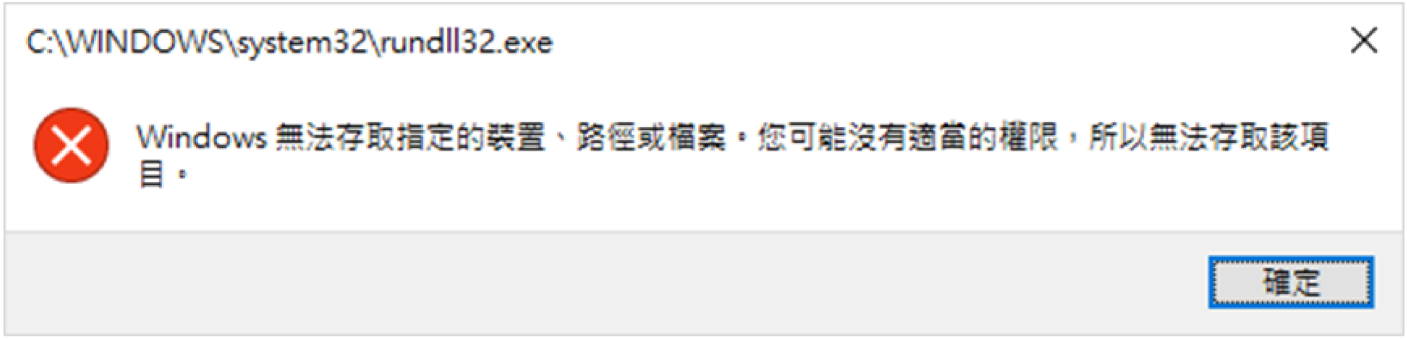
疑難雜症

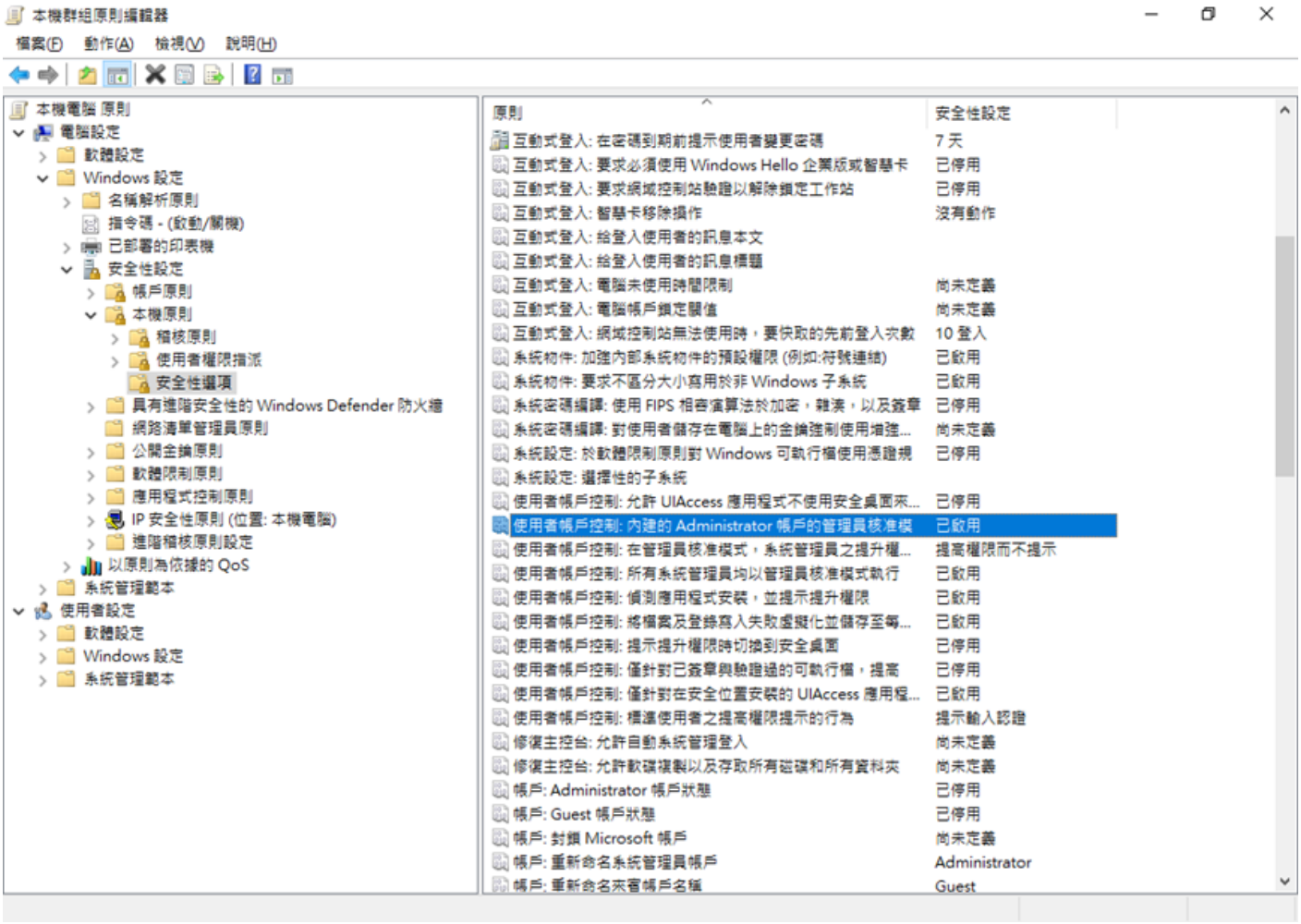
- Windows 10 / 2016+ Join Domain後進入設定跳出rundll32.exe沒有適當的權限
- Active Directory GPO 變更 Local Admin Password

Windows 10 / 2016+ Join Domain後進入設定跳出rundll32.exe沒

Windows 10 / 2016 Join Domain前都沒問題, 但Join Domain??????????????????



?? gpedit.msc => ???? => Windows?? => ????? => ???? => ????? => ??????? : ???Administrator?? xxxxxx ????”??”???????????


本機群組原則編輯器
檔案(F) 動作(A) 檢視(V) 說明(H)
本機電腦 原則
電腦設定
軟體設定
Windows 設定
名稱解析原則
指令碼 - (啟動/關機)
已部署的印表機
安全性設定
帳戶原則
本機原則
稽核原則
使用者權限指派
安全性選項
具有進階安全性的 Windows Defender 防火牆
網路清單管理員原則
公開金鑰原則
軟體限制原則
應用程式控制原則
IP 安全性原則 (位置: 本機電腦)
進階稽核原則設定
以原則為依據的 QoS
系統管理範本
使用者設定
軟體設定
Windows 設定
系統管理範本
原則
安全性設定
互動式登入: 在密碼到期前提示使用者變更密碼 7 天
互動式登入: 要求必須使用 Windows Hello 企業版或智慧卡 已停用
互動式登入: 要求網域控制站驗證以解除鎖定工作站 已停用
互動式登入: 智慧卡移除操作 沒有動作
互動式登入: 給登入使用者的訊息本文
互動式登入: 給登入使用者的訊息標題
互動式登入: 電腦未使用時間限制 尚未定義
互動式登入: 電腦帳戶鎖定閾值 尚未定義
互動式登入: 網域控制站無法使用時，要快取的先前登入次數 10 登入
系統物件: 加強內部系統物件的預設權限 (例如:符號連結) 已啟用
系統物件: 要求不區分大小寫用於非 Windows 子系統 已啟用
系統密碼編譯: 使用 FIPS 相容演算法於加密，雜湊，以及簽章 已停用
系統密碼編譯: 對使用者儲存在電腦上的金鑰強制使用增強... 尚未定義
系統設定: 於軟體限制原則對 Windows 可執行檔使用憑證規 已停用
系統設定: 選擇性的子系統
使用者帳戶控制: 允許 UIAccess 應用程式不使用安全桌面來... 已停用
使用者帳戶控制: 內建的 Administrator 帳戶的管理員核准模 已啟用
使用者帳戶控制: 在管理員核准模式，系統管理員之提升權... 提高權限而不提示
使用者帳戶控制: 所有系統管理員均以管理員核准模式執行 已啟用
使用者帳戶控制: 偵測應用程式安裝，並提示提升權限 已啟用
使用者帳戶控制: 將檔案及登錄寫入失敗虛擬化並儲存至每... 已啟用
使用者帳戶控制: 提示提升權限時切換到安全桌面 已停用
使用者帳戶控制: 僅針對已簽章與驗證過的可執行檔，提高 已停用
使用者帳戶控制: 僅針對在安全位置安裝的 UIAccess 應用程... 已啟用
使用者帳戶控制: 標準使用者之提高權限提示的行為 提示輸入認證
修復主控台: 允許自動系統管理登入 尚未定義
修復主控台: 允許軟碟複製以及存取所有磁碟和所有資料夾 尚未定義
帳戶: Administrator 帳戶狀態 已停用
帳戶: Guest 帳戶狀態 已停用
帳戶: 封鎖 Microsoft 帳戶 尚未定義
帳戶: 重新命名系統管理員帳戶 Administrator
帳戶: 重新命名來賓帳戶名稱 Guest

Active Directory GPO 變更 Local Admin Password

前言

最近剛好有個有個Case，要透過AD更改Local Admin User Password，紀錄一下設定方式。

> ‼請注意，由於密碼是明碼，請在變更完後一段時間將此GPO與ps1刪除，以策安全。

環境

Server: Windows 2019 Active Directory

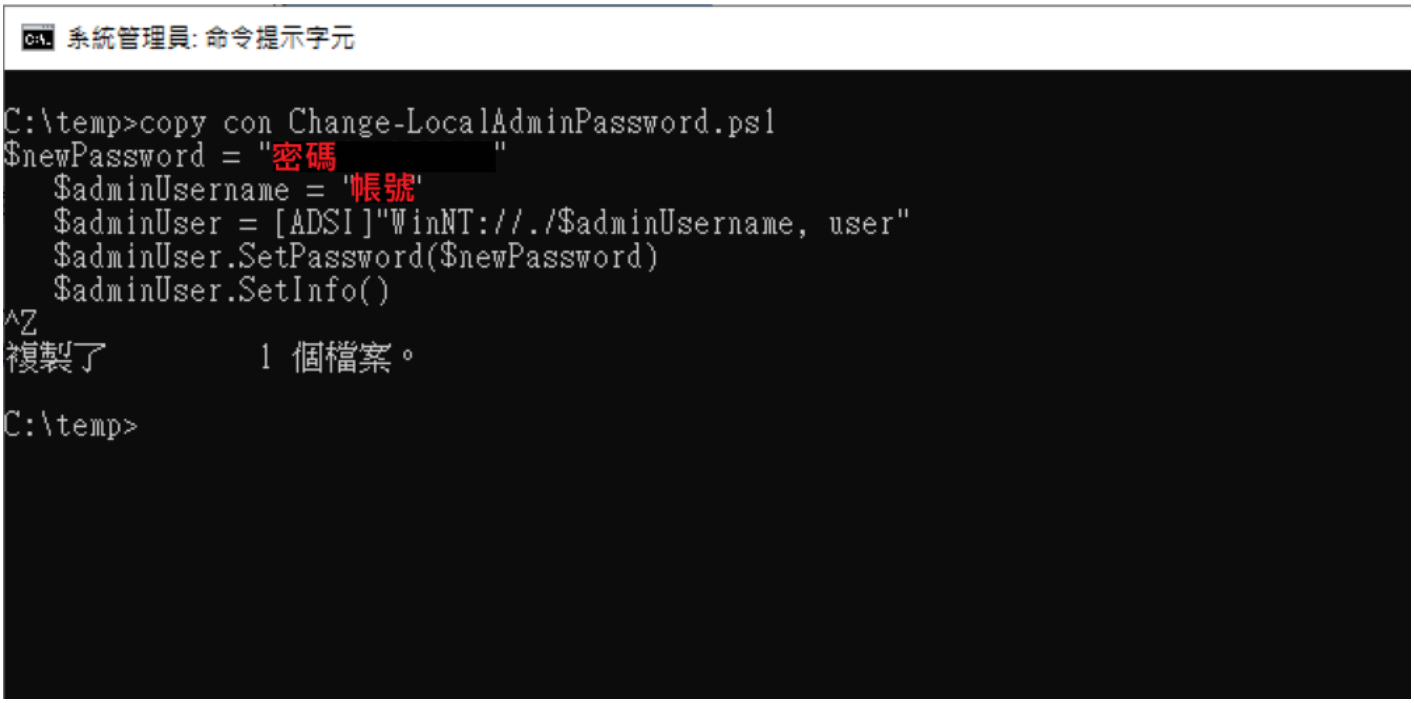
Client: Windows 11 Pro

設定方式

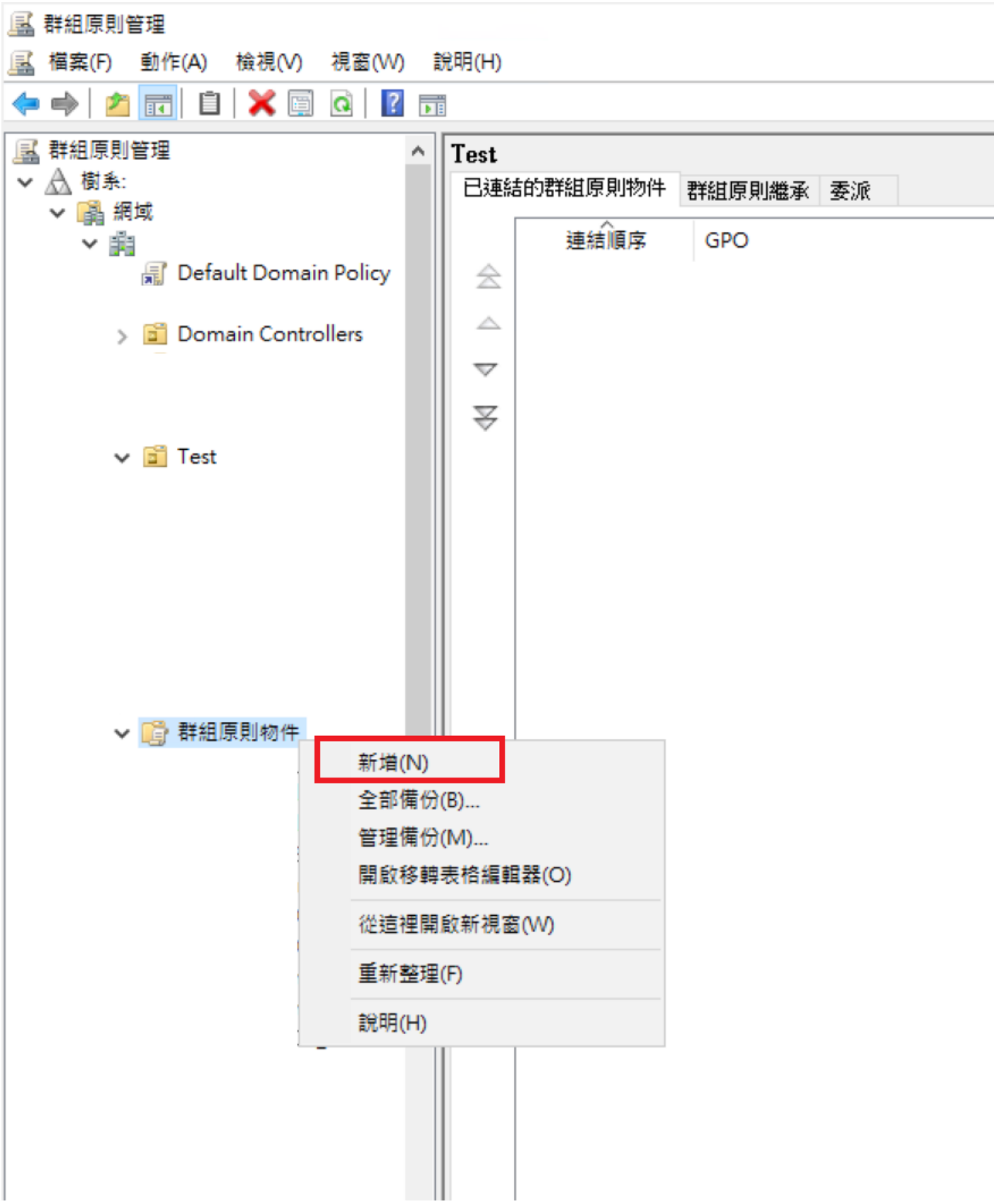
1、首先，先建議一個 Power Shell ps1檔備用。

執行命令提示字元 "cmd"，我在 C:\temp下面透過 Copy con建立一個 Change-LocalAdminPassword.ps1，將下面的指令貼入，最後 Ctrl+Z儲存

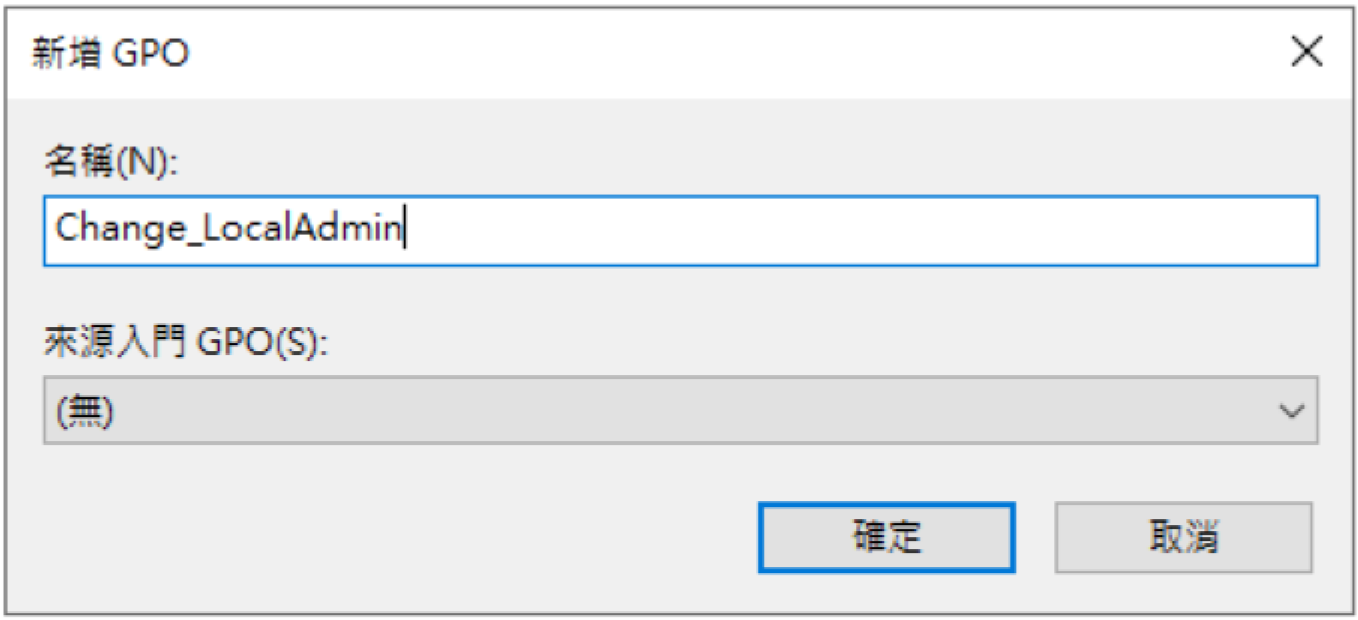
```
$newPassword = "密碼"
$adminUsername = "帳號"
$adminUser = [ADSI]"WinNT://./$adminUsername, user"
$adminUser.SetPassword($newPassword)
$adminUser.SetInfo()
```


系統管理員: 命令提示字元
C:\temp>copy con Change-LocalAdminPassword.ps1
$newPassword = "密碼
$adminUsername = '帳號'
$adminUser = [ADSI]"WinNT://./$adminUsername, user"
$adminUser.SetPassword($newPassword)
$adminUser.SetInfo()
^Z
複製了 1 個檔案。
C:\temp>

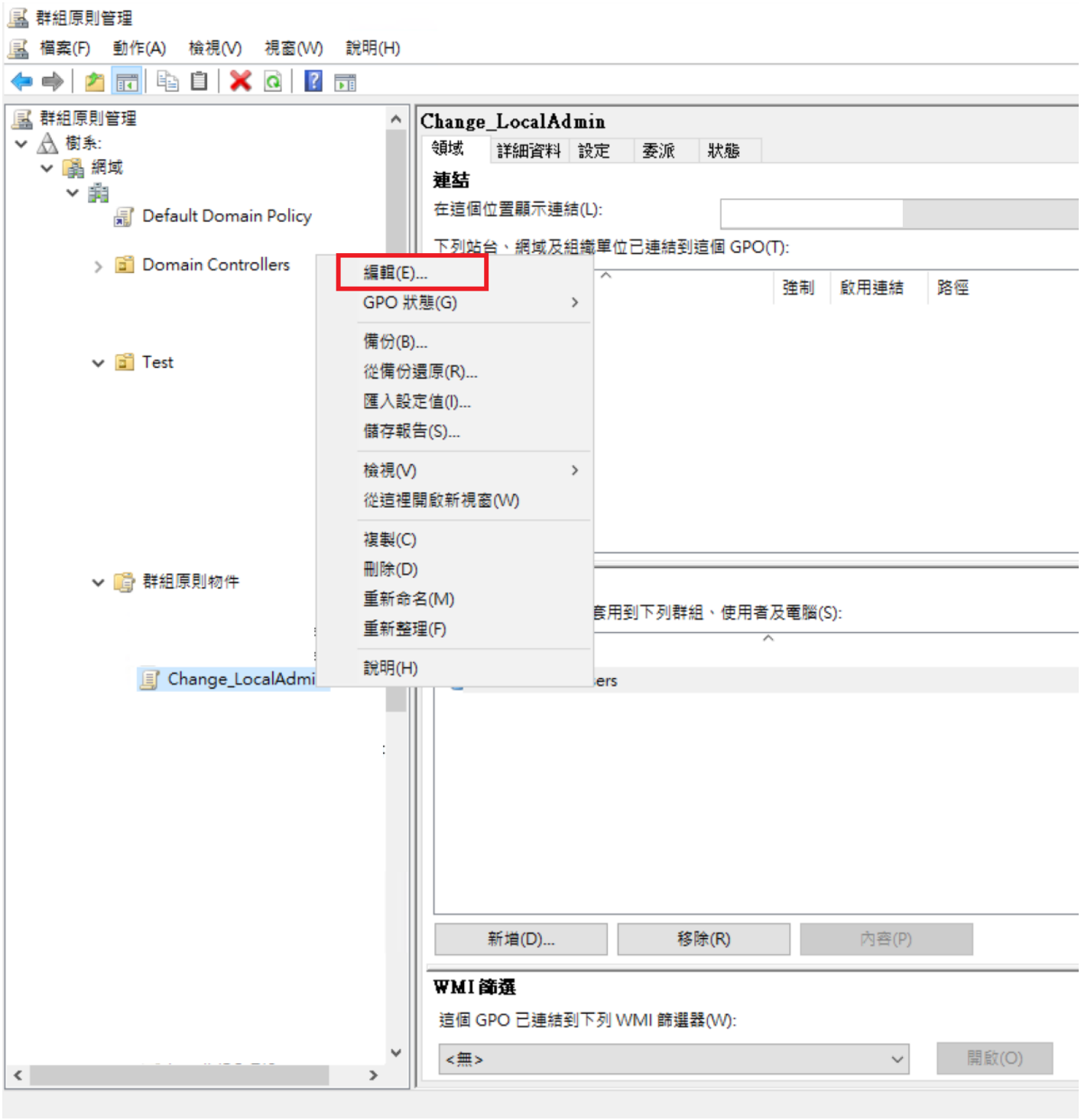
2□□□□□□□□□□□□□□□□



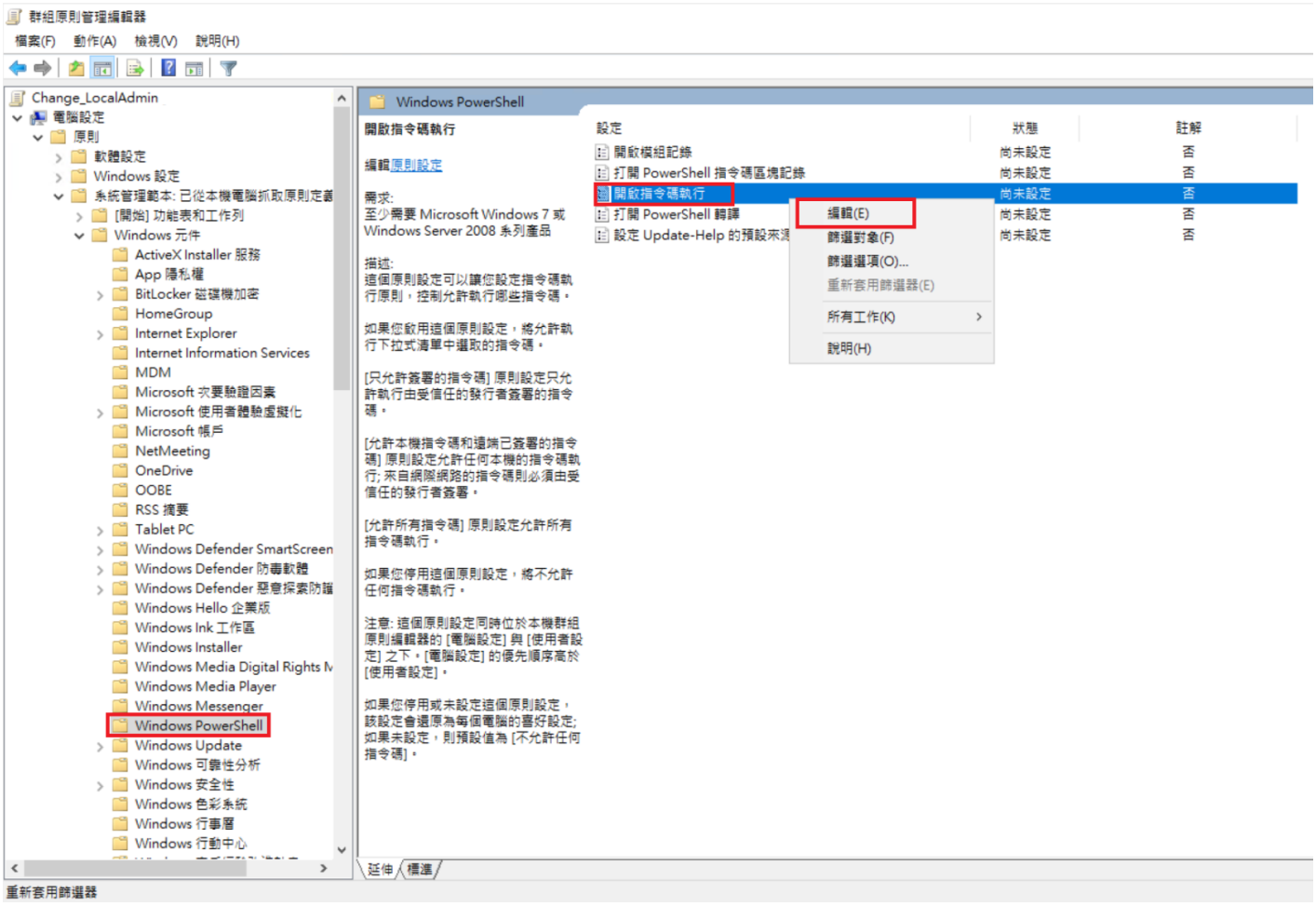
□□□□ Change_LocalAdmin□GPO□

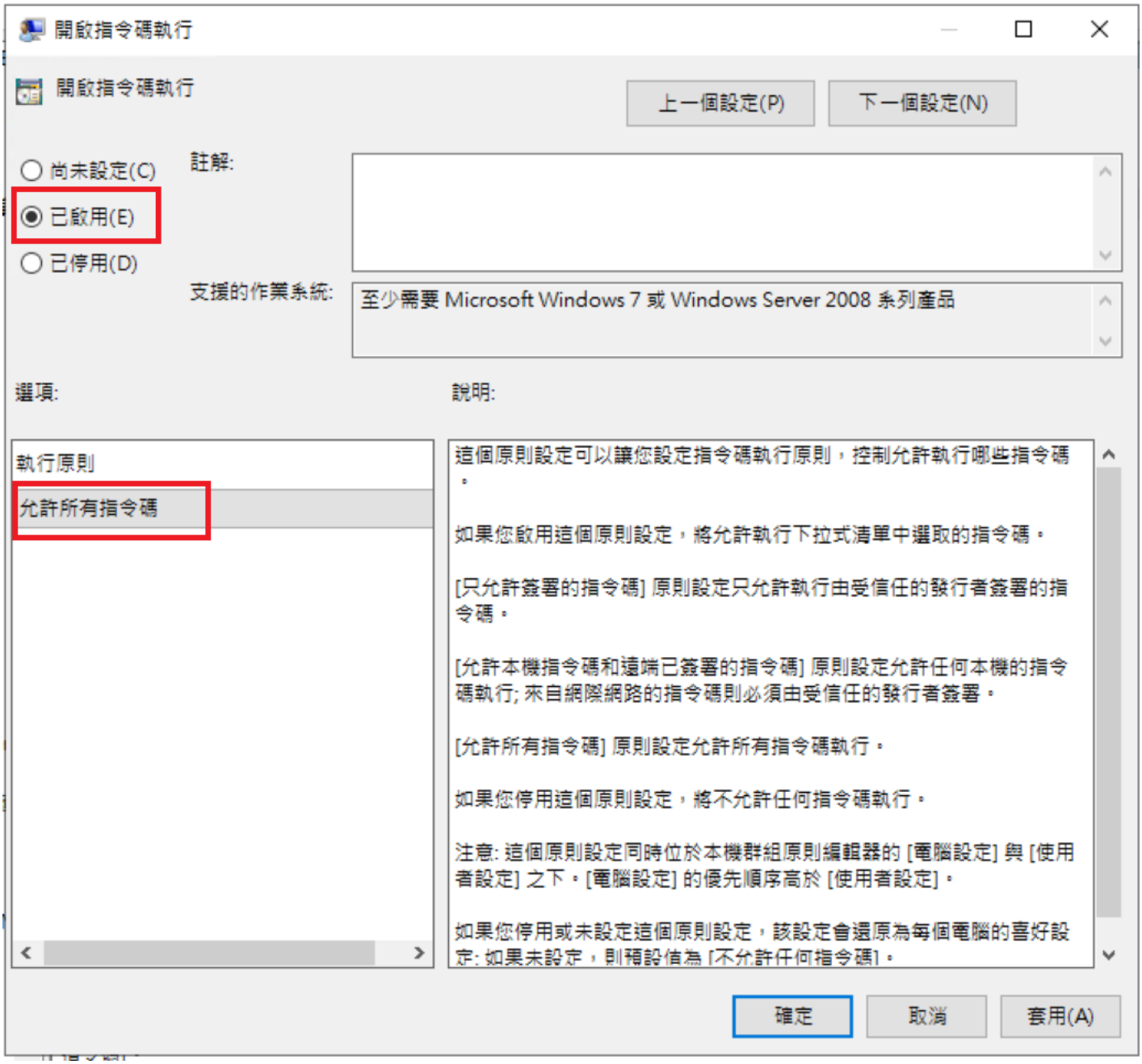


3、針對剛剛建立的物件進行編輯。

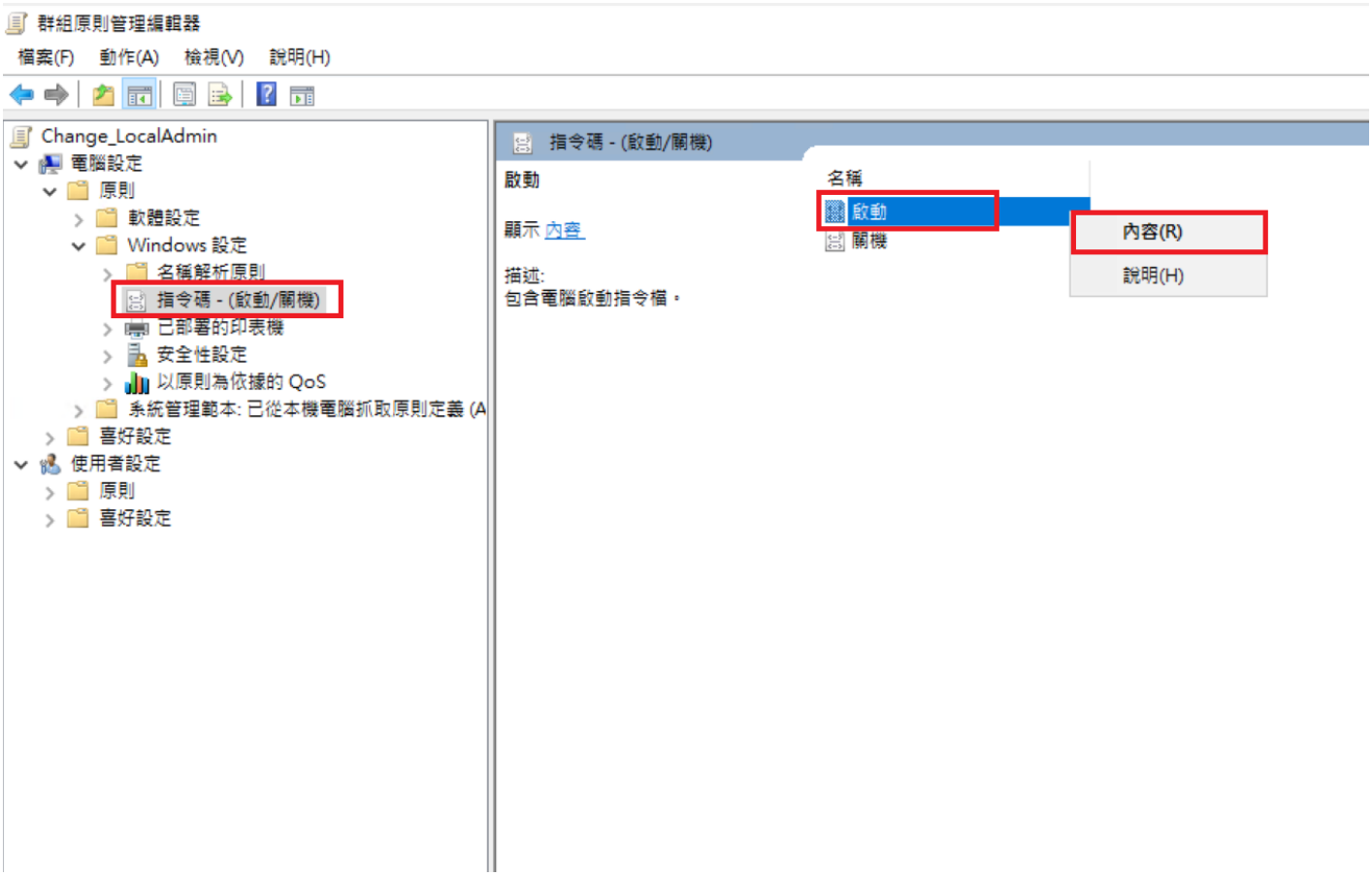


至 電腦設定 => 原則 => 系統管理範本 => Windows元件 => Windows PowerShell => 開啟指令碼執行, 允許指令碼執行。

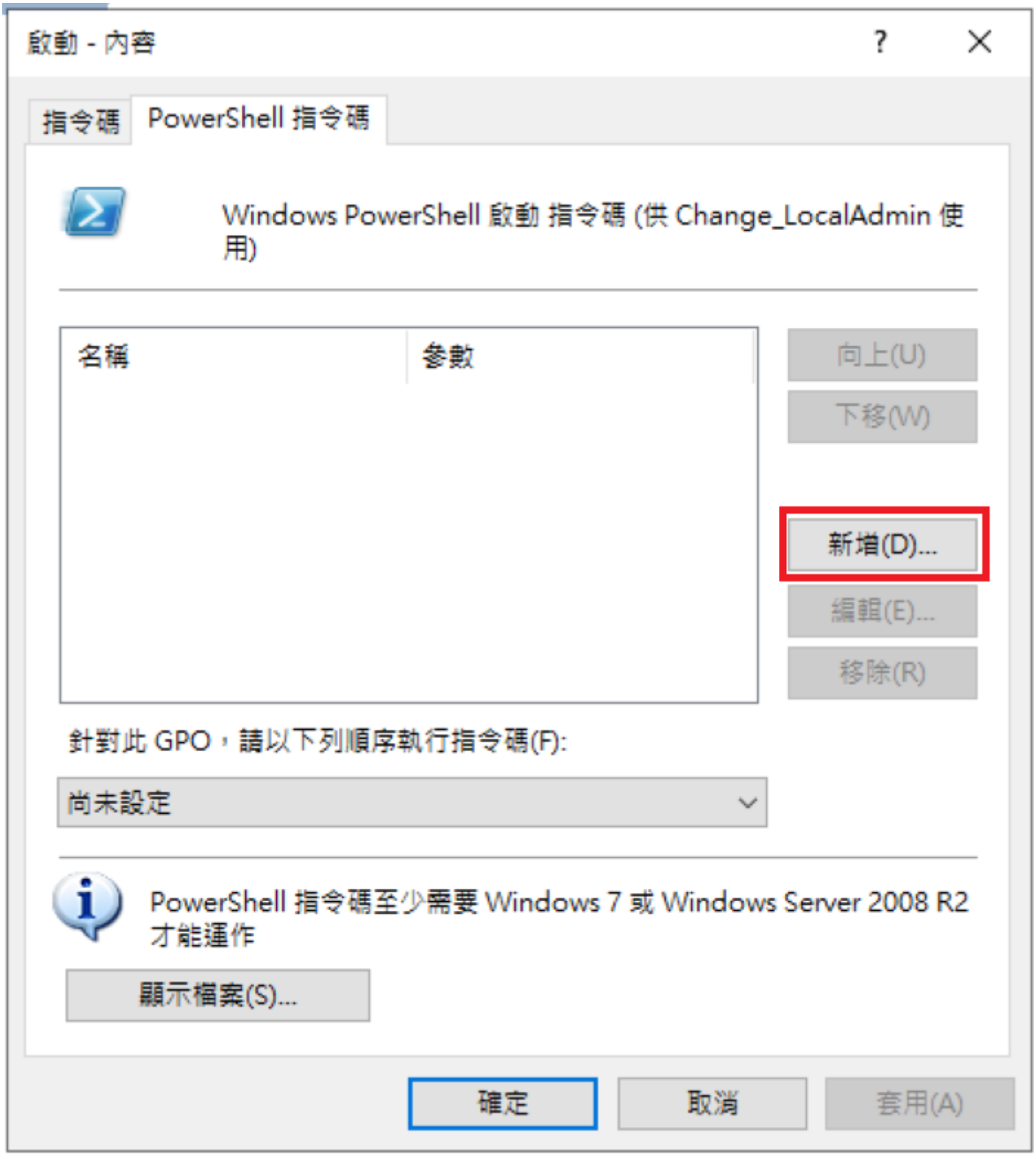

群組原則管理編輯器
檔案(F) 動作(A) 檢視(V) 說明(H)
Change_LocalAdmin
電腦設定
原則
軟體設定
Windows 設定
系統管理範本: 已從本機電腦抓取原則定義
[開始] 功能表和工作列
Windows 元件
ActiveX Installer 服務
App 隱私權
BitLocker 磁碟機加密
HomeGroup
Internet Explorer
Internet Information Services
MDM
Microsoft 次要驗證因素
Microsoft 使用者體驗虛擬化
Microsoft 帳戶
NetMeeting
OneDrive
OOBE
RSS 摘要
Tablet PC
Windows Defender SmartScreen
Windows Defender 防毒軟體
Windows Defender 惡意探索防護
Windows Hello 企業版
Windows Ink 工作區
Windows Installer
Windows Media Digital Rights M
Windows Media Player
Windows Messenger
Windows PowerShell
Windows Update
Windows 可靠性分析
Windows 安全性
Windows 色彩系統
Windows 行事曆
Windows 行動中心
Windows PowerShell
開啟指令碼執行
編輯原則設定
需求:
至少需要 Microsoft Windows 7 或 Windows Server 2008 系列產品
描述:
這個原則設定可以讓您設定指令碼執行原則，控制允許執行哪些指令碼。
如果您啟用這個原則設定，將允許執行下拉式清單中選取的指令碼。
[只允許簽署的指令碼] 原則設定只允許執行由受信任的發行者簽署的指令碼。
[允許本機指令碼和遠端已簽署的指令碼] 原則設定允許任何本機的指令碼執行; 來自網際網路的指令碼則必須由受信任的發行者簽署。
[允許所有指令碼] 原則設定允許所有指令碼執行。
如果您停用這個原則設定，將不允許任何指令碼執行。
注意: 這個原則設定同時位於本機群組原則編輯器的 [電腦設定] 與 [使用者設定] 之下，[電腦設定] 的優先順序高於 [使用者設定]。
如果您停用或未設定這個原則設定，該設定會還原為每個電腦的喜好設定; 如果未設定，則預設值為 [不允許任何指令碼]。
設定
狀態
註解
開啟模組記錄
尚未設定
否
打開 PowerShell 指令碼區塊記錄
尚未設定
否
開啟指令碼執行
尚未設定
否
打開 PowerShell 轉譯
尚未設定
否
設定 Update-Help 的預設來源
尚未設定
否
編輯(E)
篩選對象(F)
篩選選項(O)...
重新套用篩選器(E)
所有工作(K)
說明(H)
延伸
標準
重新套用篩選器



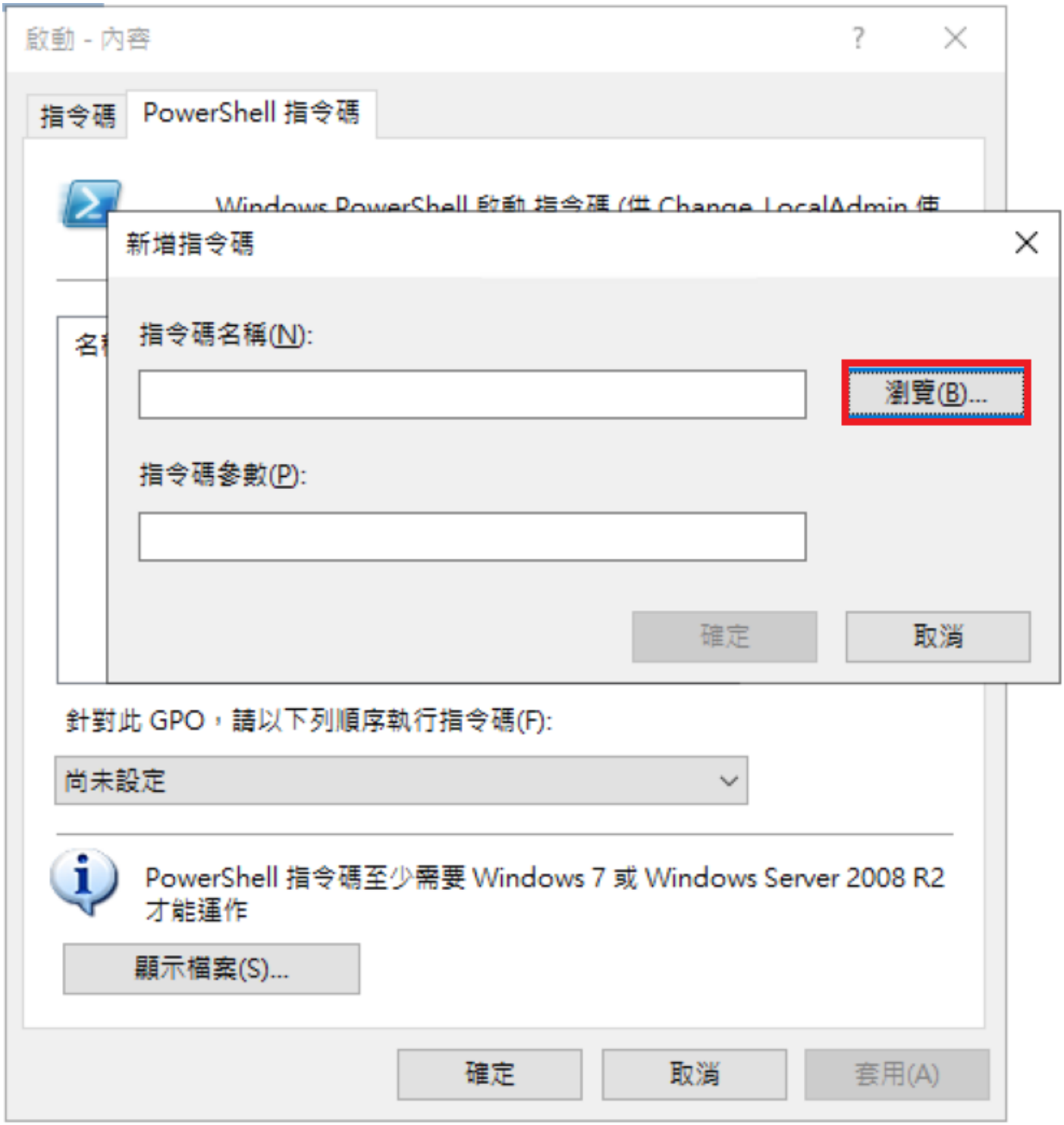
4□ □□□ => □ => Windows□ => □□ => □□□Logon Script□

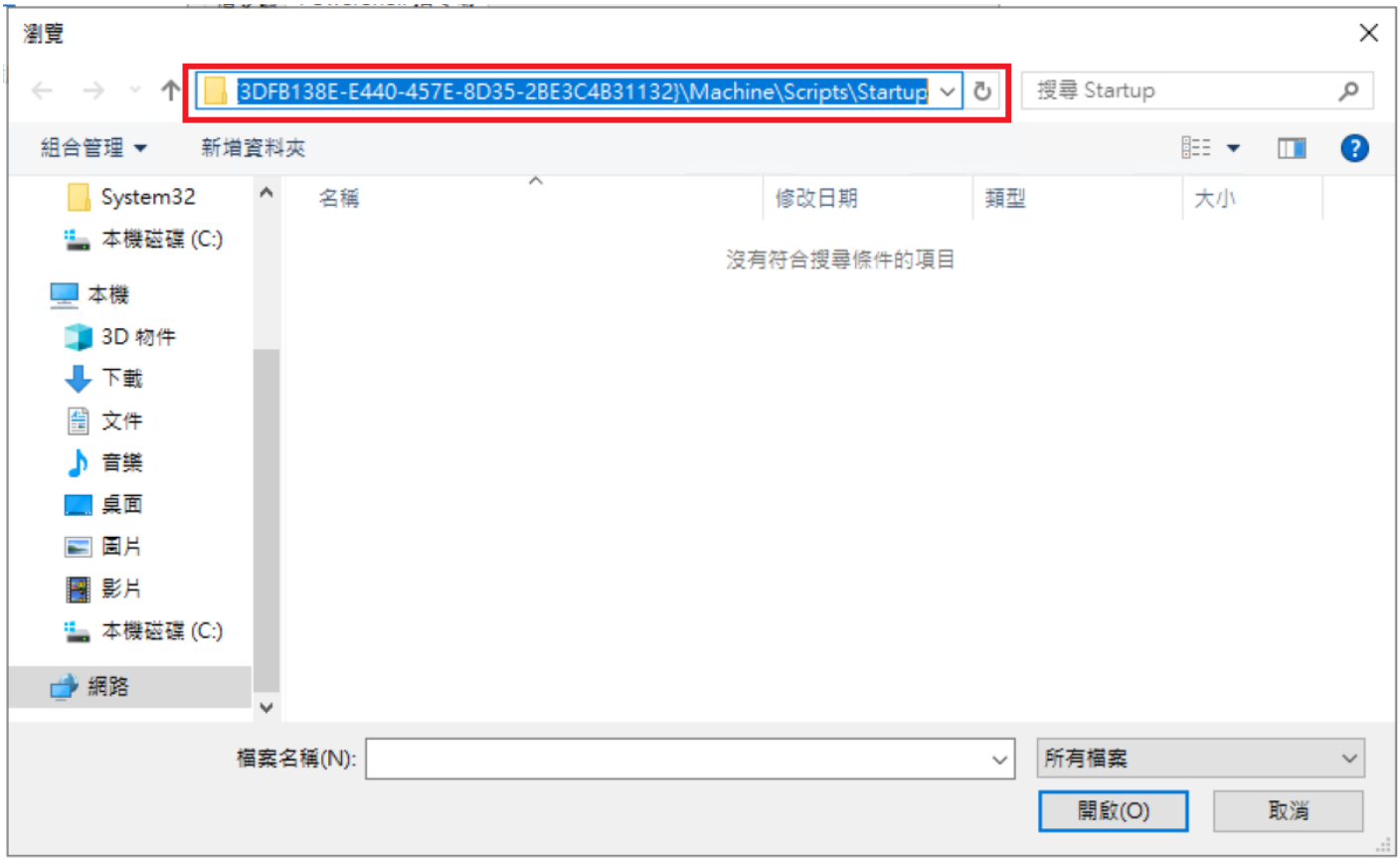

群組原則管理編輯器
檔案(F) 動作(A) 檢視(V) 說明(H)
Change_LocalAdmin
電腦設定
原則
軟體設定
Windows 設定
名稱解析原則
指令碼 - (啟動/關機)
已部署的印表機
安全性設定
以原則為依據的 QoS
系統管理範本: 已從本機電腦抓取原則定義 (A
喜好設定
使用者設定
原則
喜好設定
指令碼 - (啟動/關機)
啟動
顯示 內容
描述:
包含電腦啟動指令檔。
名稱
啟動
關機
內容(R)
說明(H)

□□PowerShell□□□□□


啟動 - 內容
?
指令碼
PowerShell 指令碼
Windows PowerShell 啟動 指令碼 (供 Change_LocalAdmin 使用)
名稱
參數
向上(U)
下移(W)
新增(D)...
編輯(E)...
移除(R)
針對此 GPO，請以下列順序執行指令碼(F):
尚未設定
PowerShell 指令碼至少需要 Windows 7 或 Windows Server 2008 R2 才能運作
顯示檔案(S)...
確定
取消
套用(A)

□□□□□□□□□□□□


啟動 - 內容
指令碼
PowerShell 指令碼
新增指令碼
指令碼名稱(N):
瀏覽(B)...
指令碼參數(P):
確定
取消
針對此 GPO，請以下列順序執行指令碼(F):
尚未設定
PowerShell 指令碼至少需要 Windows 7 或 Windows Server 2008 R2 才能運作
顯示檔案(S)...
確定
取消
套用(A)

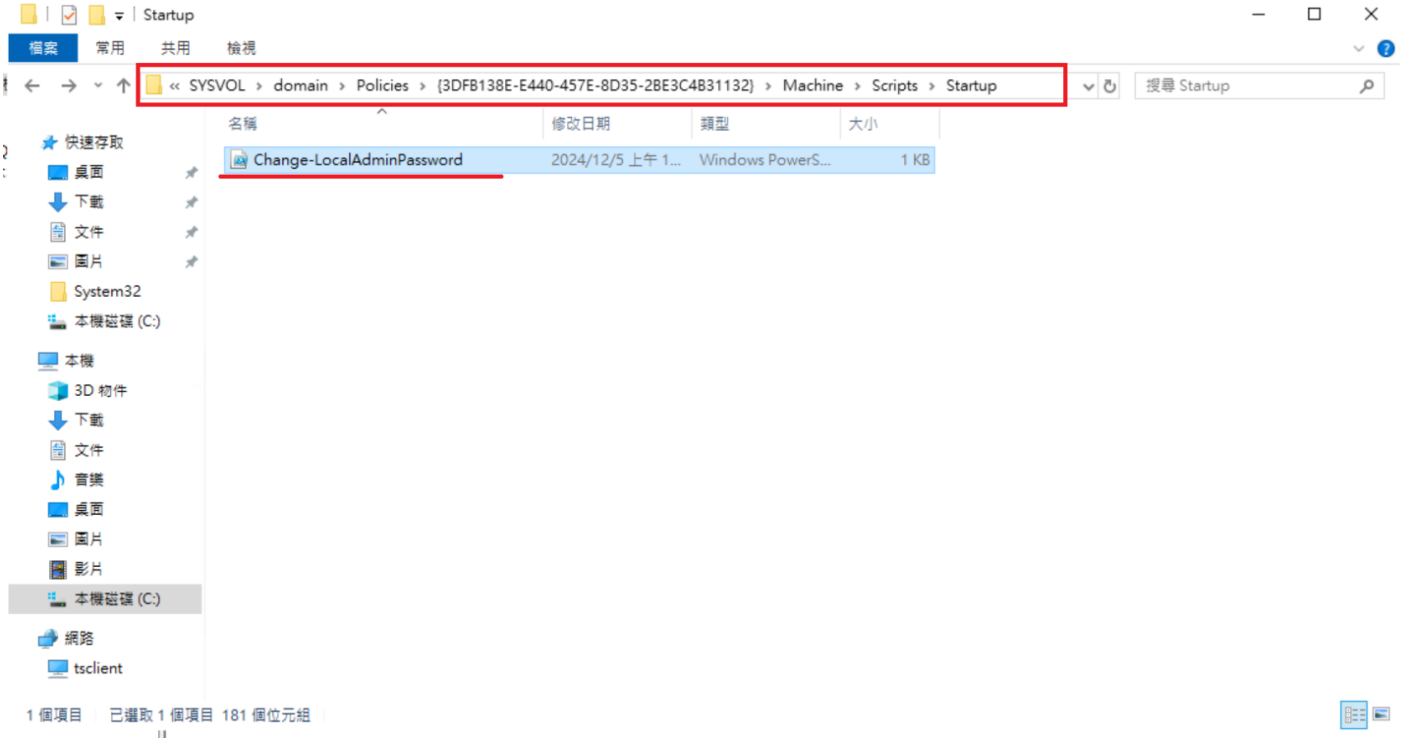


3DFB138E-E440-457E-8D35-2BE3C4B31132}\Machine\Scripts\Startup

搜尋 Startup

沒有符合搜尋條件的項目

你將會在 C:\Windows\SYSVOL\ 下面找到一樣的路徑，將步驟1建立的ps1檔Copy至此。



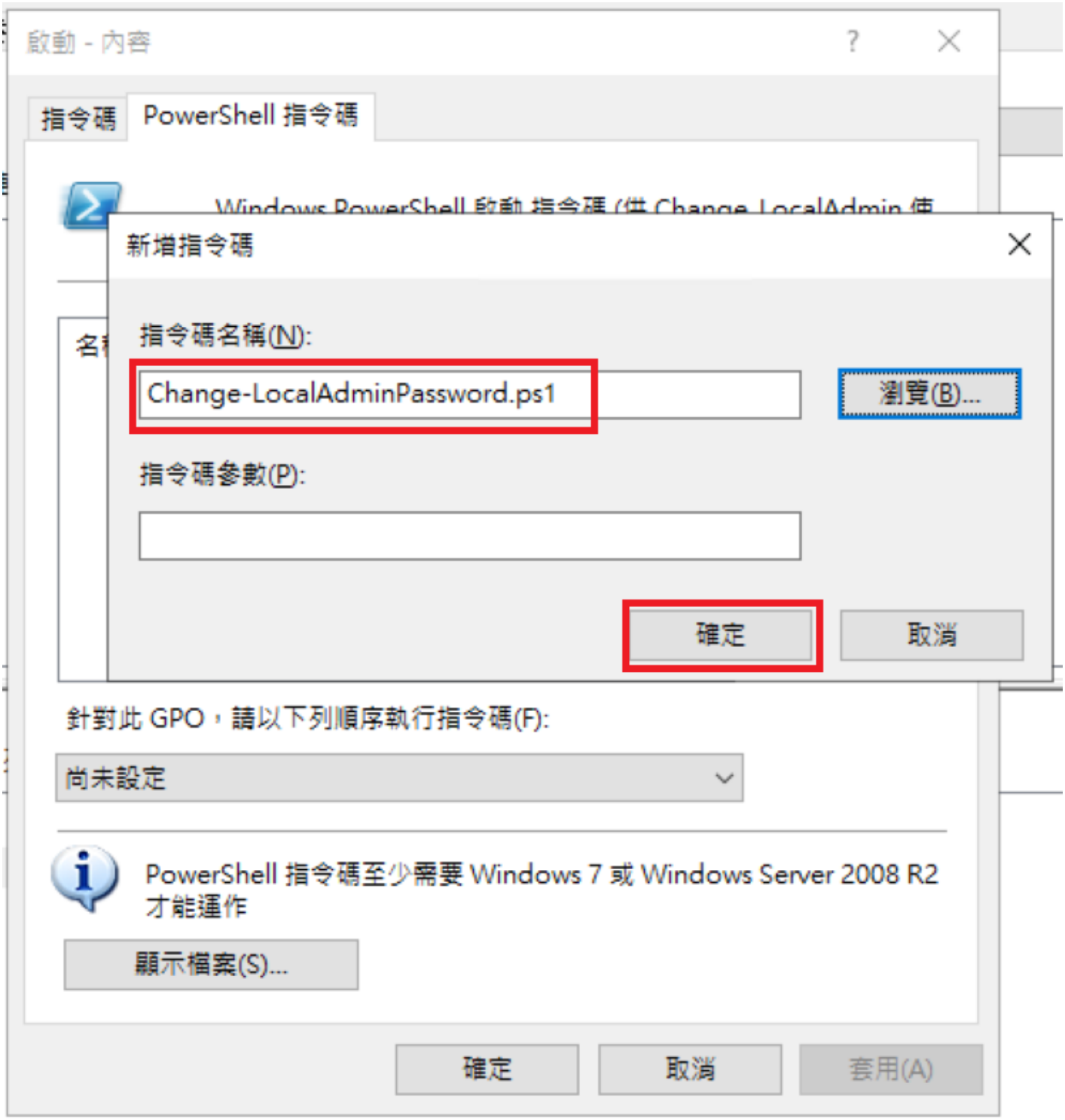
« SYSVOL › domain › Policies › {3DFB138E-E440-457E-8D35-2BE3C4B31132} › Machine › Scripts › Startup

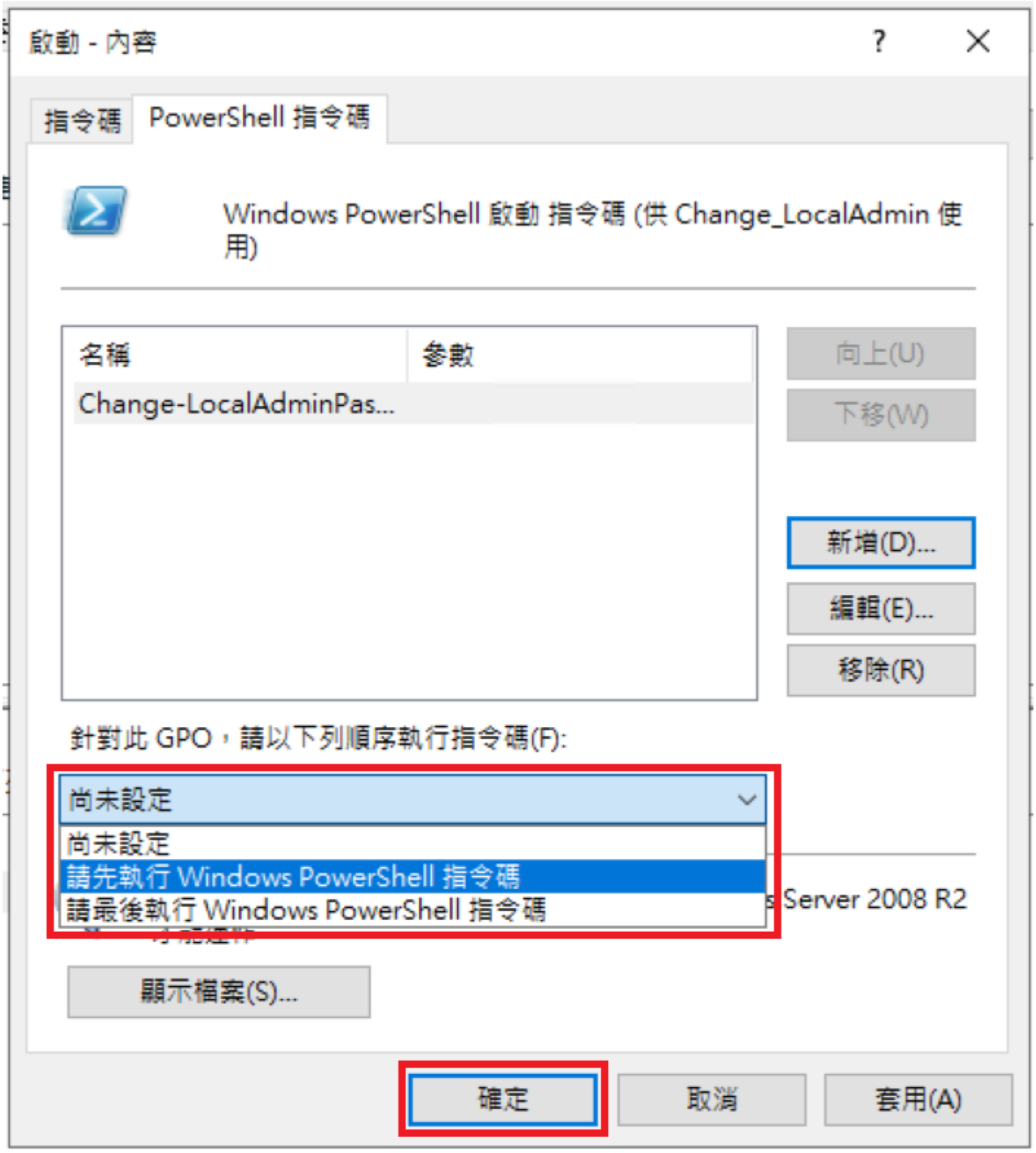
搜尋 Startup

名稱	修改日期	類型	大小
Change-LocalAdminPassword	2024/12/5 上午 1...	Windows PowerS...	1 KB

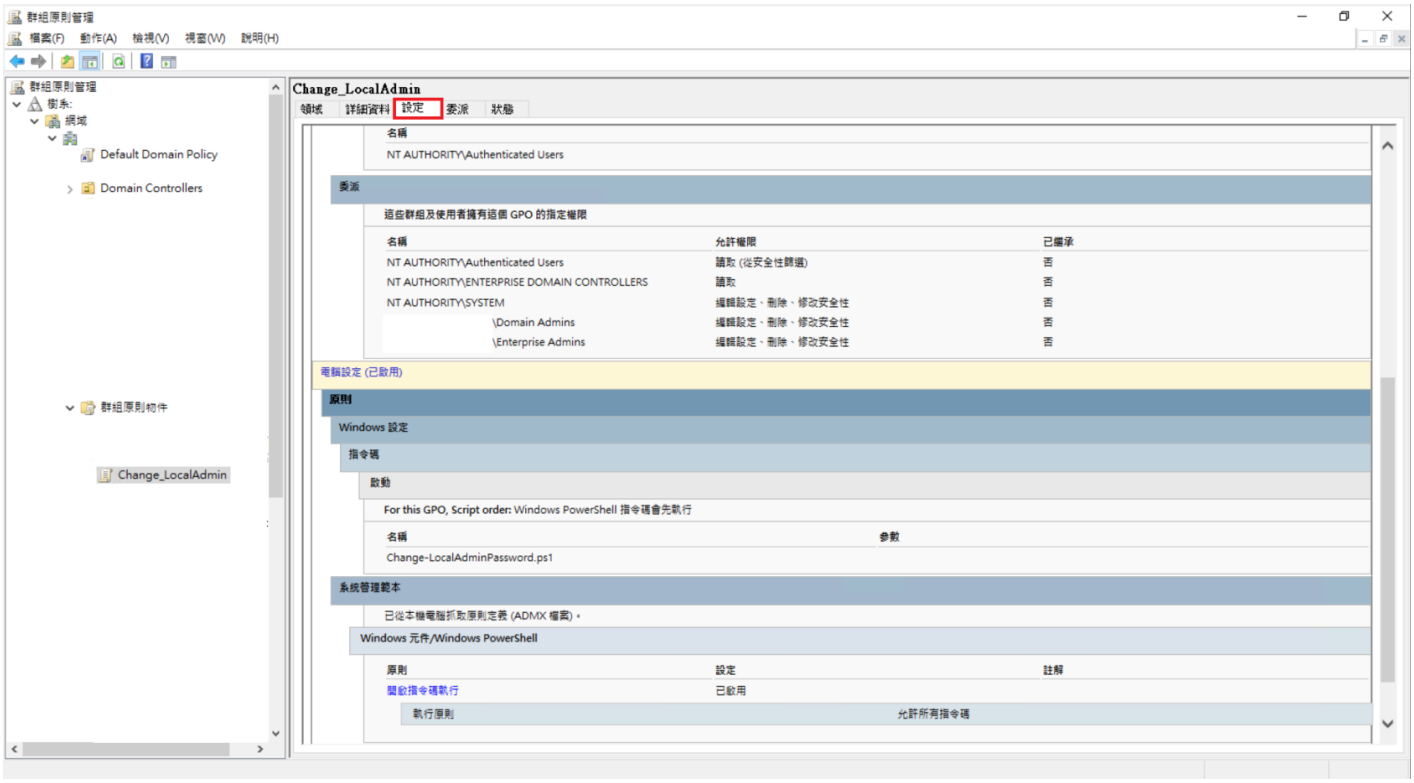
1 個項目　已選取 1 個項目 181 個位元組

回到剛剛指令碼的選擇畫面，就可以看到了

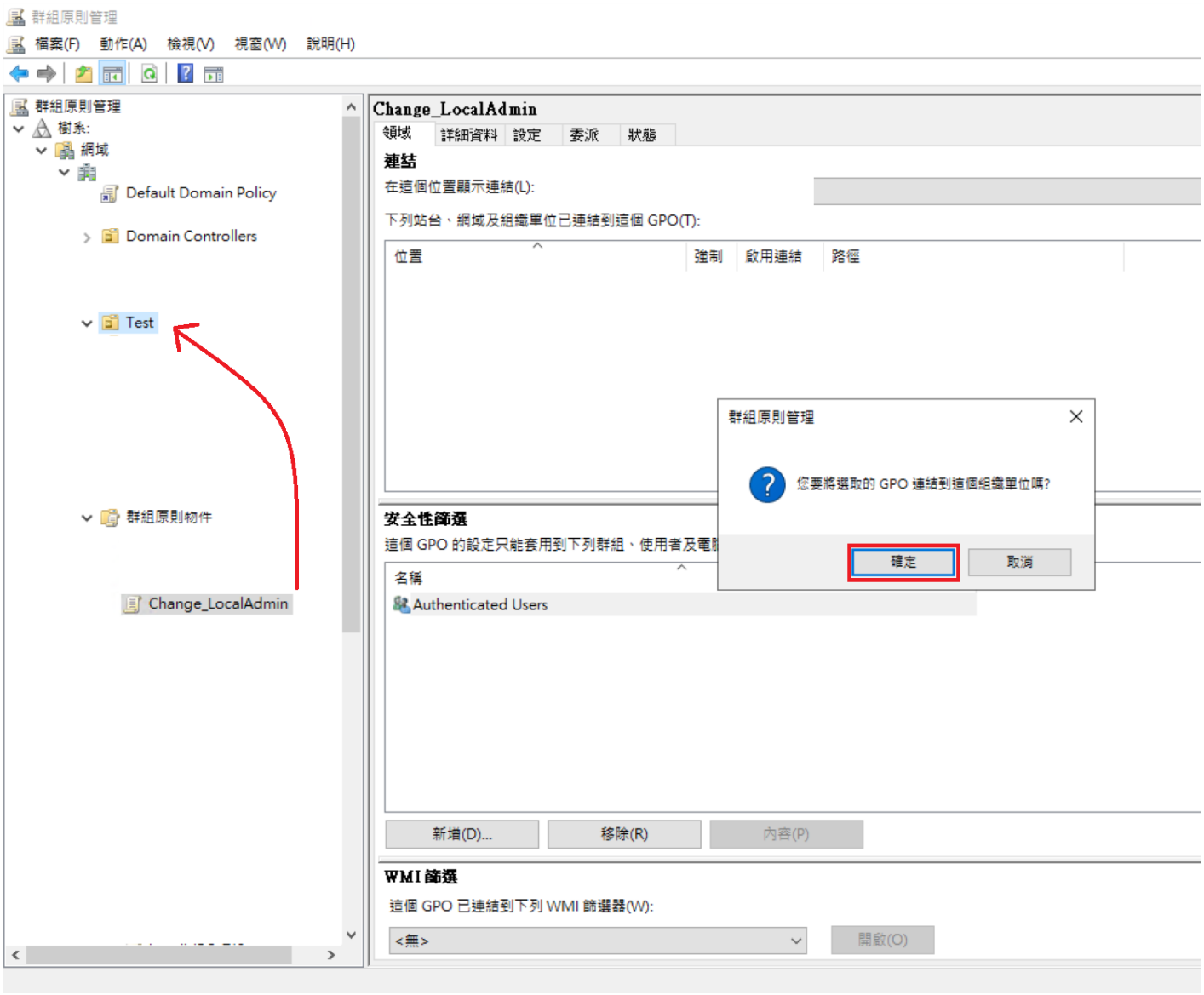

啟動 - 內容
指令碼
PowerShell 指令碼
新增指令碼
指令碼名稱(N):
Change-LocalAdminPassword.ps1
瀏覽(B)...
指令碼參數(P):
確定
取消
針對此 GPO，請以下列順序執行指令碼(F):
尚未設定
PowerShell 指令碼至少需要 Windows 7 或 Windows Server 2008 R2 才能運作
顯示檔案(S)...
確定
取消
套用(A)

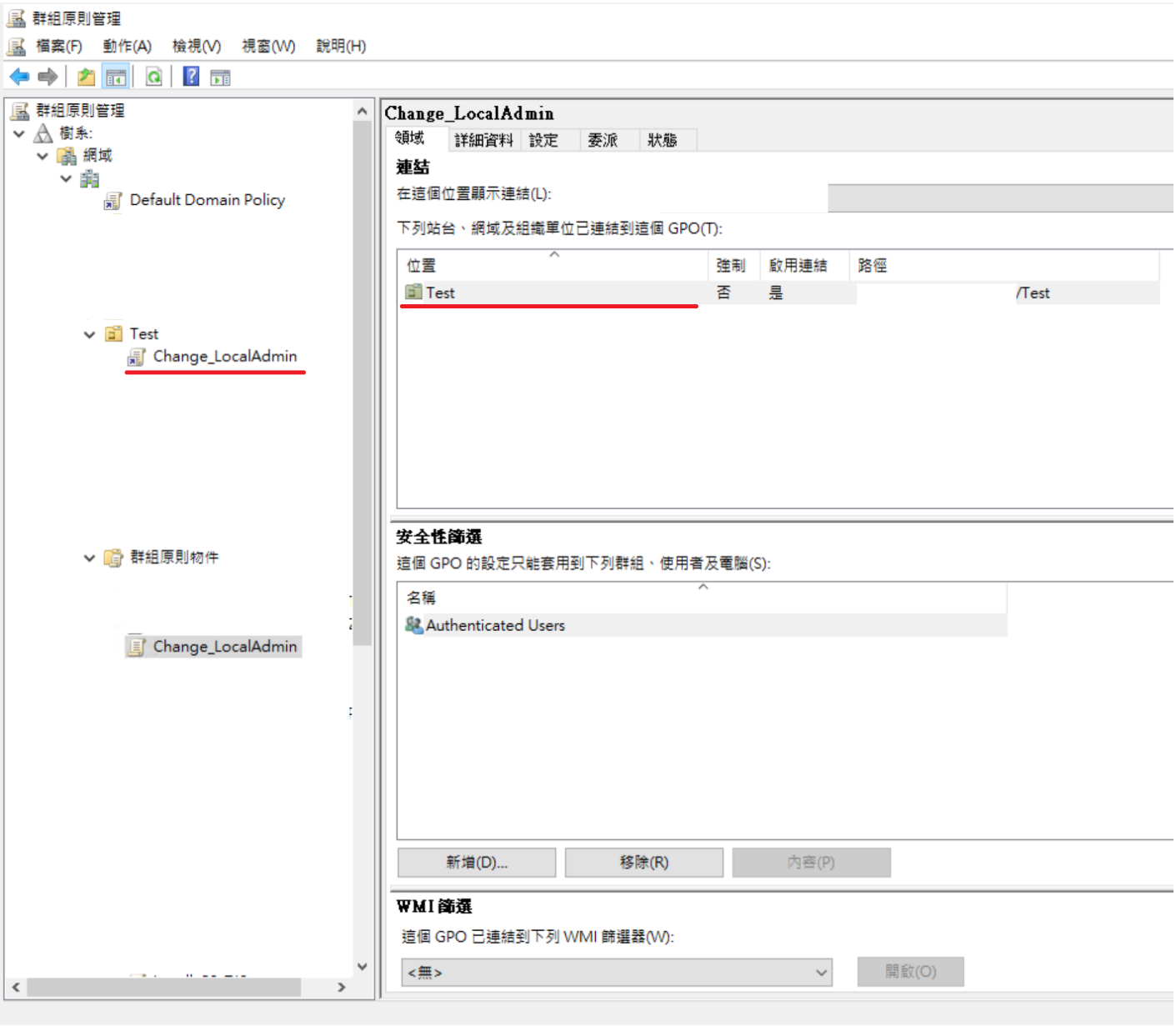


5、此時點選到GPO物件，應該就可以透過下圖看到剛剛設定的內容了。


群組原則管理
檔案(F) 動作(A) 檢視(V) 視窗(W) 說明(H)
群組原則管理
樹系:
網域
Default Domain Policy
Domain Controllers
群組原則物件
Change_LocalAdmin
Change_LocalAdmin
領域 詳細資料 設定 委派 狀態
名稱
NT AUTHORITY\Authenticated Users
委派
這些群組及使用者擁有這個 GPO 的指定權限
名稱 允許權限 已繼承
NT AUTHORITY\Authenticated Users 讀取 (從安全性篩選) 否
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS 讀取 否
NT AUTHORITY\SYSTEM 編輯設定、刪除、修改安全性 否
\Domain Admins 編輯設定、刪除、修改安全性 否
\Enterprise Admins 編輯設定、刪除、修改安全性 否
電腦設定 (已啟用)
原則
Windows 設定
指令碼
啟動
For this GPO, Script order: Windows PowerShell 指令碼會先執行
名稱 參數
Change-LocalAdminPassword.ps1
系統管理範本
已從本機電腦抓取原則定義 (ADMX 檔案)。
Windows 元件/Windows PowerShell
原則 設定 註解
開啟指令碼執行 已啟用
執行原則 允許所有指令碼

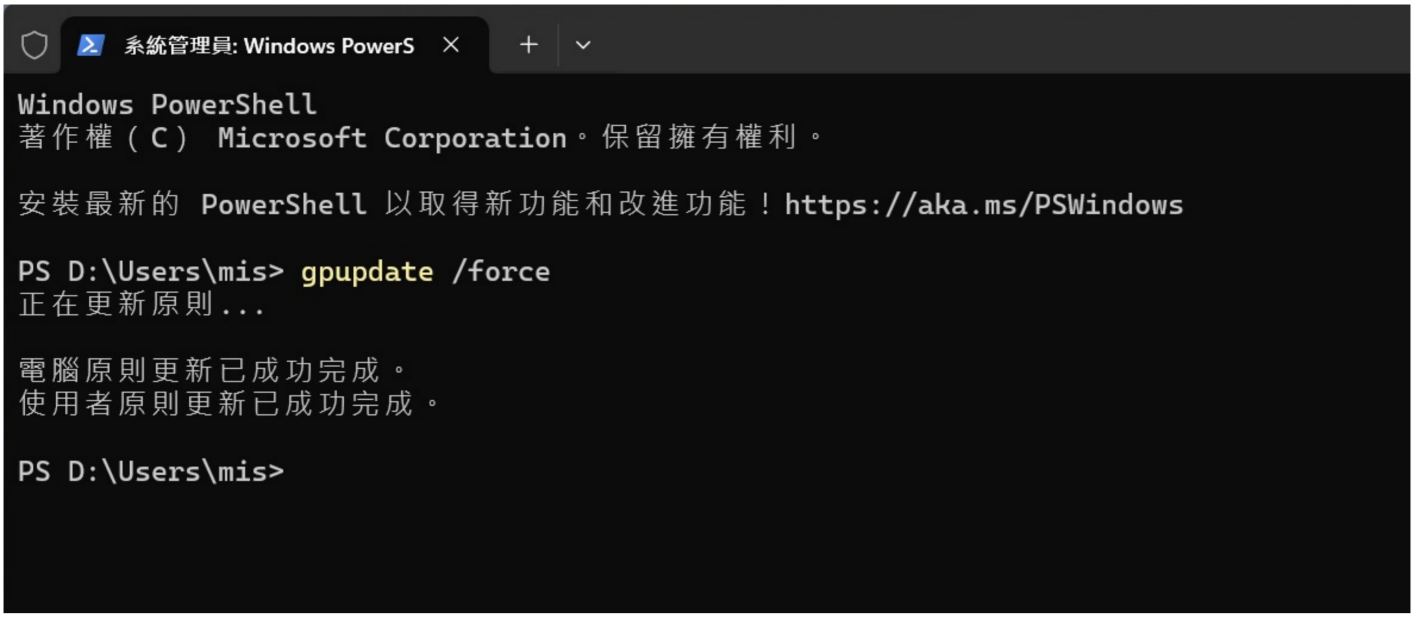
□□GPO□□□□□□□□□□□ Test OU□□□


群組原則管理
檔案(F) 動作(A) 檢視(V) 視窗(W) 說明(H)
群組原則管理
樹系:
網域
Default Domain Policy
Domain Controllers
Test
群組原則物件
Change_LocalAdmin
Change_LocalAdmin
領域 詳細資料 設定 委派 狀態
連結
在這個位置顯示連結(L):
下列站台、網域及組織單位已連結到這個 GPO(T):
位置 強制 啟用連結 路徑
群組原則管理
您要將選取的 GPO 連結到這個組織單位嗎?
確定 取消
安全性篩選
名稱
Authenticated Users
新增(D)... 移除(R) 內容(P)
WMI 篩選
這個 GPO 已連結到下列 WMI 篩選器(W):
<無>
開啟(O)



□□□□Test OU□□□□□□□ gupdate /force

```
gpupdate /force
```



再執行 gpresult /R, 確認 GPO 是否有套到, 這樣就可以了喔。

```
gpresult /R
```


系統管理員: Windows PowerS
PS D:\Users\mis> gpresult /R
Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. 著作權所有，並保留一切權利。
建立於 2024/ 12/ 5 下午 01:36:36
DESKTOP-N9RQG65\mis 的 RSOP 資料在 DESKTOP-N9RQG65: 記錄模式
作業系統設定: 成員工作站
作業系統版本: 10.0.22631
站台名稱: Default-First-Site-Name
漫遊設定檔: 不適用
本機設定檔: D:\Users\mis
用低速連結來連線?: 否
電腦設定
上次套用的群組原則: 2024/12/5 於 下午 01:34:42
套用的群組原則來自:
群組原則低速連結閾值: 500 kbps
網域名稱:
網域類型: Windows 2008 或更新版本
已套用的群組原則物件
Change_LocalAdmin
Default Domain Policy
下列 GPO 並未套用，因為它們被 WMI 篩選器
本機群組原則
篩選： 並未套用 (原因不明)