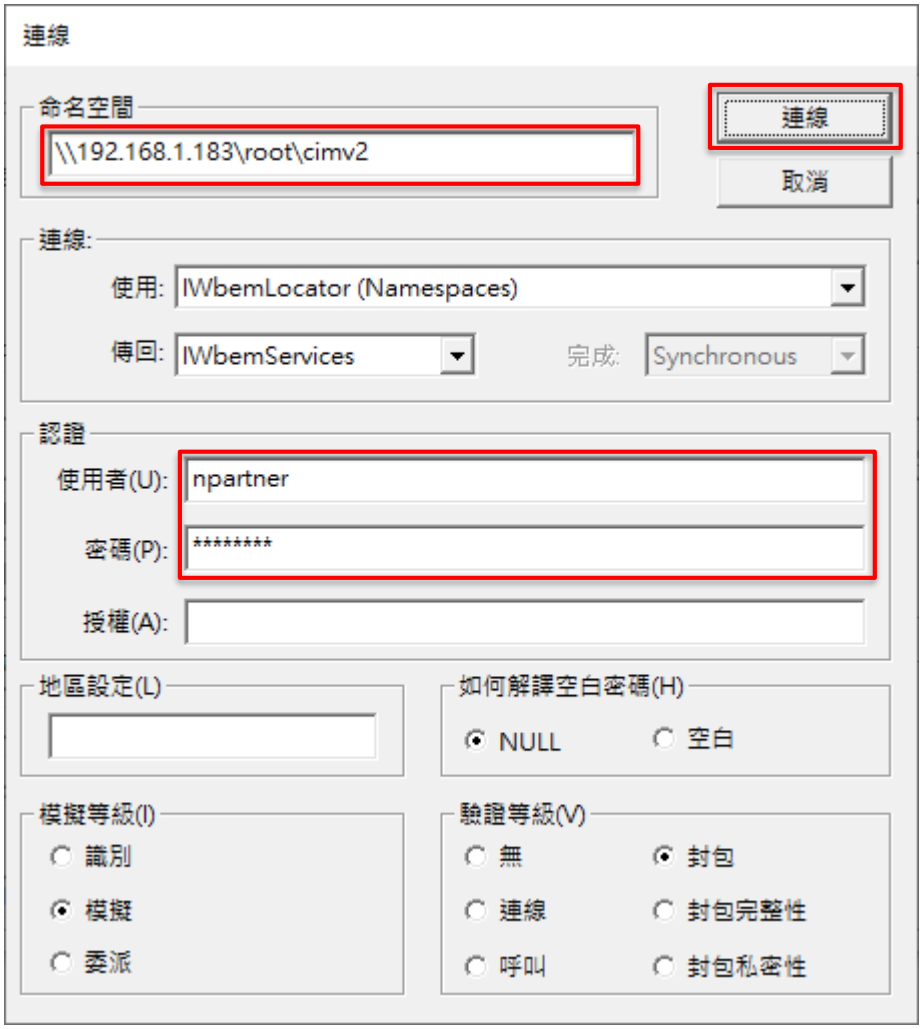
(2) 輸入 wbemtest -> 按 [確定]



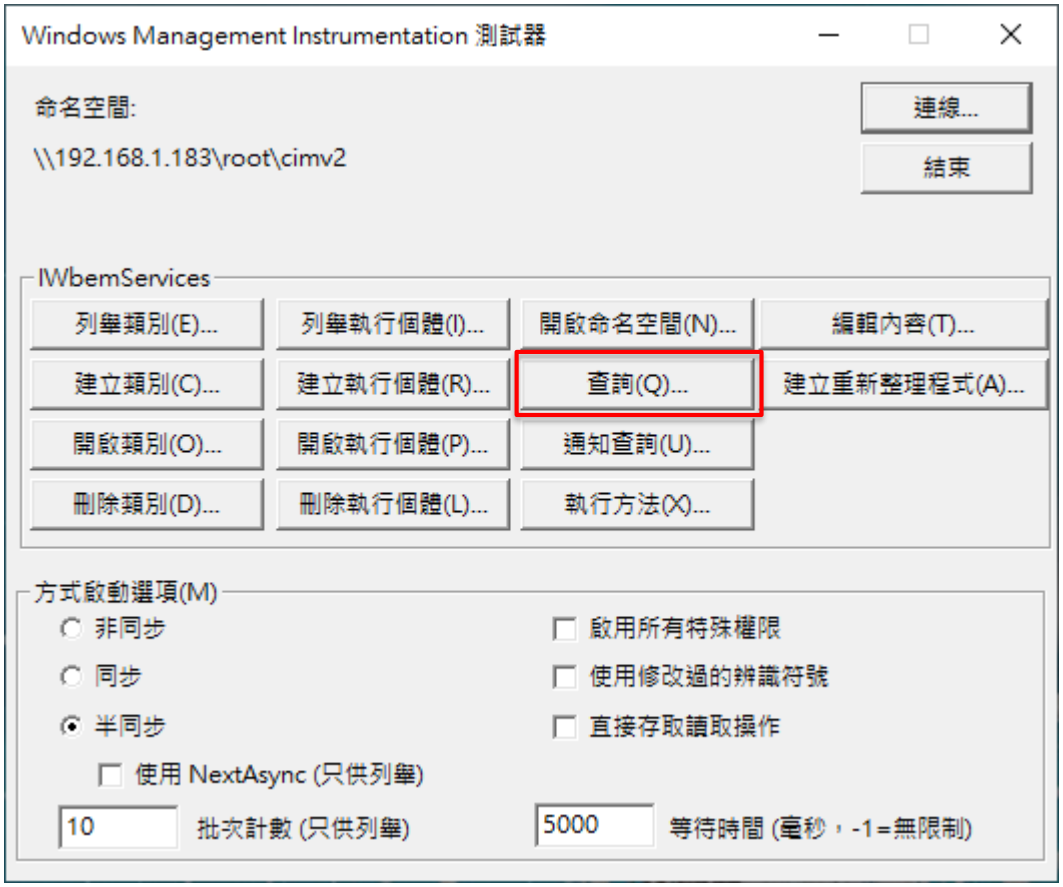
(3) 按 [連線]



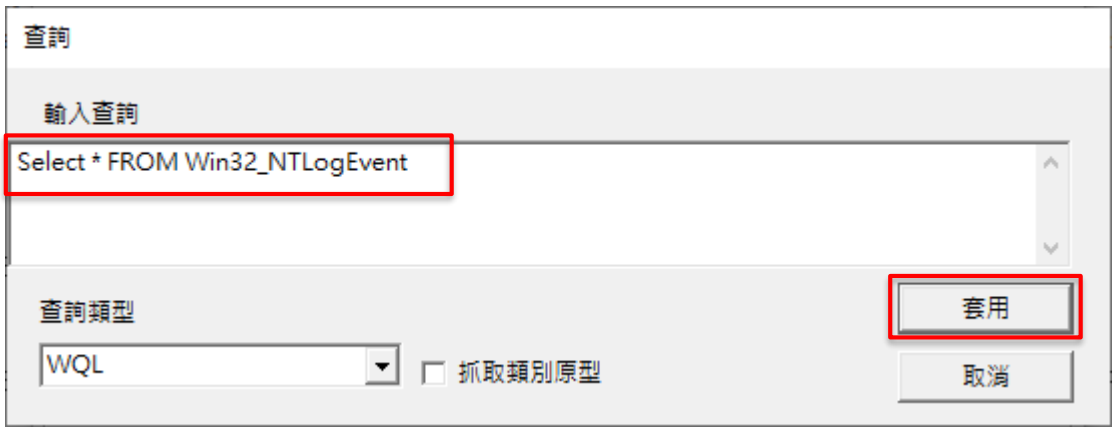
(4) 檢查**事件日誌**；輸入命名空間 \\<*Windows AD IP*>\root\cimv2 -> 使用者帳號和密碼 -> 按 [連線]



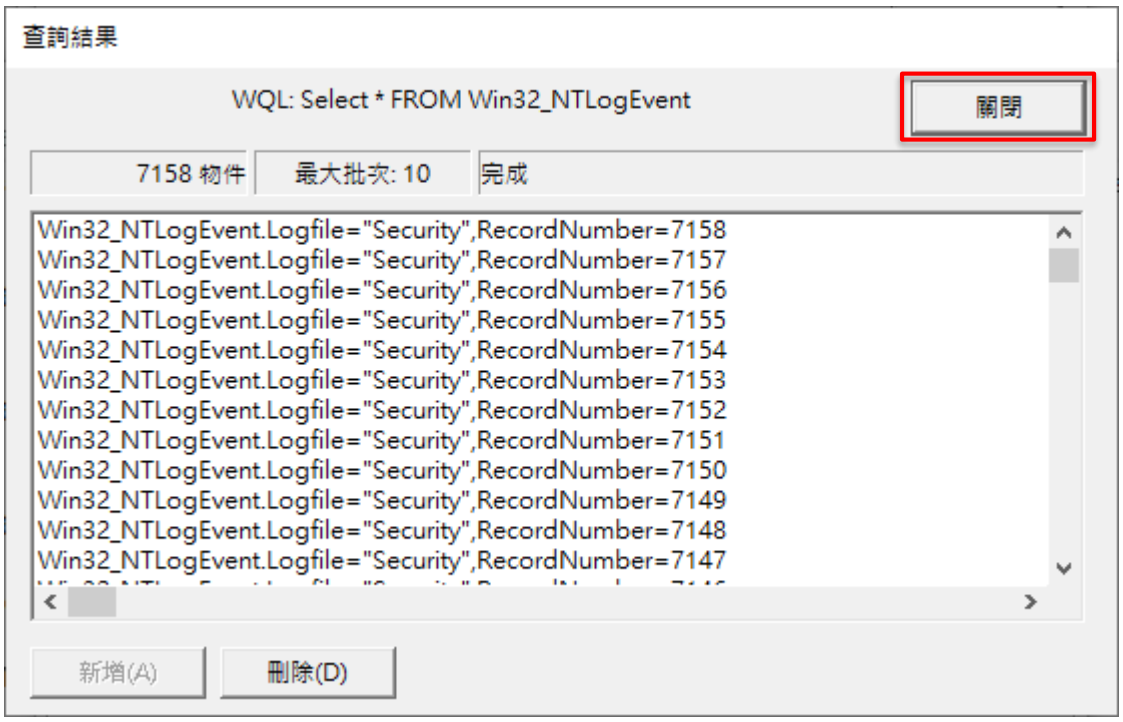
(5) 按 [查詢]



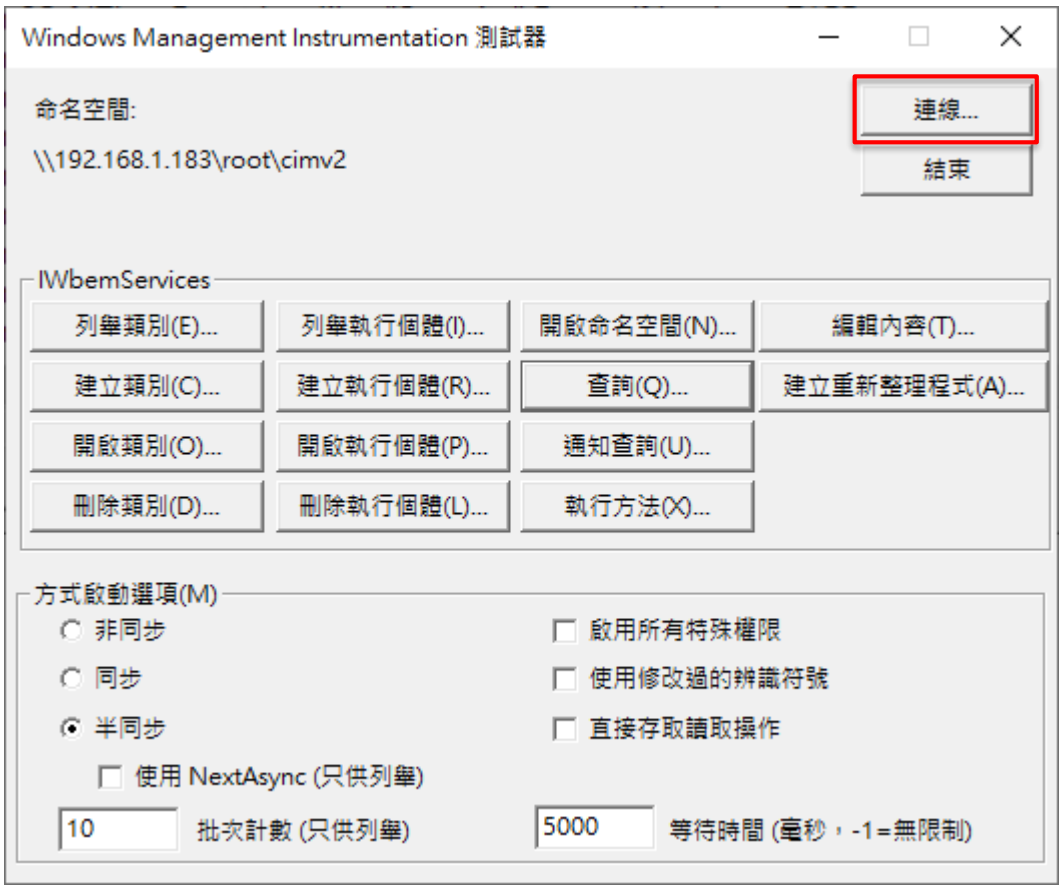
(6) 輸入查詢 Select * FROM Win32_NTLogEvent -> 按 [套用]



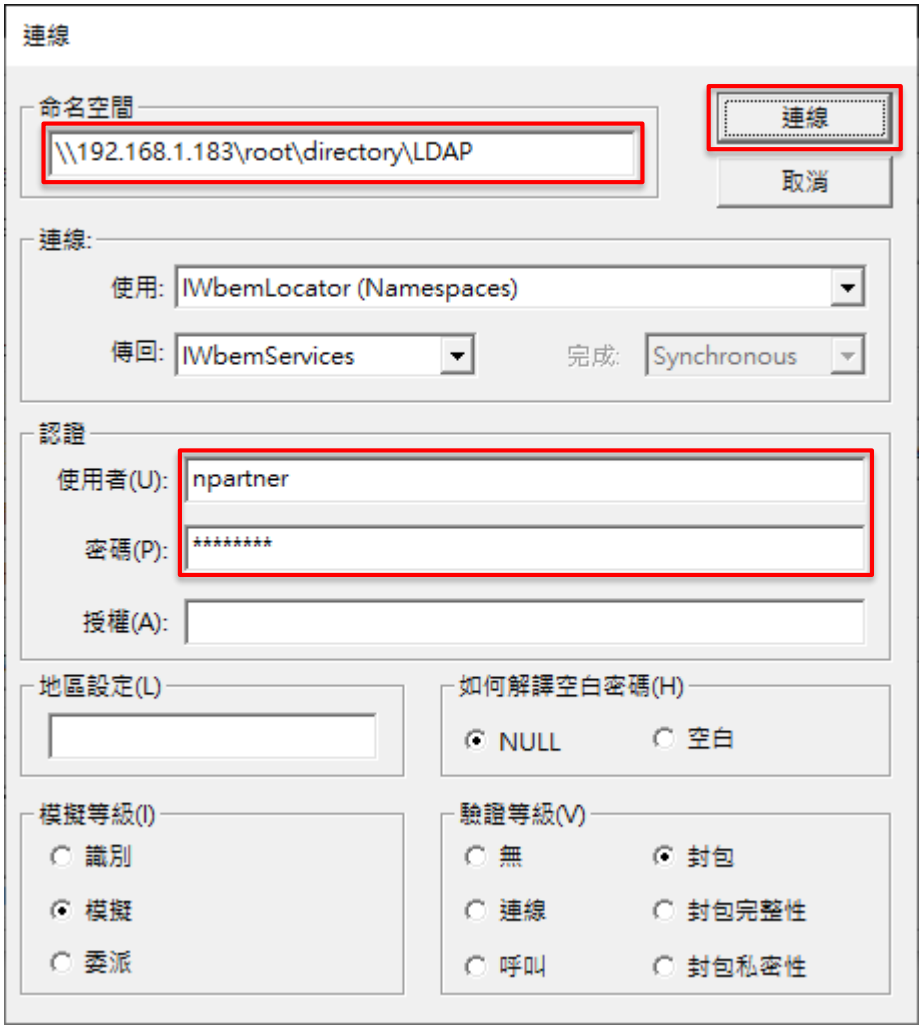
(7) 顯示查詢到資料 -> 按 [關閉]



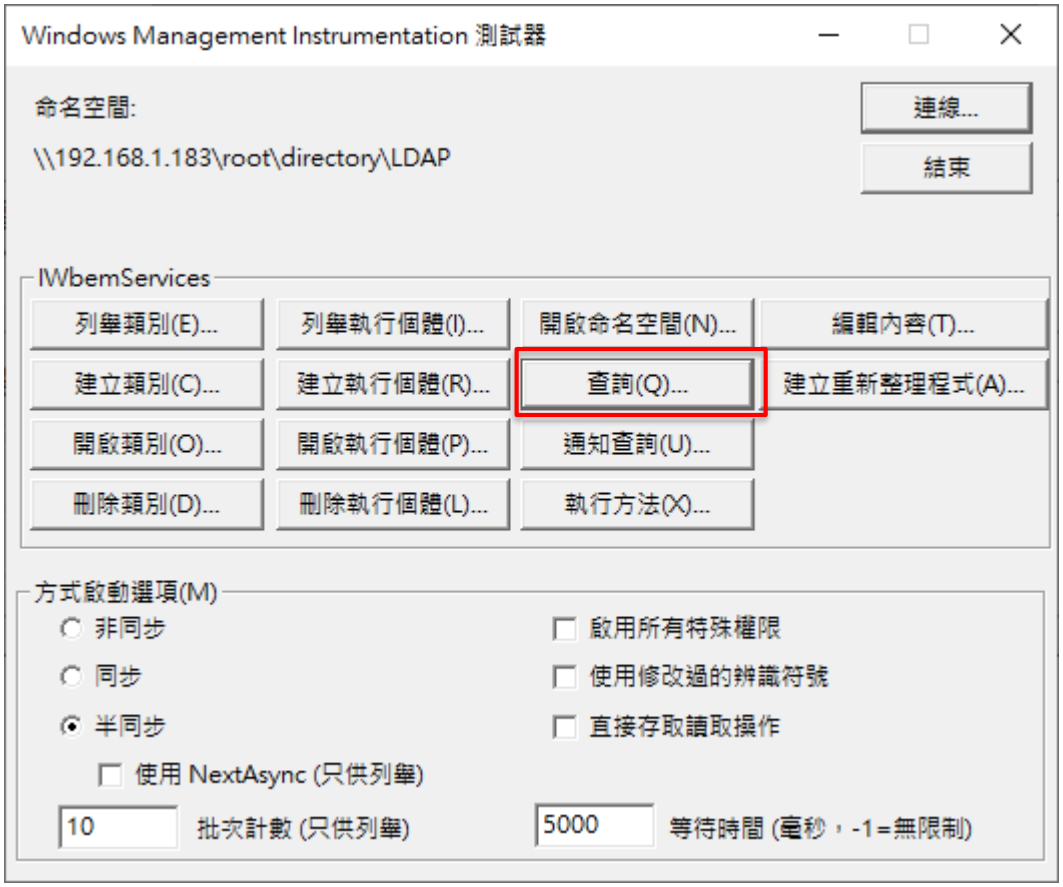
(8) 按 [連線]



(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]

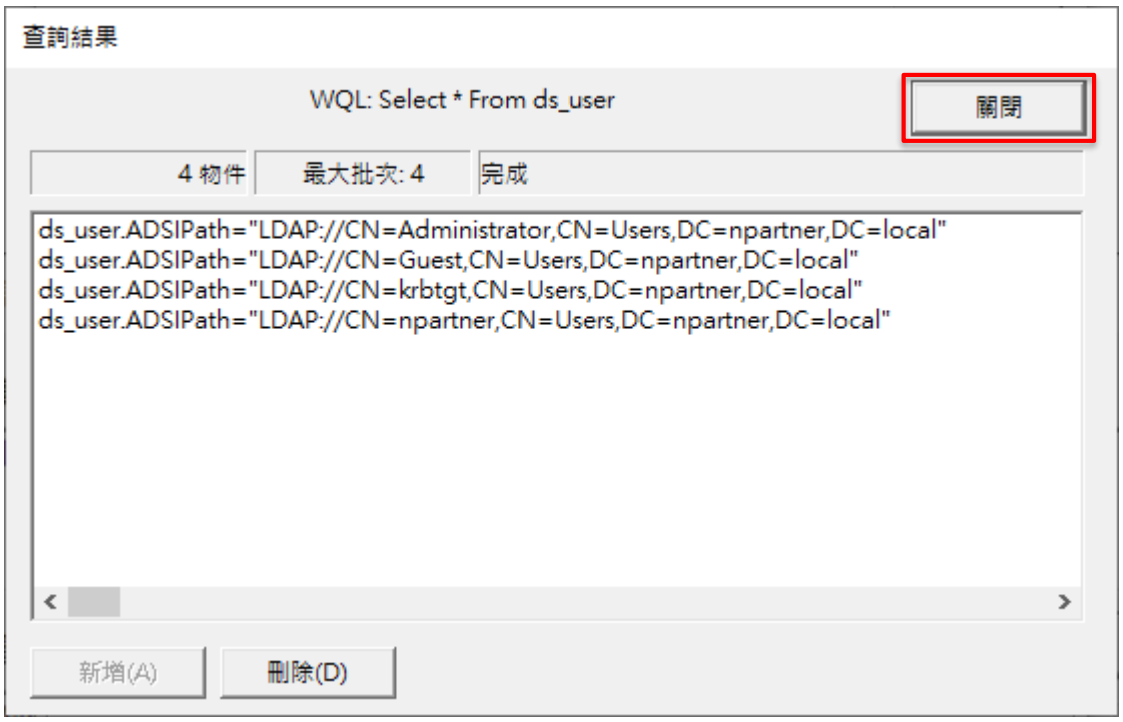


(10) 按 [查詢]

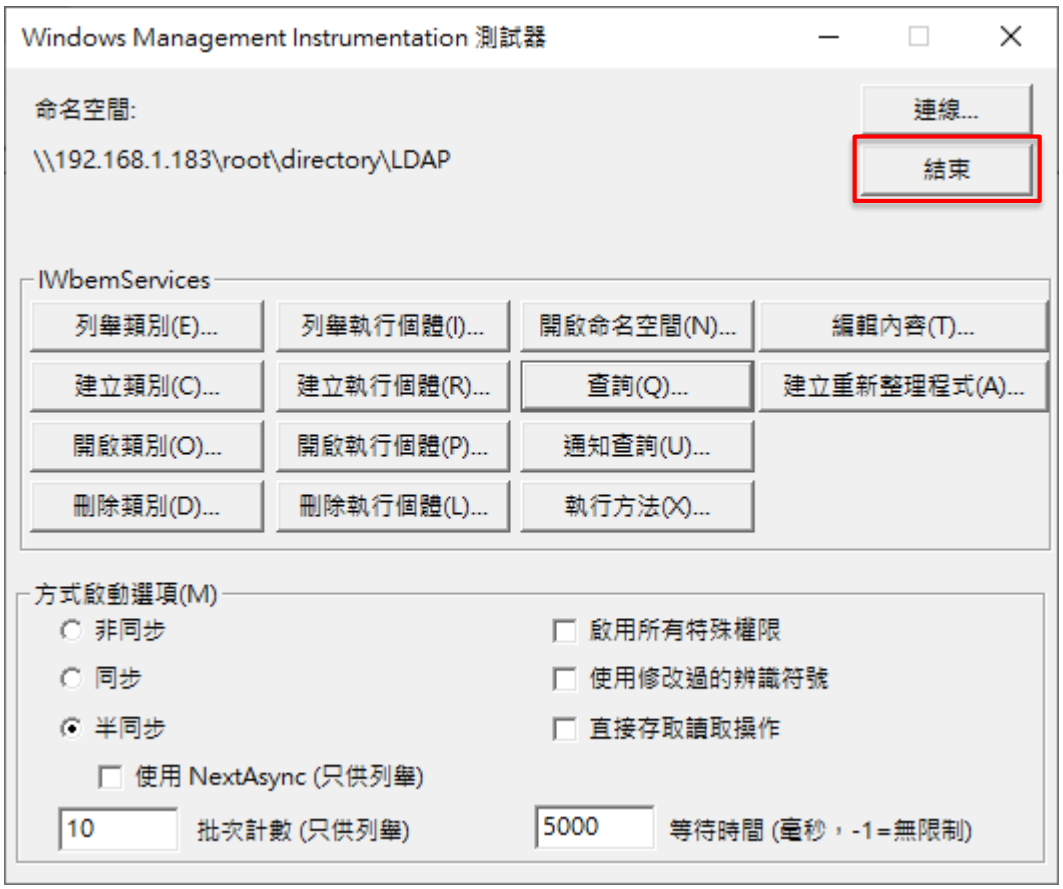


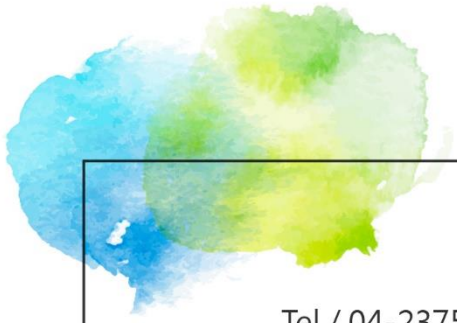
(11) 輸入查詢 Select * FROM ds_user -> 按 [套用]

(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