

政府組態基準(GCB)實作文件 Windows Server 2022

國家資通安全研究院



- 發展緣由
- 發展目的
- 政府組態基準說明
- 資安防護情境
- 政府組態基準部署實作
- 參考資料

- 自102年起，我國逐步發展與推廣使用者電腦與伺服器主機之政府組態基準(Government Configuration Baseline，簡稱GCB)
- 111年針對機關環境常用之Windows Server 2022著手發展組態基準設定，並於112年公告周知，期望藉由提供電腦作業環境一致性資安防護基準與實作指引，供政府機關透過建立安全組態，提升資安防護能力

- 發展Windows Server 2022組態基準設定之目的，在於規範機關內Windows Server 2022作業系統之一致性安全設定(如密碼最小長度)，以降低成為駭客入侵管道，進而引發資安事件之風險

1 發展一致性安全組態設定

2 提升作業系統使用安全性



政府組態基準說明

- 適用環境
 - 微軟公司所發行之Windows Server 2022作業系統
- 項數統計
 - Windows Server 2022 GCB須部署之基本項目，包含Account Settings與Common Settings共計323項設定項目，項目統計如下：

項次	GPO名稱	項數	小計
1	Windows Server 2022 Account Settings	9	323
2	Windows Server 2022 Common Settings	314	
3	Windows Server 2022 DC Server	29	29
4	Windows Server 2022 DNS Server	115	115
5	Windows Server 2022 File Server	120	120
6	Windows Server 2022 Web Server	117	117

基本項目
GPO

政府組態基準適用環境與項數統計(2/2)

–基本項目部署完成後，再依系統所安裝使用之**伺服器角色**，額外部署相對應之組態基準設定，包含**網域控制站**(以下簡稱**DC Server**)組態基準29項設定項目、**DNS Server**組態基準115項設定項目、**File Server**組態基準120項設定項目及**Web Server**組態基準117項設定項目，項目統計如下

項次	GPO名稱	項數	小計
1	Windows Server 2022 Account Settings	9	323
2	Windows Server 2022 Common Settings	314	
3	Windows Server 2022 DC Server	29	29
4	Windows Server 2022 DNS Server	115	115
5	Windows Server 2022 File Server	120	120
6	Windows Server 2022 Web Server	117	117

伺服器
角色專
用GPO

資安防護情境

資安案例

駭客透過遙控程式使用RDP(Windows遠端桌面程式)發動攻擊，並針對資料庫檔案加密，要求贖金解碼，造成網站內容無法開啟，系統服務中斷

Windows Server 2022 GCB設定

➤ TWGCB-01-011-0062

帳戶：重新命名系統管理員帳戶：
變更系統內建之Administrator帳戶名稱，降低被駭客猜測到具特殊權限之使用者名稱與通行碼組合之機率

➤ TWGCB-01-011-0108 拒絕透過遠端桌面服務登入：

拒絕Guests群組與本機帳戶登入，確保只有被授權之管理者帳戶才能使用遠端桌面服務登入主機

➤ TWGCB-01-011-0117 允許透過遠端桌面服務登入：

僅允許管理者之Administrators群組進行登入



資安案例

鎖定畫面可顯示背景執行之應用程式狀態與通知，當管理者離開伺服器主機，系統進入鎖定畫面時，可能會因應用程式通知而洩露資訊

Windows Server 2022 GCB設定

- **TWGCB-01-011-0173 關閉鎖定畫面上的應用程式通知：**
禁止鎖定畫面上應用程式之啟動與通知，避免因鎖定畫面之應用程式，而導致敏感商務或個人資料洩露
- **TWGCB-01-011-0187 防止啟用鎖定畫面投影片放映：**
停止「電腦設定」中鎖定畫面投影片放映設定，並防止在鎖定畫面上播放投影片放映，避免從登錄使用者的圖片資料夾中所顯示潛在的敏感資訊而導致資訊洩漏

按下 Ctrl+Alt+Delete 以解除鎖定。

05:59

Wed September 12
6:00 PM work

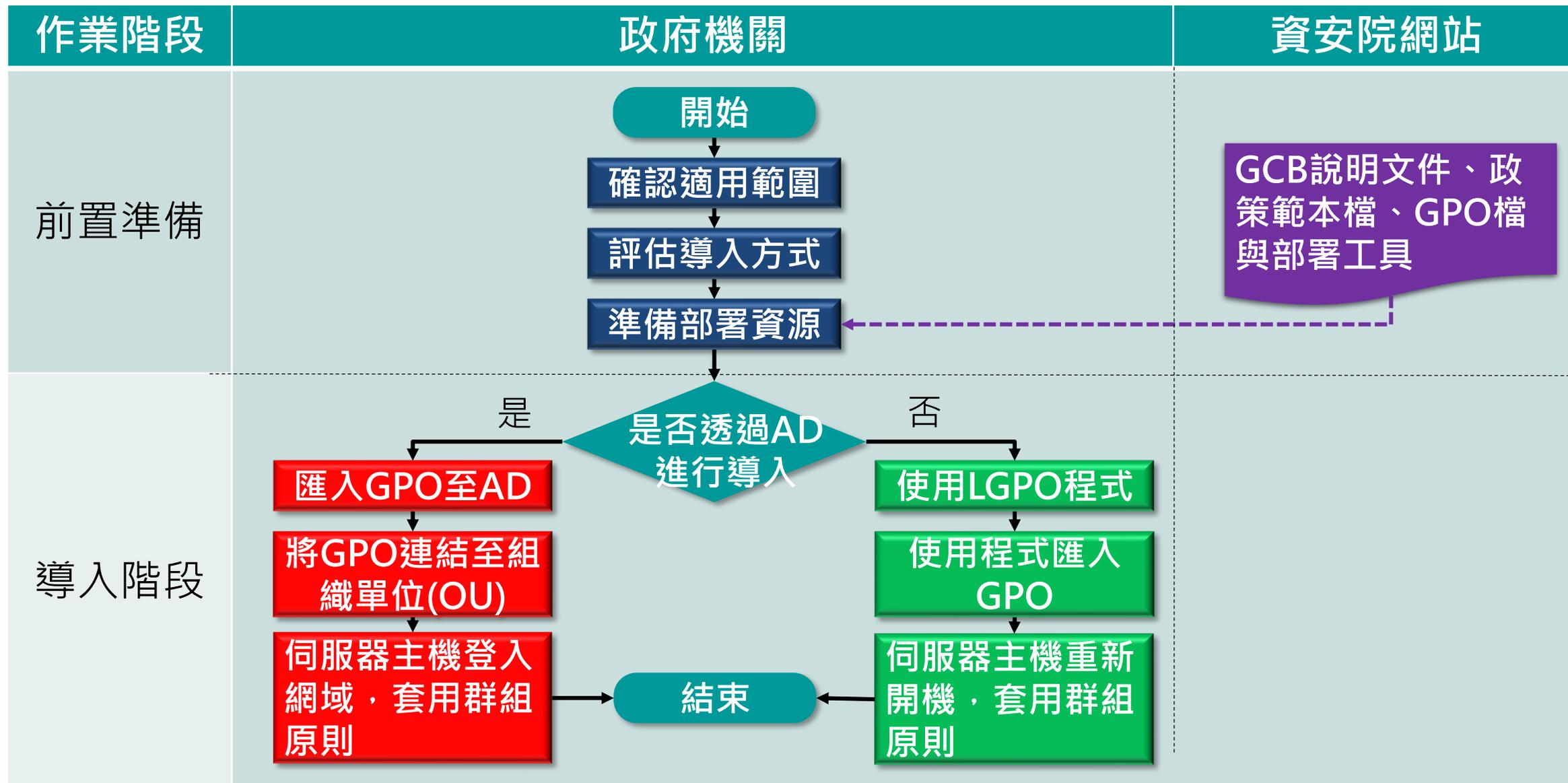
9月12日星期三

鎖定
畫面

行事曆
通知

政府組態基準部署實作

部署流程



1.前置作業

1.1 安裝SecGuide系統管理範本

- SecGuide系統管理範本

- 若須於本機群組原則編輯器(Gpedit.msc)或群組原則管理(Gpmmc.msc)等工具中顯示「**Configure SMB v1 client driver**」、「**Configure SMB v1 server**」及「**Enable Structured Exception Handling Overwrite Protection (SEHOP)**」群組原則設定，須安裝SecGuide系統管理範本

- 下載SecGuide系統管理範本

– 步驟1：至 <https://www.microsoft.com/en-us/download/details.aspx?id=55319>，點選「Download」按鈕



Security Compliance Toolkit and Baselines

This set of tools allows enterprise security administrators to download, analyze, test, edit and store Microsoft-recommended security configuration baselines for Windows and other Microsoft products, while comparing them against other security configurations.

Important! Selecting a language below will dynamically change the complete page content to that language.

Select language 1

[Expand all](#) | [Collapse all](#)

- > Details
- > System Requirements
- > Install Instructions

安裝SecGuide系統管理範本(3/6)

–步驟2：在「Choose the download you want」頁面，勾選「Windows Server 2022 Security Baseline.zip」

–步驟3：點選「Download」按鈕

The screenshot shows a dialog box titled "Choose the download you want" with a list of download options. A red box highlights the first option, "Windows Server 2022 Security Baseline.zip", which is checked. A red circle with the number "2" is next to this box. A teal speech bubble with the text "勾選檔案" (Select file) points to the checked checkbox. At the bottom of the dialog, a red box highlights the "Download" button, with a red circle containing the number "3" next to it. A teal speech bubble with the text "點選下載" (Click download) points to the "Download" button.

Download Name	Size
<input checked="" type="checkbox"/> Windows Server 2022 Security Baseline.zip	1.3 MB
<input type="checkbox"/> Windows 11 Security Baseline.zip	1.2 MB
<input type="checkbox"/> Windows 10 version 21H2 Security Baseline.zip	1.2 MB
<input type="checkbox"/> Windows 11 version 22H2 Security Baseline.zip	1.4 MB
<input type="checkbox"/> Windows 10 version 22H2 Security Baseline.zip	1.2 MB
<input type="checkbox"/> Microsoft 365 Apps for Enterprise 2306.zip	689.2 KB
<input type="checkbox"/> Microsoft Edge v117 Security Baseline.zip	338.6 KB
<input type="checkbox"/> Windows 11 v23H2 Security Baseline.zip	1.2 MB

安裝SecGuide系統管理範本(4/6)

- 安裝SecGuide系統管理範本

- 步驟1：將「Windows Server 2022 Security Baseline.zip」解壓縮

- 步驟2：進入「Templates」資料夾，找到SecGuide.admx 與 SecGuide.adml檔案

The image illustrates the process of finding the required files for SecGuide installation. It consists of two screenshots of Windows File Explorer windows.

Top Screenshot: Shows the 'Templates' folder within the path '本機 > 下載 > Windows Server 2022 Security Baseline > Windows Server-2022-Security-Baseline-FINAL > Templates'. A red box highlights the 'SecGuide.admx' file. A red circle with the number '2' is next to it. A blue speech bubble with the text '找到檔案' (Found file) points to the highlighted file.

名稱	修改日期	類型	大小
en-US	2021/9/6 上午 07:08	檔案資料夾	
AdmPwd.admx	2019/11/1 上午 12:58	ADMX 檔案	4 KB
MSS-legacy.admx	2019/11/1 上午 12:58	ADMX 檔案	19 KB
SecGuide.admx	2021/8/24 下午 03:00	ADMX 檔案	32 KB

Bottom Screenshot: Shows the 'en-US' subfolder. A red box highlights the 'SecGuide.adml' file. A red circle with the number '2' is next to it.

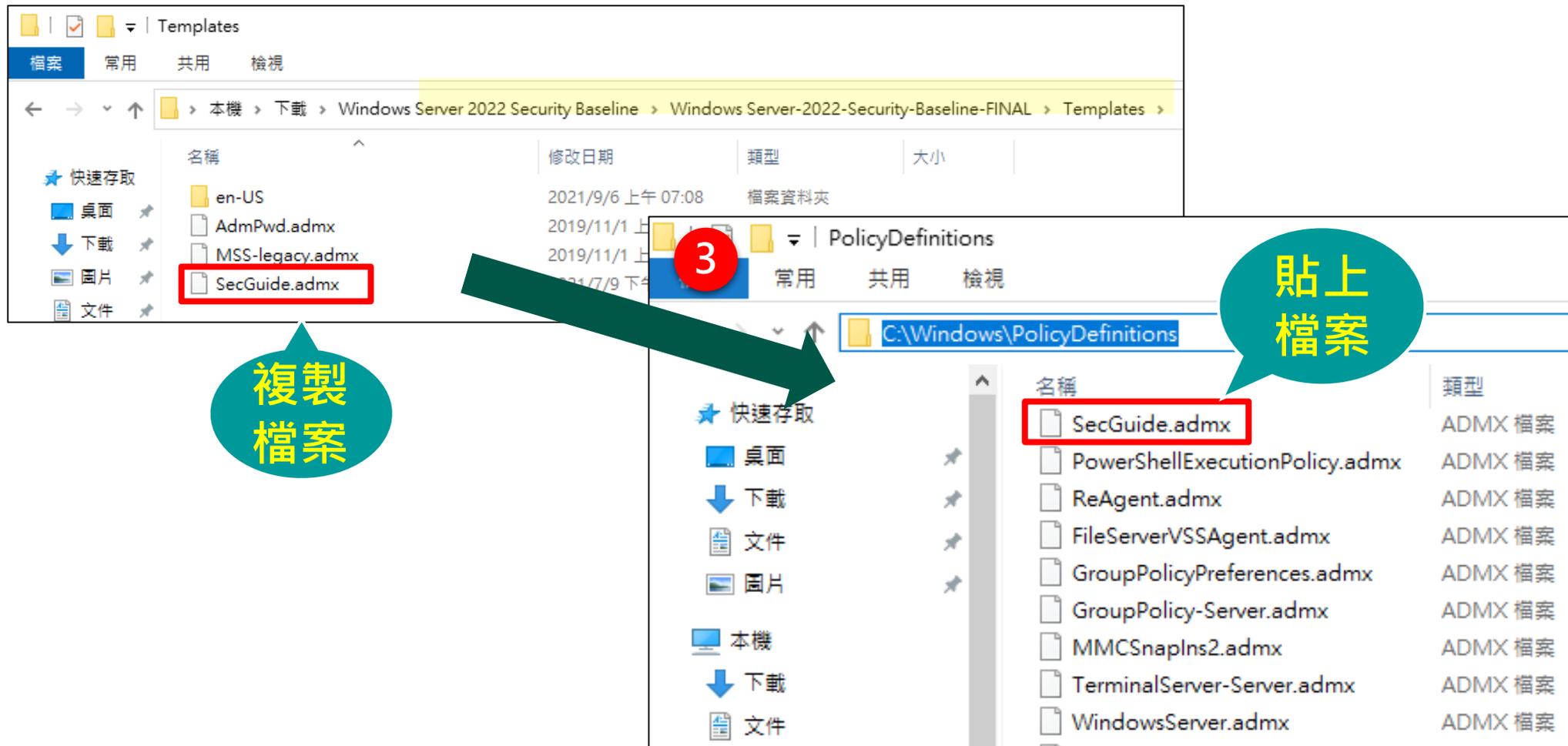
名稱	修改日期	類型	大小
AdmPwd.adml	2019/11/1 上午 12:58	ADML 檔案	4 KB
MSS-legacy.adml	2019/11/1 上午 12:58	ADML 檔案	17 KB
SecGuide.adml	2021/8/24 下午 03:00	ADML 檔案	16 KB

Annotations:

- A red circle with the number '1' is next to a blue speech bubble with the text '解壓縮資料夾' (Extract folder), which points to the 'Windows Server 2022 Security Baseline.zip' file icon on the left.
- A green arrow points from the zip file icon to the top screenshot.

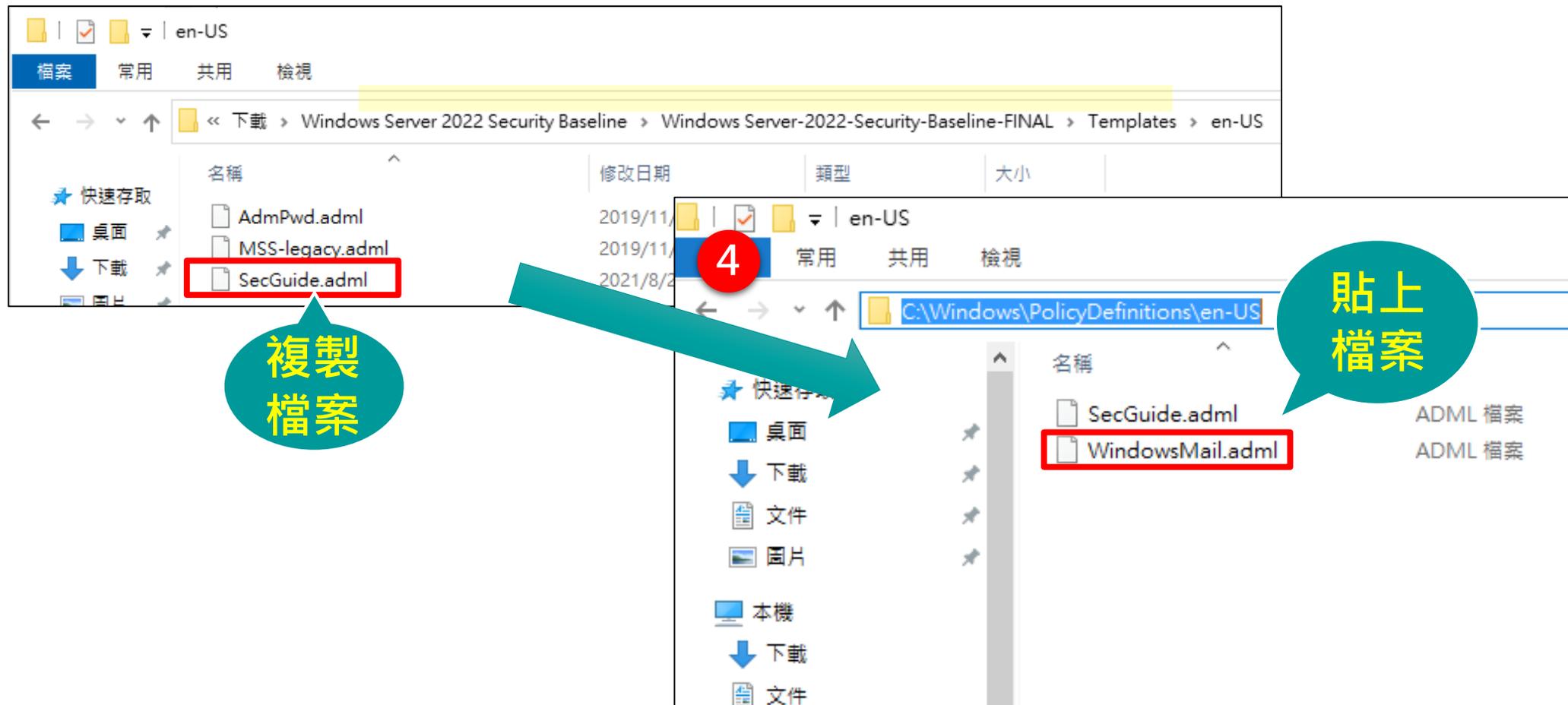
安裝SecGuide系統管理範本(5/6)

步驟3：將「SecGuide.admx」複製到「C:\Windows\PolicyDefinitions」目錄下



安裝SecGuide系統管理範本(6/6)

步驟4：將「SecGuide.adml」複製到「C:\Windows\PolicyDefinitions\en-US」目錄下



1.2 GPO檔案與單機部署工具下載

- 下載Windows Server 2022政府組態基準說明文件
 - 至資安院官網下載Windows Server 2022政府組態基準說明文件，並參閱詳細條目內容說明
 - 下載網址：
https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/GCB/GCB_Documentation/

- TWGCB-01-011_Microsoft Windows Server 2022政府組態基準說明文件v1.0_1121201
SHA256 : 511da98307f0635da1b145f9b861b08871818ed80e9d4ac5de424b0ae39a2afb
SHA256 : 89d1084da4d126061e3bd7e39b55405d61cdf67da65147f54d2dd0790304060c

DOCX

PDF

下載
檔案

- 下載Windows Server 2022 GPO檔案

- 至資安院官網下載Windows Server 2022 GPO檔案，並以此為基準部署GCB

- 下載網址：

https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/GCB/GCB_Deployment_Resources/

- GCB-WindowsServer2022-gposv1.0_1121201

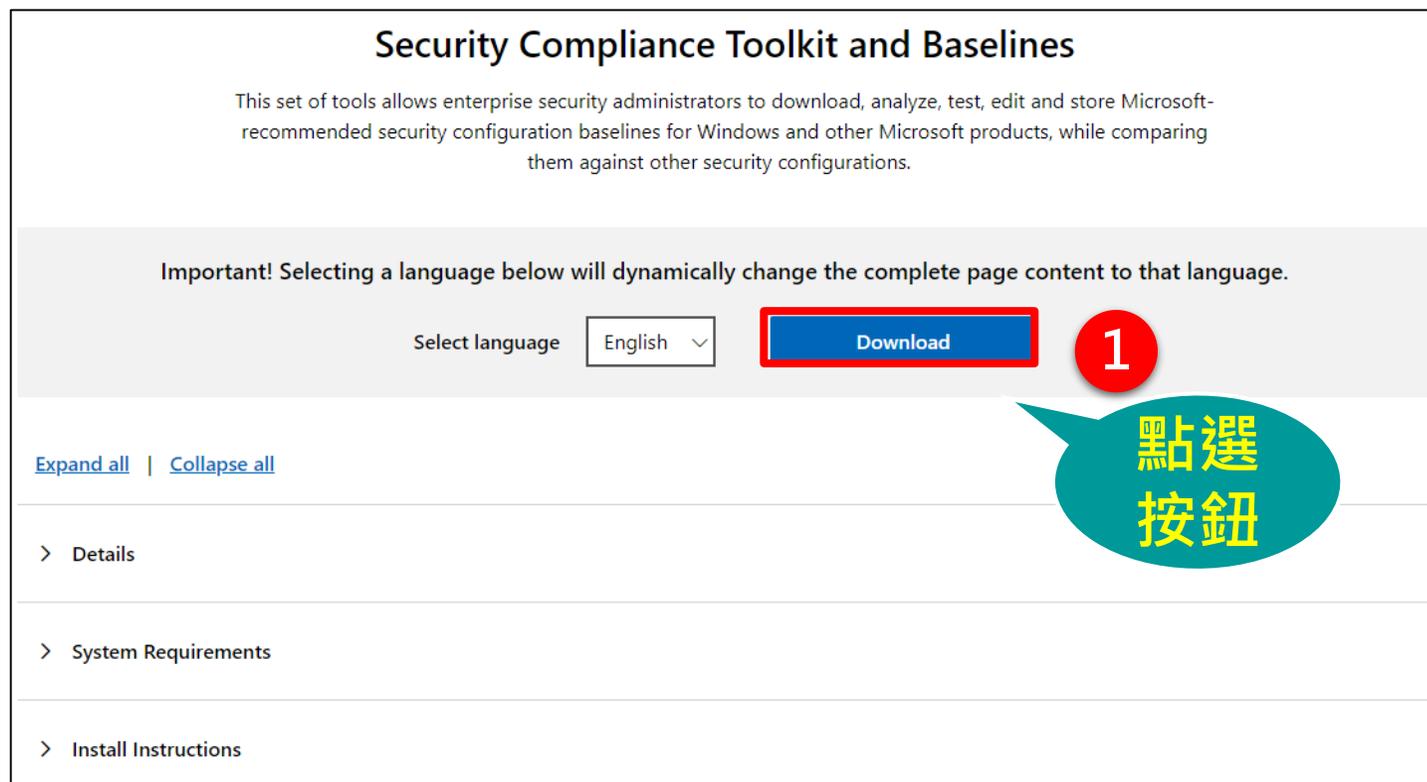
ZIP

下載
檔案

SHA256 : 7b603ce8dca7213deea3ae60715ce1f66deb2a290db42a37c72ba482d1f7544d

- 下載LGPO程式(僅適用於單機部署)

–步驟1：至<https://www.microsoft.com/en-us/download/details.aspx?id=55319>，點選「Download」按鈕



GPO檔案與單機部署工具下載(4/4)



國家資通安全研究院
National Institute of Cyber Security

–步驟2：在「Choose the download you want」頁面，勾選「LGPO.zip」

–步驟3：點選「Download」按鈕

Choose the download you want

<input type="checkbox"/> File Name	Size
<input type="checkbox"/> Windows 10 Version 1809 and Windows Server 2019 Security Baseline.zip	1.3 MB
<input type="checkbox"/> Windows 10 Version 1507 Security Baseline.zip	903.4 KB
<input type="checkbox"/> Windows 10 Version 1607 and Windows Server 2016 Security Baseline.zip	1.5 MB
<input checked="" type="checkbox"/> LGPO.zip	519.2 KB

Total size: 519..

勾選 LGPO.zip

點選 下載

↑ LGPO.zip - ZIP 壓縮檔, 未封裝大小 808,128 位元組

名稱

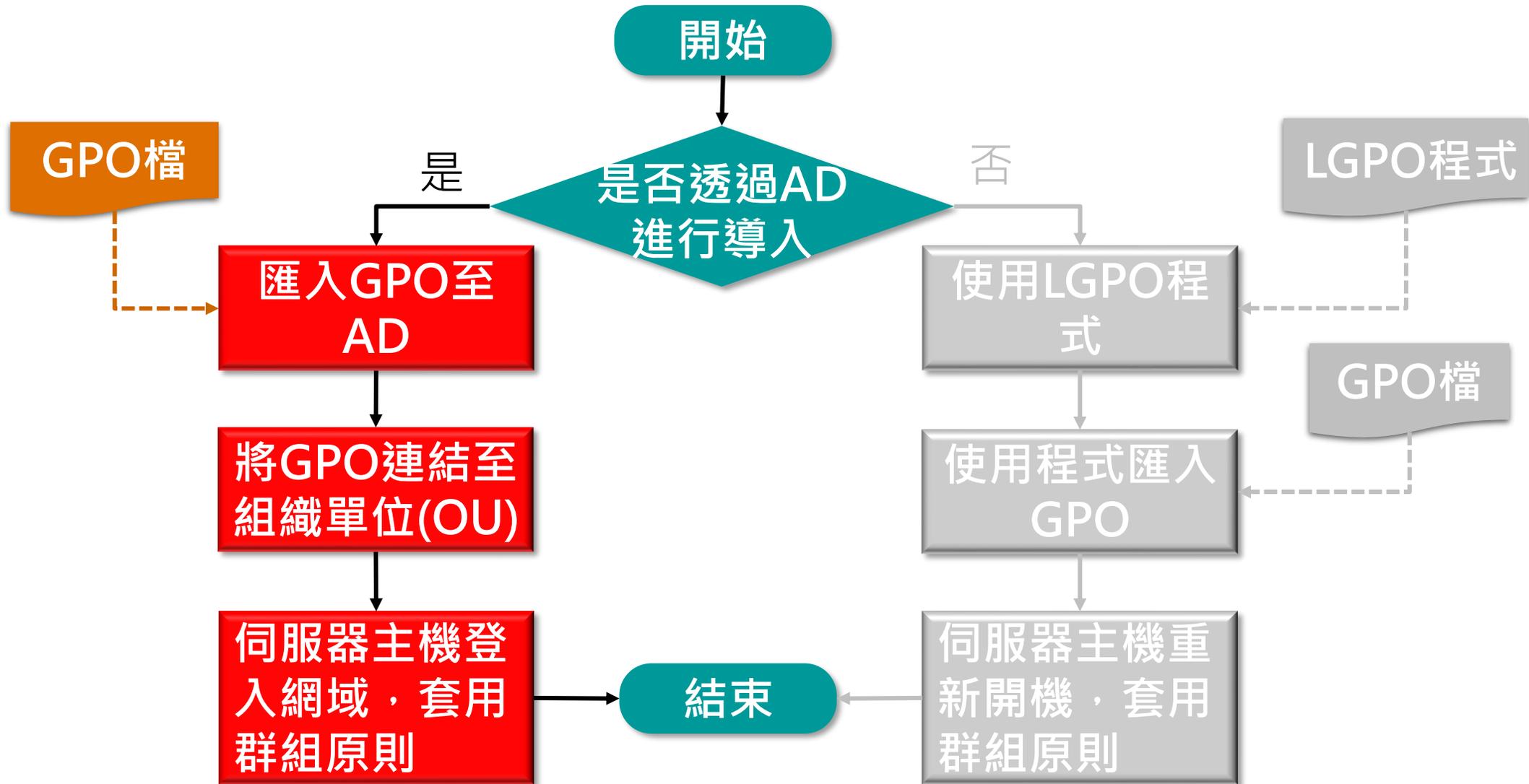
..

LGPO_30

2. 導入階段

2.1 網域環境部署

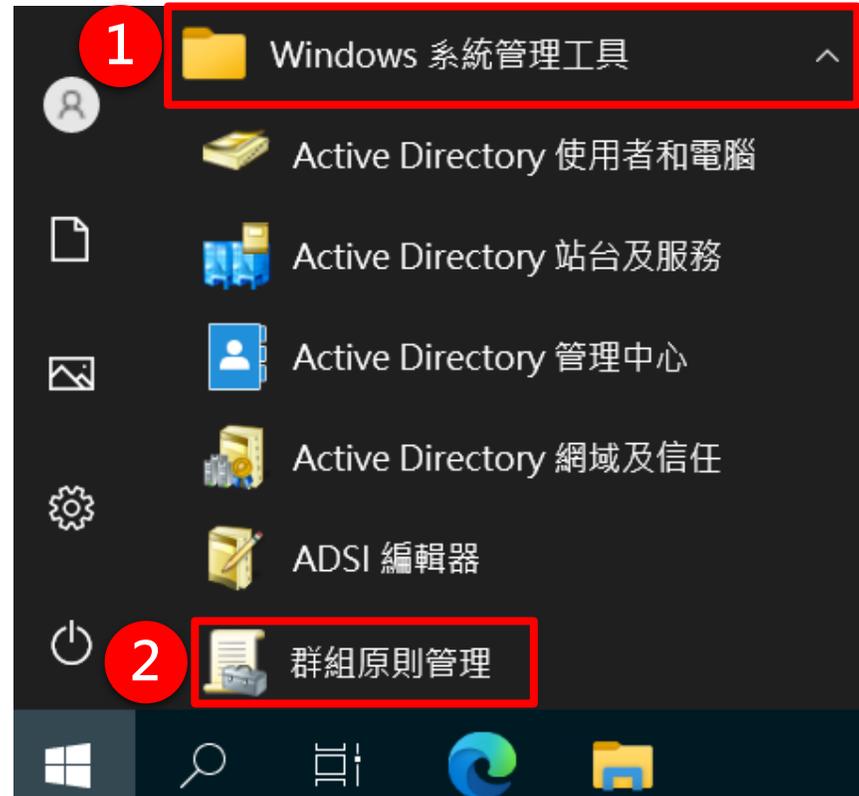
網域環境部署流程



2.1.1 使用AD部署GPO

建立GPO(1/3)

- 步驟1：點擊開始→Windows系統管理工具
- 步驟2：點擊群組原則管理



建立GPO(2/3)

- 步驟3：在群組原則物件節點按滑鼠右鍵
- 步驟4：點選「新增」



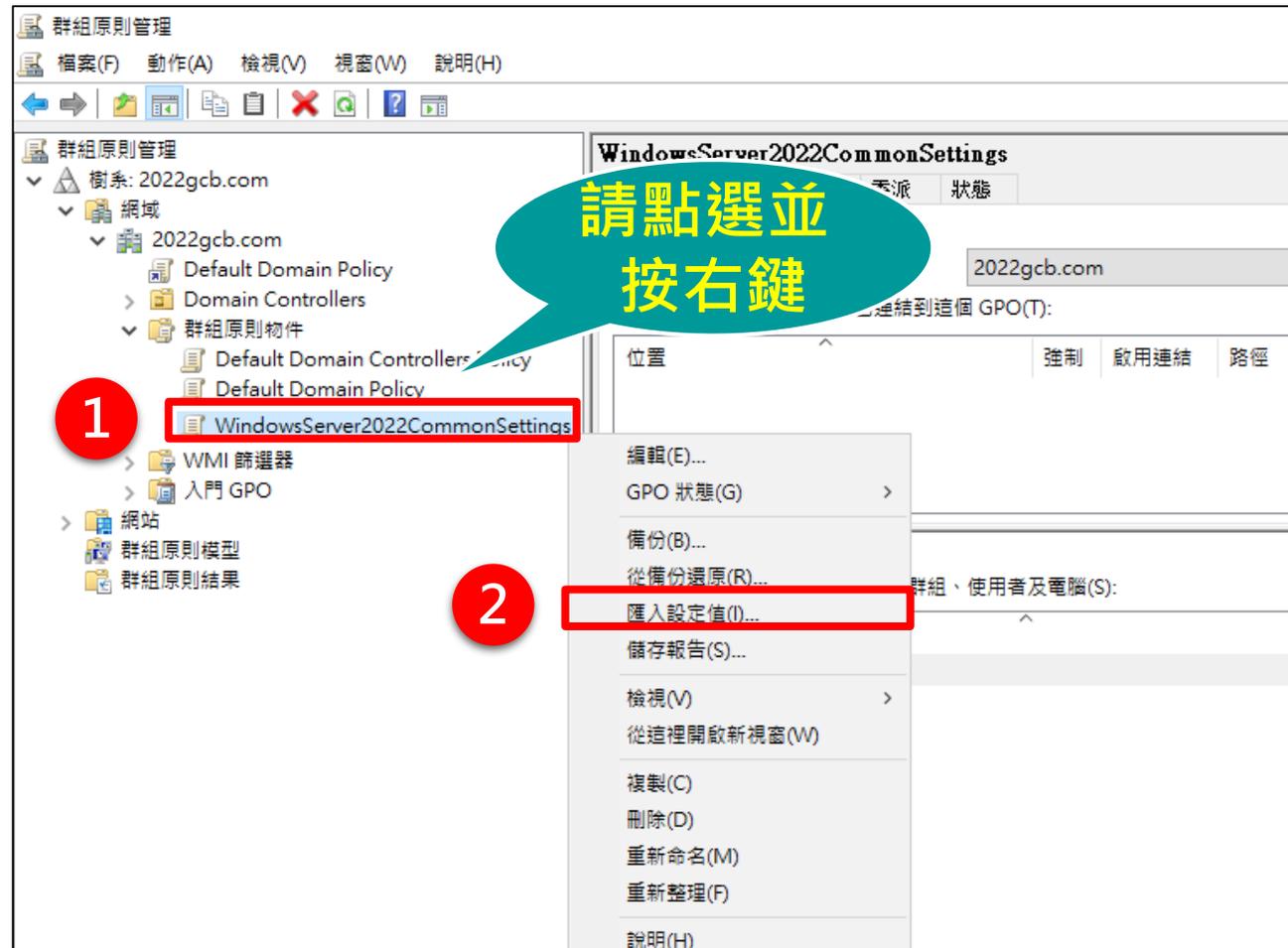
建立GPO(3/3)

- 步驟5：在「名稱」欄位輸入群組原則物件的名稱(如：
WindowsServer2022CommonSettings)
- 步驟6：點選「確定」按鈕



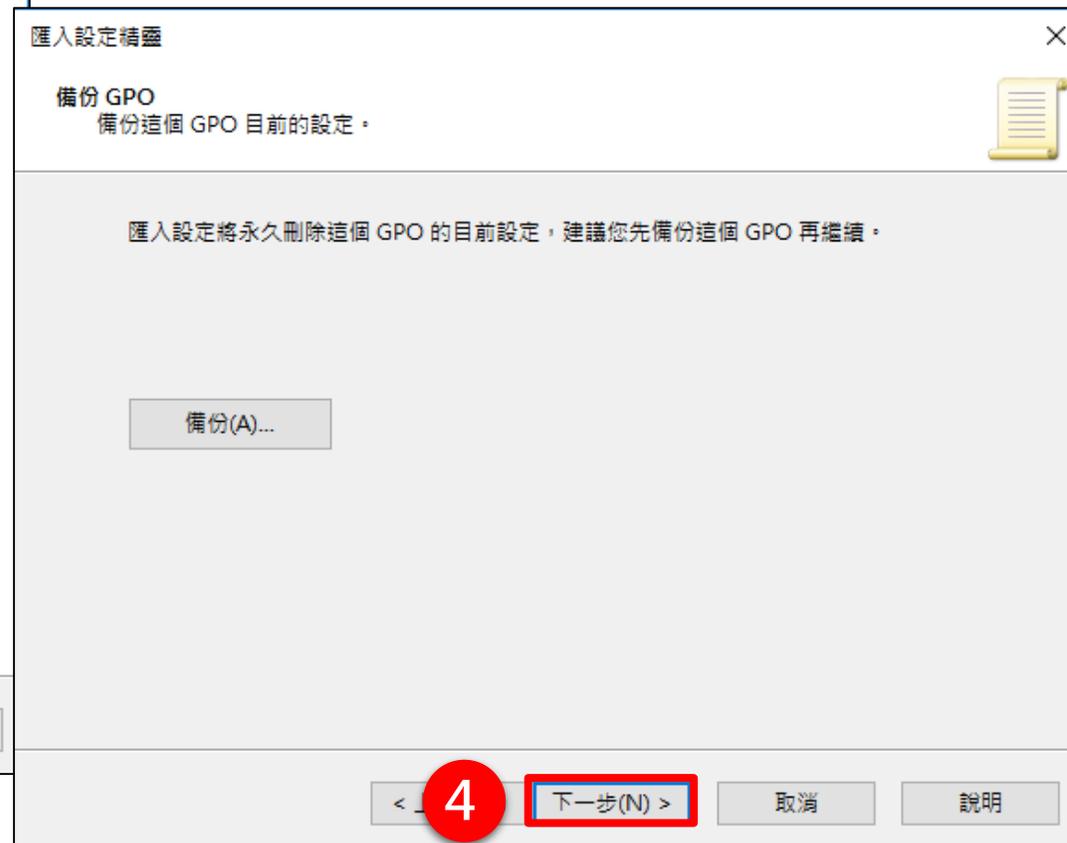
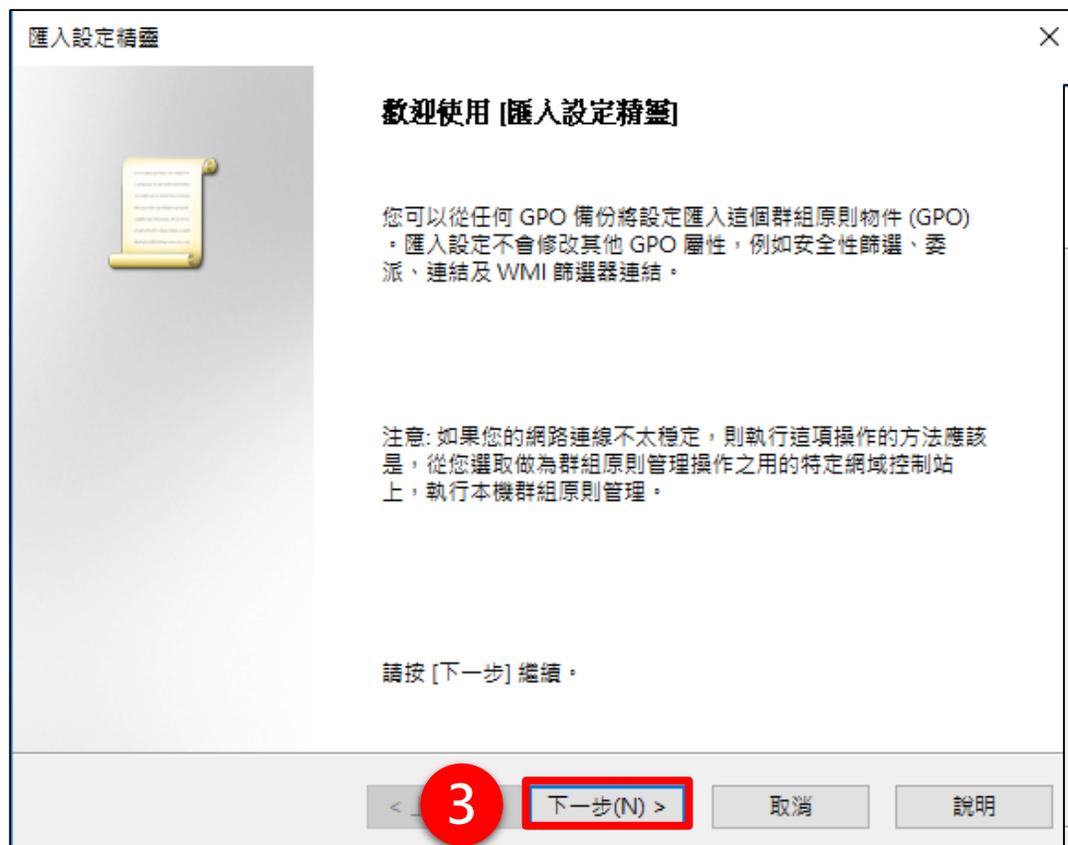
匯入公告之GPO至AD(1/5)

- 步驟1：點選新建的群組原則物件後按滑鼠右鍵
- 步驟2：選擇「匯入設定值」



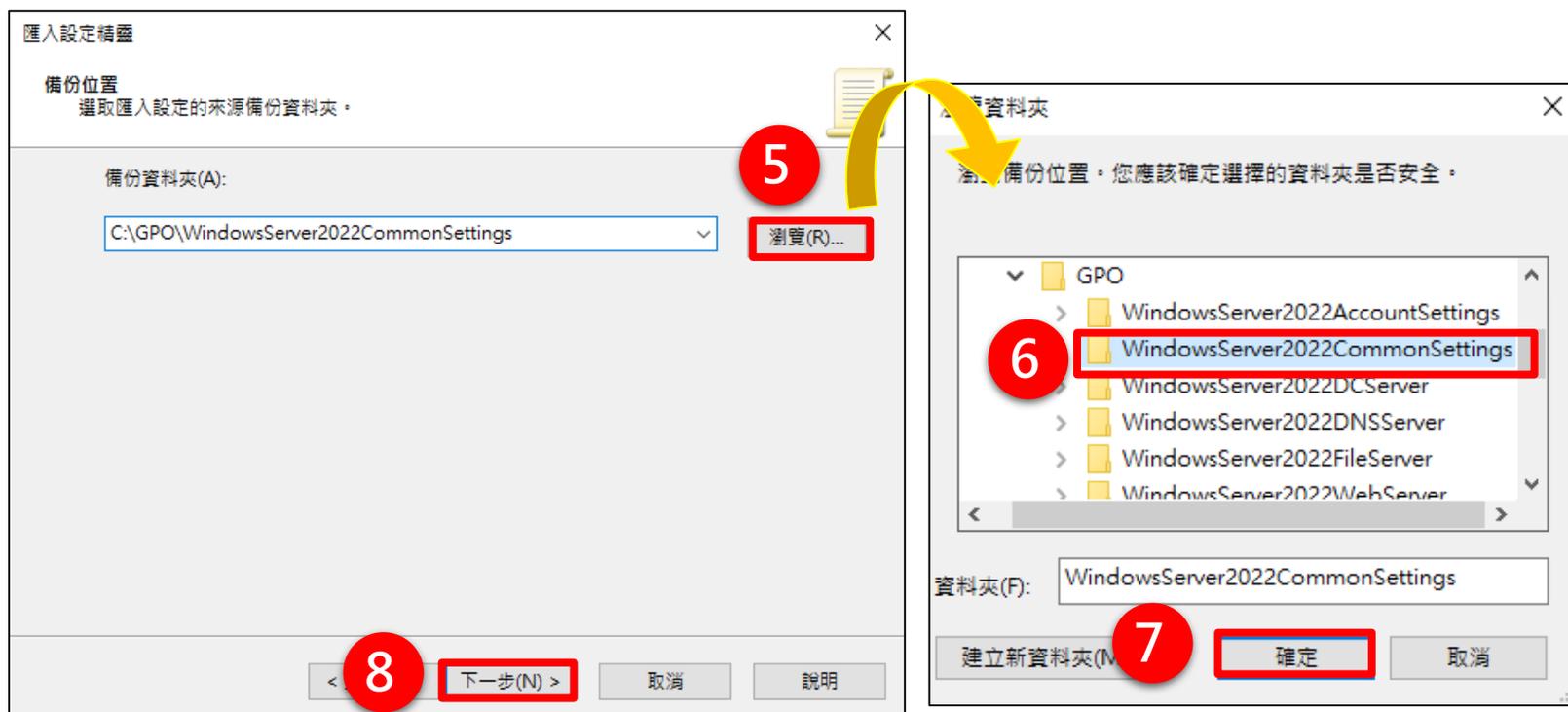
匯入公告之GPO至AD(2/5)

- 步驟3：在歡迎使用【匯入設定精靈】頁面，點選「下一步」按鈕
- 步驟4：在備份GPO頁面，點選「下一步」按鈕



匯入公告之GPO至AD(3/5)

- 步驟5：在備份位置頁面，點選「瀏覽」按鈕
- 步驟6：選擇欲匯入的GPO資料夾
- 步驟7：點選「確定」按鈕
- 步驟8：在備份位置頁面，點選「下一步」按鈕



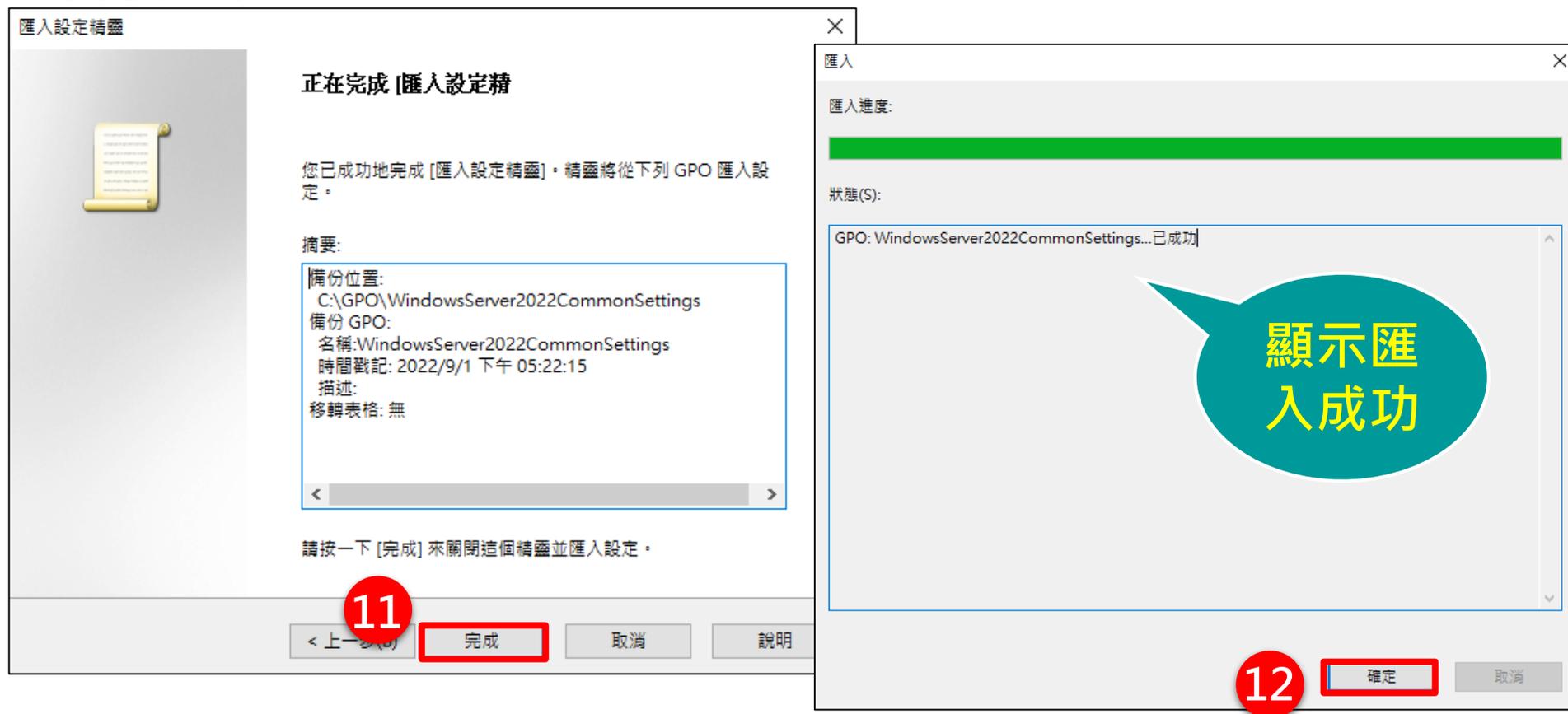
匯入公告之GPO至AD(4/5)

- 步驟9：在來源GPO頁面，確認匯入之GPO正確後，點選「下一步」按鈕
- 步驟10：在掃描備份頁面，點選「下一步」按鈕



匯入公告之GPO至AD(5/5)

- 步驟11：在正在完成匯入設定精靈頁面，點選「完成」按鈕
- 步驟12：在匯入進度頁面，點選「確定」按鈕，完成匯入GPO至群組原則物件中



將GPO連結至組織單位(OU)(1/2)

- 步驟1：點選已匯入GPO之群組原則物件
- 步驟2：拖曳至組織單位(OU)(此範例為Domain Controllers)
- 步驟3：點選「確定」按鈕，完成GPO連結至組織單位



將GPO連結至組織單位(OU)(2/2)

- 完成將GPO連結至組織單位

The screenshot shows the Group Policy Management console for the domain 2022gcb.com. The left pane displays the tree structure, with the 'Domain Controllers' organizational unit (OU) selected. Two GPOs are listed under this OU: 'WindowsServer2022CommonSettings' and 'WindowsServer2022DCServer'. A red box highlights these two GPOs. A callout bubble with the text '完成連結' (Complete Link) points to the highlighted GPOs. The right pane shows the 'Domain Controllers' policy set, with a table of linked GPOs:

連結順序	GPO
1	WindowsServer2022CommonSettings
2	WindowsServer2022DCServer

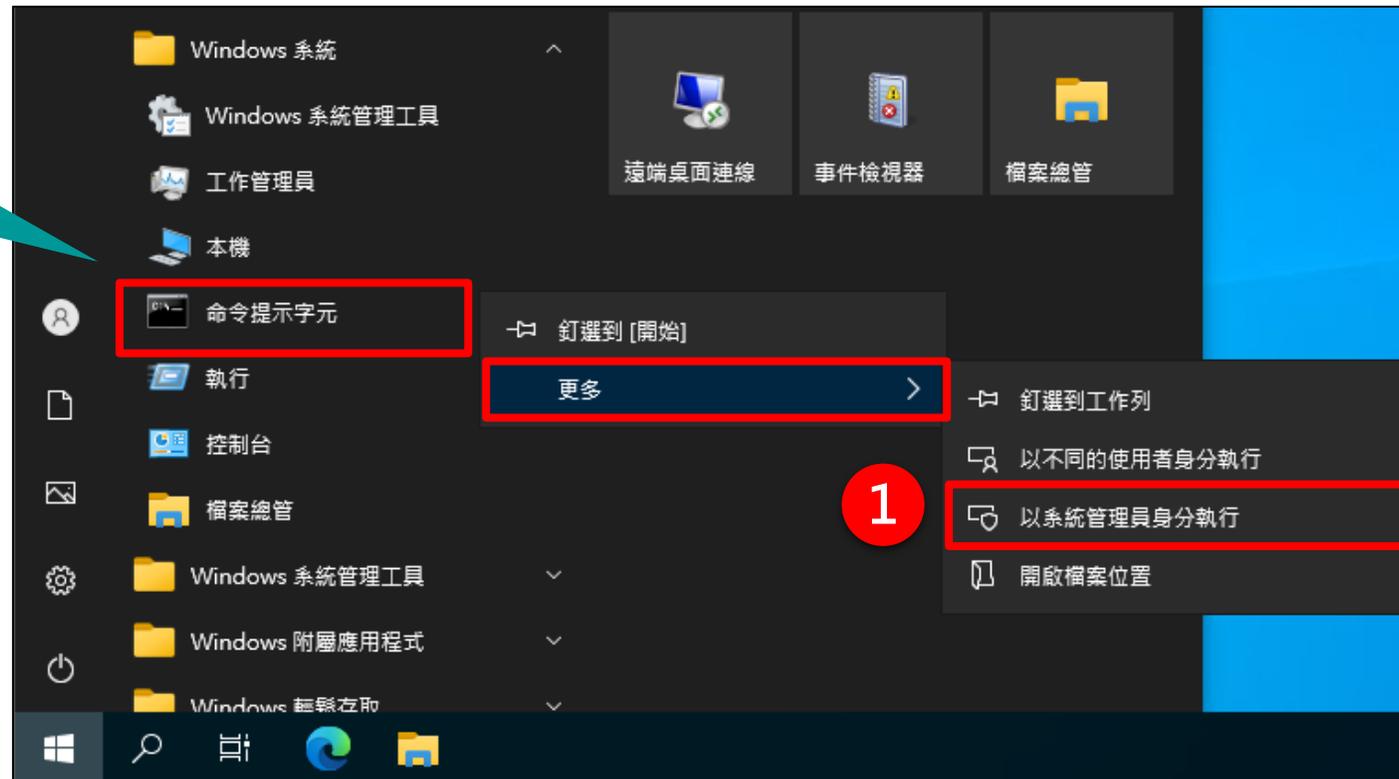
更新群組原則(1/2)

- 請選擇網域內之Windows Server 2022更新群組原則

- 方法1：將網域內Windows Server 2022重新開機

- 方法2：以系統管理者權限開啟命令提示字元(點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→更多→點選「以系統管理員身分執行」)

請點選並
按右鍵



更新群組原則(2/2)

- 請選擇網域內之Windows Server 2022更新群組原則
 - 再輸入gpupdate /force指令更新群組原則，即可套用GCB設定



```
系統管理員: 命令提示字元
Microsoft Windows [版本 10.0.20348.230]
(c) Microsoft Corporation. 著作權所有，並保留一切權利。
C:\Windows\system32>gpupdate /force
正在更新原則...

電腦原則更新已成功完成。
使用者原則更新已成功完成。

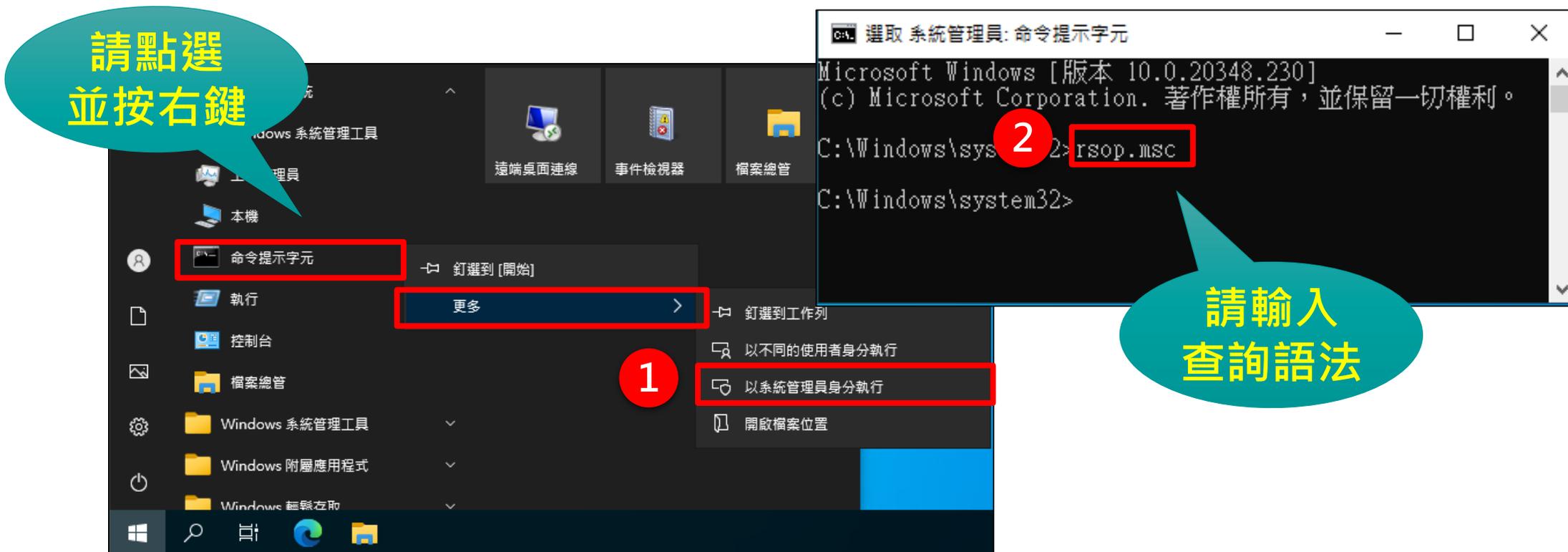
C:\Windows\system32>
```

2.1.2 GPO套用狀況檢查方式

AD環境下的檢查方式一(1/2)

● 使用RSOP檢查群組原則

- 步驟1：點擊開始→Windows系統→在「命令提示字元」按滑鼠**右鍵**→更多→點選「**以系統管理員身分執行**」
- 步驟2：於「命令提示字元」輸入**rsop.msc**查詢群組原則結果



AD環境下的檢查方式一(2/2)

● 使用RSOP檢查群組原則

– 步驟3：檢視GCB項目，確認是否確實套用(如：電腦設定\Windows設定\安全性設定\本機原則\安全性選項\互動式登入：不要顯示上次登入)

正在處理原則結果組...

這個 Microsoft Management Console 包含下列定義的 RSoP 嵌入式管理單元。

從 Microsoft Windows Vista Service Pack 1 (SP1) 開始，原則結果組 (RSoP) 報告不會再顯示所有 Microsoft 群組原則設定。若要檢視針對電腦或使用者套用的完整 Microsoft 群組原則設定，請使用命令列工具 gpresult。

正在處理，請稍候

選擇項目	設定
模式	記錄
使用者名稱	2022GCB\admin
顯示使用者原則設定值	是
電腦名稱	2022GCB\SERVER2022
顯示電腦原則設定值	是

進度:

3

顯示群組原則套用結果

原則	電腦設定	來源 GPO
Microsoft 網路伺服器: 伺服器 SPN 目標名...	關閉	WindowsServer2022CommonSettings
Microsoft 網路伺服器: 當登入時數到期時...	已啟用	WindowsServer2022CommonSettings
Microsoft 網路伺服器: 嘗試 S4U2Self 以取...	尚未定義	
Microsoft 網路伺服器: 數位簽章伺服器的...	已啟用	WindowsServer2022CommonSettings
Microsoft 網路伺服器: 數位簽章伺服器的...	已啟用	WindowsServer2022CommonSettings
Microsoft 網路伺服器: 暫停工作階段前，...	15 分鐘	WindowsServer2022CommonSettings
互動式登入: 不要在登入期間顯示使用者名稱	尚未定義	
互動式登入: 不要按 CTRL+ALT+DEL 鍵	已停用	WindowsServer2022CommonSettings
互動式登入: 不要顯示上次登入	已啟用	WindowsServer2022CommonSettings
互動式登入: 在工作階段被封鎖時顯示使用...	尚未定義	
互動式登入: 在密碼到期前提示使用者變更...	14 天	WindowsServer2022CommonSettings
互動式登入: 要求必須使用 Windows Hello...	已停用	WindowsServer2022CommonSettings
互動式登入: 要求網域控制站驗證以解除鎖...	已啟用	WindowsServer2022CommonSettings
互動式登入: 智慧卡移除操作	鎖定工作站	WindowsServer2022CommonSettings

AD環境下的檢查方式二(1/2)

- 使用Gpresult檢查群組原則

– 步驟1：點擊開始→Windows系統→在「命令提示字元」按滑鼠**右鍵**→更多
→點選「**以系統管理員身分執行**」

– 步驟2：於「命令提示字元」輸入**gpresult /h <檔案儲存路徑>\檔名.html**(此範例儲存於桌面，並命名為Report.html)

The image shows a Windows Start menu search for '命令提示字元' (Command Prompt). A red box highlights the search result, and a red box highlights the '更多' (More) button. A red circle with the number '1' is next to the '以系統管理員身分執行' (Run as administrator) option. A callout bubble says '請點選並按右鍵' (Please click and right-click). To the right, a Command Prompt window titled '系統管理員: 命令提示字元' shows the command 'gpresult /h c:\Users\Admin\Desktop\Report.html' entered, with a red box around it and a red circle with the number '2'. A callout bubble says '請輸入查詢語法' (Please enter the query syntax).

AD環境下的檢查方式二(2/2)

- 步驟3：開啟.html檔案，確認是否確實套用(如：電腦設定 \Windows設定\安全性設定\本機原則\安全性選項\互動式登入\互動式登入：不要顯示上次登入)

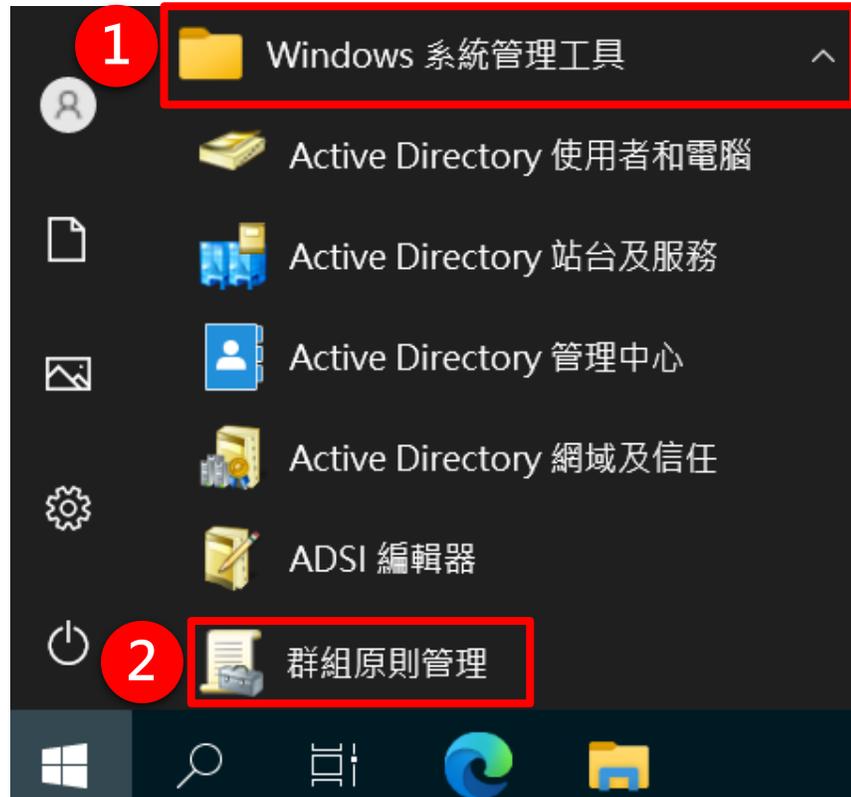
The image shows two overlapping windows. The left window is a File Explorer window showing the Desktop of an Admin user. A red circle with the number '3' highlights a file named 'Report' with a blue icon. A yellow arrow points from this file to the right window. The right window is the Windows Settings application, showing the 'Security Settings' (安全性設定) section. Under 'Local Policies' (本機原則) > 'Security Options' (安全性選項) > 'Interactive Logon' (互動式登入), the policy 'Interactive Logon: Do not display last user name' (互動式登入：不要顯示上次登入) is highlighted with a red box. The policy is set to 'Enabled' (已啟用).

原則	設定	優勢 GPO
互動式登入：不要使用 CTRL + ALT + DEL 鍵	已停用	WindowsServer2022CommonSettings
互動式登入：不要顯示上次登入	已啟用	WindowsServer2022CommonSettings
互動式登入：在密碼到期前提示使用者變更密碼	14 天	WindowsServer2022CommonSettings
互動式登入：要求必須使用 Windows Hello 企業版或智慧卡	已停用	WindowsServer2022CommonSettings
互動式登入：要求網域控制站驗證以解除鎖定工作站	已啟用	WindowsServer2022CommonSettings
互動式登入：智慧卡移除操作	鎖定工作站	WindowsServer2022CommonSettings
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	4 登入	WindowsServer2022CommonSettings

2.1.3 恢復原始設定之方式

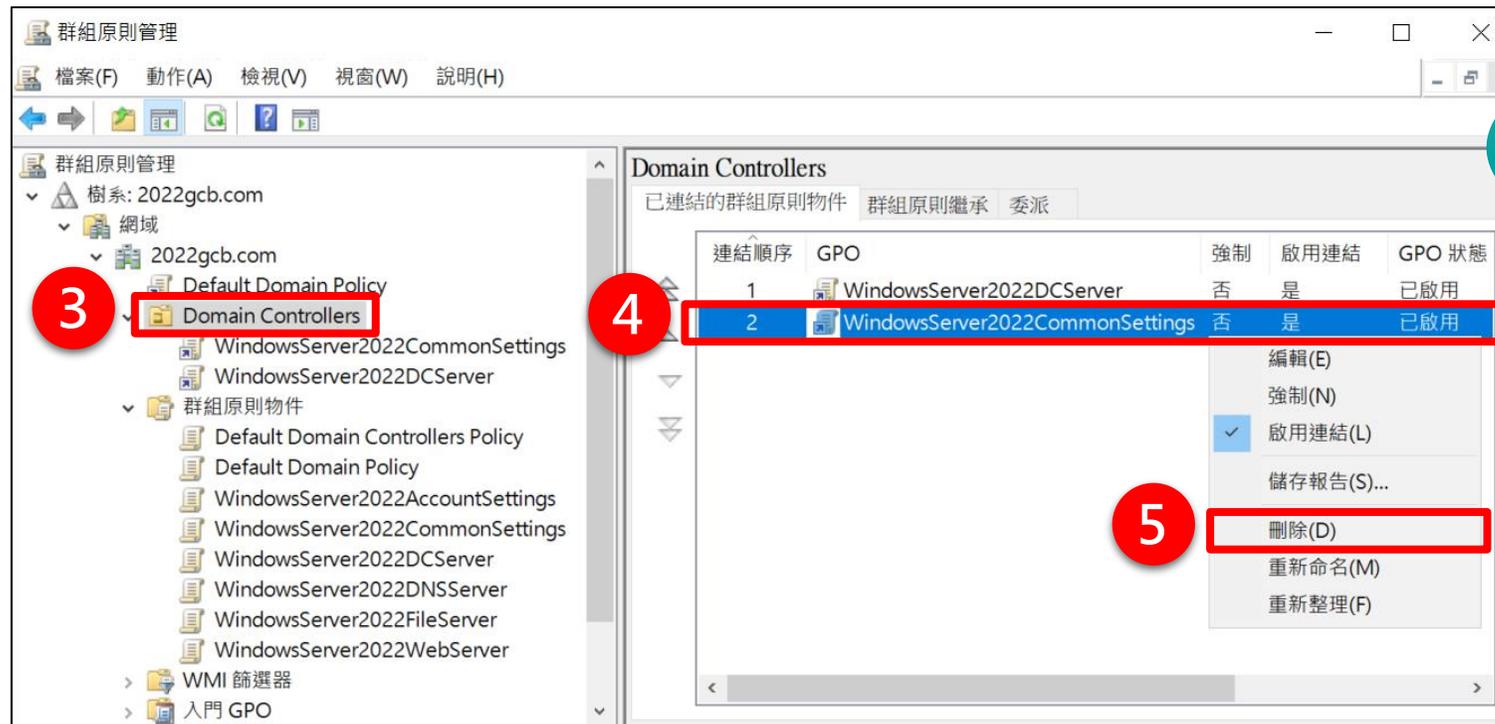
恢復原始設定之方式(1/3)

- 步驟1：點擊開始→Windows系統管理工具
- 步驟2：點擊群組原則管理



恢復原始設定之方式(2/3)

- 步驟3：點選欲取消GPO連結之組織單位(OU)
- 步驟4：在已連結的群組原則物件頁面，選取欲取消連結的GPO按滑鼠右鍵
- 步驟5：點選「刪除」將GPO自組織單位中移除



請點選
並按右鍵

恢復原始設定之方式(3/3)

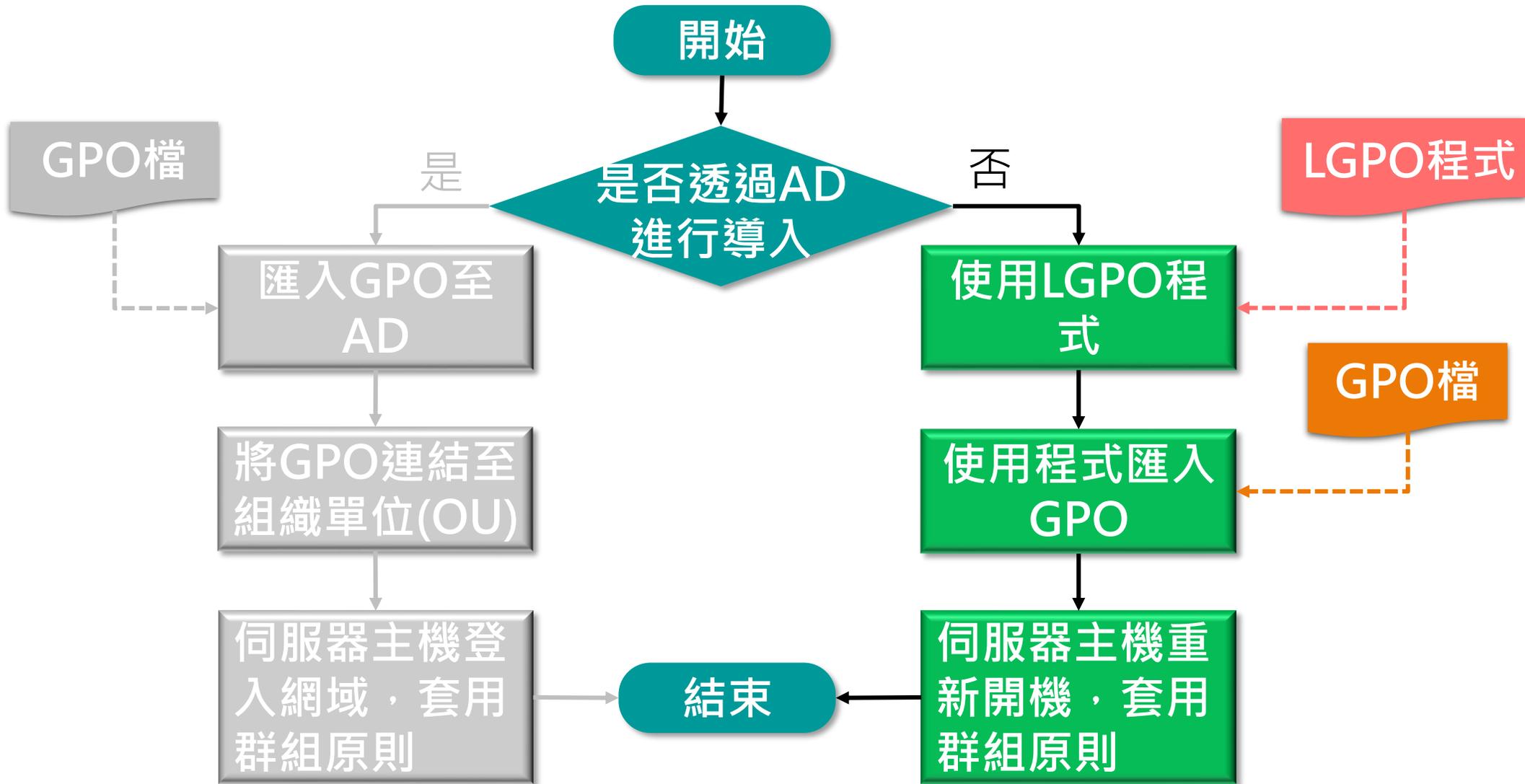
- 步驟6：請將網域內之Windows Server 2022重新開機，或以系統管理者權限開啟命令提示字元(點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→更多→點選「以系統管理員身分執行」)
- 步驟7：輸入gpupdate /force指令更新群組原則，即可恢復原始設定

請點選
並按右鍵



2.2 單機環境部署

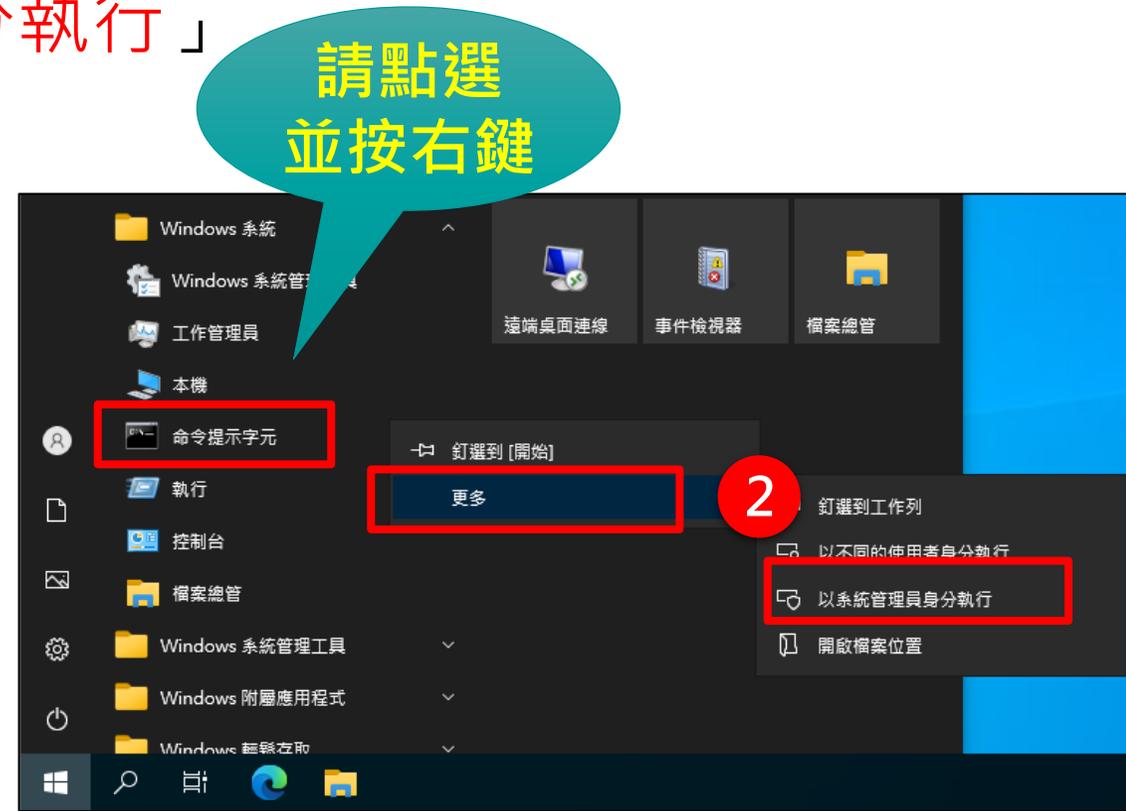
單機環境部署流程



2.2.1 使用LGPO程式導入GCB

使用LGPO部署GPO(1/5)

- 步驟1：請將下載之LGPO.zip程式解壓縮至C:\LGPO_30
- 步驟2：點擊開始→Windows系統→在「命令提示字元」按滑鼠**右鍵**→更多→點選「**以系統管理員身分執行**」



使用LGPO部署GPO(2/5)

- 步驟3：複製LGPO應用程式解壓縮後之完整目錄路徑
- 步驟4：於「命令提示字元」輸入cd <LGPO_30完整目錄路徑>，
切換至LGPO_30目錄



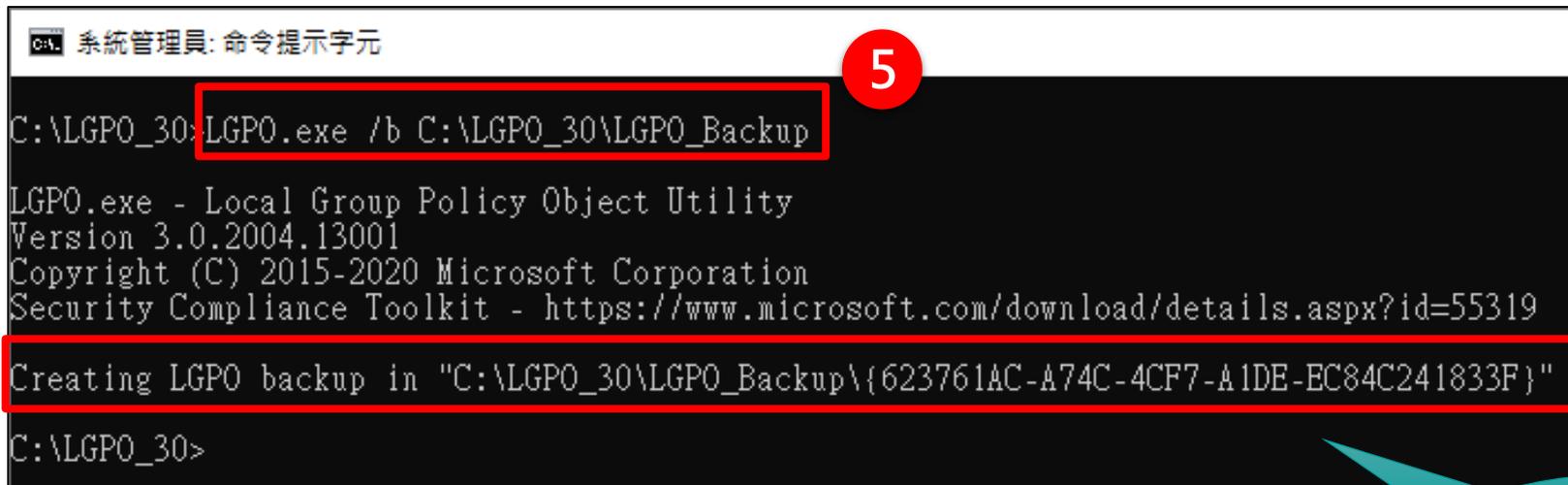
```
系統管理員: 命令提示字元
Microsoft Windows [版本 10.0.20348.230]
(c) Microsoft Corporation. 著作權所有，並保留一切權利。
C:\Windows\system32> cd C:\LGPO_30
C:\LGPO_30>
```

4

完成資料夾切換

使用LGPO部署GPO(3/5)

- 步驟5：於「命令提示字元」輸入指令 **LGPO.exe /b <絕對路徑>**，
備份電腦當下組態設定
 - 此範例備份電腦當下組態設定，儲存於C:\LGPO_30\LGPO_Backup資料夾

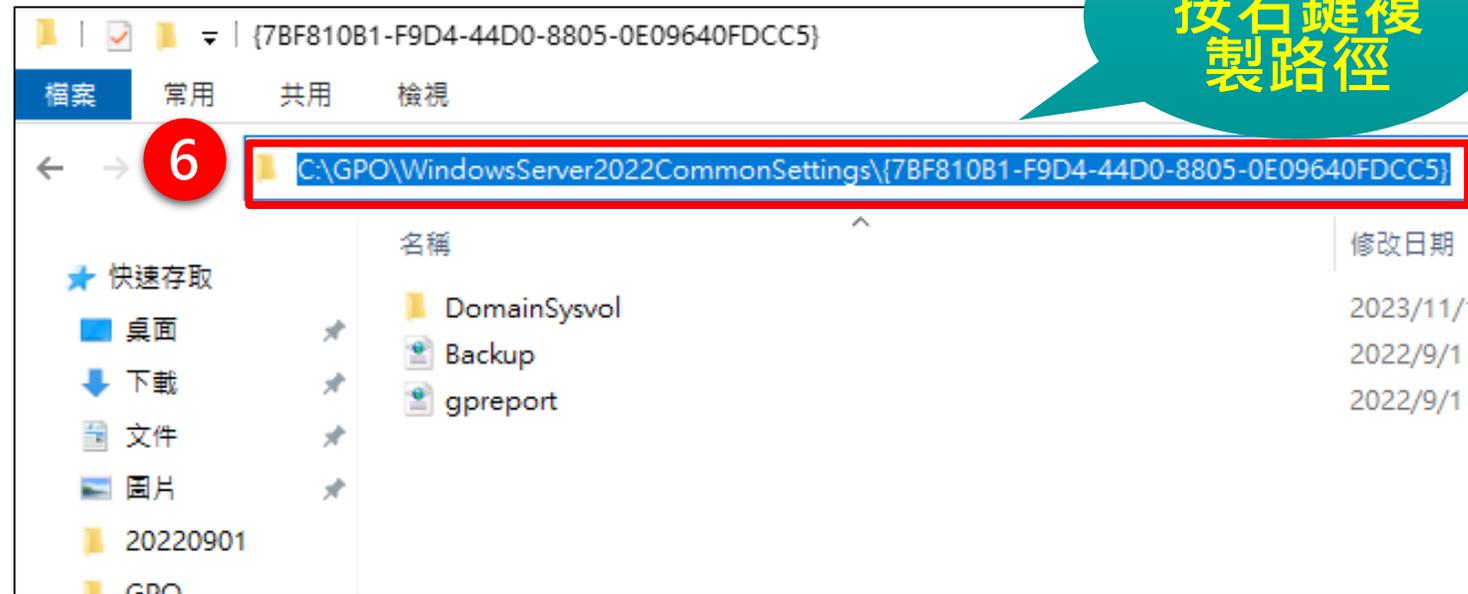


```
系統管理員: 命令提示字元
C:\LGPO_30> LGPO.exe /b C:\LGPO_30\LGPO_Backup
LGPO.exe - Local Group Policy Object Utility
Version 3.0.2004.13001
Copyright (C) 2015-2020 Microsoft Corporation
Security Compliance Toolkit - https://www.microsoft.com/download/details.aspx?id=55319
Creating LGPO backup in "C:\LGPO_30\LGPO_Backup\{623761AC-A74C-4CF7-A1DE-EC84C241833F}"
C:\LGPO_30>
```

顯示備份
成功

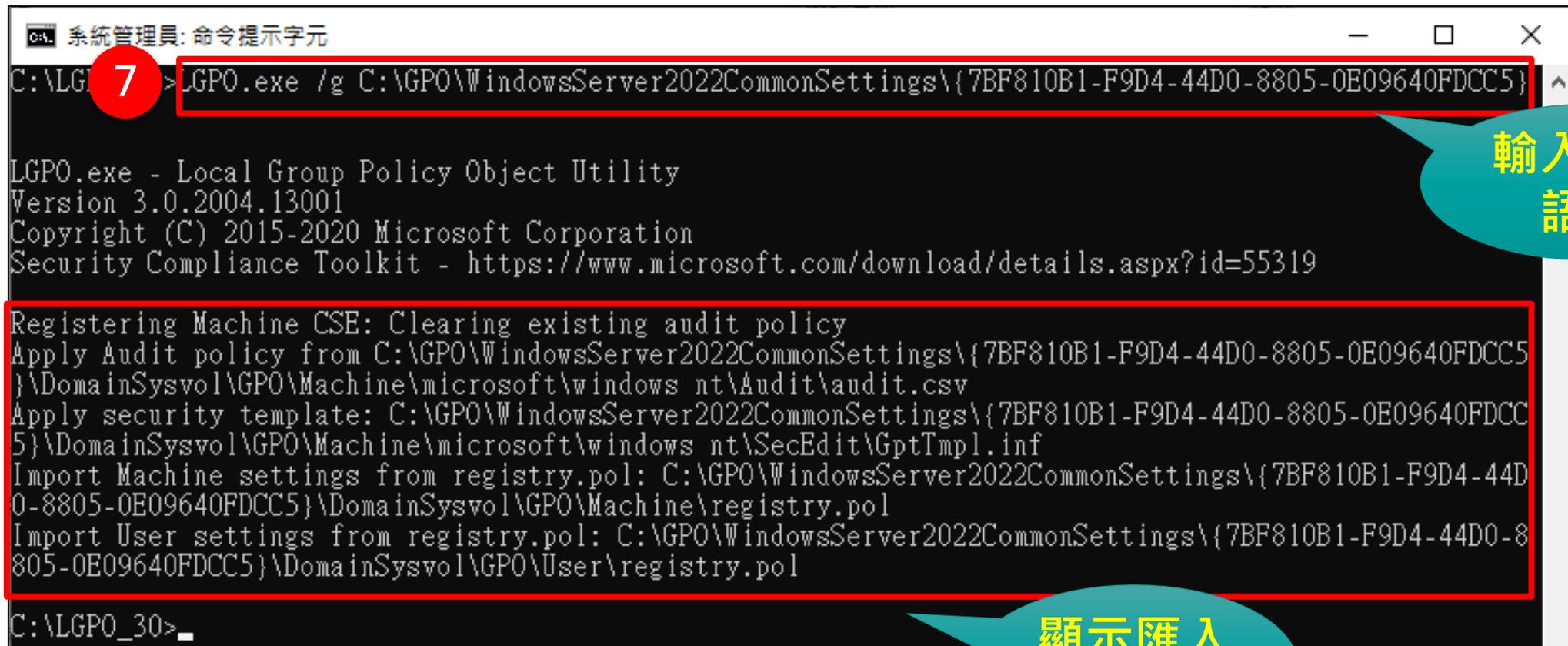
使用LGPO部署GPO(4/5)

- 步驟6：複製欲匯入之GPO完整目錄路徑
 - 此範例將GPO放置於C:\GPO資料夾，GPO完整目錄路徑為C:\GPO\WindowsServer2022CommonSettings\{7BF810B1-F9D4-44D0-8805-0E09640FDCC5}



使用LGPO部署GPO(5/5)

- 步驟7：於「命令提示字元」輸入指令 **LGPO.exe /g <GPO完整目錄路徑>**，將GPO檔案匯入電腦



```
系統管理員: 命令提示字元
C:\LGPO_30> LGPO.exe /g C:\GPO\WindowsServer2022CommonSettings\{7BF810B1-F9D4-44D0-8805-0E09640FDCC5}

LGPO.exe - Local Group Policy Object Utility
Version 3.0.2004.13001
Copyright (C) 2015-2020 Microsoft Corporation
Security Compliance Toolkit - https://www.microsoft.com/download/details.aspx?id=55319

Registering Machine CSE: Clearing existing audit policy
Apply Audit policy from C:\GPO\WindowsServer2022CommonSettings\{7BF810B1-F9D4-44D0-8805-0E09640FDCC5}\DomainSysvol\GPO\Machine\microsoft\windows nt\Audit\audit.csv
Apply security template: C:\GPO\WindowsServer2022CommonSettings\{7BF810B1-F9D4-44D0-8805-0E09640FDCC5}\DomainSysvol\GPO\Machine\microsoft\windows nt\SecEdit\GptTmpl.inf
Import Machine settings from registry.pol: C:\GPO\WindowsServer2022CommonSettings\{7BF810B1-F9D4-44D0-8805-0E09640FDCC5}\DomainSysvol\GPO\Machine\registry.pol
Import User settings from registry.pol: C:\GPO\WindowsServer2022CommonSettings\{7BF810B1-F9D4-44D0-8805-0E09640FDCC5}\DomainSysvol\GPO\User\registry.pol

C:\LGPO_30>_
```

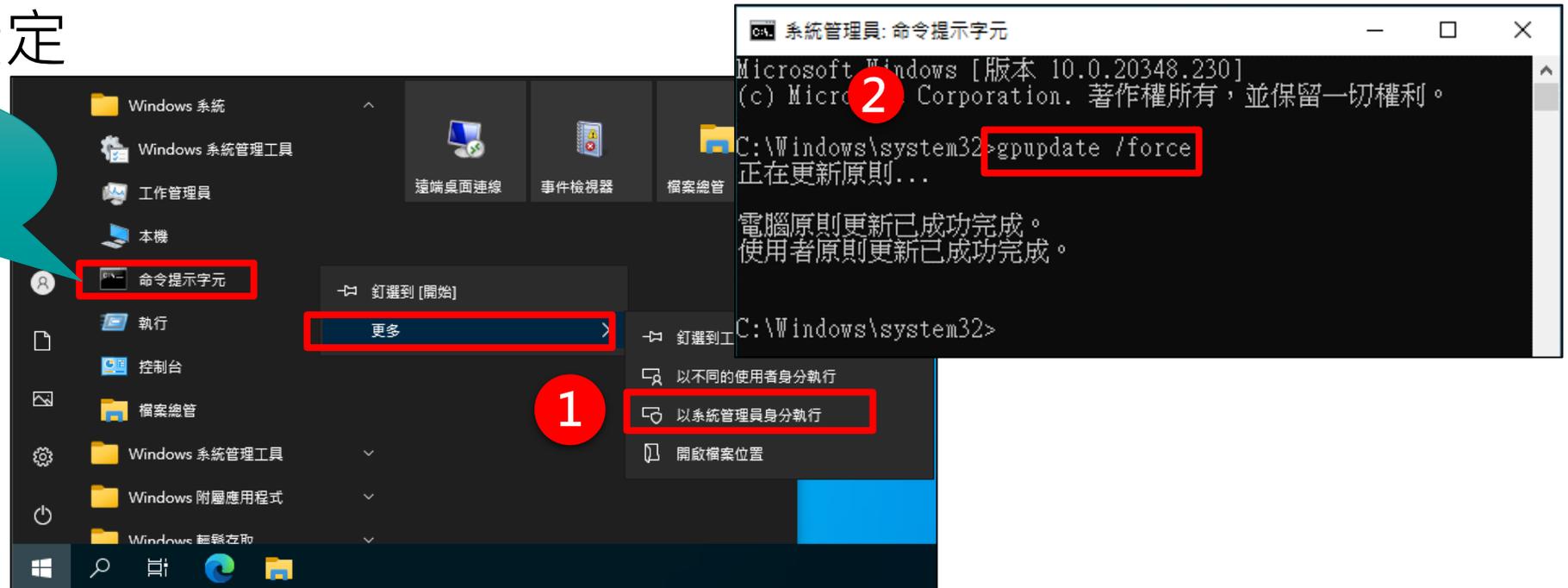
輸入匯入語法

顯示匯入結果

更新群組原則

- 方法1：將Windows Server 2022重新開機。
- 方法2：以系統管理者權限開啟命令提示字元(點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→更多→點選「以系統管理員身分執行」)，再輸入gpupdate /force指令更新群組原則，即可完成GCB設定

請點選
並按右鍵

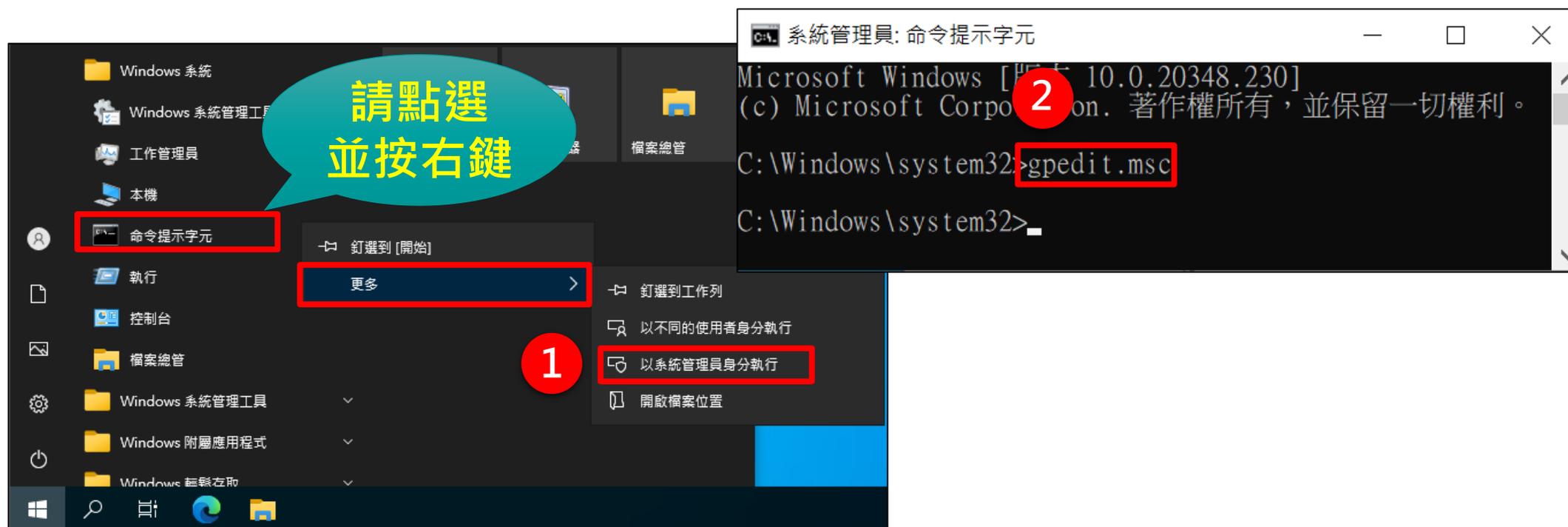


2.2.2 GPO套用狀況檢查方式

GPO套用狀況檢查方式(1/2)

● 使用GPEdit檢查本機群組原則

- 步驟1：點擊開始→Windows系統→在「命令提示字元」按滑鼠**右鍵**→更多→點選「**以系統管理員身分執行**」
- 步驟2：於「命令提示字元」輸入**gpedit.msc**查詢本機群組原則結果



GPO套用狀況檢查方式(2/2)

– 步驟3：抽檢GCB項目，確認是否確實套用(如：電腦設定\Windows設定\安全性設定\本機原則\安全性選項\互動式登入：不要顯示上次登入)

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)
 - 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)

原則	安全性設
互動式登入: 不要在登入期間顯示使用者名稱	尚未定義
互動式登入: 不要求按 CTRL+ALT+DEL 鍵	已停用
互動式登入: 不要顯示上次登入	已啟用
互動式登入: 在工作階段被封鎖時顯示使用者資訊	尚未定義
互動式登入: 在密碼到期前提示使用者變更密碼	14 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	已啟用
互動式登入: 智慧卡移除操作	鎖定工作站
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	900 秒
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	4 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

顯示群組原則套用結果

2.2.3 恢復原始設定之方式

恢復原始設定之方式(1/4)

- 步驟1：點擊開始→Windows系統→在「命令提示字元」按滑鼠**右鍵**→更多→點選「**以系統管理員身分執行**」)
- 步驟2：於「命令提示字元」輸入刪除本機群組原則資料夾指令 RD /S /Q C:\Windows\System32\GroupPolicy



恢復原始設定之方式(2/4)

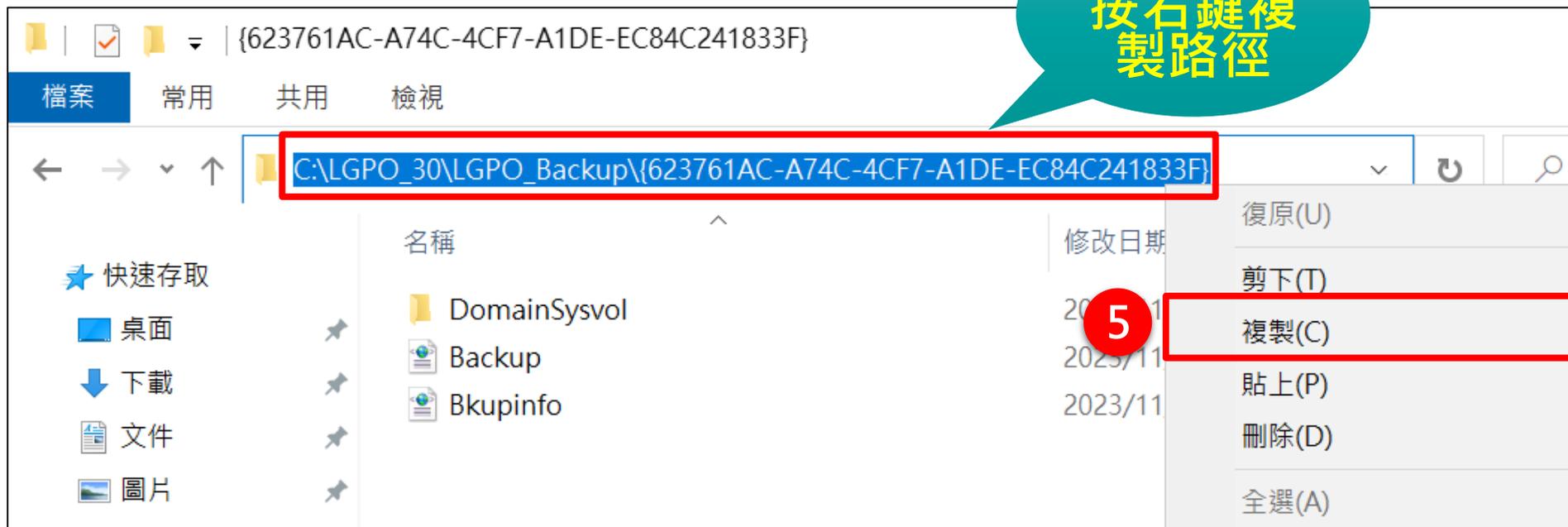
- 步驟3：複製LGPO應用程式解壓縮後之完整目錄路徑
- 步驟4：於「命令提示字元」輸入cd <LGPO完整目錄路徑>，切換至LGPO_30目錄

The image shows two screenshots illustrating the steps to navigate to the LGPO_30 directory. The top screenshot is a Windows File Explorer window showing the path C:\LGPO_30. A red circle with the number 3 is next to the address bar, and a red box highlights the path. A callout bubble says "請選取並按右鍵複製路徑" (Please select and right-click to copy the path). The bottom screenshot is a Command Prompt window showing the command cd C:\LGPO_30 being entered. A red circle with the number 4 is next to the command, and a red box highlights the path. A callout bubble says "完成資料夾切換" (Complete folder switch).

恢復原始設定之方式(3/4)

- 步驟5：複製備份的GPO完整目錄路徑

- 此範例備份之GPO，儲存於C:\LGPO_30\LGPO_Backup資料夾，完整目錄路徑為C:\LGPO_30\LGPO_Backup\{623761AC-A74C-4CF7-A1DE-EC84C241833F}



恢復原始設定之方式(4/4)

- 步驟6：於「命令提示字元」輸入LGPO.exe /g <備份的GPO完整目錄路徑>，還原部署Windows Server 2022 GPO前之設定
- 步驟7：請將Windows Server 2022重新開機，或輸入gpupdate /force指令更新群組原則，即可完成恢復原始設定

6

```
系統管理員: 命令提示字元
C:\LGPO_30>LGPO.exe /g C:\LGPO_30\LGPO_Backup\{623761AC-A74C-4CF7-A1DE-EC84C241833F}
LGPO.exe - Local Group Policy Object Utility
Version 3.0.2004.13001
Copyright (C) 2015-2020 Microsoft Corporation
Security Compliance Toolkit - https://www.microsoft.com/download/details.aspx?id=45516
Registering Machine CSE: Registry Policy, {35378EAC-683F-11D2-A89A-00C04FBBCFA2}
Registering User CSE: Registry Policy, {35378EAC-683F-11D2-A89A-00C04FBBCFA2}
Clearing existing audit policy
Apply Audit policy from C:\LGPO_30\LGPO_Backup\{623761AC-A74C-4CF7-A1DE-EC84C241833F}\
DomainSysvol\GPO\Machine\microsoft\windows nt\Audit\audit.csv
Apply security template: C:\LGPO_30\LGPO_Backup\{623761AC-A74C-4CF7-A1DE-EC84C241833F}\
DomainSysvol\GPO\Machine\microsoft\windows nt\SecEdit\GptTmpl.inf
Import Machine settings from registry.pol: C:\LGPO_30\LGPO_Backup\{623761AC-A74C-4CF7-
A1DE-EC84C241833F}\DomainSysvol\GPO\Machine\registry.pol
Import User settings from registry.pol: C:\LGPO_30\LGPO_Backup\{623761AC-A74C-4CF7-A1D
E-EC84C241833F}\DomainSysvol\GPO\User\registry.pol
C:\LGPO_30>
```

輸入匯入
語法

7

```
系統管理員: 命令提示字元
Microsoft Windows [版本 10.0.20348.230]
(c) Microsoft Corporation. 著作權所有，並保留一切權利。
C:\Windows\system32>gpupdate /force
更新原則...
更新原則更新已成功完成。
使用者原則更新已成功完成。
C:\Windows\system32>
```

更新群組
原則

顯示匯入
結果

3. 伺服器角色專用GPO部署方式

共用與專用群組原則GPO

- Account Settings與Common Settings為**共用群組原則GPO**
- DC Server、DNS Server、File Server及Web Server為**專用群組原則GPO(伺服器角色專用GPO)**

項次	GPO	項數
1	Windows Server 2022 Account Settings	9
2	Windows Server 2022 Common Settings	314
3	Windows Server 2022 DC Server	29
4	Windows Server 2022 DNS Server	115
5	Windows Server 2022 File Server	120
6	Windows Server 2022 Web Server	117

共用群組
原則GPO

專用群組
原則GPO
(伺服器角
色專用GPO)

檢查安裝之伺服器角色(1/5)

- Windows Server 2022 GCB定義之伺服器角色，係指於「伺服器管理員」安裝之角色，各角色於「伺服器管理員」之確認方式如下
- 步驟1：點擊開始→伺服器管理員



檢查安裝之伺服器角色(2/5)

- 步驟2：在「伺服器管理員」檢查是否安裝**網域控制站(DC Server)**，點選「AD DS」進入「伺服器」畫面，檢查「角色和功能」列表中是否包含「**Active Directory 網域服務**」角色服務

2

有安裝DC Server

伺服器名稱	名稱	類型	路徑
SERVER2022	Active Directory 網域服務	角色	Active Directory 網域服務

檢查安裝之伺服器角色(3/5)

–步驟3：在「伺服器管理員」檢查是否安裝**DNS伺服器(DNS Server)**，點選「DNS」進入「伺服器」畫面，檢查「角色和功能」列表中是否包含「**DNS伺服器**」角色服務

The screenshot shows the Windows Server Management console. The left-hand navigation pane has the 'DNS' option highlighted with a red box and a red circle containing the number '3'. The main content area displays the '角色和功能' (Roles and Features) section for the selected server, 'SERVER2022'. A table lists the installed roles and features, with one entry highlighted by a red box:

伺服器名稱	名稱	類型	路徑
SERVER2022	DNS 伺服器	角色	DNS 伺服器

A teal speech bubble with yellow text points to the table entry, stating: 有安裝DNS Server

檢查安裝之伺服器角色(4/5)

步驟4：在「伺服器管理員」檢查是否安裝**檔案伺服器(File Server)**，點選「檔案和存放服務」進入「伺服器」畫面，檢查「角色和功能」列表中是否包含「**檔案伺服器**」角色服務

The screenshot shows the Windows Server Manager interface. The left-hand navigation pane has '伺服器' (Servers) selected and highlighted with a red box. A red circle with the number '4' is positioned next to the '工作資料夾' (Work Folders) icon. The main area displays the '角色和功能' (Roles and Features) section for the server 'SERVER2022'. A table lists the installed roles and features, with the '檔案伺服器' (File Server) role highlighted in red.

伺服器名稱	名稱	類型	路徑
SERVER2022	檔案和存放服務	角色	檔案和存放服務
SERVER2022	檔案和 iSCSI 服務	角色服務	檔案和存放服務\檔案和 iSCSI 服務
SERVER2022	檔案伺服器	角色服務	檔案和存放服務\檔案和 iSCSI 服務\檔案伺服器
SERVER2022	存放服務	角色服務	檔案和存放服務\存放服務

有安裝File Server

檢查安裝之伺服器角色(5/5)

步驟5：在「伺服器管理員」檢查是否安裝**網頁伺服器(Web Server)**，點選「IIS」進入「伺服器」畫面，檢查「角色和功能」列表中是否包含「**網頁伺服器**」角色服務

伺服器管理員

伺服器管理員 ▸ IIS

儀表板
本機伺服器
所有伺服器
AD DS
DNS
IIS
檔案和存放服務 ▸

角色和功能
所有角色和功能 | 總計 15

篩選

伺服器名稱	名稱	類型	路徑
SERVER2022	網頁伺服器 (IIS)	角色	網頁伺服器 (IIS)
SERVER2022	管理工具	角色服務	網頁伺服器 (IIS)\管理工具
SERVER2022	IIS 管理主控台	角色服務	網頁伺服器 (IIS)\管理工具\IIS 管理主控台
SERVER2022	網頁伺服器	角色服務	網頁伺服器 (IIS)\網頁伺服器
SERVER2022	效能	角色服務	網頁伺服器 (IIS)\網頁伺服器\效能
SERVER2022	靜態內容壓縮	角色服務	網頁伺服器 (IIS)\網頁伺服器\效能\靜態內容壓縮
SERVER2022	一般 HTTP 功能	角色服務	網頁伺服器 (IIS)\網頁伺服器\一般 HTTP 功能

5

有安裝Web Server

3.1 非安裝網域控制站、DNS伺服器、檔案伺服器及網頁伺服器角色之部署說明

GPO部署說明

- 非安裝**網域控制站**、**DNS伺服器**、**檔案伺服器及網頁伺服器**角色之Windows Server 2022伺服器，僅需套用**共用群組原則**的2個GPO，不需套用**專用群組原則**GPO

項次	GPO	分類
1	Windows Server 2022 Account Settings	共用群組原則
2	Windows Server 2022 Common Settings	共用群組原則

3.2 安裝網域控制站、DNS伺服器、檔案 伺服器及網頁伺服器角色之部署說明

GPO部署說明(1/4)

- 安裝**網域控制站、DNS伺服器、檔案伺服器及網頁伺服器**角色之Windows Server 2022伺服器，除了要套用**共用群組原則**的2個GPO，必須再套用其專屬之**專用群組原則**GPO

項次	GPO	分類
1	Windows Server 2022 Account Settings	共用群組原則
2	Windows Server 2022 Common Settings	共用群組原則
3	Windows Server 2022 DC Server	專用群組原則
4	Windows Server 2022 DNS Server	專用群組原則
5	Windows Server 2022 File Server	專用群組原則
6	Windows Server 2022 Web Server	專用群組原則

GPO部署說明(2/4)

- 網域控制站、DNS伺服器、檔案伺服器及網頁伺服器所需套用之

GPO與其優勢順序列表

伺服器角色	GPO優勢順序	GPO	分類
網域控制站	1	Windows Server 2022 DC Server	專用群組原則
	2	Windows Server 2022 Account Settings	共用群組原則
	3	Windows Server 2022 Common Settings	共用群組原則
DNS伺服器	1	Windows Server 2022 DNS Server	專用群組原則
	2	Windows Server 2022 Account Settings	共用群組原則
	3	Windows Server 2022 Common Settings	共用群組原則
File伺服器	1	Windows Server 2022 File Server	專用群組原則
	2	Windows Server 2022 Account Settings	共用群組原則
	3	Windows Server 2022 Common Settings	共用群組原則
Web伺服器	1	Windows Server 2022 Web Server	專用群組原則
	2	Windows Server 2022 Account Settings	共用群組原則
	3	Windows Server 2022 Common Settings	共用群組原則

- GPO部署的優勢順序說明

- 當**專用群組原則**與**共用群組原則**之GPO同時套用於伺服器時，**專用群組原則**應優勢於**共用群組原則**GPO

- 以網域控制站GPO部署為範例

- 單機部署：使用LGPO程式導入

- 單機部署情況下，後匯入之GPO會優勢於之前匯入的GPO

- 要先匯入**共用群組原則**的2個GPO後，接續再將**專用群組原則**Windows Server 2022 DC Server GPO匯入

伺服器角色	GPO優勢順序	GPO	分類
網域控制站	1	Windows Server 2022 DC Server	專用群組原則
	2	Windows Server 2022 Account Settings	共用群組原則
	3	Windows Server 2022 Common Settings	共用群組原則

GPO部署說明(4/4)

–AD部署：使用群組原則管理工具導入

- 在已連結之群組原則物件中的優先順序，將**專用群組原則**之Windows Server 2022 DC Server GPO調整到優勢於**共用群組原則**GPO

The screenshot shows the Group Policy Management console for the domain 2022gcb.com. The left pane shows the tree structure with 'Domain Controllers' selected. The right pane shows the 'Domain Controllers' GPO list with the following priority order:

優先順序	GPO
1	WindowsServer2022DCServer
2	WindowsServer2022CommonSettings
3	WindowsServer2022AccountSettings

Annotations in the image:

- A green box labeled '專用群組原則' (Dedicated Group Policy) points to the first GPO, 'WindowsServer2022DCServer'.
- A blue box labeled '共用群組原則' (Shared Group Policy) points to the second and third GPOs, 'WindowsServer2022CommonSettings' and 'WindowsServer2022AccountSettings'.

網域控制站伺服器部署說明

- Windows Server 2022 GCB中有4項群組原則針對網域控制站與非網域控制站伺服器有不同建議設定值，此4項群組原則同時存在於DC Server與Common Settings之GPO中，網域控制站導入GCB時，會同時套用DC Server與Common Settings之GPO，需以**專用群組原則的DC Server GPO設定值為優先使用**

原則設定名稱	分類	DC Server設定值	Common Settings設定值
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	安全性選項	0次	4次以下
拒絕從網路存取這台電腦	使用者權限指派	Guests,本機帳戶	Guests,本機帳戶與Administrators群組的成員
從網路存取這台電腦	使用者權限指派	Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS	Administrators, Authenticated Users
稽核電腦帳戶管理	進階稽核原則	成功及失敗	成功

3.3 安裝複數伺服器角色之部署說明

複數伺服器角色部署說明(1/3)

- 安裝複數**專用群組原則**伺服器角色之部署說明

- 在網域控制站伺服器、DNS伺服器、檔案伺服器及網頁伺服器之**專用群組原則**GPO中，有3項**系統服務**，對前述伺服器角色分別有不同建議設定值

系統服務	DC Server 建議設定值	DNS Server 建議設定值	File Server 建議設定值	Web Server 建議設定值
Application Identity	自動	手動	手動	手動
Distributed Link Tracking Client	手動	自動	自動	自動
Windows Time	自動	手動	手動	手動

- 在需要同時部署複數**專用群組原則**GPO的情況，為確保上表的3項系統服務符合GCB建議之啟動狀態，在各GPO有不同建議設定值時，GCB的部署設定值須以「**自動** > **手動** > **已停用**」之優先度進行調整

複數伺服器角色部署說明(2/3)

- 複數伺服器角色中**包含網域控制站**之部署說明
 - 以同時部署**網域控制站**與**DNS**伺服器之GPO為範例說明，需以「**自動 > 手動 > 已停用**」之優先度調整下列3項系統服務的**設定值**
 - Application Identity
 - Distributed Link Tracking Client
 - Windows Time
 - 依**優先度調整後的設定值**如下表

系統服務	DC Server 建議設定值	DNS Server 建議設定值	依優先度調整後 的設定值
Application Identity	自動	手動	自動
Distributed Link Tracking Client	手動	自動	自動
Windows Time	自動	手動	自動

複數伺服器角色部署說明(3/3)

- 複數伺服器角色中**不包含網域控制站**之部署說明
 - 以同時部署**DNS**、**File**及**Web**伺服器之GPO為範例說明，因下列3項系統服務之建議設定值是一致的，**不需要調整設定值**
 - Application Identity
 - Distributed Link Tracking Client
 - Windows Time
 - 依**優先度調整後的設定值**如下表

系統服務	Web Server 建議設定值	File Server 建議設定值	DNS Server 建議設定值	依優先度調整 後的設定值
Application Identity	手動	手動	手動	無需調整
Distributed Link Tracking Client	自動	自動	自動	無需調整
Windows Time	手動	手動	手動	無需調整

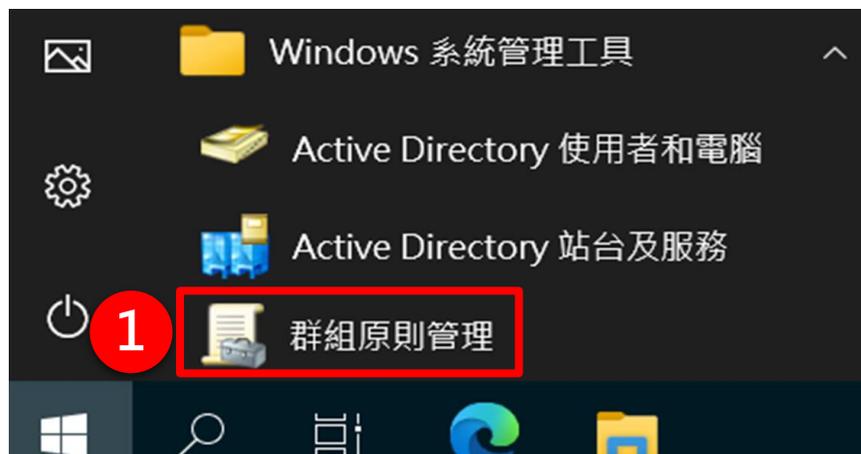
複數伺服器角色AD部署方式(1/12)

- 以同時安裝網域控制站與DNS伺服器角色為範例說明

1. 逐一建立網域控制站與DNS伺服器2個**專用群組原則**GPO，以及2個**共用群組原則**GPO

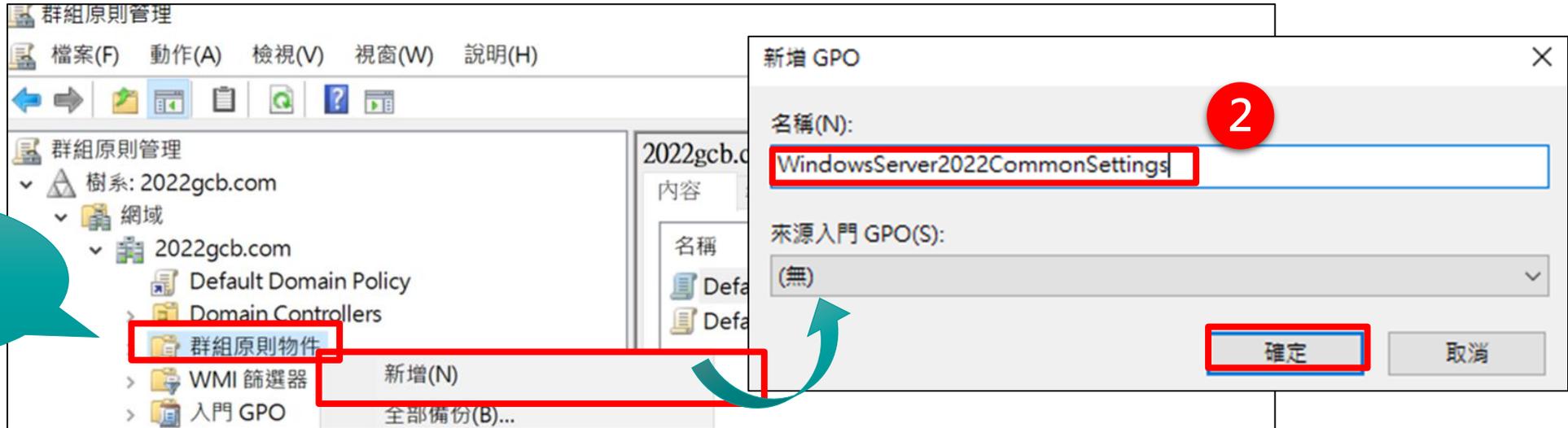
伺服器角色	GPO	分類
網域控制站 兼 DNS伺服器	Windows Server 2022 DC Server	專用群組原則
	Windows Server 2022 DNS Server	專用群組原則
	Windows Server 2022 Account Settings	共用群組原則
	Windows Server 2022 Common Settings	共用群組原則

– 步驟1：點擊開始→Windows系統管理工具→群組原則管理

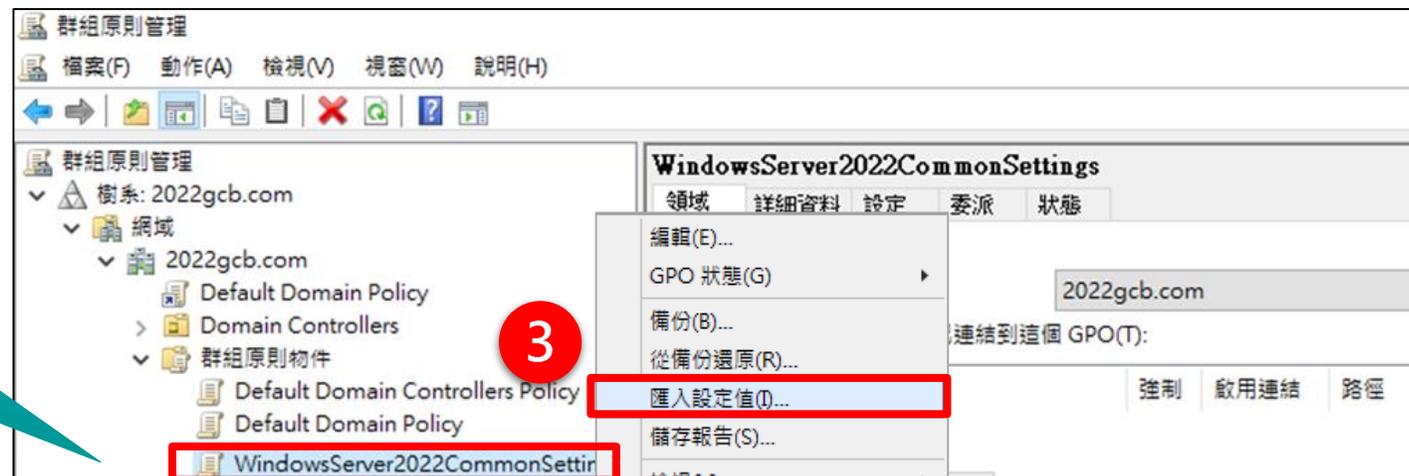


複數伺服器角色AD部署方式(2/12)

– 步驟2：在群組原則物件節點按滑鼠右鍵→新增→輸入群組原則物件之名稱

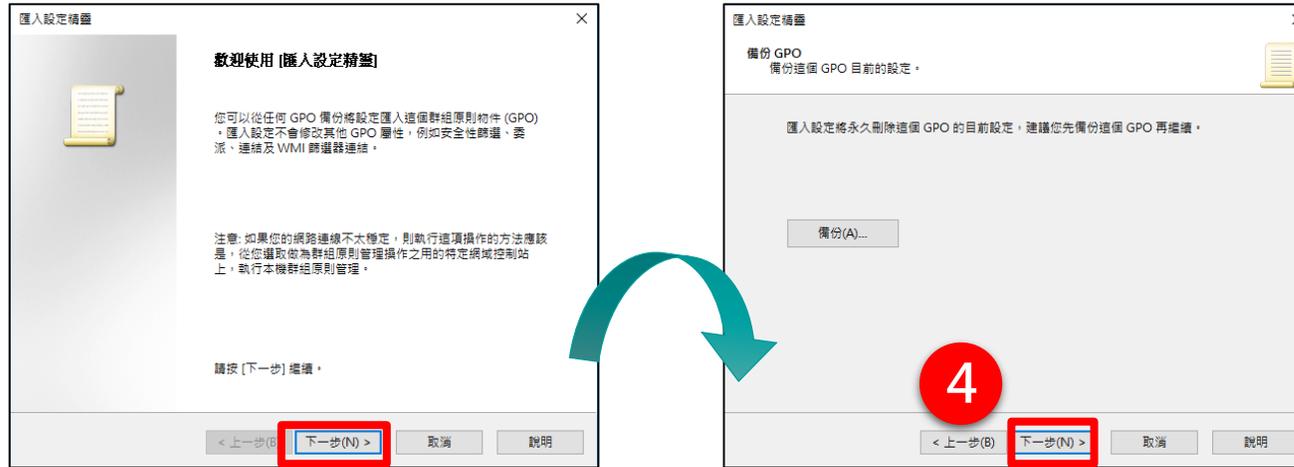


– 步驟3：點選新建之群組原則物件按滑鼠右鍵→選擇「匯入設定值」

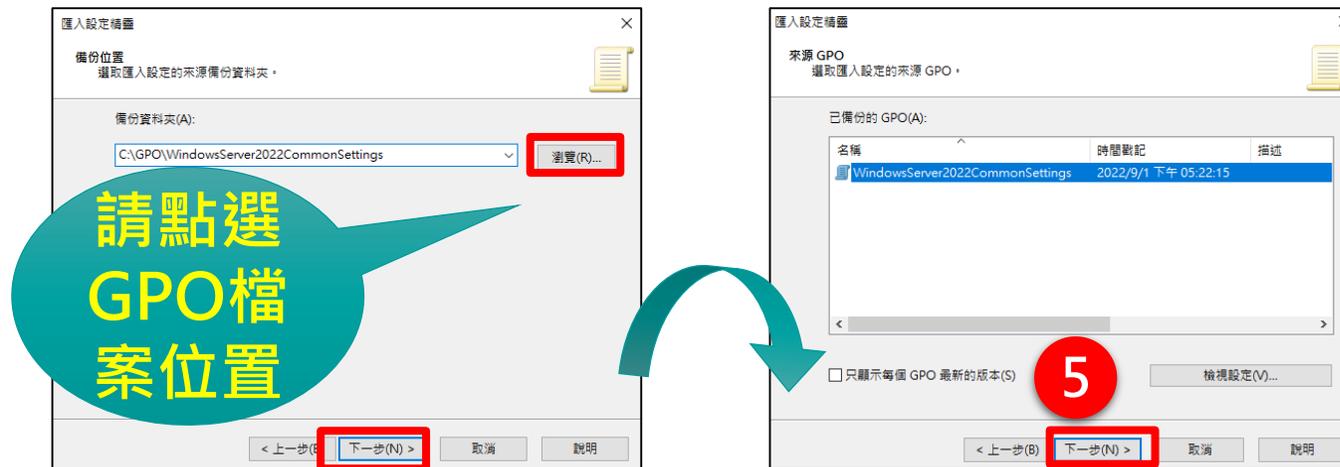


複數伺服器角色AD部署方式(3/12)

– 步驟4：在歡迎使用【匯入設定精靈】與備份GPO頁面→點選「下一步」



– 步驟5：在備份位置頁面→選取放置GPO之資料夾→點選「下一步」，
在來源GPO頁面→選取欲匯入之GPO→點選「下一步」



複數伺服器角色AD部署方式(4/12)

- 步驟6：在掃描備份頁面→點選「下一步」，
- 在正在完成匯入設定精靈頁面→點選「完成」，
- 在匯入進度頁面→點選「確定」，完成匯入GPO

匯入設定精靈

掃描備份
精靈正在掃描在備份中的設定，決定是否有任何安全性主體或 UNC 路徑參照。

掃描結果：
備份不包含任何安全性主體或 UNC 路徑的參照。請按 [下一步] 繼續。

< 上一步(B) **下一步(N) >** 取消

匯入設定精靈

正在完成 [匯入設定精靈]

您已成功地完成 [匯入設定精靈]。精靈將從下列定。

摘要：
備份位置：
C:\GPO\WindowsServer2022CommonSett
備份 GPO：
名稱:WindowsServer2022CommonSettings
時間戳記: 2022/9/1 下午 05:22:15
描述：
移轉表格: 無

請按一下 [完成] 來關閉這個精靈並匯入設定。

< 上一步(B) **完成** 取消

匯入

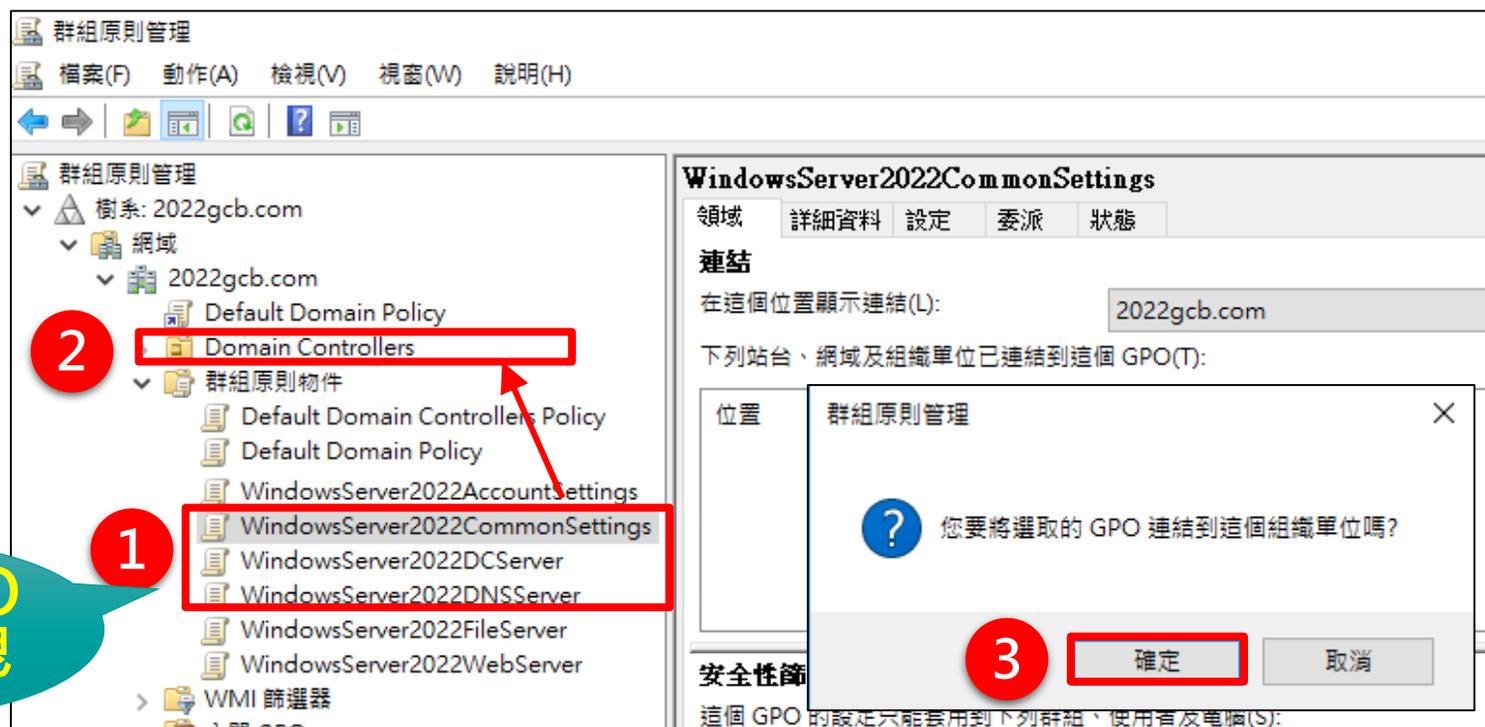
匯入進度：
狀態(S):
GPO: WindowsServer2022CommonSettings...已成功

顯示匯入成功

6 **確定** 取消

2. 將建立的GPO，逐一**拖曳**至Windows Server 2022伺服器所在之組織單位(此範例為Domain Controllers)進行連結

- 步驟1：點選已匯入GPO之群組原則物件
- 步驟2：拖曳至組織單位
- 步驟3：點選「確定」按鈕，完成將GPO連結至組織單位



請點GPO
進行拖曳

3. 將專用群組原則GPO調整到優先於共用群組原則GPO

- 步驟1：點選組織單位(此為Domain Controllers)→已連結的群組原則物件，調整DC Server與DNS Server GPO之連結順序，優先於共用群組原則
- 步驟2：點選「群組原則繼承」，確認GPO之優先順序符合專用群組原則優先於共用群組原則

The screenshot shows the Group Policy Management console. On the left, the tree view shows the hierarchy: 2022gcb.com > 網域 > 2022gcb.com > Domain Controllers. A red box highlights 'Domain Controllers' with a red circle '1'. A red box highlights the '已連結的群組原則物件' (Linked Group Policy Objects) tab. A table shows the link order of GPOs:

連結順序	GPO
1	WindowsServer2022DCServer
2	WindowsServer2022DNSServer
3	WindowsServer2022CommonSetting

A red box highlights the up/down arrows next to the link order column. A blue callout bubble says: 使用上下箭頭調整GPO的連結順序. An arrow points from this bubble to the right-hand screenshot. The right-hand screenshot shows the '群組原則繼承' (Group Policy Inheritance) tab. A message says: 這個清單不包含任何連結到站台的 GPO。請到說明參閱詳細資料。 Below is a table of GPOs with their priority and location:

優先順序	專用群組原則	位置
1	WindowsServer2022DCServer	Domain Controllers
2	WindowsServer2022DNSServer	Domain Controllers
3	WindowsServer2022CommonSettings	Domain Controllers
4	WindowsServer2022AccountSettings	2022gcb.com

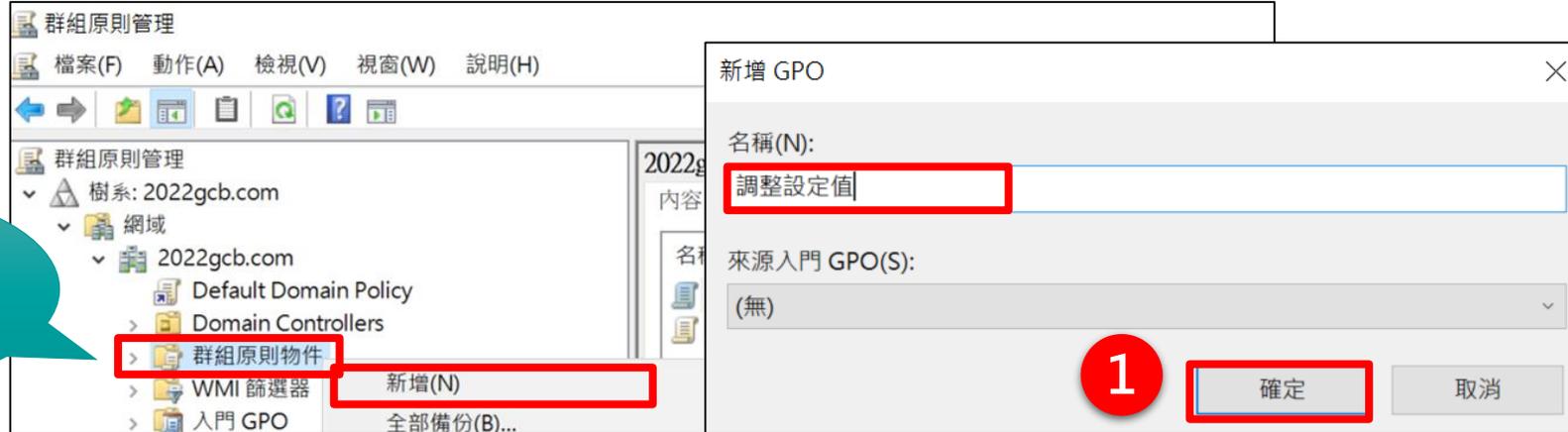
A red box highlights the first two rows (DC and DNS servers) with a red circle '2'. A blue callout bubble says: 專用群組原則. A yellow callout bubble says: 共用群組原則. An arrow points from the '專用群組原則' bubble to the first row of the table.

複數伺服器角色AD部署方式(7/12)

4. 調整「Application Identity」、「Distributed Link Tracking Client」及「Windows Time」三項系統服務之設定值為「自動」

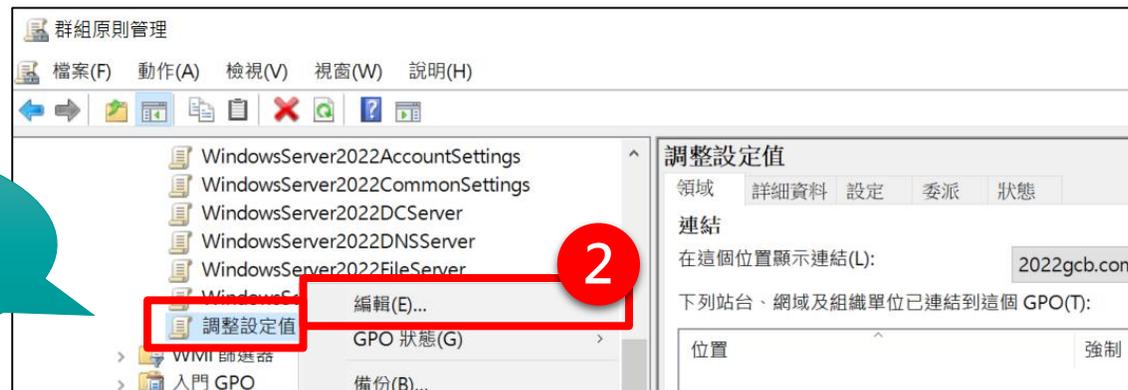
– 步驟1：在群組原則物件節點按滑鼠右鍵→新增→名稱輸入「調整設定值」

請點選
並按右鍵



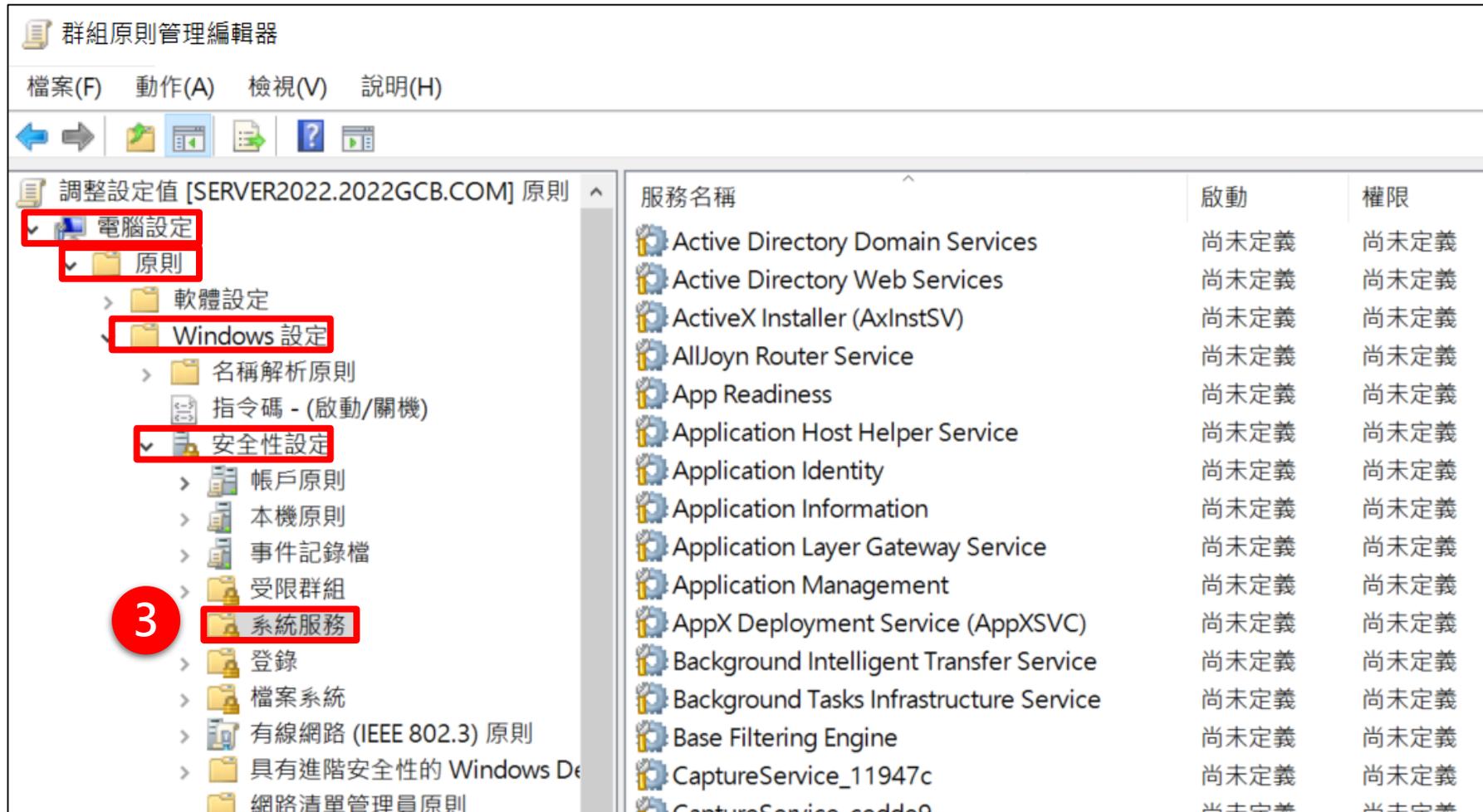
– 步驟2：點選「調整設定值」GPO，按滑鼠右鍵→選擇「編輯」

請點選
並按右鍵



複數伺服器角色AD部署方式(8/12)

– 步驟3：在「群組原則管理編輯器」視窗，點選電腦設定→原則→Windows
設定→安全性設定→系統服務



複數伺服器角色AD部署方式(9/12)

- 步驟4：在「系統服務」中，逐一點擊「Application Identity」、「Distributed Link Tracking Client」及「Windows Time」此3項系統服務，進入「內容」頁面，將服務啟動模式設定為「自動」

The screenshot shows the Windows Group Policy Editor interface. The left pane shows the tree structure with 'System Services' selected. The right pane displays a list of services with their start modes. A red box highlights the 'Application Identity', 'Distributed Link Tracking Client', and 'Windows Time' services, all of which are set to 'Automatic'. A red circle with the number '4' is placed over the 'System Services' folder in the left pane. A callout bubble points to the 'Application Identity' service in the list, and another callout bubble points to the 'Content' page of the 'Application Identity' policy, where the 'Automatic' start mode is selected. A third callout bubble points to the 'Application Identity' folder in the left pane, indicating the next step is to click into its content page.

服務名稱	啟動
Application Identity	自動
Distributed Link Tracking Client	自動
Windows Time	自動
Active Directory Domain Services	尚未定義
Active Directory Web Services	尚未定義
ActiveX Installer (AxInstSV)	尚未定義
AllJoyn Router Service	尚未定義
App Readiness	尚未定義
Application Host Helper Service	尚未定義
Application Identity	自動

3項服務調整為「自動」

4

請點擊進入內容頁面

Application Identity - 內容

定義這個原則設定(D)

選擇服務啟動模式:

自動(U)

手動(M)

停用(S)

確定 取消 套用(A)

複數伺服器角色AD部署方式(10/12)

– 步驟5：將「調整設定值」GPO拖曳至組織單位(此為Domain Controllers)進行連結

The screenshot displays the Group Policy Management console for the domain 2022gcb.com. The left-hand tree view shows the organizational structure, with the 'Domain Controllers' organizational unit highlighted by a red box. A red circle with the number '5' is placed over the 'Domain Controllers' folder. A red box also highlights the '調整設定值' (Adjust Settings) GPO in the left pane. A red arrow points from this GPO to the 'Domain Controllers' folder. A blue speech bubble with yellow text says '請拖曳 GPO 至 組織單位' (Please drag the GPO to the organizational unit). Another blue speech bubble with yellow text says '請點選 GPO 進行拖曳' (Please click the GPO to drag). A dialog box is open in the center, asking '您要將選取的 GPO 連結到這個組織單位嗎?' (Do you want to link the selected GPO to this organizational unit?). The '確定' (OK) button in the dialog box is highlighted with a red box. The right-hand pane shows the '調整設定值' GPO configuration, with the '連結' (Link) tab selected. The '在這個位置顯示連結(L):' (Link to this location) field is set to '2022gcb.com'. Below this, the '個 GPO(T):' (GPOs) section shows 'Authenticated Users' with the '啟用連結' (Link Enabled) checkbox checked.

複數伺服器角色AD部署方式(11/12)

– 步驟6：點選組織單位→已連結的群組原則物件，調整「調整設定值」GPO之連結順序，優先於DC Server與DNS Server GPO

– 步驟7：點選「群組原則繼承」，確認「調整設定值」GPO順序為最優先

The screenshot shows the Group Policy Management console. On the left, the tree view shows the hierarchy: 2022gcb.com > 網域 > 2022gcb.com > Domain Controllers. The 'Domain Controllers' folder is selected and highlighted with a red box and a red circle containing the number 6. In the main pane, the '已連結的群組原則物件' (Linked Group Policy Objects) tab is active, showing a list of GPOs with their link order. The '調整設定值' (Adjust Settings) GPO is at the top of the list. A red box highlights the up and down arrow icons next to it, with a red circle containing the number 6. A callout bubble points to these arrows with the text: 使用上下箭頭調整GPO的連結順序. To the right, the '群組原則繼承' (Group Policy Inheritance) tab is active, showing a list of GPOs. The '調整設定值' GPO is at the top of the list, highlighted with a red box and a red circle containing the number 7. A callout bubble points to this GPO with the text: 調整設定值GPO. Below this, another callout bubble points to the 'Domain Controllers' location for the '調整設定值' GPO with the text: 專用群組原則.

連結順序	GPO
1	調整設定值
2	WindowsServer2022DCServer
3	WindowsServer2022DNSServer
4	WindowsServer2022CommonSettings

優先順序	GPO	位置
1	調整設定值	Domain Controllers
2	WindowsServer2022DCServer	Domain Controllers
3	WindowsServer2022DNSServer	Domain Controllers
4	WindowsServer2022CommonSettings	Domain Controllers
5	WindowsServer2022AccountSettings	2022gcb.com

使用上下箭頭調整GPO的連結順序

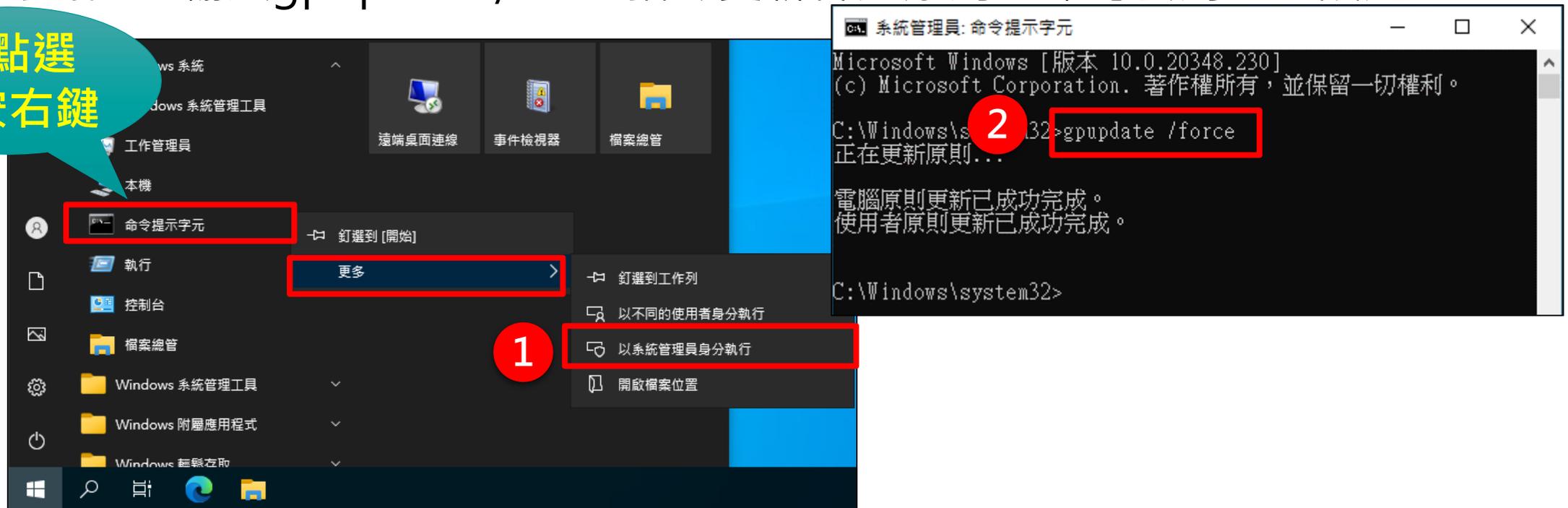
調整設定值GPO

專用群組原則

5. 更新群組原則

- 步驟1：請將Windows Server 2022重新開機，或以系統管理者權限開啟命令提示字元(點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→更多→點選「以系統管理員身分執行」)
- 步驟2：輸入gpupdate /force指令更新群組原則，即可套用GCB設定

請點選
並按右鍵



參考資料

- TWGCB-01-011_Microsoft Windows Server 2022政府組態基準說明文件
 - https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/GCB/GCB_Documentation/
- 作業系統GPO
 - https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/GCB/GCB_Deployment_Resources/
- Microsoft Security Compliance Toolkit and Baselines
 - <https://www.microsoft.com/en-us/download/details.aspx?id=55319>

報告完畢 敬請指教



國家資通安全研究院
National Institute of Cyber Security