政府組態基準
Microsoft Windows Server 2016
TWGCB-01-007
(V1.2)

行政院國家資通安全會報技術服務中心
中華民國111年2月

修訂歷史紀錄表

項次	版次	修訂日期	說明
1	1.0	108/9/26	新編
2	1.1	111/1/4	封面新增「TWGCB-ID」文件編號
3	1.2	111/2/11	▪ 表 2~表 6 部分項次說明內容修改用語，包含： i. 「此項安全性設定」與「這個原則設定」修改為「這項原則設定」 ii. 「這個原則」修改為「這項原則」 iii. 「和」修改為「與」或「及」 iv. 移除多餘之說明文字、空格、標點符號及贅字(如的、和、不、使用者) v. 調整文字段落與標點符號 vi. 刪除對 Windows Server 2016 前之舊版作業系統與非伺服器版本提醒事項 vii. 「重要：」、「警告：」及「重要事項：」修改為「注意：」 ▪ 表 2 項次 45 之說明內容，由「停用此設定就不允許 Win32 子系統區分大小寫」修改為「如果停用此設定，將允許非 Windows 子系統區分大小寫」 ▪ 表 2 項次 73 說明內容之錯別字「篡改」修改為「竄改」 ▪ 表 2 項次 84 之說明內容，由「不正確地」修改為「不正確的」 ▪ 表 2 項次 90 之說明內容，由「關閉此原則」修改為「停用此原則」 ▪ 表 2 項次 92 與 150，說明內容第一句句首補充「這項原則設定決定」、「這個原則設定」，並調整文字段落與標點符號 ▪ 表 2 項次 95 之說明內容，由「如下：」修改為「選項如下：」

			▪表 2 項次 108、109、111、134 及 135 之說明內容，由「阻止」修改為「禁止」 ▪表 2 項次 129 之說明內容，由「此設定」修改為「此權限」 ▪表 2 項次 150 與 153，表 4 項次 70，表 5 項次 75，表 6 項次 70 之說明內容，由「RD」修改為「遠端桌面」 ▪表 2 項次 156 之說明內容，由「控制能否」修改為「決定能否」 ▪表 2 項次 171 之說明內容，由「可以決定」修改為「決定是否」 ▪表 2 項次 176 與 180 之說明內容，由「收集」修改為「蒐集」 ▪表 2 項次 277 之說明內容，由「損毀時停用」修改為「損毀時關閉」 ▪表 2 項次 299 之說明內容，由「他們」修改為「使用者」 ▪表 2 項次 315 之說明內容，由「的」修改為「之」 ▪表 4 項次 115，表 5 項次 120，表 6 項次 116 之說明內容，由「Windows Updat」修改為「Windows Update」 ▪新增 10 項、刪除 1 項及修改 46 項設定項目，異動內容詳見附件 1
4			
5			

目　次

表 目 次

1. 前言

政府組態基準(Government Configuration Baseline, 以下簡稱 GCB)目的在於規範資通訊終端設備(如個人電腦等)之一致性安全設定(如密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之風險。

1.1 適用環境

本文件適用於微軟公司所發行之 Windows Server 2016 作業系統。

1.2 項數統計

政府組態基準針對電腦作業環境提供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。Windows Server 2016 組態基準基本項目(包含 Account settings 與 Common settings)共計 307 項，無論伺服器是何種角色皆須部署基本項目，接著再依不同伺服器角色，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 28 項設定項目、DNS Server 組態基準 119 項設定項目、File Server 組態基準 124 項設定項目及 Web Server 組態基準 121 項設定項目，項目統計詳見表 1。

表1　Windows Server 2016 組態基準項目統計

項次	項目	項數	小計	合計
1	Windows Server 2016 Account Settings	9	307	699
	Windows Server 2016 Common Settings	298		
2	Windows Server 2016 DC Server	28	28	
3	Windows Server 2016 DNS Server	119	119	
4	Windows Server 2016 File Server	124	124	
5	Windows Server 2016 Web Server	121	121	

資料來源：本中心整理

1.3 文件發行

本文件最新版本公布於本中心網站之「政府組態基準」專區，網址為 https://www.nccst.nat.gov.tw/GCB。

2. Windows Server 2016 政府組態基準列表

表2　Windows Server 2016 政府組態基準列表(基本項目)

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
1	Windows Server 2016 Account Settings	TWGCB-01-007-0001	密碼原則	密碼最短使用期限	▪這項原則設定決定在使用者變更密碼之前，密碼必須使用的期限(天數)。使用者可以設定 1 與 998 天之間的值，或設定天數為 0，以允許立即變更 ▪「密碼最短使用期限」不得超過「密碼最長使用期限」，除非「密碼最長使用期限」設定為 0，表示密碼永遠不會到期。如果「密碼最長使用期限」設定為 0，則「密碼最短使用期限」可以設定為介於 0 到 998 之間的任何數值 ▪如果要讓「強制執行密碼歷程記錄」生效，請將「密碼最短使用期限」設為 0 以上。若沒有設定「密碼最短使用期限」，使用者便可重複使用密碼，直到	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則\密碼最短使用期限	1 天	CCE-ID：CCE-4560 8-7

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					厭倦為止。預設值並未依循此建議，所以系統管理員可為使用者指定密碼，然後在使用者登入時要求變更系統管理員定義的密碼。如果「密碼歷程記錄」設為 0，使用者便不需選擇新密碼 ▪ 強制執行密碼歷程記錄在網域控制站上預設值為 1，獨立伺服器上預設值為 0			
2	Windows Server 2016 Account Settings	TWG CB-01-007-0002	密碼原則	密碼最長使用期限	▪ 這項原則設定決定系統要求使用者變更密碼之前，密碼可以使用的期限(天數)。使用者可以設定密碼在 1 至 999 天之後到期；或將天數設為 0，表示密碼永遠不會到期。如果「密碼最長使用期限」介於 1 到 999 天之間，則「密碼最短使用期限」不得超過「密碼最長使用期限」的天數。如果「密碼最長使用期限」設定為 0，則「密碼最短使用期限」可以是介於 0 到 998 天之間的任何	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則\密碼最長使用期限	90 天以下，但須大於 0 天	CCE-ID：CCE-44704-5

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					數值 ▪根據環境而定，「密碼最長使用期限」若設定密碼每 30 至 90 天到期。如此一來，攻擊者破解使用者密碼及存取網路資源的時間便很有限 ▪「密碼最長使用期限」預設值為 42			
3	Windows Server 2016 Account Settings	TWG CB-01-007-0003	密碼原則	最小密碼長度	▪這項原則設定決定使用者帳戶的密碼可包含的最少字元數 ▪使用者可以設定介於 1 到 14 個字元之間的值，或是將字元數設為 0，如此便不需要密碼 ▪最小密碼長度在網域控制站上預設值為 7，在獨立伺服器上預設值為 0	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則\最小密碼長度	12 個字元以上	CCE-ID：CCE-46914-8
4	Windows Server 2016 Account	TWG CB-01-007-0004	密碼原則	密碼必須符合複雜性需求	▪這項原則設定決定密碼是否必須符合複雜性需求 ▪如果啟用此項原則，則密碼必須符合下列最小需求：	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼	已啟用	CCE-ID：CCE-4730

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings				➢不包含使用者的帳戶名稱全名中，超過兩個以上的連續字元 ➢長度至少為 6 個字元 ➢包含下列四種字元中的三種： (1)英文大寫字元(A 到 Z) (2)英文小寫字元(a 到 z) (3)10 進位數字(0 到 9) (4)非英文字母字元(例如：!、$、#、%) ▪建立或變更密碼時會強制執行複雜性需求 ▪密碼必須符合複雜性需求在網域控制站上預設為啟用，在獨立伺服器上預設為停用	原則\密碼必須符合複雜性需求		9-0
5	Windows Server 2016	TWG CB-01-007-0	密碼原則	強制執行密碼歷程	▪這項原則設定決定重覆使用舊密碼前，必須與使用者帳戶相關的唯一新密碼數目。此值必須介於 0 與 24 個密碼	電腦設定\Windows 設定\安全性設定\	3 個以上記憶的密碼	CCE-ID：CCE-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
	Account Settings	005		記錄	之間 ▪ 這項原則可讓系統管理員藉由確定不再繼續重複使用舊密碼，以增加安全性 ▪ 「強制執行密碼歷程記錄」在網域控制站上預設為 24，在獨立伺服器上預設為 0	帳戶原則\密碼原則\強制執行密碼歷程記錄		44479-4
6	Windows Server 2016 Account Settings	TWGCB-01-007-0006	密碼原則	使用可還原的加密來存放密碼	▪ 這項原則設定決定作業系統是否使用可還原的加密來存放密碼 ▪ 此原則支援應用程式使用需要知道使用者密碼來進行驗證的通訊協定。使用可還原的加密來存放密碼，基本上與存放純文字密碼是相同的。基於這個理由，除非應用程式需求比保護密碼資訊重要，否則不應啟用這項設定 ▪ 當透過遠端存取或網際網路驗證服務(IAS)使用 Challenge-Handshake 驗證通訊協定來驗證時，便需要這項原則。在	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則\使用可還原的加密來存放密碼	已停用	CCE-ID：CCE-45002-3

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					網際網路資訊服務(IIS)中使用摘要式驗證時，也需要這項原則 ▪ 預設值為已停用			
7	Windows Server 2016 Account Settings	TWG CB-01-007-0007	帳戶鎖定原則	帳戶鎖定閾值	▪ 這項原則設定決定導致使用者帳戶被鎖定的嘗試登入失敗次數。除非由系統管理員重設或該帳戶的鎖定時間已到期，否則無法使用該鎖定帳戶。失敗的登入嘗試值可設定為介於 0 到 999 之間。如果將值設定為 0，將永遠不會鎖定該帳戶 ▪ 對使用 CTRL+ALT+DELETE 或受密碼保護的螢幕保護裝置來鎖定的工作站或成員伺服器輸入密碼失敗，也算是失敗的登入嘗試 ▪ 預設值為 0	電腦設定\Windows 設定\安全性設定\帳戶原則\帳戶鎖定原則\帳戶鎖定閾值	5 次以下不正確的登入嘗試，但須大於 0 次	CCE-ID：CCE-46497-4
8	Windows Server	TWG CB-01	帳戶鎖定	重設帳戶鎖定計數	▪ 這項原則設定決定在登入嘗試失敗之後必須經過幾分鐘，才會將失敗的登入	電腦設定\Windows 設定	15 分鐘以上	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
	2016 Account Settings	-007-0008	原則	器的時間間隔	嘗試計數器重設為 0 次失敗。可用的範圍是從 1 分鐘到 99,999 分鐘 ▪ 如果已定義帳戶鎖定閾值，此重設時間必須小於或等於帳戶鎖定時間	\安全性設定\帳戶原則\帳戶鎖定原則\重設帳戶鎖定計數器的時間間隔		CCE-47272-0
9	Windows Server 2016 Account Settings	TWGCB-01-007-0009	帳戶鎖定原則	帳戶鎖定時間	▪ 這項原則設定決定在鎖定帳戶自動解除鎖定之前，還會繼續鎖定的分鐘數。可用的範圍是從 0 分鐘到 99,999 分鐘。如果將帳戶鎖定時間設定為 0，將會繼續鎖定帳戶，直到系統管理員明確將該帳戶解除鎖定 ▪ 如果已定義帳戶鎖定閾值，帳戶鎖定時間必須大於或等於重設時間	電腦設定\Windows 設定\安全性設定\帳戶原則\帳戶鎖定原則\帳戶鎖定時間	15 分鐘以上	CCE-ID：CCE-47152-4
10	Windows Server 2016 Common	TWGCB-01-007-0010	安全性選項\Micro	Microsoft網路用戶端：傳送未加密的	▪ 如果啟用這項原則設定，便允許伺服器訊息區(SMB)重新導向器在驗證期間將純文字密碼傳送給不支援密碼加密的非 Microsoft SMB 伺服器	電腦設定\Windows 設定\安全性設定\本機原則\安全	已停用	CCE-ID：CCE-4613

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings		soft 網路用戶端	密碼到其他廠商的 SMB 伺服器	▪傳送未加密的密碼會有安全性風險 ▪預設為已停用	性選項\Microsoft 網路用戶端：傳送未加密的密碼到其他廠商的 SMB 伺服器		6-8
11	Windows Server 2016 Common Settings	TWG CB-01-007-0011	安全性選項\Microsoft 網路用戶端	Microsoft 網路用戶端：數位簽章用戶端的通訊(如果伺服器同意)	▪這項原則設定決定 SMB 用戶端是否嘗試交涉 SMB 封包簽章 ▪伺服器訊息區(SMB)通訊協定是 Microsoft 檔案及列印共用與許多其他網路作業(例如遠端 Windows 系統管理)的基礎。為避免攔截式攻擊修改傳送中的 SMB 封包，SMB 通訊協定支援 SMB 封包的數位簽章。這項原則設定決定 SMB 用戶端元件連線至 SMB 伺服器時，是否嘗試交涉 SMB 封包簽章 ▪若啟用此設定，Microsoft 網路用戶端將	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\Microsoft 網路用戶端：數位簽章用戶端的通訊(如果伺服器同意)	已啟用	CCE-ID：CCE-4633 4-9

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					於建立工作階段時要求伺服器執行 SMB 封包簽章。若已在伺服器上啟用封包簽章，將會交涉封包簽章 ▪ 若停用此設定，SMB 用戶端將不會交涉 SMB 封包簽章 ▪ 預設為已啟用			
12	Windows Server 2016 Common Settings	TWG CB-01-007-0012	安全性選項\Microsoft 網路用戶端	Microsoft 網路用戶端：數位簽章用戶端的通訊(自動)	▪ 這項原則設定決定 SMB 用戶端元件是否需要封包簽章 ▪ 伺服器訊息區(SMB)通訊協定是 Microsoft 檔案及列印共用與許多其他網路作業(例如遠端 Windows 系統管理)的基礎。為避免攔截式攻擊修改傳送中的 SMB 封包，SMB 通訊協定支援 SMB 封包的數位簽章。這項原則設定決定允許與 SMB 伺服器進一步通訊之前，SMB 封包簽章是否必須經過交涉 ▪ 若啟用此設定，Microsoft 網路用戶端將	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\Microsoft 網路用戶端：數位簽章用戶端的通訊(自動)	已啟用	CCE-ID：CCE-46135-0

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					不會與 Microsoft 網路伺服器通訊，除非該伺服器同意執行 SMB 封包簽章 ▪ 若停用此設定，會在用戶端與伺服器之間交涉 SMB 封包簽章 ▪ 預設為已停用			
13	Windows Server 2016 Common Settings	TWG CB-01-007-0013	安全性選項\Microsoft 網路伺服器	Microsoft 網路伺服器：伺服器 SPN 目標名稱驗證層級	▪ 這項原則設定控制具有共用資料夾的電腦或印表機(伺服器)在服務主體名稱(SPN)上執行的驗證層級，SPN 是用戶端電腦在使用伺服器訊息區(SMB)通訊協定來建立工作階段時所提供 ▪ 伺服器訊息區(SMB)通訊協定是檔案及列印共用與其他網路作業(例如遠端 Windows 系統管理)的基礎。SMB 通訊協定支援驗證 SMB 用戶端提供的驗證 blob 中的 SMB 伺服器服務主體名稱(SPN)，以防止針對 SMB 伺服器的類別攻擊(稱為 SMB 轉送攻擊)。此設定將同	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\Microsoft 網路伺服器：伺服器 SPN 目標名稱驗證層級	關閉	CCE-ID：CCE-46158-2

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					時影響 SMB1 與 SMB2 ▪ 這項原則設定可決定 SMB 伺服器在服務主體名稱(SPN)上執行的驗證層級，SPN 是 SMB 用戶端嘗試建立與 SMB 伺服器的工作階段時所提供 ▪ 選項如下： (1)關閉：SMB 伺服器不需要或不會驗證 SMB 用戶端的 SPN (2)如果是用戶端所提供則接受：SMB 伺服器將會接受與驗證 SMB 用戶端提供的 SPN，並允許當該 SPN 符合 SMB 伺服器本身的 SPN 清單時，建立工作階段。如果 SPN 不相符，將會拒絕該 SMB 用戶端的工作階段要求 (3)用戶端的要求：SMB 用戶端「必須」在工作階段設定中傳送 SPN 名稱，而且提供的 SPN 名稱「必須」符合			

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					被要求建立連線的 SMB 伺服器。如果用戶端未提供任何 SPN，或是提供的 SPN 不相符，則會拒絕該工作階段 ▪ 所有的 Windows 作業系統都支援用戶端 SMB 元件與伺服器端 SMB 元件。這項設定會影響伺服器 SMB 行為，而且應該小心評估與測試其執行，以防止檔案與列印服務功能中斷 ▪ 預設為關閉			
14	Windows Server 2016 Common Settings	TWG CB-01-007-0014	安全性選項\Microsoft 網路伺服器	Microsoft 網路伺服器：數位簽章伺服器的通訊(自動)	▪ 這項原則設定決定 SMB 伺服器元件是否需要封包簽章 ▪ 伺服器訊息區(SMB)通訊協定是 Microsoft 檔案及列印共用與許多其他網路作業(例如遠端 Windows 系統管理)的基礎。為避免攔截式攻擊修改傳送中的 SMB 封包，SMB 通訊協定支援 SMB 封包的數位簽章。這項原則設定決定允	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\Microsoft 網路伺服器：數位簽章伺服器	已啟用	CCE-ID：CCE-47038-5

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					許與 SMB 用戶端進行進一步的通訊之前，SMB 封包簽章是否必須經過交涉 ▪ 若啟用此設定，Microsoft 網路伺服器將不會與 Microsoft 網路用戶端通訊，除非該用戶端同意執行 SMB 封包簽章 ▪ 若停用此設定，會在用戶端與伺服器之間交涉 SMB 封包簽章 ▪ 預設為已停用	的通訊(自動)		
15	Windows Server 2016 Common Settings	TWG CB-01-007-0015	安全性選項\Microsoft 網路伺服器	Microsoft 網路伺服器：數位簽章伺服器的通訊(如果用戶端同意)	▪ 這項原則設定決定 SMB 伺服器是否將與要求 SMB 封包簽章的用戶端交涉 ▪ 伺服器訊息區(SMB)通訊協定是 Microsoft 檔案及列印共用與許多其他網路作業(例如遠端 Windows 系統管理)的基礎。為避免攔截式攻擊修改傳送中的 SMB 封包，SMB 通訊協定支援 SMB 封包的數位簽章。這項原則設定決定 SMB 伺服器是否將在 SMB 用戶端要求	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\Microsoft 網路伺服器：數位簽章伺服器的通訊(如果	已啟用	CCE-ID：CCE-46230-9

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
					SMB 封包簽章時進行交涉 ▪ 若啟用此設定，Microsoft 網路伺服器將在用戶端要求 SMB 封包簽章時進行交涉。也就是說，若已在用戶端啟用封包簽章，將會交涉封包簽章 ▪ 若停用此設定，SMB 用戶端將不會交涉 SMB 封包簽章	用戶端同意)		
16	Windows Server 2016 Common Settings	TWGCB-01-007-0016	安全性選項\Microsoft 網路伺服器	Microsoft 網路伺服器：暫停工作階段前，要求的閒置時間	▪ 這項原則設定決定伺服器訊息區(SMB)工作階段的連續閒置時間長度超過多少時，工作階段會因為處於非使用狀態而暫停 ▪ 系統管理員可使用此原則，控制電腦於何時暫停非使用中的 SMB 工作階段。若用戶端活動繼續，則會自動重新建立工作階段 ▪ 對於這項原則設定，零值表示在合理的時間範圍內儘速中斷工作階段的連	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\Microsoft 網路伺服器：暫停工作階段前，要求的閒置時間	15 分鐘以下，但須大於 0 分鐘	CCE-ID：CCE-4602 7-9

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					線。最大值是 99,999，實際上，此值會停用此設定			
17	Windows Server 2016 Common Settings	TWG CB-01-007-0017	安全性選項\Microsoft 網路伺服器	Microsoft 網路伺服器：當登入時數到期時，中斷用戶端連線	▪ 這項原則設定決定是否要在超出使用者帳戶的有效登入時數時，將連線到本機電腦的使用者中斷連線。此設定會影響到伺服器訊息區(SMB)元件 ▪ 啟用此設定時，便會在用戶端的登入時數到期之後，強迫將搭配 SMB 服務的用戶端工作階段中斷連線 ▪ 如果停用此設定，便允許在用戶端的登入時數到期之後，繼續維持建立的用戶端工作階段	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\Microsoft 網路伺服器：當登入時數到期時，中斷用戶端連線	已啟用	CCE-ID：CCE-44631-0
18	Windows Server 2016 Common Settings	TWG CB-01-007-0018	安全性選項\MSS	MSS：(NoDefaultExempt) Configure IPSec	▪ 這項原則設定決定是否啟用 IPSec 篩選器的預設豁免項目 ▪ 選項如下： (1)Allow all exemptions (least secure)：代表「多點傳送廣播，RSVP、	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：	Multicast, broadcast, & ISAKMP exempt	CCE-ID：CCE-45282-1

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				exemptions for various types of network traffic.	Kerberos 及 ISAKMP 流量不受限於 IPSec 篩選功能」 (2)Multicast, broadcast, & ISAKMP exempt (best for Windows XP)：代表「Kerberos 及 RSVP 流量不能免除 IPSec 篩選，但多點傳播、廣播及 ISAKMP 流量都是豁免」 (3)RSVP, Kerberos, and ISAKMP are exempt：代表「多點傳播和廣播流量不能免除 IPSec 篩選，但 RSVP、Kerberos 及 ISAKMP 流量被豁免」 (4)Only ISAKMP is exempt (recommended for Windows Server 2003)：代表「只有 ISAKMP 流量是免除 IPSec 篩選功能」	(NoDefaultExempt)Configure IPSec exemptions for various types of network traffic.	(best for Windows XP)	
19	Windows Server 2016	TWG CB-01-007-0	安全性選項	MSS：(KeepAliveTime)Ho	▪這項原則設定決定持續作用的封包多少毫秒會傳送一次，讓 TCP 藉由傳送持續作用封包，來嘗試驗證閒置連線狀態	電腦設定\Windows 設定\安全性設定\	300000 or 5 minutes(rec	CCE-ID：CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Common Settings	019	\MSS	w often keep-alive packets are sent in milliseconds	是否仍然不變 ▪ 如果遠端系統仍然可以連接與運作，就會確認持續作用傳輸 ▪ 在預設的情況下，並不會傳送持續作用封包 ▪ 這項功能可由應用程式在連線時啟用	本機原則\安全性選項\MSS：(KeepAliveTime)How often keep-alive packets are sent in milliseconds	ommended)	4528 1-3
20	Windows Server 2016 Common Settings	TWG CB-01 -007-0 020	安全性選項 \MSS	MSS：(TcpMax DataRetra nsmission s)How many times unacknow ledged data is	▪ 這項原則設定決定在放棄連線之前，透過 TCP 重傳未獲回應之資料的次數 ▪ 建議值設為 3 次，預設值設為 5 次	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：(TcpMaxDataRetransmissions) How many times unacknowledge	3 以下，但須大於 0	CCE-ID：CCE-4529 1-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
				retransmitted(3 recommended, 5 is default)		d data is retransmitted(3 recommended, 5 is default)		
21	Windows Server 2016 Common Settings	TWGCB-01-007-0021	安全性選項\MSS	MSS：(EnableICMPRedirect)Allow ICMP redirects to override OSPF generated routes	▪ 這項原則設定決定是否允許 ICMP 重新導向覆寫 OSPF 產生的路由，意謂著作業系統在回應由網路裝置(例如路由器)傳送給它的 ICMP 重新導向訊息時，是否要改變其路由表 ▪ 如果設定為啟用：作業系統在回應由網路裝置(例如路由器)傳送給它的 ICMP 重新導向訊息時，將會改變其路由表 ▪ 如果設定為停用：作業系統在回應由網路裝置(例如路由器)傳送給它的 ICMP 重新導向訊息時，不會改變其路由表	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：(EnableICMPRedirect)Allow ICMP redirects to override OSPF generated routes	已啟用	CCE-ID：CCE-45279-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
22	Windows Server 2016 Common Settings	TWGCB-01-007-0022	安全性選項\MSS	MSS：(Hidden) Hide Computer From the Browse List(not recommended except for highly secure environments)	▪ 這項原則設定決定是否從網路瀏覽列表中移除本台電腦名稱 ▪ 如果設定為啟用：將從網路瀏覽列表中移除本台電腦名稱 ▪ 如果設定為停用：網路瀏覽列表依然保留本台電腦名稱。知道本台電腦名稱之攻擊者，將可能透過網路蒐集本台電腦資訊	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：(Hidden)Hide Computer From the Browse List(not recommended except for highly secure environments)	已啟用	CCE-ID：CCE-45280-5
23	Windows Server 2016 Common	TWGCB-01-007-0023	安全性選項\MSS	MSS：(DisableIPSourceRouting)IP	▪ IP source routing 是一種允許傳送者決定資料包通過網路時應該採用 IP 路由的機制，可以用來指定一條從來源位址到目的位址之間的資料傳送路徑	電腦設定\Windows 設定\安全性設定\本機原則\安全	Highest protection, source routing is	CCE-ID：CCE-4527

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings			source routing protection level(protects against packet spoofing)	▪ 這項原則設定決定 IP source routing 防護層級(決定作業系統是否接受來源路由封包)，以避免封包偽裝(Packet Spoofing)攻擊。選項如下： (1)設為 No additional protection：代表作業系統接受與轉送來源路由封包 (2)設為 Medium：代表作業系統接受但不轉送來源路由封包 (3)設為 Highest protection：代表作業系統完全拒絕來源路由封包	性選項\MSS：(DisableIPSourceRouting)IP source routing protection level(protects against packet spoofing)	completely disabled	6-3
24	Windows Server 2016 Common Settings	TWG CB-01-007-0024	安全性選項\MSS	MSS：(DisableIPSourceRouting IPv6)IP source routing protection	▪ IP source routing 可以用來指定一條從來源位址到目的位址之間的資料傳送路徑 ▪ 這項原則設定決定 IP source routing 防護層級(決定作業系統是否接受來源路由封包)，以避免封包偽裝(Packet Spoofing)攻擊。選項如下：	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：(DisableIPSourceRouting IPv6)IP source	Highest protection, source routing is completely disabled	CCE-ID：CCE-4527 5-5

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				level(protects against packet spoofing)	(1)設為 No additional protection：代表作業系統接受與轉送來源路由封包 (2)設為 Medium：代表作業系統接受但不轉送來源路由封包 (3)設為 Highest protection：代表作業系統完全拒絕來源路由封包	routing protection level(protects against packet spoofing)		
25	Windows Server 2016 Common Settings	TWG CB-01-007-0025	安全性選項\MSS	MSS：(NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except	▪ NetBIOS(網路基本輸入/輸出系統)over TCP/IP 是一種網路通訊協定，提供簡易的解析方法，可以將登錄在 Windows 系統上的 NetBIOS 名稱解析為這些系統所設定的 IP 位址 ▪ 這項原則設定決定當電腦收到名稱釋放要求時是否釋放它的 NetBIOS 名稱 ▪ 如果設定為啟用：當電腦收到名稱釋放要求時，不會釋放它的 NetBIOS 名稱 ▪ 如果設定為停用：當電腦收到名稱釋放要求時，將會釋放它的 NetBIOS 名稱。	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：(NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests	已啟用	CCE-ID：CCE-45283-9

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				from WINS servers	惡意的使用者可以利用此通訊協定不需驗證的特質，將名稱衝突的資料包傳送到目標電腦，造成名稱釋放的情形而停止回應查詢，造成目標電腦發生連線斷斷續續的問題，或甚至造成無法使用「網路上的芳鄰」、網域登入、net send 命令，或是無法進行後續的 NetBIOS 名稱解析	except from WINS servers		
26	Windows Server 2016 Common Settings	TWG CB-01-007-0026	安全性選項\MSS	MSS：(TcpMaxDataRetransmissions IPv6)How many times unacknowledged	▪ 這項原則設定決定在放棄連線之前，透過 TCP 重傳未獲回應之資料的次數 ▪ 建議值設為 3 次，預設值設為 5 次	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：(TcpMaxDataRetransmissions IPv6)How many times unacknowledge	3 以下，但須大於 0	CCE-ID：CCE-4529 0-4

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				data is retransmitted(3 recommended, 5 is default)		d data is retransmitted(3 recommended, 5 is default)		
27	Windows Server 2016 Common Settings	TWG CB-01-007-0027	安全性選項\MSS	MSS：(PerformRouterDiscovery)Allow IRDP to detect and configure Default Gateway addresses(could lead	▪ 這項原則設定決定是否允許 Internet Router Discovery Protocol(IRDP)自動偵測與設定預設 Gateway 位址 ▪ 設定選項如下： (1)已停用 (2)已啟用 (3)僅在 DHCP 傳送路由器探查選項時啟用	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：(PerformRouterDiscovery)Allow IRDP to detect and configure Default Gateway	已啟用	CCE-ID：CCE-45285-4

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				to DoS)		addresses(could lead to DoS)		
28	Windows Server 2016 Common Settings	TWG CB-01-007-0028	安全性選項\MSS	MSS：(AutoReboot)Allow Windows to automatically restart after a system crash(recommended except for highly secure environments)	▪這項原則設定決定是否允許伺服器主機在系統發生錯誤而導致無法正常運作時，可自動重開機，以確保服務可正常執行	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：(AutoReboot)Allow Windows to automatically restart after a system crash(recommended except for highly secure environments)	已啟用	CCE-ID：CCE-45272-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
29	Windows Server 2016 Common Settings	TWGCB-01-007-0029	安全性選項\MSS	MSS：(WarningLevel)Percentage threshold for the security event log at which the system will generate a warning	▪ 當安全性事件記錄檔大小到達最大可用的百分比時，產生警告，預設值沒有指定，當定義此原則時，可以選擇50%、60%、70%、80%或 90%等臨界值 ▪ 如果安全性事件記錄檔設定為覆寫，則不會產生警告	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：(WarningLevel)Percentage threshold for the security event log at which the system will generate a warning	90%	CCE-ID：CCE-45292-0
30	Windows Server 2016 Common	TWGCB-01-007-0030	安全性選項\MSS	MSS：(SafeDllSearchMode)Enable	▪ 這項原則設定決定應用程式搜尋 DLL 檔的順序 ▪ 如果設定為啟用，搜尋 DLL 的順序如下：	電腦設定\Windows 設定\安全性設定\本機原則\安全	已啟用	CCE-ID：CCE-4528

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings			Safe DLL search mode(recommended)	➢應用程式被載入的目錄 ➢系統目錄 ➢16 位元系統目錄(如果有的話) ➢Windows 目錄 ➢目前目錄 ➢在 PATH 環境變數中列出來的目錄 ▪如果設定為停用，搜尋 DLL 的順序如下： ➢應用程式被載入的目錄 ➢目前目錄 ➢系統目錄 ➢16 位元系統目錄(如果有的話) ➢Windows 目錄 ➢在 PATH 環境變數中列出來的目錄	性選項\MSS：(SafeDllSearchMode)Enable Safe DLL search mode(recommended)		6-2
31	Windows Server	TWG CB-01	安全性選	MSS：(AutoAd	▪這項原則設定決定電腦是否採取自動登入方式	電腦設定\Windows 設定	已停用	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
	2016 Common Settings	-007-0031	項\MSS	minLogon)Enable Automatic Logon(not recommended)	▪ 如果設定為啟用：當電腦啟動時，將使用以純文字形式儲存於 Registry 內之網域、帳號及密碼資訊自動登入該電腦，因此能實體存取電腦的任何人也都能存取該電腦中的一切資訊，包括任何網路或電腦所能連線到的網路在內 ▪ 如果設定為停用：電腦將不採取自動登入方式	\安全性設定\本機原則\安全性選項\MSS：(AutoAdminLogon)Enable Automatic Logon(not recommended)		CCE-45271-4
32	Windows Server 2016 Common Settings	TWGCB-01-007-0032	安全性選項\MSS	MSS：(AutoShareServer)Enable Administrative Shares(recommended except for highly	▪ 若啟用這項原則設定，伺服器主機會自動建立特殊隱藏的系統管理共用，系統管理員、程式及服務可以用來管理的電腦環境或網路 ▪ 這些特殊的共用資源不會顯示在 Windows 檔案總管或我的電腦中的。不過，可以使用「電腦管理」中的「共用資料夾」工具來檢視共用資源 ▪ 根據電腦設定，某些或所有下列特殊共用資源可能會列在共用資料夾的共用	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：(AutoShareServer)Enable Administrative Shares(recommended except	已啟用	CCE-ID：CCE-45273-0

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				secure environments)	資料夾中： ➢磁碟機代號$：這是共用的根磁碟分割或磁碟區。共用的根磁碟分割與磁碟區會顯示成磁碟機代號名稱加上錢幣符號($)。例如，當共用磁碟機代號 C 與 D，它們會顯示為 C$及 D$ ➢ADMIN$：這是電腦的遠端管理期間所使用的資源 ➢IPC$：這是共用，必須擁有程式之間通訊的具名的管道的資源。無法刪除此資源 ➢NETLOGON：這是用在網域控制站的資源 ➢SYSVOL：這是用在網域控制站的資源 ➢列印$：這是印表機的遠端管理期間	for highly secure environments)		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
					所使用的資源 ➢FAX$：這是可供傳真用戶端在傳輸傳真期間的伺服器上的共用的資料夾			
33	Windows Server 2016 Common Settings	TWGCB-01-007-0033	安全性選項\MSS	MSS：(ScreenSaverGracePeriod)The time in seconds before the screen saver grace period expires(0 recommended)	▪ 如果啟用螢幕保護裝置的鎖定功能，在螢幕保護裝置啟動到主控台實際自動鎖定之間，Windows 設置有一段寬限期。這項原則設定決定寬限期時間(以秒計算) ▪ 可以設定為介於 0 到 255 之間的任何數值	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：(ScreenSaverGracePeriod)The time in seconds before the screen saver grace period expires(0 recommended)	0	CCE-ID：CCE-45287-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
34	Windows Server 2016 Common Settings	TWGCB-01-007-0034	安全性選項\互動式登入	互動式登入：在密碼到期前提示使用者變更密碼	▪ 這項原則設定決定在使用者的密碼即將到期時，要提前多久(天數)事先警告使用者，讓使用者有時間建構密碼強度高的密碼 ▪ 預設值為 5 天	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：在密碼到期前提示使用者變更密碼	14 天以上	CCE-ID：CCE-46026-1
35	Windows Server 2016 Common Settings	TWGCB-01-007-0035	安全性選項\互動式登入	互動式登入：要求網域控制站驗證以解除鎖定工作站	▪ 必須提供登入資訊才能夠將鎖定的電腦解除鎖定。對於網域帳戶而言，這項原則設定決定是否必須與網域控制站連絡，才能將電腦解除鎖定 ▪ 如果停用此設定，使用者便可以使用快取的認證來將電腦解除鎖定 ▪ 如果啟用此設定，網域控制站便必須驗證用以解除鎖定電腦的網域帳戶	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：要求網域控制站驗證以解除鎖定工作站	已啟用	CCE-ID：CCE-46486-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
36	Windows Server 2016 Common Settings	TWGCB-01-007-0036	安全性選項\互動式登入	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	▪ 每個唯一使用者的登入資訊會存放於本機快取，因此，若網域控制站在後續登入嘗試期間無法使用，他們仍然可以登入。快取的登入資訊是從先前的登入工作階段儲存。若網域控制站無法使用且未快取使用者的登入資訊，則會以「目前無可用的登入伺服器來服務登入請求」訊息提示使用者 ▪ 在這項原則設定中，0 值會停用登入快取。超過 50 的任何值只會快取 50 個登入嘗試。Windows 最多支援 50 個快取項目，而每一使用者耗用的項目數目取決於認證。舉例來說，在 Windows 系統中最多可以快取 50 個唯一密碼使用者帳戶，但只能快取 25 個智慧卡使用者帳戶，因為會同時儲存密碼資訊與智慧卡資訊。當擁有快取登入資訊的使用者再次登入時，會取代該使用者個人的快	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：網域控制站無法使用時，要快取的先前登入次數	4 次以下	CCE-ID：CCE-46705-0

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
					取資訊			
37	Windows Server 2016 Common Settings	TWGCB-01-007-0037	安全性選項\互動式登入	互動式登入：智慧卡移除操作	▪ 這項原則設定決定當登入使用者的智慧卡從智慧卡讀卡機移除時要執行的動作，選項如下： ➢無動作 ➢鎖定工作站 ➢強制登出 ➢如果是遠端桌面服務工作階段則中斷連線 ▪ 如果在此原則的「內容」對話方塊中按下「鎖定工作站」，便會在智慧卡移除時鎖定工作站，讓使用者帶著他們的智慧卡離開，同時繼續保護工作階段 ▪ 如果在此原則的「內容」對話方塊中按下「強制登出」，便會在智慧卡移除時，自動將使用者登出 ▪ 如果按一下「如果是遠端桌面服務工作	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：智慧卡移除操作	鎖定工作站	CCE-ID：CCE-46148-3

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					階段則中斷連線」，便會在智慧卡移除時中斷工作階段的連線，而不會將使用者登出。這能讓使用者稍後插入智慧卡並繼續該工作階段，或是在另一部配備智慧卡讀卡機的電腦繼續，無須再登入一次。如果工作階段是本機，則此原則的功能與「鎖定工作站」相同			
38	Windows Server 2016 Common Settings	TWG CB-01-007-0038	安全性選項\互動式登入	互動式登入：須有智慧卡	▪ 這項原則設定決定使用者是否需要使用智慧卡來登入電腦 ▪ 選項如下： ➢啟用：使用者只能使用智慧卡來登入電腦 ➢停用：使用者能使用任何方法來登入電腦 ▪ 預設值為停用	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：須有智慧卡	已停用	CCE-ID：CCE-46180-6
39	Windows Server	TWG CB-01	安全性選	互動式登入：不要	▪ 這項原則設定決定使用者是否需要按 CTRL+ALT+DEL 才能登入	電腦設定\Windows 設定	已停用	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
	2016 Common Settings	-007-0039	項\互動式登入	求按CTRL+ALT+DEL鍵	▪ 如果在電腦上啟用了此設定，使用者不需要按 CTRL+ALT+DEL 便可登入。不需要按 CTRL+ALT+DEL 會讓使用者容易受到嘗試攔截使用者密碼的入侵。使用者登入前需要按 CTRL+ALT+DEL，可確保使用者輸入密碼時，以受信任的路徑進行通訊 ▪ 如果停用了此設定，則任何使用者都需要按 CTRL+ALT+DEL 才能登入 Windows	\安全性設定\本機原則\安全性選項\互動式登入：不要求按 CTRL+ALT+DEL 鍵		CCE-46564-1
40	Windows Server 2016 Common Settings	TWGCB-01-007-0040	安全性選項\互動式登入	互動式登入：不要顯示上次登入的使用者名稱	▪ 這項原則設定決定是否要在 Windows 登入畫面顯示上次登入電腦的使用者名稱 ▪ 如果啟用此設定，登入畫面不會顯示上次順利登入的使用者名稱 ▪ 如果停用此設定，便會顯示上次登入的使用者名稱	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：不要顯示上次登入的使用者名稱	已啟用	CCE-ID：CCE-46330-7

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
41	Windows Server 2016 Common Settings	TWGCB-01-007-0041	安全性選項\互動式登入	互動式登入：電腦未使用時間限制	▪ 這項原則設定決定 Windows 是否會監控登入工作階段的未使用時間，而且會在未使用時間超過未使用時間限制時，執行螢幕保護裝置並鎖定該工作階段 ▪ 數值必須介於 0 及 599,940 之間	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：電腦未使用時間限制	900 秒以下，但須大於 0 秒	CCE-ID：CCE-46768-8
42	Windows Server 2016 Common Settings	TWGCB-01-007-0042	安全性選項\系統加密編譯	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式金鑰保護	▪ 這項原則設定決定是否需要密碼才能使用使用者的私密金鑰 ▪ 選項如下： ➢ 當新金鑰被儲存及使用時，不要求使用者的輸入 ➢ 金鑰第一次使用時提示使用者輸入 ➢ 使用者必須在每次使用金鑰時輸入密碼	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\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式金鑰保護	當新金鑰被儲存及使用時，不要求使用者的輸入	CCE-ID：CCE-46878-5

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
43	Windows Server 2016 Common Settings	TWG CB-01-007-0043	安全性選項\系統加密編譯	系統密碼編譯：使用 FIPS 相容演算法於加密，雜湊，以及簽章	▪ 對於 Schannel Security Service Provider(SSP)，這項原則設定會停用強度較低的安全通訊端層(SSL)通訊協定，而且只支援傳輸層安全性(TLS)通訊協定做為用戶端與伺服器(如果適用) ▪ 如果啟用此設定，傳輸層安全性/安全通訊端層(TLS/SSL)安全性提供者只會使用 FIPS 140 核准的密碼編譯演算法：3DES 與 AES 用於加密、RSA 或 ECC 公開金鑰密碼編譯用於 TLS 金鑰交換與驗證，而且只有安全雜湊演算法(SHA1、SHA256、SHA384 及 SHA512)用於 TLS 雜湊需求 ▪ 對於加密檔案系統服務(EFS)，它支援使用三重資料加密標準(DES)與進階加密標準(AES)加密演算法來加密 NTFS 檔案系統支援的檔案資料 ▪ 對於遠端桌面服務，它只支援使用三重	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\系統密碼編譯：使用 FIPS 相容演算法於加密，雜湊，以及簽章	已啟用	CCE-ID：CCE-44610-4

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					DES 加密演算法來加密遠端桌面服務網路通訊 ▪ 對於 BitLocker，在產生任何加密金鑰之前，必須先啟用此設定			
44	Windows Server 2016 Common Settings	TWG CB-01-007-0044	安全性選項\系統物件	系統物件：加強內部系統物件的預設權限(例如：符號連結)	▪ 這項原則設定決定物件的預設判別存取控制清單(DACL)的強度 ▪ Active Directory 維護共用系統資源(例如 DOS 裝置名稱、Mutex 及信號)的全域清單。如此，便可在程序之間找到與共用物件。每種類型的物件都會建立一個預設的 DACL，它指定誰可以存取物件與所授與的權限為何 ▪ 若啟用此設定，預設的 DACL 較強，允許非系統管理員的使用者讀取共用物件，但不允許這些使用者修改不是他們建立的共用物件	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\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	CCE-ID：CCE-44597-3
45	Windows	TWG	安全	系統物	▪ 這項原則設定決定是否要強制所有子	電腦設定	已啟用	CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Common Settings	CB-01-007-0045	性選項\系統物件	件：要求不區分大小寫用於非 Windows 子系統	系統區分大小寫。Win32 子系統不會區分大小寫。但是如 POSIX 等其他子系統的核心支援區分大小寫 ▪ 如果啟用此設定，便會強制所有目錄物件、符號連結及 IO 物件(包括檔案物件在內)不區分大小寫 ▪ 如果停用此設定，將允許非 Windows 子系統區分大小寫	\Windows 設定\安全性設定\本機原則\安全性選項\系統物件：要求不區分大小寫用於非 Windows 子系統		ID：CCE-44520-5
46	Windows Server 2016 Common Settings	TWG CB-01-007-0046	安全性選項\系統設定	系統設定：選擇性的子系統	這項原則設定決定可選擇性啟動哪些子系統以支援使用者的應用程式。使用這項原則設定，可依環境需求指定任意數目的子系統以支援使用者的應用程式	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\系統設定：選擇性的子系統	Posix	CCE-ID：CCE-44707-8
47	Windows Server	TWG CB-01	安全性選	系統設定：於軟	▪ 這項原則設定決定當使用者或處理程序嘗試執行副檔名為.exe 的軟體時，是	電腦設定\Windows 設定	已啟用	CCE-ID：

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 Common Settings	-007-0047	項\系統設定	體限制原則對 Windows 可執行檔使用憑證規則	否要處理數位憑證。這項原則設定可用來啟用或停用憑證規則(一種軟體限制原則規則)。使用軟體限制原則，可建立憑證規則，以允許或禁止由 Authenticode 簽署的軟體以該軟體關聯的數位憑證為基礎來執行。為使憑證規則生效，必須啟用這項原則設定 ▪ 當啟用憑證規則時，軟體限制原則會檢查憑證撤銷清單(CRL)，以確認軟體的憑證與簽署正確。這在簽署的程式啟動時會降低效能 ▪ 在「受信任的發行者內容」中，清除「發行者」與「時間戳記」核取方塊，可以停用此功能	\安全性設定\本機原則\安全性選項\系統設定：於軟體限制原則對 Windows 可執行檔使用憑證規則		CCE-45713-5
48	Windows Server 2016 Common	TWG CB-01-007-0048	安全性選項\使用者	使用者帳戶控制：提示提升權限時切	▪ 這項原則設定會控制提升權限要求提示是顯示在互動式使用者桌面或是安全桌面	電腦設定\Windows 設定\安全性設定\本機原則\安全	已啟用	CCE-ID：CCE-4727

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings		帳戶控制	換到安全桌面	▪ 選項如下： ➢ 已啟用：(預設值)不論系統管理員與標準使用者的提示行為原則設定為何，所有提升權限要求都會顯示在安全桌面上 ➢ 已停用：所有提升權限要求都會顯示在互動式使用者桌面。會使用系統管理員與標準使用者的提示行為原則設定	性選項\使用者帳戶控制：提示提升權限時切換到安全桌面		0-4
49	Windows Server 2016 Common Settings	TWG CB-01-007-0049	安全性選項\使用者帳戶控制	使用者帳戶控制：允許 UIAccess 應用程式不使用安全桌面來提示提升權限	▪ 這項原則設定控制使用者介面協助工具(UIAccess 或 UIA)程式在標準使用者使用提升權限提示時，是否自動停用安全桌面 ▪ 已啟用：UIA 程式，包括 Windows 遠端協助在內的 UIA 程式，可自動停用提升權限提示的安全桌面。如果未停用「使用者帳戶控制：提示提升權限時切換到安全桌面」原則設定，提示會出現	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\使用者帳戶控制：允許 UIAccess 應用程式不使用安全桌面來提	已停用	CCE-ID：CCE-46911-4

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					在互動式使用者的桌面上，而非安全桌面 ▪ 已停用：(預設值)只有互動式桌面的使用者才能停用安全桌面，或是停用「使用者帳戶控制：提示提升權限時切換到安全桌面」原則設定才能停用安全桌面	示提升權限		
50	Windows Server 2016 Common Settings	TWG CB-01-007-0050	安全性選項\使用者帳戶控制	使用者帳戶控制：在管理員核准模式，系統管理員之提升權限提示的行為	▪ 這項原則設定會控制系統管理員之提升權限提示的行為 ▪ 選項如下： ➢提升權限而不提示：允許具有特殊權限的帳戶執行需要提升權限的操作，而不需同意或是認證。注意：請只在最嚴謹的環境中使用此選項 ➢在安全桌面提示輸入認證：當操作需要提升權限時，會在安全桌面提示使用者輸入具有特殊權限的使用者名稱與密碼。如果使用者輸入有效	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\使用者帳戶控制：在管理員核准模式，系統管理員之提升權限提示的行為	提示要求同意非 Windows 二進位檔案	CCE-ID：CCE-4728 4-5

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					的認證，操作會以使用者的最高可用權限繼續 ➢在安全桌面提示要求同意：當操作需要提升權限時，會在安全桌面提示使用者選取「允許」或是「拒絕」。如果使用者選取「允許」，操作會以使用者的最高可用權限繼續 ➢提示輸入認證：當操作需要提升權限時，會提示使用者輸入系統管理使用者名稱與密碼。如果使用者輸入有效的認證，操作會以適用的權限繼續 ➢提示要求同意：當操作需要提升權限時，會提示使用者選取「允許」或是「拒絕」。如果使用者選取「允許」，操作會以使用者的最高可用權限繼續 ➢提示要求同意非 Windows 二進位檔			

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					案：(預設值)當非 Microsoft 應用程式的操作需要提升權限時，會在安全桌面提示使用者選取「允許」或是「拒絕」。如果使用者選取「允許」，操作會以使用者的最高可用權限繼續			
51	Windows Server 2016 Common Settings	TWG CB-01-007-0051	安全性選項\使用者帳戶控制	使用者帳戶控制：僅針對已簽章與驗證過的可執行檔，提高其權限	▪ 這項原則設定會強制公開金鑰基礎結構(PKI)簽章檢查任何要求提升權限的互動式應用程式。系統管理員可透過將憑證新增至本機電腦的受信任的發行者憑證存放區，來控制允許執行哪些應用程式 ▪ 選項如下： ➢ 已啟用：允許指定的可執行檔執行之前，強制執行 PKI 憑證路徑驗證 ➢ 已停用：(預設值)允許指定的可執行檔執行之前，不強制執行 PKI 憑證	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\使用者帳戶控制：僅針對已簽章與驗證過的可執行檔，提高其權限	已停用	CCE-ID：CCE-47151-6

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					路徑驗證			
52	Windows Server 2016 Common Settings	TWG CB-01-007-0052	安全性選項\使用者帳戶控制	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	▪ 這項原則設定會控制電腦的所有使用者帳戶控制(UAC)原則設定行為。如果變更這項原則設定，必須重新啟動電腦 ▪ 選項如下： ➢ 已啟用：(預設值)啟用管理員核准模式。必須啟用此設定，而且必須以適當的方式設定相關的 UAC 原則設定，才能允許內建的 Administrator 帳戶以及所有其他屬於 Administrators 群組成員的使用者在管理員核准模式中執行 ➢ 已停用：會停用管理員核准模式及所有相關的 UAC 原則設定。注意：如果停用這項原則設定，資訊安全中心會通知作業系統的整體安全性已降低	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\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	CCE-ID：CCE-47154-0

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
53	Windows Server 2016 Common Settings	TWG CB-01-007-0053	安全性選項\使用者帳戶控制	使用者帳戶控制：偵測應用程式安裝，並提示提升權限	▪ 這項原則設定會控制電腦的應用程式安裝偵測行為 ▪ 選項如下： ➢ 已啟用：(預設值)當偵測到應用程式安裝封裝需要提升權限時，會提示使用者輸入系統管理使用者名稱與密碼。如果使用者輸入有效的認證，操作會以適用的權限繼續 ➢ 已停用：未偵測到應用程式安裝封裝，也未提示提升權限。執行標準使用者桌面並利用委派安裝技術(例如，群組原則軟體安裝或 Systems Management Server(SMS))的企業，應該停用這項原則設定。在此情況下，不需要進行安裝程式偵測	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\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	CCE-ID：CCE-46912-2
54	Windows Server	TWG CB-01	安全性選	使用者帳戶控制：	▪ 這項原則設定會控制內建的 Administrator 帳戶的管理員核准模式行	電腦設定\Windows 設定	已啟用	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
	2016 Common Settings	-007-0054	項\使用者帳戶控制	內建的Administrator帳戶的管理員核准模式	為 ▪ 選項如下： ➢ 已啟用：內建的 Administrator 帳戶使用管理員核准模式。根據預設，任何需要提升權限的操作都會提示使用者核准操作 ➢ 已停用：(預設值)內建的 Administrator 帳戶將以完整的系統管理權限執行所有應用程式	\安全性設定\本機原則\安全性選項\使用者帳戶控制：內建的Administrator帳戶的管理員核准模式		CCE-47000-5
55	Windows Server 2016 Common Settings	TWGCB-01-007-0055	安全性選項\使用者帳戶控制	使用者帳戶控制：標準使用者之提高權限提示的行為	▪ 這項原則設定會控制標準使用者之提高權限提示的行為 ▪ 選項如下： ➢ 提示輸入認證：(預設值)當操作需要提升權限時，會提示使用者輸入系統管理使用者名稱與密碼。若使用者輸入有效的認證，該操作會以適用的權限繼續執行	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\使用者帳戶控制：標準使用者之提高權限提示的	提示輸入認證	CCE-ID：CCE-47214-2

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					➢自動拒絕提升權限要求：當操作需要提升權限時，會顯示可設定的拒絕存取錯誤訊息。以標準使用者身分執行桌上型電腦的企業可能會選擇此設定，以降低需要尋求支援部門協助的機會 ➢在安全桌面提示輸入認證：當操作需要提升權限時，會在安全桌面提示使用者輸入不同的使用者名稱與密碼。如果使用者輸入有效的認證，操作會以適用的權限繼續執行	行為		
56	Windows Server 2016 Common Settings	TWG CB-01-007-0056	安全性選項\使用者帳戶控制	使用者帳戶控制：僅針對在安全位置安裝的 UIAccess 應用程	▪這項原則設定控制是否要求以使用者介面協助工具(UIAccess)整合層級執行的應用程式必須位於檔案系統中的安全位置。安全位置僅限於下列目錄： ➢…\Program Files\，包含子目錄 ➢…\Windows\system32\	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\使用者帳戶控制：僅針對在安全位	已啟用	CCE-ID：CCE-46913-0

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				式，提高其權限	➢…\Program Files(x86)\，包含 64 位元 Windows 版本的子目錄 ▪ 注意：不論這項原則設定的狀態為何，Windows 都會針對任何要求以 UIAccess 整合層級執行的互動式應用程式，強制執行公開金鑰基礎結構(PKI)簽章檢查 ▪ 選項如下： ➢已啟用：(預設值)如果應用程式位於檔案系統的安全位置，只會以 UIAccess 整合執行 ➢已停用：即使應用程式不是位於檔案系統的安全位置，也會以 UIAccess 整合執行	置安裝的 UIAccess 應用程式，提高其權限		
57	Windows Server 2016	TWG CB-01-007-0	安全性選項\使	使用者帳戶控制：將檔案及	▪ 這項原則設定控制是否將應用程式寫入失敗重新導向到已定義的登錄與檔案系統位置。這項原則設定可減少那些	電腦設定\Windows 設定\安全性設定\	已啟用	CCE-ID：CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Common Settings	057	用者帳戶控制	登錄寫入失敗虛擬化並儲存至每一使用者位置	以系統管理員身分執行，並將執行階段應用程式資料寫入至 %ProgramFiles%、%Windir%、%Windir%\system32 或 HKLM\Software 的應用程式 ▪ 選項如下： ➢ 已啟用：(預設值)在執行階段將應用程式寫入失敗重新導向到檔案系統與登錄中已定義的使用者位置 ➢ 已停用：將資料寫入至受保護位置的應用程式失敗	本機原則\安全性選項\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一使用者位置		47157-3
58	Windows Server 2016 Common Settings	TWG CB-01-007-0058	安全性選項\修復主控台	修復主控台：允許軟碟複製以及存取所有磁碟和所有資	▪ 這項原則設定決定是否允許使用修復主控台 SET 命令 ▪ 啟用此安全性選項便可以使用修復主控台 SET 命令，此命令可設定下列修復主控台環境變數： ➢ AllowWildCards：對某些命令啟用萬	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\修復主控台：允許軟碟複製以及存	已停用	CCE-ID：CCE-46361-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
				料夾	用字元支援(例如 DEL 命令) ➢AllowAllPaths：允許存取電腦上的所有檔案和資料夾 ➢AllowRemovableMedia：允許將檔案複製到卸除式媒體，例如磁片 ➢NoCopyPrompt：不要提示正在覆寫現有的檔案	取所有磁碟和所有資料夾		
59	Windows Server 2016 Common Settings	TWGCB-01-007-0059	安全性選項\修復主控台	修復主控台：允許自動系統管理登入	▪這項原則設定決定是否必須在授與系統存取權之前提供 Administrator 帳戶的密碼 ▪如果啟用此選項，修復主控台不需要使用者提供密碼，且將會自動登入系統	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\修復主控台：允許自動系統管理登入	已停用	CCE-ID：CCE-46181-4
60	Windows Server	TWGCB-01	安全性選	帳戶：限制使用空	▪這項原則設定決定未受密碼保護的本機帳戶，是否可用來從實體電腦主控台	電腦設定\Windows 設定	已啟用	CCE-ID：

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 Common Settings	-007-0060	項\帳戶	白密碼的本機帳戶僅能登入到主控台	以外的位置登入 ▪如果已啟用，那麼未受密碼保護的本機帳戶將只能藉由電腦鍵盤登入 ▪不是位於實際安全位置的電腦，應一直針對所有本機使用者帳戶強制執行強式密碼原則。否則，每位實際存取電腦的使用者皆可使用沒有密碼的使用者帳戶登入。這對可攜式電腦來說尤其重要 ▪如果將此安全性原則套用到 Everyone 群組，則任何人都不能透過遠端桌面服務登入 ▪應用程式若使用遠端互動式登入，則可以跳過這項設定 ▪遠端桌面服務在舊版的 Windows Server 中稱為「終端機服務」	\安全性設定\本機原則\安全性選項\帳戶：限制使用空白密碼的本機帳戶僅能登入到主控台		CCE-46005-5
61	Windows	TWG	安全	帳戶：重	▪這項原則設定決定不同的帳戶名稱是	電腦設定	Renamed_	CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Common Settings	CB-01-007-0061	性選項\帳戶	新命名來賓帳戶名稱	否與「Guest」帳戶的安全性識別碼(SID)相關聯 ▪ 重新命名已知的 Guest 帳戶會使未經授權的人員較不容易猜出此使用者名稱與密碼組合 ▪ 預設值為 Guest	\Windows 設定\安全性設定\本機原則\安全性選項\帳戶：重新命名來賓帳戶名稱	Guest	ID：CCE-46218-4
62	Windows Server 2016 Common Settings	TWG CB-01-007-0062	安全性選項\帳戶	帳戶：重新命名系統管理員帳戶	▪ 這項原則設定決定不同的帳戶名稱是否與 Administrator 帳戶的安全性識別碼(SID)相關聯 ▪ 重新命名已知的 Administrator 帳戶會使未經授權的人員較不容易猜出有此特殊權限的使用者名稱與密碼組合 ▪ 預設值為 Administrator	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\帳戶：重新命名系統管理員帳戶	Renamed_Admin	CCE-ID：CCE-46321-6
63	Windows Server 2016 Common	TWG CB-01-007-0063	安全性選項\帳戶	帳戶：Administrator 帳戶狀態	▪ 這項原則設定決定要啟用或停用本機 Administrator 帳戶 ▪ 注意：若在停用 Administrator 帳戶之後嘗試重新啟用此帳戶，而現行	電腦設定\Windows 設定\安全性設定\本機原則\安全	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings				Administrator 密碼不符合密碼需求，就無法重新啟用此帳戶。在此情況下，必須由 Administrators 群組的替代成員重設 Administrator 帳戶的密碼	性選項\帳戶：Administrator 帳戶狀態		
64	Windows Server 2016 Common Settings	TWG CB-01-007-0064	安全性選項\帳戶	帳戶：Guest 帳戶狀態	▪ 這項原則設定決定啟用或停用 Guest 帳戶 ▪ 注意：如果停用 Guest 帳戶，而且「網路存取：本機帳戶的共用和安全性模型」安全性選項是設定為「僅適用於來賓」，則網路登入(例如，由 Microsoft 網路伺服器(SMB 服務)所執行的網路登入)將會失敗	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\帳戶：Guest 帳戶狀態	已停用	CCE-ID：CCE-46960-1
65	Windows Server 2016 Common Settings	TWG CB-01-007-0065	安全性選項\裝置	裝置：防止使用者安裝印表機驅動程式	▪ 要讓電腦列印至共用的印表機，必須在本機電腦上安裝共用印表機的驅動程式。這項原則設定決定誰可以在連線至共用的印表機時安裝印表機驅動程式 ▪ 如果啟用此設定，只有 Administrators	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\裝置：	已啟用	CCE-ID：CCE-44724-3

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					可以在連線至共用印表機時安裝印表機驅動程式 ▪ 如果停用此設定，任何使用者在連線至共用的印表機時，都可以安裝印表機驅動程式 ▪ 此設定不會影響新增本機印表機的能力 ▪ 此設定不會影響 Administrators	防止使用者安裝印表機驅動程式		
66	Windows Server 2016 Common Settings	TWG CB-01-007-0066	安全性選項\裝置	裝置：允許卸除而不須登入	▪ 這項原則設定決定是否可卸除可攜式電腦而不須登入 ▪ 如果已啟用此設定，則不須登入即可使用外部硬體的退出按鈕來卸除電腦 ▪ 如果停用此設定，那麼使用者必須登入且擁有「從銜接站移除電腦」特殊權限才能卸除電腦 ▪ 停用此設定可能會讓使用者使用外部硬體退出按鈕以外的方法，嘗試並實際	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\裝置：允許卸除而不須登入	已停用	CCE-ID：CCE-46547-6

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					從銜接站移除膝上型電腦。由於這樣可能會造成硬體的損壞，因此一般說來，這項設定只能在實際上很安全的膝上型電腦上停用			
67	Windows Server 2016 Common Settings	TWG CB-01-007-0067	安全性選項\裝置	裝置：允許格式化以及退出抽取式媒體	▪ 這項原則設定決定允許哪些人格式化與退出抽取式 NTFS 媒體 ▪ 此功能可指定給： ➢Administrators ➢Administrators 以及 Interactive Users	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\裝置：允許格式化以及退出抽取式媒體	Administrators	CCE-ID：CCE-44500-7
68	Windows Server 2016 Common Settings	TWG CB-01-007-0068	安全性選項\裝置	裝置：CD-ROM 存取只限於登入本機的使用	▪ 這項原則設定決定本機使用者與遠端使用者是否能同時存取 CD-ROM ▪ 如果啟用此設定，便只允許以互動方式登入的使用者存取卸除式 CD-ROM 媒體。如果啟用此設定但無人以互動方式	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\裝置：CD-ROM 存取	已停用	CCE-ID：CCE-44902-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
				者	登入，便能從網路存取該 CD-ROM	只限於登入本機的使用者		
69	Windows Server 2016 Common Settings	TWGCB-01-007-0069	安全性選項\裝置	裝置：軟碟機存取只限於登入本機的使用者	▪ 這項原則設定決定本機使用者與遠端使用者是否能同時存取卸除式軟碟機媒體 ▪ 如果啟用此設定，便只允許以互動方式登入的使用者存取卸除式軟碟機媒體。如果啟用此設定但無人以互動方式登入，便能從網路存取該軟碟機	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\裝置：軟碟機存取只限於登入本機的使用者	已停用	CCE-ID：CCE-46621-9
70	Windows Server 2016 Common Settings	TWGCB-01-007-0070	安全性選項\網域成員	網域成員：停用電腦帳戶密碼變更	▪ 這項原則設定決定是否定期變更網域成員的電腦帳戶密碼 ▪ 如果啟用此設定，網域成員便不會嘗試變更其電腦帳戶密碼 ▪ 如果停用此設定，網域成員會嘗試依「網域成員：最長電腦帳戶密碼有效期」的設定，來變更電腦帳戶密碼，預	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網域成員：停用電腦帳戶密碼變更	已停用	CCE-ID：CCE-46018-8

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					設為每隔 30 天 ▪ 注意： ➢ 這項原則設定不應啟用。電腦帳戶密碼是用於建立成員與網域控制站，以及網域內網域控制站之間的安全通道通訊。一旦建立，便會使用安全通道來傳輸建立驗證與授權決策所需的敏感資訊 ➢ 在嘗試支援使用相同電腦帳戶的雙重開機情況下，不應使用此設定。如果要對連結相同網域的兩個安裝執行雙重開機，請指定不同電腦名稱給這兩個安裝			
71	Windows Server 2016 Common	TWG CB-01-007-0071	安全性選項\網域成	網域成員：最長電腦帳戶密碼有效	這項原則設定決定網域成員嘗試變更其電腦帳戶密碼的頻率	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網域成	30 天以下，但須大於 0 天	CCE-ID：CCE-4661

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings		員	期		員：最長電腦帳戶密碼有效期		6-9
72	Windows Server 2016 Common Settings	TWG CB-01-007-0072	安全性選項\網域成員	網域成員：安全通道資料加以數位加密或簽章(自動)	▪ 這項原則設定決定網域成員啟動的所有安全通道傳輸是否必須經過簽章或加密 ▪ 當電腦加入網域時，會建立電腦帳戶。隨後，啟動系統時，系統會使用電腦帳戶密碼為其網域建立一個與網域控制站的安全通道。此安全通道用來執行諸如 NTLM 通過驗證及 LSA SID/名稱查詢的操作 ▪ 這項設定決定網域成員啟動的所有安全通道傳輸是否符合最低安全性需求。特別是決定了網域成員啟動的所有安全通道傳輸是否必須經過簽章或加密 ▪ 如果已啟用這項設定，那麼將不會建立	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網域成員：安全通道資料加以數位加密或簽章(自動)	已啟用	CCE-ID：CCE-46754-8

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					安全通道，除非已交涉所有安全通道傳輸的簽章或加密 ▪ 如果停用了這項設定，那麼所有安全通道傳輸的加密與簽章都會與網域控制站進行交涉，在此情況下，簽章與加密的等級是根據網域控制站的版本以及下列兩項原則的設定而定： ➢ 網域成員：安全通道資料加以數位加密(可能的話) ➢ 網域成員：安全通道資料加以數位簽章(自動) ▪ 注意： ➢ 如果啟用此設定，則原則「網域成員：安全通道資料加以數位簽章(可能的話)」假設已被啟用，而不考慮其目前的設定。這會確保網域成員至少嘗試交涉安全通道傳輸的簽章			

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					➢透過安全通道傳輸的登入資訊一定會經過加密，無論「所有」其他安全通道傳輸的加密是否已進行交涉			
73	Windows Server 2016 Common Settings	TWG CB-01-007-0073	安全性選項\網域成員	網域成員：安全通道資料加以數位簽章(自動)	▪這項原則設定決定網域成員是否嘗試為其所啟動的所有安全通道傳輸交涉簽章 ▪當電腦加入網域時，會建立電腦帳戶。隨後，啟動系統時，系統會使用電腦帳戶密碼為其網域建立一個與網域控制站的安全通道。此安全通道用來執行諸如 NTLM 通過驗證及 LSA SID/名稱查詢的操作 ▪這項設定決定網域成員是否嘗試為其所啟動的所有安全通道傳輸交涉簽章 ▪如果已啟用，則網域成員將要求所有安全通道傳輸的簽章。如果網域控制站支援所有安全通道傳輸的簽章，則所有安全通道傳輸都會經過簽章，如此能確保	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網域成員：安全通道資料加以數位簽章(自動)	已啟用	CCE-ID：CCE-46440-4

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					它不會在傳送時遭到竄改 ▪ 注意： ➢ 如果啟用原則「網域成員：安全通道資料加以數位加密或簽章(自動)」，則會假設這項原則為啟用狀態，無論目前設定為何 ➢ 網域控制站也是網域成員，並會與同一網域中的其他網域控制站及受信任網域中的網域控制站建立安全通道			
74	Windows Server 2016 Common Settings	TWG CB-01-007-0074	安全性選項\網域成員	網域成員：要求增強式(Windows 2000 或更新)工作階段金鑰	▪ 這項原則設定決定加密的安全通道資料是否需要 128 位元的金鑰長度 ▪ 當電腦加入網域時，會建立電腦帳戶。之後啟動系統時，系統會使用電腦帳戶密碼在該網域內建立一個具有網域控制站的安全通道。此安全通道用來執行諸如 NTLM 通過驗證或 LSA SID/名稱	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網域成員：要求增強式(Windows 2000 或更新)	已啟用	CCE-ID：CCE-4595 8-6

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					查詢之類的操作 ▪ 根據網域成員進行通訊的網域控制站上所執行的 Windows 版本，以及參數設定： ➢ 網域成員：安全通道資料加以數位加密或簽章(自動) ➢ 網域成員：安全通道資料加以數位加密(可能的話) 透過安全通道傳輸的某些或所有資訊都會經過加密，這項原則設定決定加密的安全通道資訊是否需要 128 位元的金鑰長度 ▪ 如果已啟用這項設定，除非能執行 128 位元加密，否則不會建立安全通道 ▪ 如果停用這項設定，則會與網域控制站交涉金鑰長度 ▪ 注意：	工作階段金鑰		

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					➢ 為了在成員工作站與伺服器上利用這項原則的優點，所有建構成員網域的網域控制站都必須執行 Windows 2000 或更新的版本 ➢ 為了在網域控制站上利用這項原則的優點，相同網域以及所有受信任網域上的所有網域控制站都必須執行 Windows 2000 或更新的版本			
75	Windows Server 2016 Common Settings	TWG CB-01-007-0075	安全性選項\網域成員	網域成員：安全通道資料加以數位加密(可能的話)	▪ 這項原則設定決定網域成員是否嘗試為其所啟動的所有安全通道傳輸交涉加密 ▪ 當電腦加入網域時，會建立電腦帳戶。隨後，啟動系統時，系統會使用電腦帳戶密碼為其網域建立一個與網域控制站的安全通道。此安全通道用來執行諸如 NTLM 通過驗證、LSA SID/名稱查詢之類的操作 ▪ 如果已啟用，則網域成員將要求所有安	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網域成員：安全通道資料加以數位加密(可能的話)	已啟用	CCE-ID：CCE-46546-8

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					全通道傳輸的加密。如果網域控制站支援所有安全通道傳輸的加密，則所有安全通道傳輸都會經過加密。否則，只有透過安全通道傳輸的登入資訊才會經過加密 ▪ 如果停用這項設定，則網域成員不會嘗試交涉安全通道加密 ▪ 正常情況下，不應該停用此設定。除了不必要地減少安全通道可能的機密等級，停用此設定還可能不必要地減少安全通道輸送量，因為只有當安全通道已簽署或加密時，使用安全通道的並行 API 呼叫才可行 ▪ 注意：網域控制站也是網域成員，並會與同一網域中的其他網域控制站及受信任網域中的網域控制站建立安全通道			

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
76	Windows Server 2016 Common Settings	TWG CB-01-007-0076	安全性選項\網路存取	網路存取：讓 Everyone 權限套用到匿名使用者	▪ 這項原則設定決定將授與電腦匿名連線哪些其他權限 ▪ Windows 允許匿名使用者執行特定活動，例如列舉網域帳戶與網路共用的名稱。當系統管理員想要授與使用者在受信任網域上的存取權限，而該網域不會保持交互信任時，此功能相當方便。根據預設值，會從為匿名連線建立的權杖中移除 Everyone 安全性識別碼(SID)。因此，授與 Everyone 群組的權限不會套用至匿名使用者。若設定此選項，匿名使用者只能存取已明確取得權限的資源 ▪ 若啟用此設定，Everyone SID 會新增至為匿名連線建立的權杖。在此情況下，匿名使用者可存取 Everyone 群組已取得權限的任何資源	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路存取：讓 Everyone 權限套用到匿名使用者	已停用	CCE-ID：CCE-46412-3

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
77	Windows Server 2016 Common Settings	TWG CB-01-007-0077	安全性選項\網路存取	網路存取：共用和安全性模式用於本機帳戶	▪ 這項原則設定決定如何驗證使用本機帳戶的網路登入 ▪ 若此設定設為「傳統」，則使用本機帳戶認證的網路登入會使用那些認證進行驗證。「傳統」模式可有效控制對資源的存取。使用「傳統」模式，可針對相同資源授與不同類型的存取權限給不同的使用者 ▪ 若此設定設為「僅適用於來賓」，則使用本機帳戶的網路登入會自動對應到 Guest 帳戶。使用「僅適用於來賓」模式，可以等同方式對待所有使用者。所有使用者均驗證為 Guest，且收到的特定資源存取權限等級相同，即可能是「唯讀」或「修改」 ▪ 注意： 使用「僅適用於來賓」模式，可經由網路存取電腦的所有使用者(包括匿名網	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路存取：共用和安全性模式用於本機帳戶	傳統-本機使用者以自身身分驗證	CCE-ID：CCE-46082-4

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					際網路使用者)都能存取共用資源。必須使用 Windows 防火牆或其他類似裝置來保護電腦免於未經授權存取的侵害。同樣的，使用「傳統」模式，必須使用密碼保護本機帳戶，否則任何人都可使用那些使用者帳戶存取共用系統資源			
78	Windows Server 2016 Common Settings	TWG CB-01-007-0078	安全性選項\網路存取	網路存取：不允許 SAM 帳戶的匿名列舉	▪ 這項原則設定決定將授與電腦匿名連線哪些其他權限 ▪ Windows 允許匿名使用者執行特定活動，例如列舉網域帳戶與網路共用的名稱。當系統管理員想要授與使用者在受信任網域上的存取權限，而該網域不會保持交互信任時，此功能相當方便 ▪ 此安全性選項允許在匿名連線中設定其他限制，說明如下： ➢ 已啟用：不允許列舉 SAM 帳戶。此選項會將資源之安全性權限中的	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路存取：不允許 SAM 帳戶的匿名列舉	已啟用	CCE-ID：CCE-4630 5-9

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					Everyone 取代為 Authenticated Users ➢已停用：沒有其他限制。視預設權限而定			
79	Windows Server 2016 Common Settings	TWG CB-01-007-0079	安全性選項\網路存取	網路存取：限制匿名存取具名管道和共用	▪這項原則設定決定是否限制匿名存取具名管道和共用 ▪啟用時，這項原則設定會將共用和管道的匿名存取限制為以下設定： ➢網路存取：可以匿名存取的具名管道 ➢網路存取：可以匿名存取的共用	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路存取：限制匿名存取具名管道和共用	已啟用	CCE-ID：CCE-44911-6
80	Windows Server 2016 Common Settings	TWG CB-01-007-0080	安全性選項\網路存取	網路存取：可遠端存取的登錄路徑及子路徑	▪這項原則設定決定哪些登錄路徑及子路徑可經由網路存取(不管 winreg 登錄機碼中存取控制清單(ACL)所列的使用者或群組為何) ▪注意：不正確的編輯登錄將會對系統造成嚴重的損害。在變更登錄前，應先備	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路存取：可遠端存	System\CurrentControlSet\Control\Print\Printers System\Cur	CCE-ID：CCE-46713-4

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					份電腦上任何有價值的資料	取的登錄路徑及子路徑	rentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
							System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\User Config System\CurrentControl	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
							Set\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog	
81	Windows Server	TWG CB-01	安全性選	網路存取：允許	▪ 這項原則設定決定匿名使用者是否可以要求其他使用者的安全性識別碼	電腦設定\Windows 設定	已停用	CCE-ID：

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 Common Settings	-007-0081	項\網路存取	匿名 SID/名稱轉譯	(SID)屬性 ▪ 如果啟用此設定，匿名使用者可以要求其他使用者的 SID 屬性。知道系統管理員 SID 的匿名使用者可以連絡已啟用此設定的電腦，且能使用該 SID 來取得系統管理員的名稱。此設定會影響 SID 轉譯為名稱以及名稱轉譯為 SID ▪ 如果已停用這項設定，匿名使用者將無法為其他使用者要求 SID 屬性	\安全性設定\本機原則\安全性選項\網路存取：允許匿名 SID/名稱轉譯		CCE-46028-7
82	Windows Server 2016 Common Settings	TWG CB-01-007-0082	安全性選項\網路存取	網路存取：可以匿名存取的共用	這項原則設定決定匿名使用者能夠存取哪個網路共用	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路存取：可以匿名存取的共用	無	CCE-ID：CCE-45991-7
83	Windows	TWG	安全	網路存	這項原則設定決定哪個通訊工作階段(管	電腦設定	無	CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Common Settings	CB-01-007-0083	性選項\網路存取	取：可以匿名存取的具名管道	道)將擁有允許匿名存取的屬性與權限	\Windows 設定\安全性設定\本機原則\安全性選項\網路存取：可以匿名存取的具名管道		ID：CCE-44794-6
84	Windows Server 2016 Common Settings	TWG CB-01-007-0084	安全性選項\網路存取	網路存取：可遠端存取的登錄路徑	▪ 這項原則設定決定哪些登錄機碼可經由網路存取(不管 winreg 登錄機碼中存取控制清單(ACL)所列的使用者或群組為何) ▪ 不正確的編輯登錄將會對系統造成嚴重的損害。在變更登錄前，應先備份電腦上任何有價值的資料	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路存取：可遠端存取的登錄路徑	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications	CCE-ID：CCE-44559-3

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
							Software\Microsoft\Windows NT\CurrentVersion	
85	Windows Server 2016 Common Settings	TWG CB-01-007-0085	安全性選項\網路存取	網路存取：不允許存放網路驗證的密碼與認證	▪ 這項原則設定決定認證管理員取得網域驗證時，是否儲存密碼與認證，以供稍後使用 ▪ 如果啟用此設定，認證管理員不會在電腦上儲存密碼與認證 ▪ 如果停用或未設定這項原則設定，認證管理員將會在此電腦上存放密碼與認證，以供稍後用於網域驗證 ▪ 注意：設定這項原則設定時，必須重新啟動 Windows，變更才會生效	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路存取：不允許存放網路驗證的密碼與認證	已停用	CCE-ID：CCE-46426-3
86	Windows Server	TWG CB-01	安全性選	網路存取：不允	▪ 這項原則設定決定是否允許 SAM 帳戶和共用的匿名列舉	電腦設定\Windows 設定	已啟用	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
	2016 Common Settings	-007-0086	項\網路存取	許 SAM 帳戶和共用的匿名列舉	▪ Windows 允許匿名使用者執行特定活動，例如列舉網域帳戶和網路共用的名稱。當系統管理員想要授與使用者在受信任網域上的存取權，而該網域不會保持交互信任時，此功能相當方便。如果不想要允許 SAM 帳戶和共用的匿名列舉，請啟用此設定	\安全性設定\本機原則\安全性選項\網路存取：不允許 SAM帳戶和共用的匿名列舉		CCE-46525-2
87	Windows Server 2016 Common Settings	TWGCB-01-007-0087	安全性選項\網路安全性	網路安全性：下次密碼變更時不儲存 LAN Manager 雜湊數值	▪ 這項原則設定決定在下次密碼變更時，是否要儲存新密碼的 LAN Manager 雜湊數值。與加密編譯較強的 Windows NT 雜湊相比，LM 雜湊相對較不安全，並且容易遭到攻擊。因為 LM 雜湊儲存於本機電腦的安全性資料庫中，若安全性資料庫遭到攻擊，密碼可能就會被破解	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路安全性：下次密碼變更時不儲存 LAN Manager 雜湊數值	已啟用	CCE-ID：CCE-46031-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
88	Windows Server 2016 Common Settings	TWGCB-01-007-0088	安全性選項\網路安全性	網路安全性：允許Local System對NTLM使用電腦身分識別	▪ 這項原則設定決定是否允許使用交涉的Local System服務在還原使用NTLM驗證時，使用電腦身分識別 ▪ 如果啟用這項設定，以Local System執行且使用交涉的服務會使用電腦身分識別。這可能會造成Windows作業系統之間的某些驗證要求失敗並記錄錯誤 ▪ 若停用這項設定，以Local System執行且使用交涉的服務在還原使用NTLM驗證時將會匿名驗證	電腦設定\Windows設定\安全性設定\本機原則\安全性選項\網路安全性：允許Local System對NTLM使用電腦身分識別	已啟用	CCE-ID：CCE-46338-0
89	Windows Server 2016 Common Settings	TWGCB-01-007-0089	安全性選項\網路安全性	網路安全性：LAN Manager驗證等級	▪ 這項原則設定決定使用哪種Challenge/Response驗證通訊協定登入網路 ▪ 此選擇會影響用戶端使用的驗證通訊協定層級、交涉的工作階段安全性層級，以及伺服器接受的驗證等級，選項如下：	電腦設定\Windows設定\安全性設定\本機原則\安全性選項\網路安全性：LAN Manager驗證	只傳送NTLMv2回應\拒絕LM和NTLM	CCE-ID：CCE-46565-8

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					➢傳送 LM 和 NTLM 回應：用戶端使用 LM 和 NTLM 驗證，絕不使用 NTLMv2 工作階段安全性；網域控制站接受 LM、NTLM 及 NTLMv2 驗證 ➢傳送 LM 和 NTLM：如有交涉，使用 NTLMv2 工作階段安全性：用戶端使用 LM 和 NTLM 驗證，而且若伺服器支援，則會使用 NTLMv2 工作階段安全性；網域控制站接受 LM、NTLM 以及 NTLMv2 驗證 ➢只傳送 NTLM 回應：用戶端只使用 NTLM 驗證，而且若伺服器支援，則會使用 NTLMv2 工作階段安全性；網域控制站接受 LM、NTLM 及 NTLMv2 驗證 ➢只傳送 NTLMv2 回應：用戶端只使用 NTLMv2 驗證，而且若伺服器支	等級		

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					援，則會使用 NTLMv2 工作階段安全性；網域控制站接受 LM、NTLM 及 NTLMv2 驗證 ➢只傳送 NTLMv2 回應\拒絕 LM：用戶端只使用 NTLMv2 驗證，而且若伺服器支援，則會使用 NTLMv2 工作階段安全性；網域控制站拒絕 LM(只接受 NTLM 與 NTLMv2 驗證) ➢只傳送 NTLMv2 回應\拒絕 LM 和 NTLM：用戶端只使用 NTLMv2 驗證，而且若伺服器支援，則會使用 NTLMv2 工作階段安全性；網域控制站拒絕 LM 和 NTLM(只接受 NTLMv2 驗證			
90	Windows Server 2016 Common	TWG CB-01-007-0090	安全性選項\網路安	網路安全性：允許對此電腦的	▪這項原則設定決定是否允許使用線上身分識別來向已加入網域的電腦驗證 ▪在已加入網域的電腦上預設會停用此原則，這樣便不會允許使用線上身分識	電腦設定\Windows 設定\安全性設定\本機原則\安全	已停用	CCE-ID：CCE-4603

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings		全性	PKU2U 驗證要求使用線上身分識別	別來向已加入網域的電腦驗證	性選項\網路安全性：允許對此電腦的 PKU2U 驗證要求使用線上身分識別		0-3
91	Windows Server 2016 Common Settings	TWG CB-01-007-0091	安全性選項\網路安全性	網路安全性：NTLM SSP 為主的(包含安全 RPC)伺服器的最小工作階段安全性	▪ 這項原則設定決定是否允許伺服器要求 128 位元加密和/或 NTLMv2 工作階段安全性的交涉。這些值依存於 LAN Manager 驗證等級安全性設定值。選項如下： ➢ 要求 NTLMv2 工作階段安全性：若未交涉訊息完整性，連線將會失敗 ➢ 要求 128 位元加密：若未交涉增強式加密(128 位元)，連線將會失敗	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路安全性：NTLM SSP 為主的(包含安全 RPC)伺服器的最小工作階段安全性	要求 NTLMv2 工作階段安全性 要求 128 位元加密	CCE-ID：CCE-46160-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
92	Windows Server 2016 Common Settings	TWGCB-01-007-0092	安全性選項\網路安全性	網路安全性：允許LocalSystem NULL工作階段回復	這項原則設定決定使用 LocalSystem 時，是否允許 NTLM 回復 NULL 工作階段	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路安全性：允許LocalSystem NULL 工作階段回復	已停用	CCE-ID：CCE-47296-9
93	Windows Server 2016 Common Settings	TWGCB-01-007-0093	安全性選項\網路安全性	網路安全性：NTLM SSP 為主的(包含安全RPC)用戶端的最小工作階段	▪ 這項原則設定決定是否允許用戶端要求 128 位元加密和/或 NTLMv2 工作階段安全性的交涉。這些值依存於 LAN Manager 驗證等級安全性設定值。選項如下： ➢ 要求 NTLMv2 工作階段安全性：若未交涉 NTLMv2 通訊協定，連線將會失敗 ➢ 要求 128 位元加密：若未交涉增強式	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路安全性：NTLM SSP 為主的(包含安全 RPC)用戶端的最小	要求 NTLMv2 工作階段安全性 要求 128 位元加密	CCE-ID：CCE-44861-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				安全性	加密(128 位元)，連線將會失敗	工作階段安全性		
94	Windows Server 2016 Common Settings	TWGCB-01-007-0094	安全性選項\網路安全性	網路安全性：設定 Kerberos 允許的加密類型	▪ 這項原則提供使用者設定允許 Kerberos 使用的加密類型 ▪ 如果未選取，則不允許加密類型。這項設定可能會影響與用戶端電腦或者服務與應用程式的相容性。允許選取多個項目	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路安全性：設定 Kerberos 允許的加密類型	AES128_HMAC_SHA1, AES256_HMAC_SHA1, 未來的加密類型	CCE-ID：CCE-44602-1
95	Windows Server 2016 Common Settings	TWGCB-01-007-0095	安全性選項\網路安全性	網路安全性：LDAP 用戶端簽章要求	▪ 這項原則設定決定代表發出 LDAP BIND 要求之用戶端所要求的資料簽章層級，選項如下： ➢ 無：LDAP BIND 要求隨呼叫者指定的選項發出 ➢ 交涉簽章：若未啟動傳輸層安全性/安全通訊端層(TLS\SSL)，會隨呼叫	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路安全性：LDAP 用戶端簽章要	交涉簽章	CCE-ID：CCE-47129-2

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					者指定的選項以外的 LDAP 資料簽章選項初始化 LDAP BIND 要求。若已啟動 TLS\SSL，會隨呼叫者指定的選項初始化 LDAP BIND 要求 ➢要求簽章：這與交涉簽章相同。不過，若 LDAP 伺服器的中繼 saslBindInProgress 回應未指示 LDAP 流量簽章為必要的，則會告知呼叫者 LDAP BIND 命令要求失敗	求		
96	Windows Server 2016 Common Settings	TWG CB-01-007-0097	安全性選項\稽核	稽核：當無法記錄安全性稽核時，系統立即關機	▪這項原則設定決定系統在無法記錄安全性事件時，是否要立即關機 ▪如果啟用了這項原則設定，只要無法記錄安全稽核，系統便會停止。基本上，當安全性稽核記錄檔已滿，且安全性記錄檔的保持方法設為「不要覆寫事件」或「依日期覆寫事件」，便無法再記錄事件 ▪如果安全性記錄檔已滿且無法覆寫現	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\稽核：當無法記錄安全性稽核時，系統立即關機	已停用	CCE-ID：CCE-45965-1

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					有項目，但已啟用此安全性選項，則會出現下列停止錯誤： ➢STOP：C0000244{Audit Failed}嘗試產生安全性稽核時發生失敗 ▪若要修復，系統管理員必須登入、備份記錄檔(可省略)、清除記錄檔，再依需要重設此選項。直到這項原則設定重設之前，除了 Administrators 群組的成員之外，任何使用者都無法登入此系統，即使安全性記錄檔未滿			
97	Windows Server 2016 Common Settings	TWG CB-01-007-0098	安全性選項\稽核	稽核：稽核通用系統物件的存取	▪這項原則設定決定是否稽核通用系統物件的存取 ▪如果啟用此設定，會導致系統物件(如 Mutex(互斥)、事件、信號及 DOS 裝置)在建立時便含有預設的系統存取控制清單(SACL)。只有具名的物件會被指定 SACL；SACL 不會指定給沒有名稱的物件。如果也啟用「稽核物件存取」稽核	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\稽核：稽核通用系統物件的存取	已停用	CCE-ID：CCE-46580-7

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					原則，則會稽核這些系統物件的存取 ▪ 注意：設定這項原則設定時，在重新啟動 Windows 之後，所做的變更才會生效			
98	Windows Server 2016 Common Settings	TWG CB-01-007-0099	安全性選項\稽核	稽核：稽核備份與還原權限的使用	▪ 這項原則設定決定在「稽核特殊權限使用」原則生效時，是否稽核所有使用者權限的使用，包括備份與還原。在「稽核特殊權限使用」啟用時同時啟用此選項，將會對備份或還原的每個檔案產生一個稽核事件 ▪ 如果停用此設定，即使啟用「稽核特殊權限使用」，也不會稽核備份或還原權限的使用	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\稽核：稽核備份與還原權限的使用	已停用	CCE-ID：CCE-45964-4
99	Windows Server 2016 Common Settings	TWG CB-01-007-0100	安全性選項\稽核	稽核：強制執行稽核原則子類別設定 (Windows	▪ Windows Vista 及更新版本的 Windows 允許使用稽核原則子類別，以更精確的方式來管理稽核原則。在類別層級設定稽核原則，將會覆寫新的子類別稽核原則功能。群組原則只允許稽核原則可以	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\稽核：	已啟用	CCE-ID：CCE-46406-5

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				Vista 或更新的版本)以覆寫稽核原則類別設定	在類別層級設定，而且因為新機器會加入網域或者升級至 Windows Vista 或更新的版本，所以現有的群組原則可以覆寫新機器的子類別設定。為了讓稽核原則不需變更群組原則即可使用子類別來管理，在 Windows Vista 與更新版本中有新的登錄值 SCENoApplyLegacyAuditPolicy，可防止將類別層級稽核原則套用到群組原則及「本機安全性原則」系統管理工具 ▪ 如果在這裡設定的類別層級稽核原則與目前產生的事件不一致，其原因可能是已設定此登錄機碼	強制執行稽核原則子類別設定(Windows Vista 或更新的版本)以覆寫稽核原則類別設定		
100	Windows Server 2016 Common Settings	TWG CB-01-007-0101	安全性選項\關機	關機：允許不登入就將系統關機	▪ 這項原則設定決定是否無需登入 Windows 便能夠將電腦關機 ▪ 啟用此設定時，Windows 登入畫面上可以使用「關機」命令 ▪ 停用此設定時，Windows 登入畫面上不	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\關機：	已停用	CCE-ID：CCE-46697-9

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					會顯示將電腦關機的選項。在這種情況下，使用者必須要能順利登入電腦，取得關閉系統使用者權限之後，才能執行系統關機操作	允許不登入就將系統關機		
101	Windows Server 2016 Common Settings	TWG CB-01-007-0102	安全性選項\關機	關機：清除虛擬記憶體分頁檔	▪ 這項原則設定決定系統關機時是否清除虛擬記憶體分頁檔 ▪ 虛擬記憶體支援使用系統分頁檔交換不使用的記憶體分頁至磁碟。在執行的系統上，此分頁檔由作業系統獨佔開啟，並且受到保護。不過，未設定允許以其他作業系統開機的系統，可能必須確定系統分頁檔在此系統關機時已刪除完畢。這樣可確保可能進入分頁檔的處理程序記憶體中的敏感資料，不會被直接存取分頁檔的未經授權使用者使用 ▪ 當啟用此設定時，在正常關機時會清除系統分頁檔。若啟用此安全性選項，當	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\關機：清除虛擬記憶體分頁檔	已停用	CCE-ID：CCE-46645-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
					停用休眠時，也會清除休眠檔案(hiberfil.sys)			
102	Windows Server 2016 Common Settings	TWGCB-01-007-0103	使用者權限指派	鎖定記憶體中的分頁	▪ 這項原則設定決定哪些使用者能使用處理程序來保留實體記憶體中的資料，阻止系統將資料分頁到磁碟上的虛擬記憶體 ▪ 履行此特殊權限會降低可用的隨機存取記憶體(RAM)數量，而對系統效能造成顯著影響	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\鎖定記憶體中的分頁	No One	CCE-ID：CCE-47319-9
103	Windows Server 2016 Common Settings	TWGCB-01-007-0104	使用者權限指派	增加處理程序工作組	▪ 此權限決定哪些使用者帳戶可以增加或減少處理程序的工作組大小 ▪ 處理程序的工作組是實體 RAM 記憶體中的處理程序目前可見的記憶體頁面組。這些頁面是常駐的，且可讓應用程式使用而不會觸發分頁錯誤。工作組的大小下限與上限可以影響處理程序的虛擬記憶體分頁行為	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\增加處理程序工作組	Administrators, Local Service	CCE-ID：CCE-45959-4

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪注意：增加處理程序的工作組大小會減少系統其他部分可用的實體記憶體總數			
104	Windows Server 2016 Common Settings	TWG CB-01-007-0105	使用者權限指派	關閉系統	▪這項原則設定決定哪些本機登入電腦的使用者能夠使用 Shutdown 命令將作業系統關機 ▪濫用此使用者權限會造成拒絕服務	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\關閉系統	Administrators	CCE-ID：CCE-47106-0
105	Windows Server 2016 Common Settings	TWG CB-01-007-0106	使用者權限指派	調整處理程序的記憶體配額	▪此特殊權限決定能變更處理程序可使用的最大記憶體的人員 ▪注意：此特殊權限有助於系統調整，但可能會被濫用，例如拒絕服務的攻擊	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\調整處理程序的記憶體配額	Administrators, Local Service, Network Service	CCE-ID：CCE-44626-0
106	Windows	TWG	使用	取代處理	這項原則設定決定哪些使用者帳戶能夠	電腦設定	Local	CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Common Settings	CB-01-007-0107	者權限指派	程序等級權杖	呼叫 CreateProcessAsUser()應用程式開發介面(API)，如此一個服務便能夠啟動另一個服務。工作排程器便是使用此使用者權限的處理程序範例	\Windows 設定\安全性設定\本機原則\使用者權限指派\取代處理程序等級權杖	Service, Network Service	ID：CCE-46125-1
107	Windows Server 2016 Common Settings	TWG CB-01-007-0108	使用者權限指派	取得檔案或其他物件的擁有權	▪ 這項原則設定決定哪些使用者能夠取得系統中任何安全物件的擁有權，包括 Active Directory 物件、檔案及資料夾、印表機、登錄機碼、處理程序及執行緒 ▪ 注意：指派此使用者權限可能會危及安全性。由於物件擁有者將會擁有完全控制，請只將此使用者權限指派給信任的使用者	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\取得檔案或其他物件的擁有權	Administrators	CCE-ID：CCE-46216-8
108	Windows Server 2016	TWG CB-01-007-0	使用者權限指	拒絕透過遠端桌面服務登入	這項原則設定決定會禁止哪些使用者及群組以遠端桌面服務用戶端登入	電腦設定\Windows 設定\安全性設定\	Guests,本機帳戶	CCE-ID：CCE-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
	Common Settings	109	派			本機原則\使用者權限指派\拒絕透過遠端桌面服務登入		47279-5
109	Windows Server 2016 Common Settings	TWGCB-01-007-0110	使用者權限指派	拒絕從網路存取這台電腦	這項原則設定決定會禁止哪些使用者從網路存取電腦。這項原則設定會取代「從網路存取這台電腦」原則設定，如果使用者帳戶同時受限於這兩種原則	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\拒絕從網路存取這台電腦	Guests,本機帳戶與Administrators 群組的成員	CCE-ID：CCE-44499-2
110	Windows Server 2016 Common Settings	TWGCB-01-007-0111	使用者權限指派	載入及解除載入裝置驅動程式	▪ 此使用者權限決定哪些使用者能在核心模式中動態載入與解除載入裝置驅動程式或其他程式碼。此使用者權限不適用於隨插即用裝置驅動程式。建議不要將此特殊權限指派給其他使用者 ▪ 注意：指派此使用者權限可能會危及安	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\載入及解除載入	Administrators	CCE-ID：CCE-45960-2

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					全性。不要將此使用者權限指派給不想由其掌控系統的任何使用者、群組或處理程序	裝置驅動程式		
111	Windows Server 2016 Common Settings	TWG CB-01-007-0112	使用者權限指派	拒絕以服務方式登入	▪ 這項原則設定決定會禁止哪些服務帳戶以服務方式登錄處理程序。這項原則設定會取代「以服務方式登入」原則設定，如果帳戶同時受限於這兩種原則 ▪ 注意：這項原則設定不適用於 System、Local Service 或 Network Service 帳戶	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\拒絕以服務方式登入	Guests	CCE-ID：CCE-47121-9
112	Windows Server 2016 Common Settings	TWG CB-01-007-0113	使用者權限指派	讓電腦及使用者帳戶受信賴，以進行委派	▪ 這項原則設定決定哪些使用者可以在使用者或電腦物件上設定「信任委派」設定 ▪ 擁有此特殊權限的使用者或物件，亦須擁有對使用者或電腦物件之帳戶控制旗標的寫入存取權。在被信任以便進行委派的電腦上(或在使用者環境下)，所	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\讓電腦及使用者帳戶受信賴，	No One	CCE-ID：CCE-47308-2

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					執行的伺服器處理程序可透過用戶端的委派認證來存取另一台電腦的資源，前提是用戶端帳戶不能有「無法委派帳戶」帳戶控制旗標設定 ▪ 注意：濫用此使用者權限或「信任委派」設定，會造成網路非常容易受到特洛伊木馬程式的攻擊；此程式會模擬連入用戶端，並使用其認證，取得對網路資源的存取權	以進行委派		
113	Windows Server 2016 Common Settings	TWG CB-01-007-0114	使用者權限指派	備份檔案及目錄	▪ 此使用者權限決定哪些使用者可以出於備份系統的目的，略過檔案及目錄、登錄及其他持續物件權限 ▪ 具體而言，此使用者權限類似於將系統上所有檔案及資料夾的下列權限授與相關的使用者或群組： ➢周遊資料夾/執行檔案 ➢列出資料夾/讀取資料	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\備份檔案及目錄	Administrators	CCE-ID：CCE-44987-6

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					➢讀取屬性 ➢讀取擴充屬性 ➢讀取權限 ▪注意：指派此使用者權限可能會危及安全性。由於沒有方法可確定使用者是否正在備份資料、竊取資料或複製要發行的資料，因此請只將此使用者權限指派給受信任的使用者			
114	Windows Server 2016 Common Settings	TWG CB-01-007-0115	使用者權限指派	修改物件標籤	此特殊權限可決定哪些使用者帳戶可修改物件(例如，檔案、登錄機碼或由其他使用者擁有的處理程序)的完整性標籤。在使用者帳戶下執行的處理程序不需要此特殊權限，即可修改該使用者擁有之物件的標籤	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\修改物件標籤	No One	CCE-ID：CCE-45962-8
115	Windows Server 2016	TWG CB-01-007-0	使用者權限指	當成作業系統的一部分	▪此使用者權限可讓處理程序模擬任何使用者，而無需驗證。因此處理程序就可以取得與該使用者相同的本機資源	電腦設定\Windows 設定\安全性設定\	No One	CCE-ID：CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Common Settings	116	派		存取權 ▪ 需要此特殊權限的處理程序應使用 LocalSystem 帳戶(其已包括此特殊權限),而不應使用其他特別指派此特殊權限的使用者帳戶 ▪ 注意：指派此使用者權限可能會危及安全性。請僅將此使用者權限指派給信任的使用者	本機原則\使用者權限指派\當成作業系統的一部分		46917-1
116	Windows Server 2016 Common Settings	TWG CB-01-007-0117	使用者權限指派	變更系統時間	▪ 此使用者權限決定哪些使用者與群組能夠變更電腦內部時鐘的時間與日期 ▪ 已指派此使用者權限的使用者可決定事件記錄檔的外觀 ▪ 如果系統時間遭到變更，記錄的事件將會反映出新的時間，而非事件發生的實際時間	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\變更系統時間	LOCAL SERVICE, Administrators	CCE-ID：CCE-44644-3
117	Windows Server	TWG CB-01	使用者權	允許透過遠端桌面	這項原則設定決定哪些使用者或群組擁有以遠端桌面服務用戶端登入的權限	電腦設定\Windows 設定	Administrators	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
	2016 Common Settings	-007-0118	限指派	服務登入		\安全性設定\本機原則\使用者權限指派\允許透過遠端桌面服務登入		CCE-44703-7
118	Windows Server 2016 Common Settings	TWGCB-01-007-0119	使用者權限指派	修改韌體環境值	▪ 這項原則設定決定何人可以修改韌體環境值。韌體環境變數是存放在非 x86 型電腦之非揮發性 RAM 中的設定。設定的效果需視處理器而定 ▪ 在 x86 型電腦上，可以透過指派這個使用者權限而修改的唯一韌體環境值是「上次的正確設定」，而這應該只由系統修改 ▪ 在 Itanium 型電腦上，開機資訊是儲存在非揮發性 RAM 中。必須將此使用者權限指派給使用者，使用者才能執行 bootcfg.exe 及變更「系統內容」中「啟動及修復」上的「預設作業系統」設定	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\修改韌體環境值	Administrators	CCE-ID：CCE-46761-3

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 在所有的電腦上，安裝或升級 Windows 都需要此使用者權限 ▪ 注意：這項原則設定不會影響能修改系統環境變數及使用者環境變數(位於「系統內容」的「進階」索引標籤)的使用者			
119	Windows Server 2016 Common Settings	TWG CB-01-007-0120	使用者權限指派	建立通用物件	▪ 這項原則設定決定使用者是否可以建立所有工作階段可用的全域物件。如果使用者沒有此使用者權限，仍然可以建立自己工作階段專用的物件。可以建立全域物件的使用者可能會影響其他使用者工作階段的程序，因而可能導致應用程式失敗或資料損毀 ▪ 注意：指派此使用者權限可能會危及安全性。請只將此使用者權限指派給信任的使用者	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\建立通用物件	Administrators, SERVICE, LOCAL SERVICE, NETWORK SERVICE	CCE-ID：CCE-44705-2
120	Windows Server	TWG CB-01	使用者權	監視系統效能	這項原則設定決定哪些使用者可使用效能監視工具來監視系統處理程序的效能	電腦設定\Windows 設定	Administrators,NT	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
	2016 Common Settings	-007-0121	限指派			\安全性設定\本機原則\使用者權限指派\監視系統效能	SERVICE\WdiServiceHost	CCE-46572-4
121	Windows Server 2016 Common Settings	TWGCB-01-007-0122	使用者權限指派	產生安全性稽核	▪這項原則設定決定處理程序可使用哪些帳戶將項目新增到安全性記錄，此安全性記錄檔是用來追蹤未經授權的系統存取 ▪如果啟用「稽核：當無法記錄安全性稽核時，系統立即關機」安全性原則設定，濫用此使用者權限會導致產生許多稽核事件、可能會隱藏攻擊的辨識項，或造成拒絕服務	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\產生安全性稽核	Local Service, Network Service	CCE-ID：CCE-45689-7
122	Windows Server 2016 Common	TWGCB-01-007-0123	使用者權限指派	以服務方式登入	▪這項原則設定決定是否允許安全性主體以服務方式登入 ▪服務可以設定成以 Local System、Local Service 或 Network Service 帳戶執行，	電腦設定\Windows 設定\安全性設定\本機原則\使用	No One	CCE-ID：CCE-4723

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings				這些帳戶具有內建權限可以服務方式登入。任何以個別的使用者帳戶執行的服務都必須被指派此權限	者權限指派\以服務方式登入		8-1
123	Windows Server 2016 Common Settings	TWG CB-01-007-0124	使用者權限指派	存取認證管理員做為信任的呼叫者	在備份/還原時，認證管理員會使用此設定。帳戶不應該擁有此權限，因為它只會被指派給 Winlogon。如果此權限指定給其他實體，則使用者儲存的認證可能會被洩露	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\存取認證管理員做為信任的呼叫者	No One	CCE-ID：CCE-47182-1
124	Windows Server 2016 Common Settings	TWG CB-01-007-0125	使用者權限指派	變更時區	▪ 此使用者權限決定哪些使用者與群組可以變更電腦顯示本地時間時使用的時區，也就是指電腦的系統時間加時差 ▪ 系統時間本身是絕對的，而且不受時區變更的影響	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\變更時區	LOCAL SERVICE, Administrators	CCE-ID：CCE-44960-3

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
125	Windows Server 2016 Common Settings	TWG CB-01-007-0126	使用者權限指派	執行磁碟區維護工作	▪ 這項原則設定決定哪些使用者及群組能在磁碟區上執行維護工作，例如遠端磁碟重組 ▪ 指派此使用者權限時要特別小心。具有此使用者權限的使用者可以瀏覽磁碟與將檔案延伸到包含其他資料的記憶體中。當延伸檔案開啟時，使用者能夠讀取與修改取得的資料	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\執行磁碟區維護工作	Administrators	CCE-ID：CCE-46126-9
126	Windows Server 2016 Common Settings	TWG CB-01-007-0127	使用者權限指派	建立權杖物件	▪ 這項原則設定決定處理程序可使用哪些帳戶來建立權杖，然後在處理程序使用內部應用程式開發介面(API)來建立存取權杖時，用以取得任何本機資源的存取權 ▪ 此使用者權限是由作業系統內部使用。除非有此必要，否則不要將此使用者權限指派給 Local System 以外的使用者、群組或處理程序	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\建立權杖物件	No One	CCE-ID：CCE-47295-1

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 注意：指派此使用者權限可能會危及安全性。不要將此使用者權限指派給不想由其掌控系統的任何使用者、群組或處理程序			
127	Windows Server 2016 Common Settings	TWG CB-01-007-0128	使用者權限指派	強制從遠端系統進行關閉	▪ 這項原則設定決定哪些使用者能夠從網路上的遠端位置將電腦關機 ▪ 濫用此使用者權限會造成拒絕服務	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\強制從遠端系統進行關閉	Administrators	CCE-ID：CCE-44650-0
128	Windows Server 2016 Common Settings	TWG CB-01-007-0129	使用者權限指派	建立符號連結	▪ 此特殊權限會決定使用者是否可以從登入的電腦建立符號連結 ▪ 注意：此特殊權限僅能授與信任的使用者。在並非設計來處理符號連結的應用程式中，符號連結會導致安全性風險 ▪ 注意：此設定可搭配 symlink filesystem	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\建立符號連結	Administrators	CCE-ID：CCE-44828-2

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					設定使用，透過使用命令列公用程式來控制電腦上允許的 symlinks 類型，可操縱上述設定			
129	Windows Server 2016 Common Settings	TWG CB-01-007-0130	使用者權限指派	從擴充座移除電腦	▪ 這項原則設定決定使用者是否無需登入便可從擴充座卸除可攜式電腦 ▪ 如果啟用此權限，使用者必須先登入，才能從擴充座移除可攜式電腦 ▪ 如果停用此權限，使用者無需登入便可從擴充座移除可攜式電腦	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\從擴充座移除電腦	Administrators	CCE-ID：CCE-46021-2
130	Windows Server 2016 Common Settings	TWG CB-01-007-0131	使用者權限指派	略過周遊檢查	▪ 此使用者權限決定哪些使用者即使沒有周遊目錄的權限，也能夠周遊目錄樹狀結構 ▪ 此特殊權限不允許使用者列出目錄的內容，而只能周遊目錄	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\略過周遊檢查	Administrators, Authenticated Users, Local Service, Network	CCE-ID：CCE-44799-5

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
							Service	
131	Windows Server 2016 Common Settings	TWG CB-01-007-0132	使用者權限指派	建立分頁檔	▪ 此使用者權限決定哪些使用者及群組能夠呼叫內部應用程式開發介面(API)來建立分頁檔及變更其大小 ▪ 此使用者權限是由作業系統內部使用且通常不需要指派給任何使用者	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\建立分頁檔	Administrators	CCE-ID：CCE-44695-5
132	Windows Server 2016 Common Settings	TWG CB-01-007-0133	使用者權限指派	增加排程優先順序	▪ 這項原則設定決定哪些帳戶能使用具有寫入內容的處理程序存取其他處理程序，來增加指派給其他處理程序的執行優先順序 ▪ 具有此特殊權限的使用者能夠透過「工作管理員」使用者介面來變更處理程序的排程優先順序	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\增加排程優先順序	Administrators	CCE-ID：CCE-47022-9
133	Windows Server 2016	TWG CB-01-007-0	使用者權限指	管理稽核及安全性記錄檔	▪ 此安全設定決定哪些使用者能夠指定個別資源(例如檔案、Active Directory 物件及登錄機碼)的物件存取稽核選項	電腦設定\Windows 設定\安全性設定\	Administrators	CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Common Settings	134	派		▪ 這項原則設定不允許使用者啟用檔案與物件存取稽核。如需啟用這類稽核，便必須設定「電腦設定\Windows 設定\安全性設定\本機原則\稽核原則」中的「稽核物件存取」設定 ▪ 使用者可以在事件檢視器的安全性記錄檔中檢視稽核的事件。具有此特殊權限的使用者也可以檢視與清除安全性記錄檔	本機原則\使用者權限指派\管理稽核及安全性記錄檔		46078-2
134	Windows Server 2016 Common Settings	TWG CB-01-007-0135	使用者權限指派	拒絕以批次工作登入	▪ 這項原則設定決定會禁止哪些帳戶以批次工作登入 ▪ 這項原則設定會取代「以批次工作登入」原則設定，如果使用者帳戶同時受限於這兩種原則	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\拒絕以批次工作登入	Guests	CCE-ID：CCE-47287-8
135	Windows	TWG	使用	拒絕本機	▪ 這項原則設定決定會禁止哪些使用者	電腦設定	Guests	CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Common Settings	CB-01-007-0136	者權限指派	登入	登入電腦。這項原則設定會取代「允許本機登入」原則設定，如果帳戶同時受限於這兩種原則 ▪ 注意：如果將此安全性原則套用到 Everyone 群組，將無人能夠登入本機	\Windows 設定\安全性設定\本機原則\使用者權限指派\拒絕本機登入		ID：CCE-46108-7
136	Windows Server 2016 Common Settings	TWG CB-01-007-0137	使用者權限指派	偵錯程式	▪ 此使用者權限決定哪些使用者可將偵錯工具附加到任何處理程序或核心 ▪ 不需要將此使用者權限指派給對自行開發的應用程式進行偵錯的開發人員。但開發人員需要此使用者權限，才能對新的系統元件進行偵錯。此使用者權限可對機密且關鍵的作業系統元件提供完整存取權 ▪ 注意：指派此使用者權限可能會危及安全性。只將此使用者權限指派給信任的使用者	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\偵錯程式	Administrators	CCE-ID：CCE-44927-2
137	Windows	TWG	使用	建立永久	▪ 此使用者權限決定哪些帳戶處理程序	電腦設定	No One	CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Common Settings	CB-01-007-0138	者權限指派	共用物件	可以使用物件管理員來建立目錄物件 ▪ 此使用者權限是由作業系統內部使用，且有助於延伸物件命名空間。因為此使用者權限已經指派給在核心模式下執行的元件，所以不需要特別指派	\Windows 設定\安全性設定\本機原則\使用者權限指派\建立永久共用物件		ID：CCE-46835-5
138	Windows Server 2016 Common Settings	TWG CB-01-007-0139	使用者權限指派	還原檔案及目錄	▪ 這項原則設定決定哪些使用者可以在還原備份檔案及目錄時，略過檔案、目錄、登錄及其他持續物件的權限，並決定哪些使用者可以物件擁有者的身分，設定任何有效的安全性主體 ▪ 具體而言，此使用者權限類似於將系統上所有檔案及資料夾的下列權限授予相關的使用者或群組： ➢ 周遊資料夾/執行檔案 ➢ 寫入 ▪ 注意：指派此使用者權限可能會危及	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\還原檔案及目錄	Administrators	CCE-ID：CCE-46176-4

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					安全性。由於擁有使用者權限的使用者可以覆寫登錄設定、隱藏資料及取得系統物件的所有權，請僅指派這個使用者權限給信任的使用者			
139	Windows Server 2016 Common Settings	TWG CB-01-007-0140	使用者權限指派	監視單一處理程序	這項原則設定決定哪些使用者可使用效能監視工具來監視非系統處理程序的效能	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\監視單一處理程序	Administrators	CCE-ID：CCE-46517-9
140	Windows Server 2016 Common Settings	TWG CB-01-007-0141	使用者權限指派	以批次工作登入	▪ 這項原則設定允許使用者以批次佇列設備登入，且僅提供與舊版 Windows 相容之用 ▪ 例如，當使用者以工作排程器提交工作時，工作排程器會以批次使用者登入該使用者，而不是互動式使用者	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\以批次工作登入	Administrators	CCE-ID：CCE-44731-8

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
141	Windows Server 2016 Common Settings	TWG CB-01-007-0142	使用者權限指派	在驗證後模擬用戶端	▪ 將此特殊權限指定給使用者可讓代表該使用者執行的程式模擬用戶端 ▪ 要求此使用者權限以進行此類模擬，可防止未經授權的使用者說服用戶端連接(例如，透過遠端程序呼叫(RPC)或具名管道)至他們所建立的服務然後模擬該用戶端，進而避免將未授權使用者的權限提升到管理或系統層級 ▪ 注意：指派此使用者權限可能會危及安全性。請僅將此使用者權限指派給信任的使用者	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\在驗證後模擬用戶端	Administrators, SERVICE, Local Service, Network Service	CCE-ID：CCE-44804-3
142	Windows Server 2016 Common Settings	TWG CB-01-007-0143	使用者權限指派	從網路存取這台電腦	▪ 此使用者權限決定允許哪些使用者及群組透過網路連線到這台電腦 ▪ 遠端桌面服務不受此使用者權限的影響 ▪ 注意：遠端桌面服務在舊版的 Windows Server 中稱為「終端機服務」	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\從網路存取這台	Administrators, Authenticated Users	CCE-ID：CCE-45486-8

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
						電腦		
143	Windows Server 2016 Common Settings	TWGCB-01-007-0144	使用者權限指派	允許本機登入	▪ 這項原則設定決定哪些使用者可以登入電腦 ▪ 注意：修改此設定可能會影響用戶端、服務及應用程式的相容性	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\允許本機登入	Administrators	CCE-ID：CCE-45723-4
144	Windows Server 2016 Common Settings	TWGCB-01-007-0145	系統管理範本/Windows Installer	永遠以較高的特殊權限安裝	▪ 這項原則設定會指定 Windows Installer 在安裝任何程式到系統時應使用較高的權限 ▪ 如果啟用這項原則設定，會將特殊權限延伸到所有程式。這些特殊權限通常保留給已指派給使用者的程式(在桌面上提供)、已指派給電腦的程式(自動安裝)，或可以在「控制台」的「新增或移除程式」中使用的程式。這項設定檔設定可以讓使用者安裝某些程式，而這些	電腦設定\系統管理範本\Windows 元件\Windows Installer\永遠以較高的特殊權限安裝	已停用	CCE-ID：CCE-47225-8

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					程式需要存取的目錄可能是使用者沒有權限檢視或變更的目錄(包括位在高限制性電腦上的目錄) ▪ 如果停用或未設定這項原則設定，則系統會在安裝不是由系統管理員分配或提供的程式時，套用目前使用者的使用權限 ▪ 注意：這項原則設定會同時出現在「電腦設定」及「使用者設定」資料夾中。如果要讓這項原則設定生效，必須啟用上述兩個資料夾中的設定			
145	Windows Server 2016 Common Settings	TWG CB-01-007-0146	系統管理範本/Windows Installer	允許使用者控制安裝	▪ 這項原則設定決定是否允許使用者變更某些通常僅供系統管理員使用的安裝選項 ▪ 如果啟用這項原則設定，則會略過 Windows Installer 的部分安全性功能。它能讓安裝完成，不因安全性違規而暫	電腦設定\系統管理範本\Windows 元件\Windows Installer\允許使用者控制安裝	已停用	CCE-ID：CCE-4699 3-2

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					停安裝 ▪ 如果停用或未設定這項原則設定，Windows Installer 的安全性功能會防止使用者變更某些通常保留給系統管理員的安裝選項，例如指定檔案安裝目錄 ▪ 如果 Windows Installer 偵測到某個安裝套裝軟體已允許使用者變更受保護的選項，它將會停止安裝並顯示訊息。只有當安裝程式是在可存取使用者被拒的目錄之特殊權限的安全性內容上執行時，這些安全性功能才能操作 ▪ 這項原則設定是針對較少限制的環境而設計，可用來規避安裝程式中防止軟體被安裝的錯誤			
146	Windows Server 2016 Common	TWG CB-01 -007-0	系統管理範本 /Wind	防止出現 Windows Installer 指令碼的	▪ 這項原則設定決定是否允許以網頁為基礎的程式在電腦上安裝軟體時，不需要通知使用者	電腦設定\系統管理範本 \Windows 元件 \Windows	已停用	

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
	Settings	147	ows Installer	Internet Explorer 安全性提示	▪ 如果停用或未設定這項原則設定，預設狀況下，當網際網路瀏覽器管理的指令碼嘗試將程式安裝到系統時，系統會警告使用者，並讓他們選擇或拒絕安裝 ▪ 如果啟用這項原則設定，則不會出現警告，且允許繼續安裝 ▪ 這項原則設定是針對使用以網頁為基礎的工具來發布程式給員工的企業所設計。不過，由於這項原則設定可能有安全性風險，因此應該謹慎使用	Installer\防止出現 Windows Installer 指令碼的 Internet Explorer 安全性提示		
147	Windows Server 2016 Common Settings	TWGCB-01-007-0148	系統管理範本/自動播放原則	關閉自動播放	▪ 這項原則設定決定是否關閉自動播放功能 ▪ 當使用者將媒體插入磁碟機時，自動播放會立即開始讀取該磁碟機。如此一來，程式的安裝檔案與音訊媒體上的音樂便會立即啟動 ▪ 如果啟用這項原則設定，即會停用光碟	電腦設定\系統管理範本\Windows 元件\自動播放原則\關閉自動播放	已啟用：所有磁碟機	CCE-ID：CCE-46970-0

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					機及卸除式媒體磁碟機上的自動播放，或停用所有磁碟機的自動播放功能 ▪ 這項原則設定會停用其他類型磁碟機的自動播放功能。如果磁碟機上的自動播放功能預設是停用的，就無法使用這項設定來啟用該功能 ▪ 如果停用或未設定這項原則設定，就會啟用自動播放 ▪ 注意：這項原則設定會同時出現在「電腦設定」及「使用者設定」資料夾中。如果這兩個原則設定發生衝突，則「電腦設定」中的原則設定將優先於「使用者設定」中的原則設定			
148	Windows Server 2016 Common	TWG CB-01-007-0149	系統管理範本/自動播放	不允許非磁碟區裝置的自動播放	▪ 這項原則設定決定是否不允許 MTP 裝置(如相機或電話)的自動播放 ▪ 如果啟用這項原則設定，將不允許 MTP 裝置(如相機或電話)的自動播放	電腦設定\系統管理範本\Windows 元件\自動播放原則\不允許非磁碟	已啟用	CCE-ID：CCE-4680

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings		原則		▪ 如果停用或未設定這項原則設定，將可啟用非磁碟區裝置的自動播放	區裝置的自動播放		5-8
149	Windows Server 2016 Common Settings	TWG CB-01-007-0150	系統管理範本/自動播放原則	設定 AutoRun 的預設行為	▪ 這項原則設定可指定 AutoRun 命令的預設行為 ▪ AutoRun 命令一般儲存於 autorun.inf 檔案中。它們通常會啟動安裝程式或其他常式 ▪ 如果啟用這項原則設定，系統管理員可以將 Windows Vista 或更新版本的 AutoRun 預設行為變更為下列行為： ➢ 完全停用 AutoRun 命令 ➢ 轉換回 Windows Vista 之前的行為，自動執行 AutoRun 命令 ▪ 如果停用或未設定這項原則設定，Windows Vista 或更新版本將會提示使用者是否要執行 AutoRun 命令	電腦設定\系統管理範本\Windows 元件\自動播放原則\設定 AutoRun 的預設行為	已啟用：不執行任何 Autorun 命令	CCE-ID：CCE-46760-5
150	Windows	TWG	系統	設定用戶	▪ 這項原則設定指定在遠端桌面通訊協	電腦設定\系統	已啟用：高	CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Common Settings	CB-01-007-0151	管理範本/遠端桌面服務	端連線加密層級	定(RDP)連線期間，是否必須使用特定的加密層級，來確保用戶端電腦與遠端桌面工作階段主機伺服器之間的通訊安全。當使用原生 RDP 加密時才適用這項原則。不過，不建議使用原生 RDP 加密(相對於 SSL 加密)。此原則不會套用到 SSL 加密 ▪ 如果啟用這項原則設定，在遠端連線期間，用戶端與遠端桌面工作階段主機伺服器之間的所有通訊都必須使用這項設定中指定的加密方法。加密層級預設為「高」。可用的加密方法如下： ➢ 高：設定「高」會使用增強式 128 位元加密，來加密從用戶端傳送到伺服器的資料，以及從伺服器傳送到用戶端的資料。請在只包含 128 位元用戶端(例如，執行遠端桌面連線的用戶端)的環境中使用這個加	管理範本\Windows 元件\遠端桌面服務\遠端桌面工作階段主機\安全性\設定用戶端連線加密層級	等級	ID：CCE-47193-8

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					密層級。不支援這個加密層級的用戶端無法連線到遠端桌面工作階段主機伺服器 ➢用戶端相容：設定「用戶端相容」會以用戶端支援的最大金鑰效力，加密用戶端與伺服器之間傳送的資料。請在包含不支援 128 位元加密之用戶端的環境中使用這個加密層級 ➢低：設定「低」只會使用 56 位元加密，來加密從用戶端傳送到伺服器的資料			
151	Windows Server 2016 Common Settings	TWG CB-01-007-0152	系統管理範本/遠端桌面服務	連線時永遠提示密碼	▪ 這項原則設定決定遠端桌面服務是否總是會在連線時，提示用戶端輸入密碼 ▪ 可以使用這項設定，對登入遠端桌面服務的使用者強制執行密碼提示，即使使用者已經在遠端桌面連線用戶端中提	電腦設定\系統管理範本\Windows 元件\遠端桌面服務\遠端桌面工作階段主機\安全	已啟用	CCE-ID：CCE-45743-2

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					供過密碼 ▪ 遠端桌面服務預設為允許使用者在遠端桌面連線用戶端中輸入密碼就可以自動登入 ▪ 如果啟用這項原則設定，使用者即使已經在遠端桌面連線用戶端中提供密碼，也不能自動登入遠端桌面服務。使用者會收到要求輸入登入密碼的提示 ▪ 如果停用這項原則設定，使用者只要在遠端桌面連線用戶端中提供過密碼，就一律可以自動登入遠端桌面服務 ▪ 如果未設定這項原則設定，則不會在群組原則層級指定自動登入	性\連線時永遠提示密碼		
152	Windows Server 2016 Common	TWG CB-01-007-0153	系統管理範本/遠端	需要安全的 RPC 通訊	▪ 指定遠端桌面工作階段主機伺服器與所有用戶端之間必須進行安全的 RPC 通訊，還是允許非安全性通訊 ▪ 可以使用這項設定，藉由只允許已驗證	電腦設定\系統管理範本\Windows 元件\遠端桌面服務	已啟用	CCE-ID：CCE-4449

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings		桌面服務		及已加密的要求，來加強與用戶端的 RPC 通訊安全性 ▪ 如果狀態設定為「啟用」，遠端桌面服務會接受支援安全要求的 RPC 用戶端提出的要求，但不允許與不信任的用戶端進行非安全性通訊 ▪ 如果狀態設定為「停用」，遠端桌面服務一律會對所有 RPC 傳輸要求安全性。不過，如果 RPC 用戶端未回應要求，即允許非安全性通訊 ▪ 如果狀態設定為「尚未設定」，則允許非安全性通訊 ▪ 注意：RPC 介面是用於管理及設定遠端桌面服務	\遠端桌面工作階段主機\安全性\需要安全的 RPC 通訊		6-8
153	Windows Server 2016	TWG CB-01-007-0	系統管理範本/	不允許磁碟重新導向	▪ 這項原則設定決定在遠端桌面服務工作階段中，是否要防止對應用戶端磁碟機(磁碟機重新導向)	電腦設定\系統管理範本\Windows 元件	已啟用	CCE-ID：CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Common Settings	154	遠端桌面服務		▪ 根據預設，遠端桌面工作階段主機伺服器會在連線時自動對應用戶端磁碟機。對應的磁碟機會以「<磁碟機代號>於<電腦名稱>」的格式，顯示在「檔案總管」或電腦的工作階段資料夾樹狀目錄中。可以使用這項原則設定覆寫這種行為 ▪ 如果啟用這項原則設定，就不允許在遠端桌面服務工作階段中，重新導向用戶端磁碟機 ▪ 如果停用這項原則設定，就一律允許重新導向用戶端磁碟機。此外，如果允許剪貼簿重新導向，就永遠允許剪貼簿檔案複製重新導向 ▪ 如果未設定這項原則設定，則不會在群組原則層級指定用戶端磁碟機重新導向與剪貼簿檔案複製重新導向	\遠端桌面服務\遠端桌面工作階段主機\裝置及資源重新導向\不允許磁碟重新導向		46771-2

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
154	Windows Server 2016 Common Settings	TWG CB-01-007-0155	系統管理範本/遠端桌面服務	不要使用每一工作階段的暫存資料夾	▪ 這項原則設定決定是否防止遠端桌面服務建立特定工作階段的暫存資料夾 ▪ 可以使用這項原則設定，停用在遠端電腦上為每個工作階段建立個別的暫存資料夾。根據預設，遠端桌面服務會針對使用者在遠端電腦上保持的每一個使用中工作階段建立個別的暫存資料夾。這些暫存資料夾建立於遠端電腦上使用者設定檔資料夾下的 Temp 資料夾中，名稱為 sessionid ▪ 如果啟用這項原則設定，就不會建立每一工作階段的暫存資料夾。遠端電腦上所有工作階段的使用者暫存檔會儲存在遠端電腦上使用者設定檔資料夾下的共用 Temp 資料夾中 ▪ 如果停用這項原則設定，則會建立每一工作階段的暫存資料夾，即使伺服器系統管理員指定了不一樣的設定	電腦設定\系統管理範本\Windows 元件\遠端桌面服務\遠端桌面工作階段主機\暫存資料夾\不要使用每一工作階段的暫存資料夾	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 如果未設定這項原則設定，則會建立每一工作階段的暫存資料夾，除非伺服器系統管理員指定了不一樣的設定			
155	Windows Server 2016 Common Settings	TWG CB-01-007-0156	系統管理範本/遠端桌面服務	結束後不刪除暫存資料夾	▪ 這項原則設定決定當使用者登出時，遠端桌面服務是否會保留使用者每一工作階段的暫存資料夾 ▪ 可以使用這項設定，在遠端電腦上保存使用者特定工作階段的暫存資料夾，即使使用者已登出該工作階段。根據預設，遠端桌面服務會在使用者登出時，刪除其暫存資料夾 ▪ 如果啟用這項原則設定，使用者登出工作階段時，每一工作階段的暫存資料夾會保留下來 ▪ 如果停用這項原則設定，則使用者登出時會刪除暫存資料夾，即使伺服器系統管理員指定了不一樣的設定	電腦設定\系統管理範本\Windows 元件\遠端桌面服務\遠端桌面工作階段主機\暫存資料夾\結束後不刪除暫存資料夾	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 如果未設定這項原則設定，則遠端桌面服務會在使用者登出時，刪除遠端電腦上的暫存資料夾，除非伺服器系統管理員指定了不一樣的設定 ▪ 注意：這項設定只有在伺服器使用每一工作階段的暫存資料夾時，才會生效。如果啟用「不要使用每一工作階段的暫存資料夾」原則設定，則這項原則設定無效			
156	Windows Server 2016 Common Settings	TWG CB-01-007-0157	系統管理範本/遠端桌面服務	不允許儲存密碼	▪ 這項原則設定決定能否從遠端桌面連線將密碼儲存在這部電腦上 ▪ 如果啟用這項設定，「遠端桌面連線」的密碼儲存核取方塊將會停用，而且使用者再也無法儲存密碼。當使用者使用遠端桌面連線開啟 RDP 檔案並儲存其設定後，所有先前存在於 RDP 檔案中的密碼都將予以刪除 ▪ 如果停用或未做這項設定，則使用者能	電腦設定\系統管理範本\Windows 元件\遠端桌面服務\遠端桌面連線用戶端\不允許儲存密碼	已啟用	CCE-ID：CCE-44880-3

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					夠使用遠端桌面連線儲存密碼			
157	Windows Server 2016 Common Settings	TWG CB-01-007-0158	事件記錄服務/安全性	指定記錄檔大小上限(KB)	▪ 這項原則設定可指定記錄檔的大小上限(以 KB 為單位) ▪ 如果啟用這項原則設定，即可將記錄檔大小上限設定為介於 1 MB(1,024 KB)至 2TB(2,147,483,647 KB)之間(以 KB 為遞增單位) ▪ 如果停用或未設定這項原則設定，則記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更這個值，此值預設為 20 MB	電腦設定\系統管理範本\Windows 元件\事件記錄服務\安全性\指定記錄檔大小上限(KB)	已啟用：196,608KB 以上	CCE-ID：CCE-44526-2
158	Windows Server 2016 Common Settings	TWG CB-01-007-0159	事件記錄服務/安全性	控制記錄檔達到其大小上限時的事件記錄檔行	▪ 這項原則設定可以控制記錄檔達到其大小上限時的事件記錄檔行為 ▪ 如果啟用這項原則設定，且記錄檔達到其大小上限時，新事件將不會寫入記錄檔且會遺失	電腦設定\系統管理範本\Windows 元件\事件記錄服務\安全性\控制	已停用	CCE-ID：CCE-47101-1

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				為	▪ 如果停用或未設定這項原則設定，且記錄檔達到其大小上限，則新事件會覆寫舊事件 ▪ 注意：舊事件的保留與否，是根據「記錄檔已滿時自動備份」原則設定所決定	記錄檔達到其大小上限時的事件記錄檔行為		
159	Windows Server 2016 Common Settings	TWG CB-01-007-0160	事件記錄服務/系統	指定記錄檔大小上限(KB)	▪ 這項原則設定可指定記錄檔的大小上限(以 KB 為單位) ▪ 如果啟用這項原則設定，即可將記錄檔大小上限設定為介於 1 MB(1,024 KB)至 2TB(2,147,483,647 KB)之間(以 KB 為遞增單位) ▪ 如果停用或未設定這項原則設定，則記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更這個值，此值預設為 20 MB	電腦設定\系統管理範本\Windows 元件\事件記錄服務\系統\指定記錄檔大小上限(KB)	已啟用：32,768KB 以上	CCE-ID：CCE-46651-6
160	Windows	TWG	事件	控制記錄	▪ 這項原則設定可以控制記錄檔達到其	電腦設定\系統	已停用	CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Common Settings	CB-01-007-0161	記錄服務/系統	檔達到其大小上限時的事件記錄檔行為	大小上限時的事件記錄檔行為 ▪ 如果啟用這項原則設定，且記錄檔達到其大小上限時，新事件將不會寫入記錄檔且會遺失 ▪ 如果停用或未設定這項原則設定，且記錄檔達到其大小上限，則新事件會覆寫舊事件 ▪ 注意：舊事件的保留與否，是根據「記錄檔已滿時自動備份」原則設定所決定	管理範本\Windows 元件\事件記錄服務\系統\控制記錄檔達到其大小上限時的事件記錄檔行為		ID：CCE-46104-6
161	Windows Server 2016 Common Settings	TWG CB-01-007-0162	事件記錄服務/應用程式	指定記錄檔大小上限(KB)	▪ 這項原則設定可指定記錄檔的大小上限(以 KB 為單位) ▪ 如果啟用這項原則設定，即可將記錄檔大小上限設定為介於 1 MB(1,024 KB)至 2TB(2,147,483,647 KB)之間(以 KB 為遞增單位) ▪ 如果停用或未設定這項原則設定，則記錄檔大小上限將會設定為本機設定	電腦設定\系統管理範本\Windows 元件\事件記錄服務\應用程式\指定記錄檔大小上限(KB)	已啟用：32,768KB 以上	CCE-ID：CCE-44494-3

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					值。本機系統管理員可使用「記錄內容」對話方塊來變更這個值，此值預設為 20 MB			
162	Windows Server 2016 Common Settings	TWG CB-01-007-0163	事件記錄服務/應用程式	控制記錄檔達到其大小上限時的事件記錄檔行為	▪ 這項原則設定可以控制記錄檔達到其大小上限時的事件記錄檔行為 ▪ 如果啟用這項原則設定，且記錄檔達到其大小上限時，新事件將不會寫入記錄檔且會遺失 ▪ 如果停用或未設定這項原則設定，且記錄檔達到其大小上限，則新事件會覆寫舊事件 ▪ 注意：舊事件的保留與否，是根據「記錄檔已滿時自動備份」原則設定所決定	電腦設定\系統管理範本\Windows 元件\事件記錄服務\應用程式\控制記錄檔達到其大小上限時的事件記錄檔行為	已停用	CCE-ID：CCE-4562 5-1
163	Windows Server 2016 Common	TWG CB-01-007-0164	Windows 元件\OneD	防止使用 OneDrive 儲存檔案	▪ 這項原則設定可防止應用程式與功能使用 OneDrive 上的檔案 ▪ 如果啟用這項原則設定： ➢使用者不能從 OneDrive 應用程式與	電腦設定\系統管理範本\Windows 元件\OneDrive\防	已啟用	CCE-ID：CCE-4540

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings		rive		檔案選擇器存取 OneDrive ➢Windows 市集應用程式不能使用 WinRT API 存取 OneDrive ➢OneDrive 不會顯示在檔案總管的瀏覽窗格中 ➢OneDrive 檔案不會與雲端保持同步 ➢使用者不可以從手機相簿資料夾自動上傳相片與影片 ▪ 如果停用或未設定這項原則設定，應用程式與功能就可以使用 OneDrive 檔案儲存空間	止使用 OneDrive 儲存檔案		5-8
164	Windows Server 2016 Common Settings	TWG CB-01-007-0165	系統管理範本/Windows 遠端殼	允許遠端殼層存取	▪ 這項原則設定可設定遠端殼層的存取權 ▪ 若啟用或未設定這項原則設定，伺服器將會接受新的遠端殼層連線 ▪ 若將這項原則設定為「已停用」，伺服器將會拒絕新的遠端殼層連線	電腦設定\系統管理範本\Windows 元件\Windows 遠端殼層\允許遠端殼層存取	已停用	CCE-ID：CCE-47001-3

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
			層					
165	Windows Server 2016 Common Settings	TWGCB-01-007-0166	系統管理範本/Windows 登入選項	系統起始的重新啟動之後自動登入最後一個互動式使用者	▪ 這項原則設定可控制裝置是否在 Windows Update 重新啟動系統之後自動登入最後一個互動式使用者 ▪ 如果啟用或未設定這項原則設定，裝置會安全地儲存使用者的認證(包括使用者名稱、網域及加密的密碼)，在 Windows Update 重新啟動之後設定自動登入。Windows Update 重新啟動之後，使用者會自動登入，且工作階段會自動以針對該使用者設定的所有鎖定畫面的應用程式鎖定 ▪ 如果停用這項原則設定，裝置不會儲存 Windows Update 重新啟動之後自動登入的使用者認證。系統重新啟動之後，使用者鎖定畫面的應用程式不會重新啟動	電腦設定\系統管理範本\Windows 元件\Windows 登入選項\系統起始的重新啟動之後自動登入最後一個互動式使用者	已停用	CCE-ID：CCE-47341-3

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
166	Windows Server 2016 Common Settings	TWG CB-01-007-0167	系統管理範本/市集	關閉市集應用程式	▪ 這項原則設定決定拒絕或允許存取市集應用程式 ▪ 如果啟用這項設定，將拒絕存取市集應用程式。必須能夠存取市集才能安裝應用程式更新 ▪ 如果停用或未設定這項設定，將允許存取市集應用程式	電腦設定\系統管理範本\Windows 元件\市集\關閉市集應用程式	已啟用	CCE-ID：CCE-45212-8
167	Windows Server 2016 Common Settings	TWG CB-01-007-0168	系統管理範本/市集	關閉自動下載和安裝更新	▪ 這項原則設定決定啟用或停用自動下載和安裝應用程式更新 ▪ 如果啟用這項設定，將會關閉自動下載和安裝應用程式更新 ▪ 如果停用這項設定，將會開啟自動下載和安裝應用程式更新 ▪ 如果未設定這項設定，自動下載和安裝應用程式更新是由登錄設定決定，使用者可以使用 Windows 市集中的「設定」進行變更	電腦設定\系統管理範本\Windows 元件\市集\關閉自動下載和安裝更新	已啟用	CCE-ID：CCE-45209-4

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
168	Windows Server 2016 Common Settings	TWG CB-01-007-0169	系統管理範本/市集	關閉更新至最新版 Windows 的服務	▪ 這項原則設定決定啟用或停用透過市集更新至最新版 Windows 的服務 ▪ 如果啟用這項設定，市集應用程式將不提供更新至最新版 Windows ▪ 如果停用或未設定這項設定，市集應用程式將提供更新至最新版 Windows	電腦設定\系統管理範本\Windows 元件\市集\關閉更新至最新版 Windows 的服務	已啟用	CCE-ID：CCE-45211-0
169	Windows Server 2016 Common Settings	TWG CB-01-007-0170	系統管理範本/登入	不要顯示網路選取 UI	▪ 這項原則設定可控制是否讓任何人在登入畫面上與可用的網路 UI 互動 ▪ 如果啟用這項原則設定，則登入 Windows 之後才能變更電腦的網路連線狀態 ▪ 如果停用或未設定這項原則設定，任何人不用登入 Windows 就可以中斷電腦與網路的連線或將電腦連線到其他可用的網路	電腦設定\系統管理範本\系統\登入\不要顯示網路選取 UI	已啟用	CCE-ID：CCE-47340-5
170	Windows	TWG	系統	列舉加入	▪ 這項原則設定決定是否允許列舉加入	電腦設定\系統	已停用	CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Common Settings	CB-01-007-0171	管理範本/登入	網域電腦上的本機使用者	網域電腦上的本機使用者 ▪ 如果啟用這項原則設定，登入介面將會列舉加入網域電腦上的本機使用者 ▪ 如果停用或未設定這項原則設定，則登入介面將不會列舉加入網域電腦上的連線使用者	管理範本\系統\登入\列舉加入網域電腦上的本機使用者		ID：CCE-46382-8
171	Windows Server 2016 Common Settings	TWG CB-01-007-0172	系統管理範本/登入	關閉鎖定畫面上的應用程式通知	▪ 這項原則設定決定是否不要在鎖定畫面上顯示應用程式通知 ▪ 如果啟用這項原則設定，則不會在鎖定畫面上顯示應用程式通知 ▪ 如果停用或未設定這項原則設定，則使用者可以選擇要在鎖定畫面上顯示通知的應用程式	電腦設定\系統管理範本\系統\登入\關閉鎖定畫面上的應用程式通知	已啟用	
172	Windows Server 2016 Common	TWG CB-01-007-0173	系統管理範本/稽核	在建立處理程序事件中包含命令列	▪ 這項原則設定可決定建立新的處理程序之後，要將哪些資訊記錄到安全性稽核事件中 ▪ 必須啟用「稽核建立處理程序」原則後	電腦設定\系統管理範本\系統\稽核建立處理程序\在建立處	已停用	CCE-ID：CCE-4541

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings		建立處理程序		才能套用這項設定 ▪ 如果啟用這項原則設定，每個處理程序的命令列資訊會以純文字形式記錄到安全性事件記錄中，做為套用這項原則設定之工作站與伺服器上稽核建立處理程序事件 4688「已建立新的處理程序」的一部分 ▪ 如果停用或未設定這項原則設定，處理程序的命令列資訊將不會包含在稽核建立處理程序事件中 ▪ 注意：如果啟用這項原則設定，具有讀取安全性事件存取權的任何使用者，將能夠讀取任何成功建立的處理程序的命令列引數。命令列引數可以包含敏感或私人資訊，如密碼或使用者資料	理程序事件中包含命令列		1-6
173	Windows Server 2016	TWG CB-01-007-0	系統管理範本/	允許加密檔案索引	▪ 這項原則設定決定是否允許對加密項目編製索引	電腦設定\系統管理範本\Windows 元件	已停用	CCE-ID：CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Common Settings	174	搜尋		▪如果啟用這項原則設定，索引將嘗試解密，並為內容編製索引(但仍適用存取限制) ▪如果停用這項原則設定，搜尋服務元件(包含非 Microsoft 元件)預期將不會為加密的項目或加密的儲存區編製索引。預設不會設定這項原則設定 ▪如果未設定這項原則設定，則將使用經由控制台所設定的本機設定。依據預設，會將控制台設定設為不為加密的內容編製索引 ▪啟用或停用此設定時，會完全重建索引 ▪使用者必須為索引存放位置使用完整磁碟區加密(例如，BitLocker 磁碟機加密或非 Microsoft 解決方案)，以維護加密檔案的安全性	\搜尋\允許加密檔案索引		45005-6
174	Windows	TWG	系統	設定「搜	▪這項原則設定可以控制在「搜尋」中使	電腦設定\系統	已啟用：匿	CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Common Settings	CB-01-007-0175	管理範本/搜尋	尋」中可以分享的資訊	用 Bing 分享哪些資訊 ▪ 如果啟用這項原則設定，則可以指定 3 個設定的其中 1 個，而且使用者不能變更這些設定： ➢ 使用者資訊和位置：分享使用者個人化搜尋及其他 Microsoft 經驗的搜尋歷程記錄、某些 Microsoft 帳戶資訊以及特定位置 ➢ 僅使用者資訊：分享使用者個人化搜尋及其他 Microsoft 經驗的搜尋歷程記錄與某些 Microsoft 帳戶資訊 ➢ 匿名資訊：分享使用資訊，但不分享搜尋歷程記錄、Microsoft 帳戶資訊或特定位置 ▪ 如果停用或未設定這項原則設定，使用者可選擇「搜尋」中要分享哪些資訊	管理範本\Windows 元件\搜尋\設定「搜尋」中可以分享的資訊	名資訊	ID：CCE-45381-1
175	Windows	TWG	系統	允許選用	▪ 這項原則設定可控制需要帳戶登入的	電腦設定\系統	已啟用	CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Common Settings	CB-01-007-0176	管理範本/應用程式執行階段	Microsoft 帳戶	Windows 市集應用程式是否可以選用 Microsoft 帳戶 ▪ 這項原則設定只會影響支援該功能的 Windows 市集應用程式 ▪ 如果啟用這項原則設定，通常需要 Microsoft 帳戶登入的 Windows 市集應用程式，將允許使用者改用企業帳戶登入 ▪ 如果停用或未設定這項原則設定，則使用者必須使用 Microsoft 帳戶登入	管理範本\Windows 元件\應用程式執行階段\允許選用 Microsoft 帳戶		ID：CCE-47342-1
176	Windows Server 2016 Common Settings	TWG CB-01-007-0177	系統管理範本/網際網路通訊管理	關閉 Windows Messenger 客戶經驗改進計畫	▪ 這項原則設定指定 Windows Messenger 是否蒐集關於 Windows Messenger 軟體與服務使用情形的匿名資訊 ▪ 使用者可以透過客戶經驗改進計畫讓 Microsoft 蒐集關於產品使用情形的匿名資訊，這項資訊將用來改善未來上市的產品	電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉 Windows Messenger 客戶經驗改進計	已啟用	CCE-ID：CCE-46724-1

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 如果啟用這項原則設定，Windows Messenger 將不會蒐集使用資訊，而且也不會顯示啟用蒐集使用資訊的使用者設定 ▪ 如果停用這項原則設定，Windows Messenger 將蒐集匿名使用資訊，而且不會顯示該設定 ▪ 如果未設定這項原則設定，使用者將能選擇參加，並允許資料蒐集	畫		
177	Windows Server 2016 Common Settings	TWG CB-01-007-0178	系統管理範本/網際網路通訊管理	關閉搜尋小幫手內容檔更新	▪ 這項原則設定指定搜尋小幫手是否應該在本機與網際網路進行搜尋時，自動下載內容更新 ▪ 當使用者搜尋本機電腦或網際網路時，搜尋小幫手有時會連線到 Microsoft 下載更新過的隱私權原則與其他用來格式化及顯示結果的內容檔 ▪ 如果啟用這項原則設定，搜尋小幫手將	電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉搜尋小幫手內容檔更新	已啟用	CCE-ID：CCE-46921-3

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					不會在進行搜尋時下載內容更新 ▪ 如果停用或未設定這項原則設定，除非使用者使用的是傳統搜尋，否則搜尋小幫手將會下載內容更新 ▪ 注意：網際網路搜尋還是會將搜尋文字與搜尋的相關資訊傳送給 Microsoft 與選用的搜尋提供者。選擇傳統搜尋將會完全關閉搜尋小幫手的功能			
178	Windows Server 2016 Common Settings	TWG CB-01-007-0179	系統管理範本/網際網路通訊管理	關閉檔案及資料夾的[發佈到網站]工作	▪ 這項原則設定指定「Windows」資料夾的檔案及資料夾工作是否有「將此檔案發佈到網站」、「將此資料夾發佈到網站」或「將選取項目發佈到網站」選項 ▪ 網頁發佈精靈可以用來下載提供者清單，並讓使用者發佈內容到網站 ▪ 如果啟用這項原則設定，將會從「Windows」資料夾的檔案及資料夾工作中移除這些工作	電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉檔案及資料夾的[發佈到網站]工作	已啟用	CCE-ID：CCE-45817-4

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 如果停用或未設定這項原則設定，將顯示該工作			
179	Windows Server 2016 Common Settings	TWG CB-01-007-0180	系統管理範本/網際網路通訊管理	關閉 HTTP 上的列印	▪ 這項原則設定可以指定是否允許這個用戶端透過 HTTP 列印 ▪ 透過 HTTP 列印可以讓用戶端列印到內部網路與網際網路上的印表機 ▪ 注意：這項原則設定只會影響網際網路列印的用戶端。它不會禁止這部電腦成為網際網路列印伺服器，並透過 HTTP 讓其他使用者使用其共用印表機 ▪ 如果啟用這項原則設定，它會阻止這個用戶端透過 HTTP 列印到網際網路印表機 ▪ 如果停用或未設定這項原則設定，使用者將可以選擇透過 HTTP 列印到網際網路印表機	電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉 HTTP 上的列印	已啟用	
180	Windows	TWG	系統	關閉	▪ 這項原則設定會關閉 Windows 客戶經	電腦設定\系統	已啟用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Common Settings	CB-01-007-0181	管理範本/網際網路通訊管理	Windows 客戶經驗改進計畫	驗改進計畫。「Windows 客戶經驗改進計畫」會蒐集關於硬體設定以及使用者如何使用軟體與服務的資訊，以便確定使用傾向以及使用形態。Microsoft 不會蒐集使用者的姓名、地址或其他個人識別資訊。不需要填寫問卷，不會有推銷電話，可以不受干擾繼續工作。非常簡單且方便使用 ▪ 如果啟用這項原則設定，所有使用者都不能加入「Windows 客戶經驗改進計畫」 ▪ 如果停用這項原則設定，所有使用者都能加入「Windows 客戶經驗改進計畫」 ▪ 如果未設定這項原則設定，系統管理員可以使用「控制台」中的「問題報告及解決方案」元件對所有使用者啟用「Windows 客戶經驗改進計畫」	管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉 Windows 客戶經驗改進計畫		

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
181	Windows Server 2016 Common Settings	TWG CB-01-007-0182	系統管理範本/網際網路通訊管理	關閉手寫辨識錯誤報告	▪ 這項原則設定決定是否允許使用者啟動手寫辨識錯誤報告工具，並將錯誤報告傳送給 Microsoft ▪ 使用者可以使用手寫辨識錯誤報告工具來報告在「Tablet PC 輸入面板」中發生的錯誤。此工具可產生錯誤報告，並透過安全連線將報告傳輸至 Microsoft。Microsoft 將使用這些錯誤報告來改善未來 Windows 版本中的手寫辨識功能 ▪ 如果啟用這項設定，使用者將無法啟動手寫辨識錯誤報告工具，或是將錯誤報告傳送給 Microsoft ▪ 如果停用這項設定，則 Tablet PC 使用者可以將手寫辨識錯誤報告給 Microsoft ▪ 如果未設定這項原則，則 Tablet PC 使用者可以將手寫辨識錯誤報告給	電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉手寫辨識錯誤報告	已啟用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					Microsoft			
182	Windows Server 2016 Common Settings	TWG CB-01-007-0183	系統管理範本/網際網路通訊管理	關閉市集的存取權	▪ 這項原則設定指定是否使用市集服務尋找應用程式來開啟具有未處理檔案類型或通訊協定關聯的檔案 ▪ 當使用者所開啟的檔案類型或通訊協定與電腦上任何應用程式都沒有關聯時，使用者可以選擇使用本機應用程式或市集服務來尋找應用程式 ▪ 如果啟用這項原則設定，將會移除「開啟檔案」對話方塊中的「在市集尋找應用程式」項目 ▪ 如果停用或未設定這項原則設定，使用者將可以使用市集服務，而且還可以在「開啟檔案」對話方塊中使用市集項目	電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉市集的存取權	已啟用	
183	Windows Server 2016	TWG CB-01-007-0	系統管理範本/	關閉透過 HTTP 下載印表機	▪ 這項原則設定可以指定是否允許這個用戶端透過 HTTP 下載印表機驅動程式套件	電腦設定\系統管理範本\系統\網際網路通訊	已啟用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Common Settings	184	網際網路通訊管理	驅動程式	▪ 如果要設定 HTTP 列印，需要透過 HTTP 下載不在 Windows CD 上或未與印表機隨附的驅動程式 ▪ 注意：這項原則設定不會禁止用戶端透過 HTTP 在內部網路或網際網路上的印表機進行列印。它只會禁止下載尚未在本機安裝的驅動程式 ▪ 如果啟用這項原則設定，將無法透過 HTTP 下載列印驅動程式 ▪ 如果停用或未設定這項原則設定，使用者可以透過 HTTP 下載列印驅動程式	管理\網際網路通訊設定\關閉透過 HTTP 下載印表機驅動程式		
184	Windows Server 2016 Common Settings	TWG CB-01-007-0185	系統管理範本/個人化	防止啟用鎖定畫面投影片放映	▪ 這項原則設定決定是否防止在鎖定畫面上播放投影片放映 ▪ 停用「電腦設定」中鎖定畫面投影片放映設定，防止在鎖定畫面上播放投影片放映 ▪ 如果啟用這項設定，使用者將無法修改	電腦設定\系統管理範本\控制台\個人化\防止啟用鎖定畫面投影片放映	已啟用	CCE-ID：CCE-47339-7

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					「電腦設定」中投影片放映設定，也不會開始任何投影片放映			
185	Windows Server 2016 Common Settings	TWG CB-01-007-0186	系統管理範本/個人化	防止啟用鎖定畫面相機	▪ 這項原則設定決定是否防止在鎖定畫面上啟用相機 ▪ 停用「電腦設定」中鎖定畫面相機切換開關，防止在鎖定畫面上啟用相機 ▪ 根據預設，使用者可以在鎖定畫面上啟用可用的相機 ▪ 如果啟用這項設定，使用者將無法啟用或停用「電腦設定」中鎖定畫面相機存取，而且在鎖定畫面上不能啟用相機	電腦設定\系統管理範本\控制台\個人化\防止啟用鎖定畫面相機	已啟用	CCE-ID：CCE-47338-9
186	Windows Server 2016 Common Settings	TWG CB-01-007-0187	系統管理範本/個人化	以密碼保護螢幕保護裝置	▪ 這項原則設定決定是否要以密碼保護電腦上使用的螢幕保護裝置 ▪ 如果啟用這項設定，所有螢幕保護裝置都會受到密碼保護 ▪ 如果停用這項設定，則無法在任何螢幕保護裝置上設定密碼保護	使用者設定\系統管理範本\控制台\個人化\以密碼保護螢幕保護裝置	已啟用	CCE-ID：CCE-44793-8

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 這項設定也會停用「個人化」或「顯示」控制台的「螢幕保護裝置」對話方塊中的「受密碼保護」核取方塊，以防止使用者變更密碼保護設定 ▪ 如果未做這項設定，使用者可以選擇是否要在每個螢幕保護裝置上設定密碼保護 ▪ 若要確保電腦受到密碼保護，必須啟用「啟用螢幕保護裝置」設定，並透過「螢幕保護裝置逾時」設定指定逾時 ▪ 注意：若要移除「螢幕保護裝置」對話方塊，請使用「防止變更螢幕保護裝置」設定			
187	Windows Server 2016 Common	TWG CB-01-007-0188	系統管理範本/個人	啟用螢幕保護裝置	▪ 這項原則設定決定是否啟用螢幕保護裝置 ▪ 如果停用這項設定，螢幕保護裝置不會執行。此外，這項設定會停用「個人化」	使用者設定\系統管理範本\控制台\個人化\啟用螢幕保護	已啟用	CCE-ID：CCE-4469

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings		化		或「顯示」控制台中的「螢幕保護裝置」對話方塊中的「螢幕保護裝置」區段。因此，使用者無法變更螢幕保護裝置選項 ▪ 如果未做這項設定，這項設定對系統沒有作用 ▪ 如果啟用這項設定，只要下列兩個條件成立，螢幕保護裝置就會執行： (1)已透過「螢幕保護裝置執行檔名稱」設定或用戶端電腦上的「控制台」，在用戶端上指定有效的螢幕保護裝置 (2)已透過設定或「控制台」將螢幕保護裝置逾時設定為非零的值	裝置		8-9
188	Windows Server 2016	TWG CB-01-007-0	系統管理範本/	強制特定螢幕保護裝置	▪ 這項原則設定決定是否強制使用特定螢幕保護裝置 ▪ 如果停用這項設定，螢幕保護裝置不會	使用者設定\系統管理範本\控制台\個人化\	已啟用：並指定特定螢幕保護	CCE-ID：CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Common Settings	189	個人化		執行。此外，這項設定會停用「個人化」或「顯示」控制台中的「螢幕保護裝置」對話方塊中的「螢幕保護裝置」區段。因此，使用者無法變更螢幕保護裝置選項 ▪ 如果未做這項設定，這項設定對系統沒有作用 ▪ 如果啟用這項設定，只要下列兩個條件成立，螢幕保護裝置就會執行： (1) 已透過「螢幕保護裝置執行檔名稱」設定或用戶端電腦上的「控制台」，在用戶端上指定有效的螢幕保護裝置 (2) 已透過設定或「控制台」將螢幕保護裝置逾時設定為非零的值	強制特定螢幕保護裝置	裝置(如scrnsave.scr)	45697-0
189	Windows Server	TWG CB-01	系統管理	Configure SMB v1	▪ 這項原則設定決定 SMBv1 用戶端驅動程式的啟動類型	電腦設定\系統管理範本\MS	已啟用：Disable	

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
	2016 Common Settings	-007-0190	範本\MS Security Guide	client driver	▪要停用 SMBv1 協定的用戶端處理，請選擇「啟用」選項按鈕，然後從下拉式功能表中選擇「停用驅動程式」 ▪注意：在任何情況下，不要選擇「停用」選項按鈕 ▪對此設定的更改需要重新開機才能生效 ▪若須於本機群組原則編輯器(Gpedit.msc)或群組原則管理(Gpmc.msc)等工具中顯示這項原則設定，請安裝 1703 以上版本之 SecGuide 系統管理範本	Security Guide\Configure SMB v1 client driver	driver (recommended)	
190	Windows Server 2016 Common Settings	TWGCB-01-007-0191	系統管理範本\MS Security	Configure SMB v1 server	▪這項原則設定決定啟用或停用 SMBv1 協定的伺服器端處理 ▪停用此設定，將停用 SMBv1 協定的伺服器端處理 ▪啟用此設定，將啟用 SMBv1 協定的伺	電腦設定\系統管理範本\MS Security Guide\Configure SMB v1	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
			Guide		服器端處理 ▪對此設定的更改需要重新開機才能生效 ▪若須於本機群組原則編輯器(Gpedit.msc)或群組原則管理(Gpmc.msc)等工具中顯示這項原則設定，請安裝 1703 以上版本之 SecGuide 系統管理範本	server		
191	Windows Server 2016 Common Settings	TWG CB-01-007-0192	系統管理範本/緩和選項	封鎖未受信任的字型	▪這項原則設定決定是否防止程式載入未受信任的字型 ▪未受信任的字型是安裝在 %windir%\Fonts 目錄以外的任何字型。此功能有 3 種緩和選項： (1) 封鎖未受信任的字型並記錄事件 (2) 不封鎖未受信任的字型 (3) 記錄事件，而不封鎖未受信任的字型	電腦設定\系統管理範本\系統\緩和選項\封鎖未受信任的字型	已啟用：封鎖未受信任的字型並記錄事件	CCE-ID：CCE-45231-8

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪啟用這項功能後，可能會在以下情況中遇到功能減少問題： ➢將列印工作傳送到使用這項功能且尚未明確排除多工緩衝處理器處理程序的遠端印表機伺服器。在此情況下，將不會使用任何未在伺服器的%windir%/Fonts 資料夾中的字型 ➢使用由已安裝之印表機圖形.dll 檔案提供的字型(在%windir%/Fonts 資料夾之外)列印 ➢使用運用記憶體字型的第一方或第三方應用程式 ➢使用 Internet Explorer 查看使用內嵌字型的網站。在此情況下，此功能會封鎖內嵌字型，因而導致網站使用預設字型。不過，並非所有字型都具有全部的字元，因此網站可能會以不同的方式呈現			

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					➢使用傳統型 Office 查看含有內嵌字型的文件。在此情況下，內容會以 Office 挑選的預設字型顯示			
192	Windows Server 2016 Common Settings	TWG CB-01-007-0193	系統管理範本/Lanman 工作站	啟用不安全的來賓登入	▪這項原則設定可決定 SMB 用戶端是否允許以不安全的來賓身分登入 SMB 伺服器 ▪若啟用這項原則設定或未設定這項原則設定，SMB 用戶端將允許不安全的來賓登入 ▪若停用這項原則設定，SMB 用戶端將拒絕不安全的來賓登入 ▪檔案伺服器使用不安全的來賓登入來允許共用資料夾的未經驗證存取。雖然在企業環境中不常見，做為檔案伺服器的消費性「網路連接儲存裝置」(NAS)設備經常使用不安全的來賓登入。Windows 檔案伺服器需要驗證，而且預設不會使用不安全的來賓登入。因為不	電腦設定\系統管理範本\網路\Lanman 工作站\啟用不安全的來賓登入	已停用	CCE-ID：CCE-45201-1

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					安全的來賓登入未經驗證，重要安全性功能(例如「SMB 簽署」與「SMB 加密」)會被停用。因此，允許不安全的來賓登入的用戶端容易遭受各種攔截式攻擊，進而導致資料遺失、資料損毀與暴露於惡意程式碼。此外，使用不安全的來賓登入方式寫入到檔案伺服器的所有資料可能可供網路上的任何人存取。Microsoft 建議停用不安全的來賓登入，並將檔案伺服器設定為要求驗證的存取			
193	Windows Server 2016 Common Settings	TWG CB-01-007-0194	進階稽核原則\DS 存取	稽核詳細目錄服務複寫	▪ 這項原則設定決定是否稽核因網域控制站之間的詳細 Active Directory 網域服務(AD DS)複寫而產生的事件 ▪ 預設值：沒有稽核	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\DS 存取\稽核詳細目錄服務	沒有稽核	CCE-ID：CCE-4565 3-3

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						複寫		
194	Windows Server 2016 Common Settings	TWG CB-01-007-0195	進階稽核原則\DS 存取	稽核目錄服務複寫	▪ 這項原則設定決定是否稽核兩部 Active Directory 網域服務(AD DS)網域控制站之間的複寫 ▪ 如果設定這項原則設定，則會在 AD DS 複寫期間產生稽核事件。成功稽核會記錄成功複寫，而失敗稽核則會記錄失敗複寫 ▪ 如果未設定這項原則設定，則不會在 AD DS 複寫期間產生稽核事件 ▪ 注意：這個子類別中的事件只會記錄在網域控制站上 ▪ 預設值：沒有稽核	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\DS 存取\稽核目錄服務複寫	沒有稽核	CCE-ID：CCE-46411-5
195	Windows Server 2016 Common	TWG CB-01-007-0196	進階稽核原則\系統	稽核系統完整性	▪ 這項原則設定決定是否稽核會破壞安全性子系統完整性的事件，例如： ➢ 因稽核系統發生問題而無法寫入事件記錄檔的事件	電腦設定\Windows 設定\安全性設定\進階稽核原則	成功與失敗	CCE-ID：CCE-4602

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings				➢使用本機程序呼叫(LPC)連接埠的處理程序，而此連接埠在透過與用戶端位址空間之間的回覆、讀取或寫入來嘗試模擬用戶端的過程中無效 ➢偵測到危害系統完整性的遠端程序呼叫(RPC) ➢偵測到程式碼完整性判斷為無效之可執行檔的雜湊值 ➢危害系統完整性的加密編譯操作 ▪預設值：成功與失敗	設定\稽核原則\系統\稽核系統完整性		3-8
196	Windows Server 2016 Common Settings	TWG CB-01-007-0197	進階稽核原則\系統	稽核 IPsec 驅動程式	▪這項原則設定決定是否稽核因 IPsec 篩選器驅動程式而產生的事件，例如： ➢IPsec 服務的啟動及關閉 ➢因完整性檢查失敗而丟棄的網路封包 ➢因重新執行檢查失敗而丟棄的網路封包	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\系統\稽核 IPsec 驅動程式	成功與失敗	CCE-ID：CCE-46482-6

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					➢因格式為純文字而丟棄的網路封包 ➢接收到具有不正確安全性參數索引(SPI)的網路封包。這可能表示網路卡未正確運作，或需要更新驅動程式 ➢無法處理 IPsec 篩選器 ▪如果設定這項原則設定，則會在 IPsec 篩選器驅動程式操作上產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪如果未設定這項原則設定，則不會在 IPsec 篩選器驅動程式操作上產生稽核事件 ▪預設值：沒有稽核			
197	Windows Server 2016	TWG CB-01-007-0	進階稽核原則\	稽核安全性系統延伸	▪這項原則設定決定是否稽核與安全性系統延伸或服務相關的事件，例如： ➢載入安全性系統延伸(如驗證、通知	電腦設定\Windows 設定\安全性設定\	成功與失敗	CCE-ID：CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Common Settings	198	系統		或安全性封裝)，並向本機安全性授權(LSA)進行註冊。它是用來驗證登入嘗試、提交登入要求，以及任何帳戶或密碼變更。Kerberos 及 NTLM 是安全性系統延伸的範例 ➢安裝服務，並向服務控制管理員進行註冊。稽核記錄包含服務名稱、二進位、類型、啟動類型及服務帳戶的相關資訊 ▪如果設定這項原則設定，則會在嘗試載入安全性系統延伸時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪如果未設定這項原則設定，則不會在嘗試載入安全性系統延伸時產生稽核事件 ▪預設值：沒有稽核	進階稽核原則設定\稽核原則\系統\稽核安全性系統延伸		47111-0

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
198	Windows Server 2016 Common Settings	TWG CB-01-007-0199	進階稽核原則\系統	稽核其他系統事件	▪ 這項原則設定決定是否稽核下列任一事件： ➢Windows 防火牆服務及驅動程式的啟動及關閉 ➢Windows 防火牆服務的安全性原則處理 ➢加密編譯金鑰檔案及移轉操作 ▪ 預設值：成功，失敗	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\系統\稽核其他系統事件	成功與失敗	CCE-ID：CCE-46518-7
199	Windows Server 2016 Common Settings	TWG CB-01-007-0200	進階稽核原則\系統	稽核安全性狀態變更	▪ 這項原則設定決定是否稽核因電腦安全性狀態變更而產生的事件，例如下列事件： ➢電腦的啟動及關閉 ➢系統時間的變更 ➢從 CrashOnAuditFail 復原系統，這是在安全性事件記錄檔已滿且設定 CrashOnAuditFail 登錄項目時於系	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\系統\稽核安全性狀態變更	成功與失敗	CCE-ID：CCE-45968-5

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					統重新啟動之後記錄 ▪ 預設值：成功			
200	Windows Server 2016 Common Settings	TWG CB-01-007-0201	進階稽核原則\物件存取	稽核其他物件存取事件	▪ 這項原則設定決定是否稽核因管理工作排程器物件或 COM+物件而產生的事件 ▪ 如果是排程器工作，則會稽核下列項目： ➢建立工作 ➢刪除工作 ➢啟用工作 ➢停用工作 ➢更新工作 ▪ 如果是 COM+物件，則會稽核下列項目： ➢新增類別目錄物件 ➢更新類別目錄物件	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\物件存取\稽核其他物件存取事件	成功與失敗	CCE-ID：CCE-45980-0

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					➢刪除類別目錄物件			
201	Windows Server 2016 Common Settings	TWG CB-01-007-0202	進階稽核原則\物件存取	稽核控制代碼操作	▪ 這項原則設定決定是否稽核開啟或關閉物件控制代碼時產生的事件。只有具有相符系統存取控制清單(SACL)的物件才會產生安全性稽核事件 ▪ 如果設定這項原則設定，則會在操作控制代碼時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在操作控制代碼時產生稽核事件 ▪ 注意：這個子類別中的事件只有針對啟用對應物件存取子類別的物件類型，才會產生事件。例如，如果啟用檔案系統物件存取，則會產生控制代碼操作安全性稽核事件。如果未啟用登錄物件存取，則不會產生控制代碼操作安全性稽	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\物件存取\稽核控制代碼操作	沒有稽核	CCE-ID：CCE-46407-3

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					核事件			
202	Windows Server 2016 Common Settings	TWG CB-01-007-0203	進階稽核原則\物件存取	稽核檔案共用	▪ 這項原則設定決定是否稽核存取共用資料夾的嘗試 ▪ 如果設定這項原則設定，則會在嘗試存取共用資料夾時產生稽核事件。如果定義這項原則設定，則系統管理員可以指定只稽核成功、只稽核失敗，或同時稽核兩者 ▪ 注意：共用資料夾沒有系統存取控制清單(SACL)。如果啟用這項原則設定，則會稽核系統上所有共用資料夾的存取	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\物件存取\稽核檔案共用	成功與失敗	CCE-ID：CCE-47269-6
203	Windows Server 2016 Common Settings	TWG CB-01-007-0204	進階稽核原則\物件存取	稽核篩選平台連線	▪ 這項原則設定決定是否稽核 Windows 篩選平台(WFP)允許或封鎖的連線。包含下列事件： ➢Windows 防火牆服務封鎖應用程式，使其無法接受網路的連入連線 ➢WFP 允許連線	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\物件存取\稽	沒有稽核	CCE-ID：CCE-45979-2

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					➢WFP 封鎖連線 ➢WFP 允許本機連接埠的繫結 ➢WFP 封鎖本機連接埠的繫結 ➢WFP 允許連線 ➢WFP 封鎖連線 ➢WFP 允許應用程式或服務接聽進行連入連線的連接埠 ➢WFP 封鎖應用程式或服務接聽進行連入連線的連接埠 ▪ 如果設定這項原則設定，則會在 WFP 允許或封鎖連線時產生稽核事件。成功稽核會記錄允許連線時產生的事件，而失敗稽核則會記錄封鎖連線時產生的事件 ▪ 如果未設定這項原則設定，則不會在 WFP 允許或封鎖連線時產生稽核事件	核篩選平台連線		

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
204	Windows Server 2016 Common Settings	TWG CB-01-007-0205	進階稽核原則\物件存取	稽核憑證服務	▪ 這項原則設定決定是否稽核 Active Directory 憑證服務(AD CS)操作 ▪ AD CS 操作包括： ➢AD CS 啟動/關閉/備份/還原 ➢憑證撤銷清單(CRL)的變更 ➢新的憑證要求 ➢憑證的發出 ➢憑證的撤銷 ➢AD CS 的憑證管理員設定變更 ➢AD CS 組態的變更 ➢憑證服務範本的變更憑證的匯入 ➢憑證授權單位憑證的發布是針對 ActiveDirectory 網域服務 ➢AD CS 的安全性權限變更 ➢金鑰的封存 ➢金鑰的匯入	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\物件存取\稽核憑證服務	沒有稽核	CCE-ID：CCE-4597 8-4

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					➢金鑰的抓取 ➢線上憑證狀態通訊協定(OCSP)回應程式服務的啟動 ➢線上憑證狀態通訊協定(OCSP)回應程式服務的停止			
205	Windows Server 2016 Common Settings	TWG CB-01-007-0206	進階稽核原則\物件存取	稽核檔案系統	▪這項原則設定決定是否稽核使用者存取檔案系統物件的嘗試。只有已指定系統存取控制清單(SACL)的物件，以及要求的存取類型(如寫入、讀取或修改)及提出要求的帳戶符合 SACL 中的設定時，才會產生安全性稽核事件 ▪如果設定這項原則設定，則會在每次帳戶存取具有相符 SACL 的檔案系統物件時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪如果未設定這項原則設定，則不會在每次帳戶存取具有相符 SACL 的檔案系統	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\物件存取\稽核檔案系統	沒有稽核	CCE-ID：CCE-4589 3-5

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					物件時產生稽核事件 ▪ 注意：可以使用該物件之「內容」對話方塊的「安全性」索引標籤，設定檔案系統物件的 SACL			
206	Windows Server 2016 Common Settings	TWG CB-01-007-0207	進階稽核原則\物件存取	稽核 SAM	▪ 這項原則設定決定是否稽核因嘗試存取安全性帳戶管理員(SAM)物件而產生的事件 ▪ SAM 物件包括： ➢SAM_ALIAS--本機群組 ➢SAM_GROUP--不是本機群組的群組 ➢SAM_USER-使用者帳戶 ➢SAM_DOMAIN-網域 ➢SAM_SERVER-電腦帳戶 ▪ 如果設定這項原則設定，則會在嘗試存取核心物件時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\物件存取\稽核 SAM	沒有稽核	CCE-ID：CCE-46229-1

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					失敗嘗試 ▪ 如果未設定這項原則設定，則不會在嘗試存取核心物件時產生稽核事件 ▪ 注意：只可以修改 SAM_SERVER 的系統存取控制清單(SACL)			
207	Windows Server 2016 Common Settings	TWG CB-01-007-0208	進階稽核原則\物件存取	稽核篩選平台封包丟棄	這項原則設定決定是否稽核 Windows 篩選平台(WFP)丟棄的封包	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\物件存取\稽核篩選平台封包丟棄	沒有稽核	CCE-ID：CCE-46844-7
208	Windows Server 2016 Common	TWG CB-01-007-0209	進階稽核原則\物件	稽核產生的應用程式	▪ 這項原則設定決定是否稽核使用 Windows 稽核應用程式開發介面(API)產生事件的應用程式。設計成使用 Windows 稽核 API 的應用程式，會使用	電腦設定\Windows 設定\安全性設定\進階稽核原則	沒有稽核	CCE-ID：CCE-4602

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings		存取		這個子類別來記錄與其功能相關的稽核事件 ▪這個子類別中的事件包含： ➢應用程式用戶端內容的建立 ➢應用程式用戶端內容的刪除 ➢應用程式用戶端內容的初始化 ➢其他使用 Windows 稽核 API 的應用程式操作	設定\稽核原則\物件存取\稽核產生的應用程式		4-6
209	Windows Server 2016 Common Settings	TWG CB-01-007-0210	進階稽核原則\物件存取	稽核登錄	▪這項原則設定決定是否稽核存取登錄物件的嘗試。只有已指定系統存取控制清單(SACL)的物件，以及要求的存取類型(如讀取、寫入或修改)及提出要求的帳戶符合 SACL 中的設定時，才會產生安全性稽核事件 ▪如果設定這項原則設定，則會在每次帳戶存取具有相符 SACL 的登錄物件時產生稽核事件。成功稽核會記錄成功嘗	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\物件存取\稽核登錄	沒有稽核	CCE-ID：CCE-44498-4

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在每次帳戶存取具有相符 SACL 的登錄物件時產生稽核事件 ▪ 注意：可以使用「使用權限」對話方塊來設定登錄物件的 SACL			
210	Windows Server 2016 Common Settings	TWG CB-01-007-0211	進階稽核原則\物件存取	稽核詳細的檔案共用	▪ 這項原則設定決定是否稽核存取共用資料夾中之檔案及資料夾的嘗試。「詳細的檔案共用」設定記錄每次存取檔案或資料夾的事件，而「檔案共用」設定對於用戶端與檔案共用之間建立的任何連線只會記錄一次事件。「詳細的檔案共用」稽核的事件，包括關於權限或用來授與或拒絕存取之其他條件的詳細資訊 ▪ 如果設定這項原則設定，當嘗試存取共用上的檔案或資料夾時，就會產生稽核事件。系統管理員可以指定只稽核成	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\物件存取\稽核詳細的檔案共用	失敗	CCE-ID：CCE-47141-7

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					功、只稽核失敗，或同時稽核兩者 ▪ 注意：共用資料夾沒有系統存取控制清單(SACL)。如果啟用這項原則設定，則會稽核系統上所有共用檔案與資料夾的存取			
211	Windows Server 2016 Common Settings	TWG CB-01-007-0212	進階稽核原則\物件存取	稽核核心物件	▪ 這項原則設定決定是否稽核存取核心的嘗試(包含 Mutex 及旗號) ▪ 只有具有相符系統存取控制清單(SACL)的核心物件才會產生安全性稽核事件 ▪ 注意：「稽核：稽核通用系統物件的存取」原則設定可控制核心物件的預設 SACL	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\物件存取\稽核核心物件	沒有稽核	CCE-ID：CCE-46520-3
212	Windows Server 2016 Common	TWG CB-01-007-0213	進階稽核原則\原則	稽核篩選平台原則變更	▪ 這項原則設定決定是否稽核因 Windows 篩選平台(WFP)變更而產生的事件，例如： ➢IPsec 服務狀態	電腦設定\Windows 設定\安全性設定\進階稽核原則	沒有稽核	CCE-ID：CCE-4715

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings		變更		➢IPsec 原則設定的變更 ➢Windows 防火牆原則設定的變更 ➢WFP 提供者及引擎的變更 ▪ 如果設定這項原則設定，則會在嘗試變更 WFP 時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在變更 WFP 時產生稽核事件 ▪ 預設值：沒有稽核	設定\稽核原則\原則變更\稽核篩選平台原則變更		6-5
213	Windows Server 2016 Common Settings	TWG CB-01-007-0214	進階稽核原則\原則變更	稽核驗證原則變更	▪ 這項原則設定決定是否稽核因驗證原則變更而產生的事件，例如： ➢建立樹系及網域信任 ➢修改樹系及網域信任 ➢移除樹系及網域信任 ▪ 變更下列位置下的 Kerberos 原則：電腦	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\原則變更\稽核驗證原則變	成功	CCE-ID：CCE-4649 6-6

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					設定\Windows 設定\安全性設定\帳戶原則\Kerberos 原則 ▪ 將下列任何使用者權限授與使用者或群組： ➢ 從網路存取這台電腦 ➢ 允許本機登入 ➢ 允許透過終端機服務登入 ➢ 以批次工作登入 ➢ 以服務方式登入 ➢ 命名空間衝突。例如，新信任的名稱與現有命名空間名稱相同時 ▪ 如果設定這項原則設定，則會在嘗試變更驗證原則時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在變更驗證原則時產生稽核事件	更		

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 注意：套用群組原則時，會記錄安全性稽核事件。而修改設定時，則不會發生該事件 ▪ 預設值：成功			
214	Windows Server 2016 Common Settings	TWG CB-01-007-0215	進階稽核原則\原則變更	稽核授權原則變更	▪ 這項原則設定決定是否稽核因授權原則變更而產生的事件，例如： ➢ 指派未透過「驗證原則變更」子類別稽核的使用者權限(如 SeCreateTokenPrivilege) ➢ 移除未透過「驗證原則變更」子類別稽核的使用者權限(如 SeCreateTokenPrivilege) ➢ 加密檔案系統(EFS)原則的變更 ➢ 物件之資源屬性的變更 ➢ 套用至物件之集中存取原則(CAP)的變更 ▪ 如果設定這項原則設定，則會在嘗試變	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\原則變更\稽核授權原則變更	成功	CCE-ID：CCE-46306-7

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					更授權原則時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在變更授權原則時產生稽核事件 ▪ 預設值：沒有稽核			
215	Windows Server 2016 Common Settings	TWG CB-01-007-0216	進階稽核原則\原則變更	稽核「稽核原則變更」	▪ 這項原則設定決定是否稽核安全性稽核原則設定變更，例如： ➢稽核原則物件上的設定權限及稽核設定 ➢系統稽核原則的變更 ➢安全性事件來源的註冊 ➢解除安全性事件來源的註冊 ➢每個使用者稽核設定的變更 ➢CrashOnAuditFail 值的變更 ➢檔案系統或登錄物件上的系統存取	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\原則變更\稽核「稽核原則變更」	成功與失敗	CCE-ID：CCE-4596 6-9

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					控制清單變更 ➢特殊群組清單的變更 ▪ 注意：物件的 SACL 變更而且已啟用原則變更類別時，會進行系統存取控制清單(SACL)變更稽核。啟用物件存取稽核且設定物件的 SACL 以稽核 DACL/擁有者變更時，會稽核判別存取控制清單(DACL)及擁有權變更 ▪ 如果設定這項原則設定，則會在嘗試遠端 RPC 連線時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在嘗試遠端 RPC 連線時產生稽核事件 ▪ 預設值：成功			
216	Windows Server	TWG CB-01	進階稽核	稽核 MPSSVC	▪ 這項原則設定決定是否稽核因 Microsoft 保護服務(MPSSVC)使用之原	電腦設定\Windows 設定	成功與失敗	CCE-ID：

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 Common Settings	-007-0217	原則\原則變更	規則層級原則變更	則規則變更而產生的事件。這個服務是供 Windows 防火牆使用。包含下列事件： ➢報告 Windows 防火牆服務啟動時的使用中原則 ➢Windows 防火牆規則的變更 ➢Windows 防火牆例外清單的變更 ➢Windows 防火牆設定的變更 ➢Windows 防火牆服務忽略或未套用的規則 ➢Windows 防火牆群組原則設定的變更 ▪ 如果設定這項原則設定，則會在嘗試變更 MPSSVC 所使用的原則規則時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，在 MPSSVC	\安全性設定\進階稽核原則設定\稽核原則\原則變更\稽核 MPSSVC 規則層級原則變更		CCE-45967-7

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					使用的原則規則變更時則不會產生稽核事件 ▪ 預設值：沒有稽核			
217	Windows Server 2016 Common Settings	TWG CB-01-007-0218	進階稽核原則\原則變更	稽核其他原則變更事件	▪ 這項原則設定決定是否稽核原則變更類別未稽核之其他安全性原則變更所產生的事件，例如： ➢ 信賴平台模組(TPM)組態變更 ➢ 核心模式密碼編譯自我測試 ➢ 密碼編譯提供者操作 ➢ 密碼編譯內容操作或修改 ➢ 已套用的集中存取原則(CAP)變更 ➢ 開機設定資料(BCD)修改 ▪ 預設值：沒有稽核	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\原則變更\稽核其他原則變更事件	失敗	CCE-ID：CCE-46936-1
218	Windows Server 2016	TWG CB-01-007-0	進階稽核原則\	稽核機密特殊權限使用	▪ 這項原則設定決定是否稽核使用機密特殊權限(使用者權限)時產生的事件，例如：	電腦設定\Windows 設定\安全性設定\	成功與失敗	CCE-ID：CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Common Settings	219	特殊權限使用		➢呼叫特許服務 ➢呼叫下列其中一種權限： (1)當成作業系統的一部分 (2)備份檔案及目錄 (3)建立權杖物件 (4)偵錯程式 (5)讓電腦及使用者帳戶受信賴，以進行委派 (6)產生安全性稽核 (7)在驗證後模擬用戶端 (8)載入及解除載入裝置驅動程式 (9)管理稽核及安全性記錄檔 (10)修改韌體環境值 (11)取代處理程序等級權杖 (12)還原檔案及目錄 (13)取得檔案或其他物件的擁有權	進階稽核原則設定\稽核原則\特殊權限使用\稽核機密特殊權限使用		45981-8

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 如果設定這項原則設定，則會在進行機密特殊權限要求時產生稽核事件。成功稽核會記錄成功要求，而失敗稽核則會記錄失敗要求 ▪ 如果未設定這項原則設定，則不會在進行機密特殊權限要求時產生稽核事件			
219	Windows Server 2016 Common Settings	TWG CB-01-007-0220	進階稽核原則\特殊權限使用	稽核非機密特殊權限使用	▪ 這項原則設定決定是否稽核因使用非機密特殊權限(使用者權限)而產生的事件 ▪ 下列是非機密的特殊權限： ➢存取認證管理員做為信任的呼叫者 ➢從網路存取這台電腦 ➢將工作站新增至網域 ➢調整處理程序的記憶體配額 ➢允許本機登入 ➢允許透過終端機服務登入	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\特殊權限使用\稽核非機密特殊權限使用	沒有稽核	CCE-ID：CCE-4654 9-2

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					➢略過周遊檢查 ➢變更系統時間 ➢建立分頁檔 ➢建立通用物件 ➢建立永久共用物件 ➢建立符號連結 ➢拒絕從網路存取這台電腦 ➢拒絕以批次工作登入 ➢拒絕以服務方式登入 ➢拒絕本機登入 ➢拒絕透過終端機服務登入 ➢強制從遠端系統進行關閉 ➢增加處理程序工作集 ➢增加排程優先順序 ➢鎖定記憶體中的分頁			

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					➢以批次工作登入 ➢以服務方式登入 ➢修改物件標籤 ➢執行磁碟區維護工作 ➢監視單一處理程序 ➢監視系統效能 ➢從銜接站移除電腦 ➢關閉系統 ➢同步處理目錄服務資料 ▪如果設定這項原則設定，則會在呼叫非機密特殊權限時產生稽核事件。成功稽核會記錄成功呼叫，而失敗稽核則會記錄失敗呼叫 ▪如果未設定這項原則設定，則不會在呼叫非機密特殊權限時產生稽核事件			
220	Windows	TWG	進階	稽核其他	▪這項原則設定決定是否稽核其他特殊	電腦設定	沒有稽核	CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Common Settings	CB-01-007-0221	稽核原則\特殊權限使用	特殊權限使用事件	權限(使用者權限)時產生的事件 ▪ 如果設定這項原則設定，則會在呼叫其他特殊權限時產生稽核事件。成功稽核會記錄成功呼叫，而失敗稽核則會記錄失敗呼叫 ▪ 如果未設定這項原則設定，則不會在呼叫其他特殊權限時產生稽核事件	\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\特殊權限使用\稽核其他特殊權限使用事件		ID：CCE-46918-9
221	Windows Server 2016 Common Settings	TWG CB-01-007-0222	進階稽核原則\帳戶登入	稽核 Kerberos 驗證服務	▪ 這項原則設定決定是否稽核因 Kerberos 驗證票證授權票證(TGT)要求而產生的事件 ▪ 如果設定這項原則設定，則會在 Kerberos 驗證 TGT 要求之後產生稽核事件。成功稽核會記錄成功要求，而失敗稽核則會記錄失敗要求 ▪ 如果未設定這項原則設定，則不會在 Kerberos 驗證 TGT 要求之後產生稽核事件	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\帳戶登入\稽核 Kerberos 驗證服務	成功與失敗	CCE-ID：CCE-45812-5

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 伺服器版本的預設值：成功			
222	Windows Server 2016 Common Settings	TWG CB-01-007-0223	進階稽核原則\帳戶登入	稽核認證驗證	▪ 這項原則設定決定是否稽核因使用者帳戶登入認證的驗證測試而產生的事件 ▪ 只有在授權可以使用那些認證的電腦上，才會發生這個子類別中的事件 ▪ 如果是網域帳戶，則網域控制站具有授權 ▪ 如果是本機帳戶，則本機電腦具有授權 ▪ 伺服器版本的預設值：成功	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\帳戶登入\稽核認證驗證	成功與失敗	CCE-ID：CCE-44732-6
223	Windows Server 2016 Common Settings	TWG CB-01-007-0224	進階稽核原則\帳戶登入	稽核 Kerberos 服務票證操作	▪ 這項原則設定決定是否稽核因針對使用者帳戶提交 Kerberos 驗證票證授權票證(TGT)要求而產生的事件 ▪ 如果設定這項原則設定，則會在針對使用者帳戶要求 Kerberos 驗證 TGT 之後產生稽核事件。成功稽核會記錄成功要求，而失敗稽核則會記錄失敗要求	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\帳戶登入\稽核 Kerberos 服	成功與失敗	CCE-ID：CCE-44466-1

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 如果未設定這項原則設定，則不會在針對使用者帳戶要求 Kerberos 驗證 TGT 之後產生稽核事件 ▪ 伺服器版本的預設值：成功	務票證操作		
224	Windows Server 2016 Common Settings	TWG CB-01-007-0225	進階稽核原則\帳戶登入	稽核其他帳戶登入事件	▪ 這項原則設定決定是否稽核因回應針對使用者帳戶登入提交的認證要求而產生的事件，而這些要求不是認證驗證或 Kerberos 票證 ▪ 預設值：沒有稽核	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\帳戶登入\稽核其他帳戶登入事件	沒有稽核	CCE-ID：CCE-45103-9
225	Windows Server 2016 Common Settings	TWG CB-01-007-0226	進階稽核原則\帳戶管理	稽核應用程式群組管理	▪ 這項原則設定決定是否稽核因應用程式群組變更而產生的事件，例如： ➢建立、變更或刪除應用程式群組 ➢在應用程式群組中新增或移除成員 ▪ 如果設定這項原則設定，則會在嘗試變	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則	沒有稽核	CCE-ID：CCE-46332-3

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					更應用程式群組時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在應用程式群組變更時產生稽核事件 ▪ 預設值：沒有稽核	\帳戶管理\稽核應用程式群組管理		
226	Windows Server 2016 Common Settings	TWG CB-01-007-0227	進階稽核原則\帳戶管理	稽核電腦帳戶管理	▪ 這項原則設定決定是否稽核因電腦帳戶變更(如建立、變更或刪除電腦帳戶時)而產生的事件 ▪ 如果設定這項原則設定，則會在嘗試變更電腦帳戶時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在電腦帳戶變更時產生稽核事件 ▪ 伺服器版本的預設值：成功	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\帳戶管理\稽核電腦帳戶管理	成功	CCE-ID：CCE-4590 5-7
227	Windows	TWG	進階	稽核其他	▪ 這項原則設定決定是否稽核因這個類	電腦設定	成功與失	CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Common Settings	CB-01-007-0228	稽核原則\帳戶管理	帳戶管理事件	別未涵蓋的其他使用者帳戶變更而產生的事件，例如： ➢已存取使用者帳戶的密碼雜湊。這一般是在 Active Directory 管理工具密碼移轉期間發生 ➢已呼叫密碼原則檢查 API。在惡意應用程式測試原則以減少密碼字典攻擊期間的嘗試次數時，呼叫這個功能會是一種攻擊 ➢下列群組原則路徑下的預設網域群組原則變更： (1)電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則 (2)電腦設定\Windows 設定\安全性設定\帳戶原則\帳戶鎖定原則 ▪注意：套用原則設定時，會記錄安全性稽核事件。而修改設定時，則不會發生	\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\帳戶管理\稽核其他帳戶管理事件	敗	ID：CCE-45973-5

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					該事件 ▪ 預設值：沒有稽核			
228	Windows Server 2016 Common Settings	TWG CB-01-007-0229	進階稽核原則\帳戶管理	稽核安全性群組管理	▪ 這項原則設定決定是否稽核因安全性群組變更而產生的事件，例如： ➢建立、變更或刪除安全性群組 ➢在安全性群組中新增或移除成員 ➢變更群組類型 ▪ 如果設定這項原則設定，則會在嘗試變更安全性群組時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在安全性群組變更時產生稽核事件 ▪ 預設值：成功	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\帳戶管理\稽核安全性群組管理	成功與失敗	CCE-ID：CCE-46702-7
229	Windows Server	TWG CB-01	進階稽核	稽核發佈群組管理	▪ 這項原則設定決定是否稽核因發佈群組變更而產生的事件，例如：	電腦設定\Windows 設定	成功	CCE-ID：

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 Common Settings	-007-0230	原則\帳戶管理		➢建立、變更或刪除發佈群組 ➢在發佈群組中新增或移除成員 ➢變更發佈群組類型 ▪如果設定這項原則設定，則會在嘗試變更發佈群組時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪如果未設定這項原則設定，則不會在發佈群組變更時產生稽核事件 ▪注意：這個子類別中的事件只會記錄在網域控制站上 ▪預設值：沒有稽核	\安全性設定\進階稽核原則設定\稽核原則\帳戶管理\稽核發佈群組管理		CCE-46519-5
230	Windows Server 2016 Common Settings	TWG CB-01-007-0231	進階稽核原則\帳戶管理	稽核使用者帳戶管理	▪這項原則設定決定是否稽核使用者帳戶的變更。包含下列事件： ➢建立、變更、刪除、重新命名、停用、啟用、鎖定或解除鎖定使用者帳戶	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則	成功與失敗	CCE-ID：CCE-46552-6

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					➢設定或變更使用者帳戶的密碼 ➢將安全性識別碼(SID)新增到使用者帳戶的 SID 歷程記錄 ➢設定目錄服務還原模式密碼 ➢變更管理使用者帳戶的權限 ➢備份或還原認證管理員認證 ▪如果設定這項原則設定，則會在嘗試變更使用者帳戶時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪如果未設定這項原則設定，則不會在使用者帳戶變更時產生稽核事件 ▪預設值：成功	\帳戶管理\稽核使用者帳戶管理		
231	Windows Server 2016 Common	TWG CB-01-007-0232	進階稽核原則\登入/	稽核帳戶鎖定	▪這項原則設定決定是否稽核因嘗試登入的帳戶被鎖定而失敗所產生的事件 ▪若設定這項原則設定，則會在帳戶因鎖定而無法登入電腦時產生稽核事件。成	電腦設定\Windows 設定\安全性設定\進階稽核原則	失敗	CCE-ID：CCE-4648

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings		登出		功稽核會記錄成功的嘗試，而失敗稽核則會記錄不成功的嘗試 ▪ 預設值：成功	設定\稽核原則\登入/登出\稽核帳戶鎖定		3-4
232	Windows Server 2016 Common Settings	TWG CB-01-007-0233	進階稽核原則\登入/登出	稽核 IPsec 延伸模式	▪ 這項原則設定決定是否稽核網際網路金鑰交換通訊協定(IKE)及已驗證網際網路通訊協定(AuthIP)在延伸模式交涉期間產生的事件 ▪ 如果設定這項原則設定，則會在 IPsec 延伸模式交涉期間產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在 IPsec 延伸模式交涉期間產生稽核事件 ▪ 預設值：沒有稽核	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\登入/登出\稽核 IPsec 延伸模式	沒有稽核	CCE-ID：CCE-46617-7
233	Windows Server 2016	TWG CB-01-007-0	進階稽核原則\	稽核網路原則伺服器	▪ 這項原則設定決定是否稽核 RADIUS(IAS)及網路存取保護(NAP)使用者存取要求所產生的事件。這些要求	電腦設定\Windows 設定\安全性設定\	成功	CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Common Settings	234	登入/登出		可以是授與、拒絕、捨棄、隔離、鎖定及解除鎖定 ▪ 如果設定這項原則設定，則會針對每個 IAS 及 NAP 使用者存取要求產生稽核事件。成功稽核會記錄成功的使用者存取要求，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會稽核 IAS 及 NAP 使用者存取要求 ▪ 預設值：成功，失敗	進階稽核原則設定\稽核原則\登入/登出\稽核網路原則伺服器		46843-9
234	Windows Server 2016 Common Settings	TWG CB-01-007-0235	進階稽核原則\登入/登出	稽核 IPsec 主要模式	▪ 這項原則設定決定是否稽核網際網路金鑰交換通訊協定(IKE)及已驗證網際網路通訊協定(AuthIP)在主要模式交涉期間產生的事件 ▪ 如果設定這項原則設定，則會在 IPsec 主要模式交涉期間產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\登入/登出\稽核 IPsec 主要模式	沒有稽核	CCE-ID：CCE-45975-0

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 如果未設定這項原則設定，則不會在 IPsec 主要模式交涉期間產生稽核事件 ▪ 預設值：沒有稽核			
235	Windows Server 2016 Common Settings	TWG CB-01-007-0236	進階稽核原則\登入/登出	稽核其他登入/登出事件	▪ 這項原則設定決定是否稽核「登入/登出」原則設定未涵蓋的其他登入/登出相關事件，例如： ➢ 終端機服務工作階段中斷連線 ➢ 新的終端機服務工作階段 ➢ 鎖定及解除鎖定工作站 ➢ 呼叫螢幕保護裝置 ➢ 解除螢幕保護裝置 ➢ 偵測 Kerberos 重新執行攻擊，在這類攻擊中，會接收到具有相同資訊的 Kerberos 要求兩次。這個狀況可能是網路設定錯誤而造成 ➢ 將無線網路存取權限授與使用者或	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\登入/登出\稽核其他登入/登出事件	沒有稽核	CCE-ID：CCE-46129-3

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					電腦帳戶 ➢將有線 802.1x 網路存取權限授與使用者或電腦帳戶 ▪預設值：沒有稽核			
236	Windows Server 2016 Common Settings	TWG CB-01-007-0237	進階稽核原則\登入/登出	稽核登出	▪這項原則設定決定是否稽核因關閉登入工作階段而產生的事件。這些事件發生於被存取的電腦上。如果是互動式登出，則會在使用者帳戶登入的電腦上產生安全性稽核事件 ▪如果設定這項原則設定，則會在關閉登入工作階段時產生稽核事件。成功稽核會記錄成功關閉工作階段嘗試，而失敗稽核則會記錄失敗關閉工作階段嘗試 ▪如果未設定這項原則設定，則不會在關閉登入工作階段時產生稽核事件 ▪預設值：成功	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\登入/登出\稽核登出	成功	CCE-ID：CCE-46491-7
237	Windows	TWG	進階	稽核登入	▪這項原則設定決定是否稽核因電腦上	電腦設定	成功與失	CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Common Settings	CB-01-007-0238	稽核原則\登入/登出		的使用者帳戶登入嘗試而產生的事件 ▪ 這個子類別中的事件是與建立登入工作階段有關，而且發生在被存取的電腦上。如果是互動式登入，則會在使用者帳戶登入的電腦上產生安全性稽核事件。如果是網路登入(如存取網路上的共用資料夾)，則會在裝載資源的電腦上產生安全性稽核事件。包含下列事件： ➢成功登入嘗試 ➢失敗登入嘗試 ➢使用明確認證的登入嘗試。處理程序嘗試明確指定該帳戶的認證來登入帳戶時，會產生這個事件。這最常發生於批次登入設定(如排定的工作或使用 RUNAS 命令時) ▪ 伺服器版本的預設值：成功，失敗	\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\登入/登出\稽核登入	敗	ID：CCE-45977-6
238	Windows	TWG	進階	稽核	▪ 這項原則設定決定是否稽核網際網路	電腦設定	沒有稽核	CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Common Settings	CB-01-007-0239	稽核原則\登入/登出	IPsec 快速模式	金鑰交換通訊協定(IKE)及已驗證網際網路通訊協定(AuthIP)在快速模式交涉期間產生的事件 ▪ 如果設定這項原則設定，則會在 IPsec 快速模式交涉期間產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在 IPsec 快速模式交涉期間產生稽核事件 ▪ 預設值：沒有稽核	\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\登入/登出\稽核 IPsec 快速模式		ID：CCE-45976-8
239	Windows Server 2016 Common Settings	TWG CB-01-007-0240	進階稽核原則\登入/登出	稽核特殊登入	▪ 這項原則設定決定是否稽核因特殊登入而產生的事件，例如： ➢使用特殊登入，這是具有管理員同等權限而且可以用來將處理程序提高為較高等級的登入 ➢特殊群組成員的登入。特殊群組可稽核特定群組成員登入網路時產生的	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\登入/登出\稽核特殊登入	成功	CCE-ID：CCE-46703-5

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					事件。可以在登錄中設定群組安全性識別碼(SID)清單。如果上述任一 SID 在登入期間被新增至權杖，而且子類別已啟用，則會記錄事件 ▪ 預設值：成功			
240	Windows Server 2016 Common Settings	TWG CB-01-007-0241	進階稽核原則\詳細追蹤	稽核 RPC 事件	▪ 這項原則設定決定是否稽核傳入遠端程序呼叫(RPC)連線 ▪ 如果設定這項原則設定，則會在嘗試遠端 RPC 連線時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在嘗試遠端 RPC 連線時產生稽核事件	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\詳細追蹤\稽核 RPC 事件	沒有稽核	CCE-ID：CCE-46942-9
241	Windows Server 2016 Common	TWG CB-01-007-0242	進階稽核原則\詳細	稽核 DPAPI 活動	▪ 這項原則設定決定是否稽核對資料保護應用程式介面(DPAPI)進行加密或解密要求時產生的事件。DPAPI 是用來保護秘密資訊(如儲存的密碼及金鑰資訊)	電腦設定\Windows 設定\安全性設定\進階稽核原則	沒有稽核	CCE-ID：CCE-4630

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings		追蹤		▪ 如果設定這項原則設定，則會在對 DPAPI 進行加密或解密要求時產生稽核事件。成功稽核會記錄成功要求，而失敗稽核則會記錄失敗要求 ▪ 如果未設定這項原則設定，則不會在對 DPAPI 進行加密或解密要求時產生稽核事件	設定\稽核原則\詳細追蹤\稽核 DPAPI 活動		7-5
242	Windows Server 2016 Common Settings	TWG CB-01-007-0243	進階稽核原則\詳細追蹤	稽核建立處理程序	▪ 這項原則設定決定是否稽核建立或啟動處理程序時產生的事件，也會稽核建立處理程序的應用程式或使用者名稱 ▪ 如果設定這項原則設定，則會在建立處理程序時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在建立處理程序時產生稽核事件	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\詳細追蹤\稽核建立處理程序	成功	CCE-ID：CCE-46177-2
243	Windows	TWG	進階	稽核終止	▪ 這項原則設定決定是否稽核處理程序	電腦設定	沒有稽核	CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Common Settings	CB-01-007-0244	稽核原則\詳細追蹤	處理程序	結束時產生的事件 ▪ 如果設定這項原則設定，則會在處理程序結束時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在處理程序結束時產生稽核事件	\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\詳細追蹤\稽核終止處理程序		ID：CCE-45974-3
244	Windows Server 2016 Common Settings	TWG CB-01-007-0245	Windows 防火牆/網域設定檔	Windows 防火牆：網域設定檔：輸出連線	這項原則設定決定 Windows 防火牆對於輸出連線的預設行為	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\網域設定檔\輸出連線	允許(預設)	CCE-ID：CCE-46484-2

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
245	Windows Server 2016 Common Settings	TWGCB-01-007-0246	Windows 防火牆/網域設定檔	Windows 防火牆：網域設定檔：防火牆狀態	這項原則設定決定是否開啟 Windows 防火牆	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\網域設定檔\防火牆狀態	開啟(建議選項)	CCE-ID：CCE-45982-6
246	Windows Server 2016 Common Settings	TWGCB-01-007-0247	Windows 防火牆/網域設定檔	Windows 防火牆：網域設定檔：輸入連線	這項原則設定決定 Windows 防火牆對於輸入連線的預設行為	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的	封鎖(預設)	CCE-ID：CCE-46649-0

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						Windows 防火牆\內容\網域設定檔\輸入連線		
247	Windows Server 2016 Common Settings	TWG CB-01-007-0248	Windows 防火牆/網域設定檔	Windows 防火牆：網域設定檔：套用本機防火牆規則	這項原則設定決定是否允許套用本機系統管理員所建立的本機防火牆規則	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\網域設定檔\設定\套用本機防火牆規則	是(預設)	CCE-ID：CCE-47201-9
248	Windows Server	TWG CB-01	Windows 防	Windows 防火牆：	這項原則設定決定當程式因為接收輸入連線而被封鎖時，是否為使用者顯示通	電腦設定\Windows 設定	是	CCE-ID：

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 Common Settings	-007-0249	火牆/網域設定檔	網域設定檔：顯示通知	知	\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\網域設定檔\設定\顯示通知		CCE-46308-3
249	Windows Server 2016 Common Settings	TWG CB-01-007-0250	Windows 防火牆/網域設定檔	Windows 防火牆：網域設定檔：套用本機連線安全性規則	這項原則設定決定是否允許套用本機系統管理員所建立的本機連線安全性規則	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\網域	是(預設)	CCE-ID：CCE-46222-6

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						設定檔\設定\套用本機連線安全性規則		
250	Windows Server 2016 Common Settings	TWG CB-01-007-0251	Windows 防火牆/網域設定檔	Windows 防火牆：網域設定檔：允許單點傳播回應	這項原則設定決定此電腦是否接收其傳出之多點傳送或廣播訊息的單點傳送回應	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\網域設定檔\設定\允許單點傳播回應	否	CCE-ID：CCE-46387-7
251	Windows Server 2016	TWG CB-01-007-0	Windows 防火牆/	Windows 防火牆：私人設定	這項原則設定決定是否開啟 Windows 防火牆	電腦設定\Windows 設定\安全性設定\	開啟(建議選項)	CCE-ID：CCE-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
	Common Settings	252	私人設定檔	檔：防火牆狀態		具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\私人設定檔\防火牆狀態		46223-4
252	Windows Server 2016 Common Settings	TWGCB-01-007-0253	Windows 防火牆/私人設定檔	Windows 防火牆：私人設定檔：輸入連線	這項原則設定決定 Windows 防火牆對於輸入連線的預設行為	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\私人設定檔\輸入連	封鎖(預設)	CCE-ID：CCE-46147-5

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
						線		
253	Windows Server 2016 Common Settings	TWGCB-01-007-0254	Windows 防火牆/私人設定檔	Windows 防火牆：私人設定檔：套用本機防火牆規則	這項原則設定決定是否允許套用本機系統管理員所建立的本機防火牆規則	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\私人設定檔\設定\套用本機防火牆規則	是(預設)	CCE-ID：CCE-45983-4
254	Windows Server 2016 Common	TWGCB-01-007-0255	Windows 防火牆/私人設定	Windows 防火牆：私人設定檔：顯示	這項原則設定決定當程式因為接收輸入連線而被封鎖時，是否為使用者顯示通知	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows	是	CCE-ID：CCE-4638

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings		檔	通知		防火牆\具有進階安全性的 Windows 防火牆\內容\私人設定檔\設定\顯示通知		8-5
255	Windows Server 2016 Common Settings	TWG CB-01-007-0256	Windows 防火牆/私人設定檔	Windows 防火牆：私人設定檔：允許單點傳播回應	這項原則設定決定此電腦是否接收其傳出之多點傳送或廣播訊息的單點傳送回應	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\私人設定檔\設定\允許單點傳播回應	否	CCE-ID：CCE-46130-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
256	Windows Server 2016 Common Settings	TWGCB-01-007-0257	Windows 防火牆/私人設定檔	Windows 防火牆：私人設定檔：套用本機連線安全性規則	這項原則設定決定是否允許套用本機系統管理員所建立的本機連線安全性規則	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\私人設定檔\設定\套用本機連線安全性規則	是(預設)	CCE-ID：CCE-46666-4
257	Windows Server 2016 Common Settings	TWGCB-01-007-0258	Windows 防火牆/私人設定檔	Windows 防火牆：私人設定檔：輸出連線	這項原則設定決定 Windows 防火牆對於輸出連線的預設行為	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進	允許(預設)	CCE-ID：CCE-45984-2

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						階安全性的 Windows 防火牆\內容\私人設定檔\輸出連線		
258	Windows Server 2016 Common Settings	TWG CB-01-007-0259	Windows 防火牆/公用設定檔	Windows 防火牆：公用設定檔：允許單點傳播回應	這項原則設定決定此電腦是否接收其傳出之多點傳送或廣播訊息的單點傳送回應	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\公用設定檔\設定\允許單點傳播回應	否	CCE-ID：CCE-46333-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
259	Windows Server 2016 Common Settings	TWGCB-01-007-0260	Windows 防火牆/公用設定檔	Windows 防火牆：公用設定檔：顯示通知	這項原則設定決定當程式因為接收輸入連線而被封鎖時，是否為使用者顯示通知	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\公用設定檔\設定\顯示通知	是	CCE-ID：CCE-46550-0
260	Windows Server 2016 Common Settings	TWGCB-01-007-0261	Windows 防火牆/公用設定檔	Windows 防火牆：公用設定檔：套用本機連線安全性規則	這項原則設定決定是否允許套用本機系統管理員所建立的本機連線安全性規則	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的	是(預設)	CCE-ID：CCE-46408-1

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						Windows 防火牆\內容\公用設定檔\設定\套用本機連線安全性規則		
261	Windows Server 2016 Common Settings	TWG CB-01-007-0262	Windows 防火牆/公用設定檔	Windows 防火牆：公用設定檔：輸入連線	這項原則設定決定 Windows 防火牆對於輸入連線的預設行為	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\公用設定檔\輸入連線	封鎖(預設)	CCE-ID：CCE-46127-7
262	Windows Server	TWG CB-01	Windows 防	Windows 防火牆：	這項原則設定決定是否允許套用本機系	電腦設定\Windows 設定	是(預設)	CCE-ID：

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
	2016 Common Settings	-007-0263	火牆/公用設定檔	公用設定檔：套用本機防火牆規則	統管理員所建立的本機防火牆規則	\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\公用設定檔\設定\套用本機防火牆規則		CCE-46867-8
263	Windows Server 2016 Common Settings	TWGCB-01-007-0264	Windows 防火牆/公用設定檔	Windows 防火牆：公用設定檔：輸出連線	這項原則設定決定 Windows 防火牆對於輸出連線的預設行為	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火	允許(預設)	CCE-ID：CCE-46653-2

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						牆\內容\公用設定檔\輸出連線		
264	Windows Server 2016 Common Settings	TWG CB-01-007-0265	Windows 防火牆/公用設定檔	Windows 防火牆：公用設定檔：防火牆狀態	這項原則設定決定是否開啟 Windows 防火牆	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\公用設定檔\防火牆狀態	開啟(建議選項)	CCE-ID：CCE-46891-8
265	Windows Server 2016 Common	TWG CB-01-007-0	系統管理範本/RSS	防止下載隨函附件	▪ 這項原則設定可防止使用者從摘要下載隨函附件(檔案附件)到使用者的電腦 ▪ 如果啟用這項原則設定，使用者將無法	電腦設定\系統管理範本\Windows 元件\RSS 摘要\防	已啟用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings	266	摘要		透過「摘要」內容頁將 Feed Sync Engine 設成下載隨函附件。開發人員無法透過「摘要」API 來變更下載設定 ▪ 如果停用或未設定這項原則設定，使用者可以透過「摘要」內容頁來設定 Feed Sync Engine 下載隨函附件。開發人員可以透過「摘要 API」來變更下載設定	止下載隨函附件		
266	Windows Server 2016 Common Settings	TWG CB-01-007-0267	系統管理範本/Windows Defender	加入 Microsoft 地圖	▪ 這項原則設定決定是否加入 Microsoft MAPS。Microsoft MAPS 是協助使用者選擇如何回應潛在威脅的線上社群。這個社群也可協助停止散佈新惡意軟體的感染 ▪ 可以選擇傳送偵測到之軟體的基本或其他資訊。額外的資訊可協助 Microsoft 建立新的定義，以協助它保護使用者的電腦。這項資訊可能包含移除有害軟體後，偵測到的項目在電腦上的位置。這個資訊會被自動蒐集與傳送。在某些情	電腦設定\系統管理範本\Windows 元件\Windows Defender\MAPS\加入 Microsoft 地圖	已停用	CCE-ID：CCE-45565-9

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					況下，可能會意外將個人資訊傳送給 Microsoft。不過，Microsoft 不會使用這些資訊來識別使用者的身分或與使用者聯繫 ▪ 可能的選項為： ➢(0x0)已停用(預設) ➢(0x1)基本成員資格 ➢(0x2)進階成員資格 ▪ 基本成員資格將會傳送有關偵測到之軟體的基本資訊給 Microsoft，包括軟體來源、使用者採取的動作或自動採取的動作，以及這些動作是否成功 ▪ 進階成員資格除了基本資訊之外，還會將更多有關惡意軟體、間諜軟體以及潛在的垃圾軟體的資訊傳送給 Microsoft，包括軟體位置、檔案名稱、軟體運作方式，以及對電腦的影響			

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 如果啟用這項設定，將以指定的成員資格加入 Microsoft MAPS ▪ 如果停用或未設定這項設定，將不會加入 Microsoft MAPS			
267	Windows Server 2016 Common Settings	TWG CB-01-007-0268	系統管理範本/Windows 遠端管理(WinRM)	不允許摘要式驗證	▪ 這項原則設定可管理 Windows 遠端管理(WinRM)用戶端是否使用摘要式驗證 ▪ 如果啟用這項原則設定，WinRM 用戶端不會使用摘要式驗證 ▪ 如果停用或未設定這項原則設定，WinRM 用戶端會使用摘要式驗證	電腦設定\系統管理範本\Windows 元件\Windows 遠端管理(WinRM)\WinRM 用戶端\不允許摘要式驗證	已啟用	CCE-ID：CCE-46014-7
268	Windows Server 2016 Common	TWG CB-01-007-0269	系統管理範本/Wind	允許未加密的流量	▪ 這項原則設定可管理 Windows 遠端管理(WinRM)用戶端是否透過網路傳送與接收未加密的訊息 ▪ 如果啟用這項原則設定，WinRM 用戶	電腦設定\系統管理範本\Windows 元件\Windows 遠端	已停用	CCE-ID：CCE-4637

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings		ows 遠端管理 (WinRM)		端會透過網路傳送與接收未加密的訊息 ▪ 如果停用或未設定這項原則設定，WinRM 用戶端只會透過網路傳送或接收加密的訊息	管理 (WinRM)\WinRM 用戶端\允許未加密的流量		8-6
269	Windows Server 2016 Common Settings	TWG CB-01-007-0270	系統管理範本/Windows 遠端管理 (WinRM)	允許基本驗證	▪ 這項原則設定可管理 Windows 遠端管理(WinRM)用戶端是否使用基本驗證 ▪ 如果啟用這項原則設定，WinRM 用戶端會使用基本驗證。如果將 WinRM 設定為使用 HTTP 傳輸，使用者名稱及密碼就會以純文字在網路上傳送 ▪ 如果停用或未設定這項原則設定，WinRM 用戶端不會使用基本驗證	電腦設定\系統管理範本\Windows 元件\Windows 遠端管理 (WinRM)\WinRM 用戶端\允許基本驗證	已停用	CCE-ID：CCE-46295-2
270	Windows Server 2016	TWG CB-01-007-0	系統管理範本	不允許 WinRM 儲存	▪ 這項原則設定可管理 Windows 遠端管理(WinRM)服務是否不允許儲存任何外掛程式的 RunAs 認證	電腦設定\系統管理範本\Windows 元件	已啟用	CCE-ID：CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Common Settings	271	/Windows 遠端管理(WinRM)	RunAs 認證	▪ 如果啟用這項原則設定，WinRM 服務將不允許任何外掛程式設定 RunAsUser 或 RunAsPassword 設定值。如果外掛程式已經設定 RunAsUser 及 RunAsPassword 設定值，則會從這部電腦的認證儲存區刪除 RunAsPassword 設定值 ▪ 如果停用或未設定這項原則設定，WinRM 服務將允許外掛程式設定 RunAsUser 與 RunAsPassword 設定值，而且可安全地儲存 RunAsPassword 值 ▪ 如果啟用後又停用這項原則設定，必須重設先前設定的所有 RunAsPassword 值	\Windows 遠端管理(WinRM)\WinRM 服務\不允許 WinRM 儲存 RunAs 認證		46708-4
271	Windows Server 2016 Common Settings	TWG CB-01-007-0272	系統管理範本/Windows 遠	允許未加密的流量	▪ 這項原則設定可管理 Windows 遠端管理(WinRM)服務是否透過網路傳送與接收未加密的訊息 ▪ 如果啟用這項原則設定，WinRM 用戶端會透過網路傳送與接收未加密的訊	電腦設定\系統管理範本\Windows 元件\Windows 遠端管理	已停用	CCE-ID：CCE-45060-1

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
			端管理(WinRM)		息 ▪ 如果停用或未設定這項原則設定，WinRM 用戶端只會透過網路傳送或接收加密的訊息	(WinRM)\WinRM 服務\允許未加密的流量		
272	Windows Server 2016 Common Settings	TWGCB-01-007-0273	系統管理範本/Windows 遠端管理(WinRM)	允許基本驗證	▪ 這項原則設定可管理 Windows 遠端管理(WinRM)服務是否接受來自遠端用戶端的基本驗證 ▪ 如果啟用這項原則設定，WinRM 服務會接受來自遠端用戶端的基本驗證 ▪ 如果停用或未設定這項原則設定，WinRM 服務不會接受來自遠端用戶端的基本驗證	電腦設定\系統管理範本\Windows 元件\Windows 遠端管理(WinRM)\WinRM 服務\允許基本驗證	已停用	CCE-ID：CCE-45061-9
273	Windows Server 2016 Common	TWGCB-01-007-0274	系統管理範本/定位	關閉定位	▪ 這項原則設定決定是否關閉這部電腦的定位功能 ▪ 如果啟用這項原則設定，將會關閉定位功能，而且這部電腦的所有程式都將無	電腦設定\系統管理範本\Windows 元件\定位和感應器	已啟用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings		和感應器		法使用定位功能的位置資訊 ▪ 如果停用或未設定這項原則設定，則這部電腦的所有程式都不會被禁止使用定位功能的位置資訊	\關閉定位		
274	Windows Server 2016 Common Settings	TWG CB-01-007-0275	系統管理範本/認證使用者介面	不要顯示密碼顯示按鈕	▪ 這項原則設定可設定當使用者輸入密碼時，是否顯示密碼顯示按鈕 ▪ 如果啟用這項原則設定，當使用者在密碼輸入文字方塊中輸入密碼後，就不會顯示密碼顯示按鈕 ▪ 如果停用或未設定這項原則設定，當使用者在密碼輸入文字方塊中輸入密碼後，會顯示密碼顯示按鈕 ▪ 根據預設，使用者在密碼輸入文字方塊中輸入密碼後，會顯示密碼顯示按鈕。若要顯示密碼，按一下密碼顯示按鈕 ▪ 這項原則適用於所有使用 Windows 系統控制項的 Windows 元件與應用程	電腦設定\系統管理範本\Windows 元件\認證使用者介面\不要顯示密碼顯示按鈕	已啟用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					式，包含 Internet Explorer			
275	Windows Server 2016 Common Settings	TWG CB-01-007-0276	系統管理範本/認證使用者介面	提升權限時列舉系統管理員帳戶	▪ 這項原則設定可以控制當使用者嘗試以提升的權限執行應用程式時，是否要顯示系統管理員帳戶。根據預設，當使用者嘗試以提升的權限執行應用程式時，不會顯示系統管理員帳戶 ▪ 如果啟用這項原則設定，會顯示電腦上的所有本機系統管理員帳戶，讓使用者可以選擇系統管理員帳戶並輸入正確的密碼 ▪ 如果停用這項原則設定，每次提升權限時都會要求使用者輸入使用者名稱與密碼	電腦設定\系統管理範本\Windows 元件\認證使用者介面\提升權限時列舉系統管理員帳戶	已停用	
276	Windows Server 2016 Common	TWG CB-01-007-0277	系統管理範本/檔案	設定 Windows SmartScreen 篩選工	▪ 這項原則設定可管理 Windows SmartScreen 篩選工具的行為 ▪ Windows SmartScreen 篩選工具會在執行從網際網路下載且無法辨識的程式	電腦設定\系統管理範本\Windows 元件\檔案總管\設	已啟用	CCE-ID：CCE-4488

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Settings		總管	具	之前警告使用者，使電腦更加安全。啟用此功能時，會將檔案以及在電腦上執行之程式的某些資訊傳送給 Microsoft ▪ 若啟用這項原則設定，可以透過設定下列其中一個選項來控制 Windows SmartScreen 篩選工具的行為： ➢ 在執行已下載的不明軟體之前對使用者提出警告 ➢ 關閉 SmartScreen 篩選工具 ▪ 若停用或未設定這項原則設定，電腦的系統管理員可以使用「安全性與維護」中的「Windows SmartScreen 篩選工具設定」來管理 Windows SmartScreen 篩選工具的行為	定 Windows SmartScreen 篩選工具		4-5
277	Windows Server 2016	TWG CB-01-007-0	系統管理範本/	損毀時關閉終止堆集	▪ 這項原則設定決定損毀時是否關閉終止堆集 ▪ 損毀時關閉終止堆集可讓特定的舊版	電腦設定\系統管理範本\Windows 元件	已停用	CCE-ID：CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Common Settings	278	檔案總管		外掛應用程式不需立即中止檔案總管即可運作，雖然檔案總管稍後可能仍會無預期地終止	\檔案總管\損毀時關閉終止堆集		47028-6
278	Windows Server 2016 Common Settings	TWG CB-01-007-0279	系統管理範本/檔案總管	關閉殼層通訊協定受保護模式	▪ 這項原則設定能夠設定殼層通訊協定可以擁有的功能數量。當使用這個通訊協定的完整功能時，應用程式可以開啟資料夾並且啟動檔案。受保護模式會降低這個通訊協定的功能，只允許應用程式開啟一組有限的資料夾。處於受保護模式時，應用程式無法以這個通訊協定開啟檔案。建議讓這個通訊協定處於受保護模式，以提高 Windows 的安全性 ▪ 如果啟用這項原則設定，則會完整啟用通訊協定，允許開啟資料夾及檔案 ▪ 如果停用這項原則設定，則通訊協定處於受保護模式，只允許應用程式開啟一組有限的資料夾 ▪ 如果未設定這項原則設定，通訊協定將	電腦設定\系統管理範本\Windows 元件\檔案總管\關閉殼層通訊協定受保護模式	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					會處於受保護模式，只允許應用程式開啟一組有限的資料夾			
279	Windows Server 2016 Common Settings	TWG CB-01-007-0280	系統管理範本/檔案總管	關閉檔案總管的資料執行防止	▪ 這項原則設定決定是否關閉檔案總管的資料執行防止功能 ▪ 停用資料執行防止可使某些舊版的外掛應用程式不需終止檔案總管即可執行	電腦設定\系統管理範本\Windows 元件\檔案總管\關閉檔案總管的資料執行防止	已停用	CCE-ID：CCE-45876-0
280	Windows Server 2016 Common Settings	TWG CB-01-007-0281	系統管理範本/開機初期啟動的反惡意程式	開機啟動驅動程式初始化原則	▪ 這項原則設定允許根據開機初期啟動的反惡意程式碼開機啟動驅動程式所判斷的分類，指定要初始化哪些開機啟動驅動程式。開機初期啟動的反惡意程式碼開機啟動驅動程式可以針對每個開機啟動驅動程式傳回下列分類： ➢ 良好：驅動程式已經過簽署，且未遭竄改 ➢ 不良：驅動程式已被識別為惡意程式	電腦設定\系統管理範本\系統\開機初期啟動的反惡意程式碼\開機啟動驅動程式初始化原則	已啟用：良好和不明	CCE-ID：CCE-44468-7

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
			碼		碼。建議不要初始化已知的不良驅動程式 ➢不良，但為開機所需：驅動程式已被識別為惡意程式碼，但電腦必須載入此驅動程式才能成功開機 ➢不明：此驅動程式尚未經由惡意程式碼偵測應用程式保證，也尚未經由開機初期啟動的反惡意程式碼開機啟動驅動程式分類 ▪ 如果啟用這項原則設定，可以選擇下次電腦啟動時要初始的啟動開機驅動程式 ▪ 如果停用或未設定這項原則設定，便會初始化判斷為「良好」、「不明」或「不良，但為開機關鍵」的開機啟動驅動程式，但不會初始判斷為「不良」的驅動程式			

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
281	Windows Server 2016 Common Settings	TWG CB-01-007-0282	系統管理範本/睡眠設定	喚醒電腦時必須使用密碼(一般電源)	▪ 這項原則設定可指定系統從睡眠狀態中恢復時，是否會提示使用者輸入密碼 ▪ 如果啟用或未設定這項原則設定，當系統從睡眠狀態中恢復時，就會提示使用者輸入密碼 ▪ 如果停用這項原則設定，當系統從睡眠狀態中恢復時，就不會提示使用者輸入密碼	電腦設定\系統管理範本\系統\電源管理\睡眠設定\喚醒電腦時必須使用密碼(一般電源)	已啟用	
282	Windows Server 2016 Common Settings	TWG CB-01-007-0283	系統管理範本/睡眠設定	喚醒電腦時必須使用密碼(使用電池)	▪ 這項原則設定可指定系統從睡眠狀態中恢復時，是否會提示使用者輸入密碼 ▪ 如果啟用或未設定這項原則設定，當系統從睡眠狀態中恢復時，就會提示使用者輸入密碼 ▪ 如果停用這項原則設定，當系統從睡眠狀態中恢復時，就不會提示使用者輸入密碼	電腦設定\系統管理範本\系統\電源管理\睡眠設定\喚醒電腦時必須使用密碼(使用電池)	已啟用	
283	Windows	TWG	系統	Microsoft	▪ 這項原則設定會設定 Microsoft 支援服	電腦設定\系統	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Common Settings	CB-01-007-0284	管理範本/疑難排解與診斷	支援服務診斷工具：開啟 MSDT 與支援提供者的互動式通訊	務診斷工具(MSDT)與支援提供者的互動式通訊。MSDT 會蒐集診斷資料，供專業支援人員進行分析 ▪ 如果啟用這項原則設定，使用者可以使用 MSDT 蒐集診斷資料，並將該資料傳送給支援專業人員以解決問題 ▪ 支援提供者預設為 Microsoft Corporation ▪ 如果停用這項原則設定，MSDT 無法以支援模式執行，而且不會蒐集任何資料，或傳送給支援提供者 ▪ 如果未設定這項原則設定，則預設會啟用 MSDT 支援模式 ▪ 這項原則設定不需重新開機或重新啟動服務就會生效。變更會立即生效	管理範本\系統\疑難排解與診斷\Microsoft 支援服務診斷工具\Microsoft 支援服務診斷工具：開啟 MSDT 與支援提供者的互動式通訊		
284	Windows Server	TWG CB-01	系統管理	啟用/停用 PerfTrack	▪ 這項原則設定會指定要啟用或停用回應事件的追蹤	電腦設定\系統管理範本\系統	已停用	

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
	2016 Common Settings	-007-0285	範本/疑難排解與診斷		▪ 如果啟用這項原則設定，就會處理並彙總回應事件。彙總的資料會透過 SQM 傳到 Microsoft ▪ 如果停用這項原則設定，就不會處理回應事件 ▪ 如果未設定這項原則設定，診斷原則服務(Diagnostic Policy Service)預設會啟用 Windows 效能 PerfTrack	\疑難排解與診斷\Windows 效能 PerfTrack\啟用/停用 PerfTrack		
285	Windows Server 2016 Common Settings	TWGCB-01-007-0286	系統管理範本/遠端協助	設定提供遠端協助	▪ 這項原則設定可以在這部電腦上開啟或關閉「提供(未經要求)遠端協助」 ▪ 如果啟用這項原則設定，這部電腦上的使用者可使用「提供(未經要求)遠端協助」，從公司的技術支援團隊取得協助 ▪ 如果停用這項原則設定，這部電腦上的使用者無法使用「提供(未經要求)遠端協助」，從公司的技術支援團隊取得協助	電腦設定\系統管理範本\系統\遠端協助\設定提供遠端協助	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 如果未設定這項原則設定，這部電腦上的使用者無法使用「提供(未經要求)遠端協助」，從公司的技術支援團隊取得協助			
286	Windows Server 2016 Common Settings	TWG CB-01-007-0287	系統管理範本/遠端協助	設定請求遠端協助	▪ 這項原則設定可以在這部電腦上開啟或關閉「請求(要求)遠端協助」 ▪ 如果啟用這項原則設定，這部電腦上的使用者即可使用電子郵件或檔案傳輸來要求他人協助。此外，使用者可以使用立即訊息程式，讓他人可以連線到這部電腦，也可以設定其他遠端協助設定 ▪ 如果停用這項原則設定，這部電腦上的使用者無法使用電子郵件或檔案傳輸來要求他人協助。此外，使用者無法使用立即訊息程式允許他人連線到這部電腦 ▪ 如果未設定這項原則設定，使用者可以在「控制台」的「系統內容」中自行開	電腦設定\系統管理範本\系統\遠端協助\設定請求遠端協助	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					啟或關閉「請求(要求)遠端協助」。使用者也可以設定遠端協助設定 ▪ 如果啟用這項原則設定，有兩種方法可以讓協助人員提供遠端協助：「只允許協助人員檢視電腦」或「允許協助人員從遠端控制電腦」 ▪ 「票證時間最大值」原則設定可設定使用電子郵件或檔案傳輸所建立的遠端協助邀請可維持開啟的時間限制 ▪ 「選擇傳送電子郵件邀請的方法」設定可指定傳送遠端協助邀請時，要使用何種電子郵件標準。視電子郵件程式而定，可以使用 Mailto 標準(透過網際網路連結連接的邀請收件者)或 SMAPI(Simple MAPI)標準(附加至電子郵件訊息的邀請)。這項原則設定在 Windows Vista 中無法使用，因為 SMAPI 是唯一支援的方法			

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 如果啟用這項原則設定，也應該啟用適當的防火牆例外，以允許遠端協助通訊			
287	Windows Server 2016 Common Settings	TWG CB-01-007-0288	系統管理範本/Microsoft 對等網路服務	關閉 Microsoft 對等網路服務	▪ 這項原則設定決定是否完全關閉 Microsoft 對等網路服務，並導致所有依存的應用程式停止運作 ▪ 對等通訊協定允許 RTC、協同作業、內容發布與分散式處理等領域的應用程式 ▪ 如果啟用此設定，將會關閉對等通訊協定 ▪ 如果停用或沒有進行此設定，將會開啟對等通訊協定	電腦設定\系統管理範本\網路\Microsoft 對等網路服務\關閉 Microsoft 對等網路服務	已啟用	
288	Windows Server 2016 Common Settings	TWG CB-01-007-0289	系統管理範本/Windows	使用 Windows Connect Now 進行無線設定	▪ 這項原則設定允許使用 Windows Connect Now(WCN)進行無線設定。WCN 登錄器可經由 Windows 可攜式裝置 API(WPD)與 USB 快閃磁碟機，尋找設定乙太網路(UPnP)與頻內 802.11	電腦設定\系統管理範本\網路\Windows Connect Now\使用 Windows	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
			Connect Now		WLAN 上的裝置 ▪ 其他選項則允許在特定媒體上進行搜索與設定 ▪ 若啟用這項原則設定，會有額外選項可以關閉特定媒體上的操作 ▪ 若停用這項原則設定，會停用所有媒體上的操作 ▪ 若未設定這項原則設定，會啟用所有媒體上的操作 ▪ 這項原則設定的預設值可允許所有媒體上的操作	Connect Now 進行無線設定		
289	Windows Server 2016 Common Settings	TWG CB-01-007-0290	系統管理範本/Windows Conne	禁止存取 Windows Connect Now 精靈	▪ 這項原則設定決定是否禁止存取 Windows Connect Now(WCN)精靈 ▪ 如果啟用這項原則設定，就會關閉精靈，使用者會無法存取任何精靈工作。所有與設定相關的工作，包含「設定無線路由器或存取點」與「新增無線裝置」	電腦設定\系統管理範本\網路\Windows Connect Now\禁止存取 Windows	已啟用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
			ct Now		都會被停用 ▪ 如果停用或未設定這項原則設定，使用者可存取精靈工作，包含「設定無線路由器或存取點」與「新增無線裝置」。根據預設，這項原則設定會允許使用者存取所有的 WCN 精靈	Connect Now 精靈		
290	Windows Server 2016 Common Settings	TWG CB-01-007-0291	系統管理範本/連結階層拓樸搜索	開啟 Mapper I/O(LLTDIO)驅動程式	▪ 這項原則設定決定是否變更 Mapper I/O 網路通訊協定驅動程式的操作行為 ▪ LLTDIO 允許電腦搜索其連線網路的拓撲。也允許電腦起始服務品質(Quality-of-Service)要求，例如頻寬估計與網路狀態分析 ▪ 如果啟用這項原則設定，可以使用其他選項來微調選取項目。可以選擇「允許在網域中操作」選項，以允許 LLTDIO 在連線到受管理網路的網路介面上操作。另一方面，如果網路介面連線到未受管理的網路，就可以改為選擇「允許	電腦設定\系統管理範本\網路\連結階層拓樸搜索\開啟 Mapper I/O(LLTDIO)驅動程式	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					在公用網路中操作」與「禁止在私人網路中操作」 ▪ 如果停用或未設定這項原則設定，將套用 LLTDIO 的預設行為			
291	Windows Server 2016 Common Settings	TWG CB-01-007-0292	系統管理範本/連結階層拓樸搜索	開啟 Responder (RSPNDR)驅動程式	▪ 這項原則設定決定是否變更 Responder 網路通訊協定驅動程式的操作行為 ▪ Responder 允許電腦加入「連結階層拓撲搜索」要求，以便能在網路上搜索並找到該電腦。也允許電腦加入服務品質(Quality-of-Service)活動，例如頻寬估計與網路狀態分析 ▪ 如果啟用這項原則設定，可以使用其他選項來微調選取項目。可以選擇「允許在網域中操作」選項，以允許 Responder 在連線到受管理網路的網路介面上操作。另一方面，如果網路介面連線到未受管理的網路，就可以改為選擇「允許在公用網路中操作」與「禁止在私人網	電腦設定\系統管理範本\網路\連結階層拓樸搜索\開啟 Responder(RSPNDR)驅動程式	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					路中操作」 ▪ 如果停用或未設定這項原則設定，將套用 Responder 的預設行為			
292	Windows Server 2016 Common Settings	TWG CB-01-007-0293	系統管理範本/網路連線	要求網域使用者在設定網路的位置時必須提升權限	▪ 這項原則設定會決定是否要求網域使用者在設定網路的位置時必須提升權限 ▪ 如果啟用這項原則設定，網域使用者在設定網路的位置時必須提升權限 ▪ 如果停用或未設定這項原則設定，則網域使用者不必提升權限就可以設定網路的位置	電腦設定\系統管理範本\網路\網路連線\要求網域使用者在設定網路的位置時必須提升權限	已啟用	
293	Windows Server 2016 Common Settings	TWG CB-01-007-0294	系統管理範本/網路連線	禁止在您的 DNS 網域網路上安裝、設定及使用網路橋接	▪ 這項原則設定決定使用者是否可以安裝及設定網路橋接器 ▪ 注意：這項設定與位置有關。只有當電腦連線到原先在該電腦上更新設定時所連線的相同 DNS 網域網路時，才會套用這項設定。如果更新設定之後，電	電腦設定\系統管理範本\網路\網路連線\禁止在您的 DNS 網域網路上安裝、設定及使	已啟用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					腦又連線到其他不同的 DNS 網域網路，這項設定就不會生效 ▪ 網路橋接器可以讓使用者建立層級 2 MAC 橋接器，而啟用橋接器可以將兩個(含)以上的網路區段連在一起。這個連線會出現在「網路連線」資料夾中 ▪ 如果停用或沒有進行此設定，則使用者可以建立並修改網路橋接器的設定。啟用這項設定並不會從使用者的電腦移除現存的網路橋接器	用網路橋接		
294	Windows Server 2016 Common Settings	TWG CB-01-007-0295	系統管理範本/通知	在鎖定畫面上關閉快顯通知	▪ 這項原則設定決定是否在鎖定畫面上關閉快顯通知 ▪ 如果啟用這項原則設定，應用程式將無法在鎖定畫面上引發快顯通知 ▪ 如果停用或未設定這項原則設定，則可在鎖定畫面上啟用快顯通知，並可讓系統管理員或使用者關閉通知	使用者設定\系統管理範本\「開始」功能表和工作列\通知\在鎖定畫面上關閉快顯通知	已啟用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 這項原則設定不需重新開機或重新啟動服務就會生效			
295	Windows Server 2016 Common Settings	TWG CB-01-007-0296	系統管理範本/Windows Media Player	防止轉碼器下載	▪ 這項原則設定可防止 Windows Media Player 下載轉碼器 ▪ 如果啟用這項原則設定，會防止 Player 自動將轉碼器下載至電腦。此外，Player 中「播放程式」索引標籤上的「自動下載轉碼器」核取方塊也無法使用 ▪ 如果停用這項原則設定，轉碼器會自動下載，且無法使用「自動下載轉碼器」核取方塊 ▪ 如果未設定這項原則設定，使用者可以變更「自動下載轉碼器」核取方塊的設定	使用者設定\系統管理範本\Windows 元件\Windows Media Player\播放\防止轉碼器下載	已啟用	
296	Windows Server 2016	TWG CB-01-007-0	系統管理範本/	不要保留檔案附件的區域資	▪ 這項原則設定可以管理 Windows 是否用資訊的來源區域來標示附件檔案(例如，受限、網際網路、內部網路、本機)。	使用者設定\系統管理範本\Windows 元件	已停用	CCE-ID：CCE-

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
	Common Settings	297	附件管理員	訊	這必須透過 NTFS 才能正確運作，在 FAT32 上會失敗，不會另外通知。如果沒有保留區域資訊，Windows 無法正確評定風險 ▪ 如果啟用這項原則設定，Windows 就不會標示附件檔案的區域資訊 ▪ 如果停用這項原則設定，Windows 會標示附件檔案的區域資訊 ▪ 如果未設定這項原則設定，Windows 會標示附件檔案的區域資訊	\附件管理員\不要保留檔案附件的區域資訊		45128-6
297	Windows Server 2016 Common Settings	TWGCB-01-007-0298	系統管理範本/附件管理員	開啟附件時通知防毒程式	▪ 這項原則設定可管理已登錄防毒程式的通知行為。如果已登錄多種程式，將會全部通知。如果已登錄的防毒程式已經執行即時檢查或即時掃描傳送到電腦的電子郵件伺服器上的所有檔案，任何其他呼叫都是多餘的 ▪ 如果啟用這項原則設定，Windows 會命	使用者設定\系統管理範本\Windows 元件\附件管理員\開啟附件時通知防毒程式	已啟用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					令已登錄的防毒程式在使用者開啟附件檔案時掃描該檔案。如果防毒程式失敗，將無法開啟附件 ▪ 如果停用這項設定，Windows 就不會在開啟附件檔案時呼叫已登錄防毒程式 ▪ 如果未設定這項設定，Windows 就不會在開啟附件檔案時呼叫已登錄防毒程式			
298	Windows Server 2016 Common Settings	TWG CB-01-007-0299	系統管理範本/網路共用	防止使用者共用其設定檔內的檔案	▪ 這項原則設定會指定使用者是否可以共用設定檔內的檔案。根據預設，系統管理員在電腦中加以選擇之後，便允許使用者與其網路上的其他使用者共用他們設定檔內的檔案。系統管理員可以使用共用精靈，在電腦上進行選擇，以共用使用者設定檔內的檔案 ▪ 如果啟用這項原則設定，使用者將不能使用共用精靈，來共用其設定檔內的檔案。 同時，共用精靈也不會在	使用者設定\系統管理範本\Windows 元件\網路共用\防止使用者共用其設定檔內的檔案	已啟用	CCE-ID：CCE-45608-7

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					%root%users 上建立共用，而且該精靈只可用來在資料夾上建立 SMB 共用 ▪ 如果停用或未設定這項原則設定，系統管理員在電腦中加以選擇之後，使用者便可共用其使用者設定檔中的檔案			
299	Windows Server 2016 Common Settings	TWG CB-01-007-0691	系統管理範本\MS Security Guide	Enable Structured Exception Handling Overwrite Protection (SEHOP)	▪ 這項原則設定決定是否啟用結構化例外處理覆防寫(SEHOP)之保護機制 ▪ SEHOP 保護機制用於封鎖運用結構化例外處理常式(SEH)覆寫技術之入侵，由於此保護機制是在執行階段提供，因此無論應用程式是否已使用最新的改進功能進行編譯，都有助於保護應用程式 ▪ 如果啟用這項原則設定，將啟用 SEHOP 保護機制 ▪ 如果停用或未設定這項原則設定，將停用 SEHOP 保護機制	電腦設定\系統管理範本\MS Security Guide\Enable Structured Exception Handling Overwrite Protection (SEHOP)	已啟用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪若須於本機群組原則編輯器(Gpedit.msc)或群組原則管理(Gpmc.msc)等工具中顯示這項原則設定，請安裝 1703 以上版本之 SecGuide 系統管理範本			
300	Windows Server 2016 Common Settings	TWG CB-01-007-0692	系統管理範本\Microsoft 帳戶	封鎖所有消費者 Microsoft 帳戶使用者驗證	▪這項原則設定控制使用者是否能透過提供 Microsoft 帳戶，進行應用程式或服務的身分驗證 ▪如果啟用這項設定，此裝置上所有應用程式與服務，將無法透過 Microsoft 帳戶進行身分驗證 ▪這項設定同時適用於裝置目前的使用者以及可能新增的新使用者，但是對於已驗證使用者的應用程式或服務，在身分快取驗證過期前，啟用這項設定將不會造成任何影響 ▪建議在任何使用者登入裝置前啟用這	電腦設定\系統管理範本\Windows 元件\Microsoft 帳戶\封鎖所有消費者 Microsoft 帳戶使用者驗證	已啟用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					項設定，可避免快取權杖出現 ▪如果停用或未設定這項設定，應用程式與服務可以使用 Microsoft 帳戶進行身分驗證 ▪在預設情況下，這項設定將被停用 ▪注意：這項設定不影響使用者是否能透過 Microsoft 帳戶登入裝置，或使用者透過瀏覽器提供 Microsoft 帳戶以進行 Web 架構應用程式身分驗證之能力 ▪若須於本機群組原則編輯器(Gpedit.msc)或群組原則管理(Gpmc.msc)等工具中顯示這項原則設定，請安裝 1703 以上版本之 MSAPolicy 系統管理範本			
301	Windows Server 2016	TWG CB-01-007-0	系統管理範本\	允許簡訊服務雲端同步	▪這項原則設定決定是否允許將行動數據簡訊備份及還原到 Microsoft 雲端服務	電腦設定\系統管理範本\Windows 元件	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Common Settings	693	訊息中心		▪如果啟用這項設定，則允許簡訊服務雲端同步 ▪如果停用這項設定，則不允許簡訊服務雲端同步 ▪若須於本機群組原則編輯器(Gpedit.msc)或群組原則管理(Gpmc.msc)等工具中顯示這項原則設定，請安裝 1709 以上版本之 Messaging 系統管理範本	\訊息中心\允許簡訊服務雲端同步		
302	Windows Server 2016 Common Settings	TWG CB-01-007-0694	系統管理範本/遠端桌面服務	需要對遠端(RDP)連線使用特定的安全層	▪這項原則設定決定在遠端桌面通訊協定(RDP)連線期間，是否必須使用特定的安全性階層，來確保用戶端與遠端桌面工作階段主機伺服器之間的通訊安全 ▪如果啟用這項原則設定，在遠端連線期間，用戶端與遠端桌面工作階段主機伺服器之間的所有通訊都必須使用這項設定中指定的安全性方法，可用之安全	電腦設定\系統管理範本\Windows 元件\遠端桌面服務\遠端桌面工作階段主機\安全性\需要對遠端(RDP)連線使用特定的安全	已啟用：SSL	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					性方法如下： ➢交涉：交涉方法會強制執行用戶端支援的最安全方法。如果支援傳輸層安全性(TLS)，就使用 TLS 來驗證遠端桌面工作階段主機伺服器。如果不支援 TLS，則使用原始遠端桌面通訊協定(RDP)加密來確保通訊安全，但不會驗證遠端桌面工作階段主機伺服器 ➢RDP：RDP 方法會使用原始 RDP 加密，確保用戶端與遠端桌面工作階段主機伺服器之間的通訊安全。如果選取這項設定，就不會驗證遠端桌面工作階段主機伺服器 ➢SSL：必須使用 TLS 來驗證遠端桌面工作階段主機伺服器。如果不支援 TLS，連線會失敗 ▪如果停用或未設定這項原則設定，則不	層		

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					會在群組原則層級指定遠端桌面工作階段主機伺服器在遠端連線所要使用的安全性方法			
303	Windows Server 2016 Common Settings	TWG CB-01-007-0695	系統管理範本/遠端桌面服務	透過使用網路層級驗證以要求對遠端連線進行使用者驗證	▪這項原則設定決定是否要使用網路層級驗證來對連至遠端桌面工作階段主機伺服器的遠端連線要求使用者驗證。此原則設定要求使用者驗證在遠端連線處理程序初期執行，以增強安全性 ▪如果啟用這項原則設定，只有支援網路層級驗證的用戶端電腦能夠連線到遠端桌面工作階段主機伺服器，若要判斷用戶端電腦是否支援網路層級驗證，請在用戶端電腦上啟動「遠端桌面連線」，按一下「遠端桌面連線」對話方塊左上角的圖示，然後按一下「關於」。在「關於遠端桌面連線」對話方塊中，尋找是否出現「支援網路層級驗證」 ▪如果停用這項原則設定，則在允許遠端	電腦設定\系統管理範本\Windows 元件\遠端桌面服務\遠端桌面工作階段主機\安全性\透過使用網路層級驗證以要求對遠端連線進行使用者驗證	已啟用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					連線到遠端桌面工作階段主機伺服器之前，不必使用網路層級驗證進行使用者驗證 ▪如果未設定這項原則設定，則將強制執行目標電腦上的本機設定 ▪注意：停用這項原則設定將提供較低的安全性，因為使用者驗證將在遠端連線處理程序後期執行			
304	Windows Server 2016 Common Settings	TWG CB-01-007-0696	系統管理範本/認證委派	加密預示修復	▪這項原則設定適用於使用 CredSSP 元件(例如：遠端桌面連線)之應用程式 ▪CredSSP 通訊協定某些版本有弱點，容易受到針對用戶端的加密 Oracle 攻擊所威脅 ▪這項原則會控制易受攻擊的用戶端與伺服器之相容性，可讓使用者設定加密 Oracle 弱點所需的保護層級 ▪如果啟用這項原則設定，就會依據下列	電腦設定\系統管理範本\系統\認證委派\加密預示修復	已啟用：強制使用更新的用戶端	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					選項來選取 CredSSP 版本支援： ➢強制使用更新的用戶端：使用 CredSSP 的用戶端應用程式將無法回復成不安全的版本，並且使用 CredSSP 的服務將不會接受未修補的用戶端 ➢已降低影響：使用 CredSSP 的用戶端應用程式將無法回復成不安全的版本，但使用 CredSSP 的服務可接受未修補的用戶端 ➢易受攻擊：使用 CredSSP 的用戶端應用程式可支援回復成不安全的版本，且使用 CredSSP 的服務可接受未修補的用戶端，進而導致遠端伺服器容易遭受攻擊 ▪注意：除非所有遠端主機都已支援最新的版本，否則不應該使用「強制使用更新的用戶端」選項			

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪若須於本機群組原則編輯器(Gpedit.msc)或群組原則管理(Gpmc.msc)等工具中顯示這項原則設定，請安裝 1803 以上版本之 CredSsp 系統管理範本			
305	Windows Server 2016 Common Settings	TWG CB-01-007-0697	系統管理範本/認證委派	遠端主機允許委派不可匯出的認證	▪這項原則設定決定遠端主機是否允許委派不可匯出的認證 ▪使用認證委派時，裝置會將可匯出版本的認證提供給遠端主機，這會讓使用者暴露在遠端主機上攻擊者偷取認證的風險下 ▪如果啟用這項原則設定，主機支援「受限的系統管理」或「Remote Credential Guard」模式 ▪如果停用或未設定這項原則設定，則不支援「受限的系統管理」與「Remote Credential Guard」模式，使用者一律需	電腦設定\系統管理範本\系統\認證委派\遠端主機允許委派不可匯出的認證	已啟用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					要將其認證傳遞給主機 ▪ 若須於本機群組原則編輯器(Gpedit.msc)或群組原則管理(Gpmc.msc)等工具中顯示這項原則設定，請安裝 1703 以上版本之 CredSsp 系統管理範本			
306	Windows Server 2016 Common Settings	TWG CB-01-007-0698	系統管理範本/檔案總管框架窗格	開啟或關閉詳細資料窗格	▪ 這項原則設定決定是否在「檔案總管」中顯示或隱藏「詳細資料」窗格 ▪ 如果啟用這項原則設定並設定為隱藏窗格，就會隱藏「檔案總管」中的「詳細資料」窗格，且使用者無法將其開啟 ▪ 如果啟用這項原則設定並設定為顯示窗格，就一律會顯示「檔案總管」中的「詳細資料」窗格，且使用者無法將其隱藏。這項設定的副作用是無法切換成「預覽」窗格，因為「詳細資料」窗格不能與「預覽」窗格同時顯示	使用者設定\系統管理範本\Windows 元件\檔案總管\檔案總管框架窗格\開啟或關閉詳細資料窗格	已啟用：一律隱藏	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果停用或未設定這項原則設定，則會依預設隱藏「詳細資料」窗格，且使用者可以將其顯示，這是預設的原則設定			
307	Windows Server 2016 Common Settings	TWG CB-01-007-0699	系統管理範本/檔案總管框架窗格	關閉預覽窗格	▪這項原則設定決定是否隱藏「檔案總管」中的「預覽」窗格 ▪如果啟用這項原則設定，就會隱藏「檔案總管」中的「預覽」窗格，且使用者無法將其開啟 ▪如果停用或未設定這項原則設定，則會依預設隱藏「預覽」窗格，但使用者可以將其顯示	使用者設定\系統管理範本\Windows 元件\檔案總管\檔案總管框架窗格\關閉預覽窗格	已啟用	

資料來源：本中心整理

表3　Windows Server 2016 DC Server 政府組態基準列表

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
1	Windows Server 2016 DC Server	TWGCB-01-007-0300	安全性選項\互動式登入	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	▪每個唯一使用者的登入資訊會存放於本機快取，因此，若網域控制站在後續登入嘗試期間無法使用，使用者仍然可以登入。快取的登入資訊是從先前的登入工作階段儲存。若網域控制站無法使用且未快取使用者的登入資訊，則會以「目前無可用的登入伺服器來服務登入請求」訊息提示使用者 ▪在這項原則設定中，0 值會停用登入快取。超過 50 的任何值只會快取 50 個登入嘗試。Windows 最多支援 50 個快取項目，而每一使用者耗用的項目數目取決於認證。舉例來說，在 Windows 系統中最多可以快取 50 個唯一密碼使用者帳戶，但只能快取 25 個智慧卡使用者帳戶，因為會同時儲存密碼資訊與智慧卡資訊。當擁有快取登入資訊	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：網域控制站無法使用時，要快取的先前登入次數	0 次	CCE-ID：CCE-46705-0

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					的使用者再次登入時，會取代該使用者個人的快取資訊 ▪ 預設值為 10 次			
2	Windows Server 2016 DC Server	TWG CB-01-007-0301	安全性選項\網域控制站	網域控制站：拒絕電腦帳戶密碼變更	▪ 這項原則設定決定網域控制站是否會拒絕成員電腦變更電腦帳戶密碼的要求 ▪ 根據預設值，成員電腦每 30 天就會變更電腦帳戶密碼一次。如果啟用，網域控制站將會拒絕電腦帳戶密碼的變更要求 ▪ 如果啟用，此設定便不允許網域控制站接受對電腦帳戶的密碼所做的任何變更	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網域控制站：拒絕電腦帳戶密碼變更	已停用	CCE-ID：CCE-47052-6
3	Windows Server 2016 DC Server	TWG CB-01-007-0302	安全性選項\網域控	網域控制站：允許伺服器操作者排程	▪ 這項原則設定決定是否允許 Server Operators 以 AT 排程設備提交工作 ▪ 注意：這項原則設定只會影響到 AT 排程設備，但不會影響到工作排程器	電腦設定\Windows 設定\安全性設定\本機原則\安全性	已停用	CCE-ID：CCE-4678

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
			制站	工作	設備	選項\網域控制站：允許伺服器操作者排程工作		7-8
4	Windows Server 2016 DC Server	TWG CB-01-007-0303	安全性選項\網域控制站	網域控制站：LDAP 伺服器簽章要求	▪ 這項原則設定決定 LDAP 伺服器是否需要與 LDAP 用戶端交涉簽章，如下所示： ➢ 無：不需要資料簽章即可與伺服器連結。如果用戶端要求資料簽章，伺服器可提供支援 ➢ 要求簽章：除非使用 TLS\SSL，否則必須交涉 LDAP 資料簽章選項 ▪ 預設值為「無」 ▪ 如果將伺服器設定為「要求簽章」，那麼也必須設定用戶端。如果未設定用戶端，會造成與伺服器的連線中斷 ▪ 此設定對於 LDAP 簡單繫結或透過	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網域控制站：LDAP 伺服器簽章要求	要求簽章	CCE-ID：CCE-46228-3

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					SSL 進行的 LDAP 簡單繫結沒有任何影響。Windows XP Professional 隨附的所有 Microsoft LDAP 用戶端均不使用 LDAP 簡單繫結或透過 SSL 進行的 LDAP 簡單繫結與網域控制站通訊 ▪ 如果需要簽章，則將拒絕 LDAP 簡單繫結與透過 SSL 進行的 LDAP 簡單繫結			
5	Windows Server 2016 DC Server	TWG CB-01-007-0304	使用者權限指派	拒絕從網路存取這台電腦	這項原則設定決定會阻止哪些使用者從網路存取電腦。這項原則設定會取代「從網路存取這台電腦」原則設定，如果使用者帳戶同時受限於這兩種原則	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\拒絕從網路存取這台電腦	Guests,本機帳戶	CCE-ID：CCE-44499-2
6	Windows Server	TWG CB-01	使用者權	將工作站新增至網	▪ 這項原則設定決定哪些群組或使用者可將工作站新增至網域	電腦設定\Windows 設定\	Administrators	CCE-ID：

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 DC Server	-007-0305	限指派	域	▪ 這項原則設定只在網域控制站有效。任何已驗證的使用者預設都有這個權限，而且最多可在網域內建立 10 個電腦帳戶 ▪ 將電腦帳戶新增到網域，可讓電腦參與 Active Directory 為主的網路功能。例如，將工作站加入網域，可讓該工作站辨識 Active Directory 中的帳戶與群組 ▪ 注意：在 Active Directory 電腦容器中擁有「建立電腦物件」特殊權限的使用者，也可以在網域中建立電腦帳戶。不同的是，容器上具有權限的使用者不會受到只能建立 10 個電腦帳戶的限制，此外，利用「將工作站新增至網域」所建立的電腦帳戶將網域系統管理員當作電腦帳戶擁有者，而利用電腦容器權限所建立的電腦帳戶將	安全性設定\本機原則\使用者權限指派\將工作站新增至網域		CCE-44709-4

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					建立者當作電腦帳戶擁有者。如果使用者擁有容器權限，也擁有「將工作站新增至網域」使用者權限，則會根據電腦容器權限來新增電腦，而非根據使用者權限			
7	Windows Server 2016 DC Server	TWG CB-01-007-0306	使用者權限指派	同步處理目錄服務資料	這項原則設定決定授權哪些使用者及群組同步處理所有目錄服務資料。這也稱為 Active Directory 同步處理	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\同步處理目錄服務資料	No One	CCE-ID：CCE-45710-1
8	Windows Server 2016 DC Server	TWG CB-01-007-0307	使用者權限指派	從網路存取這台電腦	▪ 此使用者權限決定允許哪些使用者及群組透過網路連線到這台電腦 ▪ 遠端桌面服務不受此使用者權限的影響 ▪ 注意：遠端桌面服務在舊版的	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派\從網路存取這台電	Administrators, Authenticated Users, ENTERPRISE	CCE-ID：CCE-45486-8

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					Windows Server 中稱為「終端機服務」	腦	DOMAIN CONTROLLERS	
9	Windows Server 2016 DC Server	TWG CB-01-007-0308	系統服務	Active Directory Domain Services	▪ 這項原則設定決定此電腦是否可使用 AD DS 網域控制站之服務 ▪ 如果此服務停止，使用者就無法登入網路 ▪ 如果此服務停用，所有明確依存於它的服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Active Directory Domain Services	自動	
10	Windows Server 2016 DC Server	TWG CB-01-007-0309	系統服務	Active Directory Web Services	▪ 這項原則設定決定此電腦是否可使用 AD Web 服務 ▪ 這項服務提供 Web 服務介面，供這個伺服器上本機執行的目錄服務(AD DS 及 AD LDS)執行個體使用 ▪ 如果停止或停用這個服務，則用戶端應用程式(如 Active Directory	電腦設定\Windows 設定\安全性設定\系統服務\Active Directory Web Services	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					PowerShell)會無法存取或管理這部伺服器上本機執行的任何目錄服務執行個體			
11	Windows Server 2016 DC Server	TWG CB-01-007-0310	系統服務	Application Identity	▪ 這項原則設定決定此電腦是否可使用 Application Identity 之服務，用以判斷並確定應用程式的識別 ▪ 如果停用此服務將使 AppLocker 無法強制執行	電腦設定\Windows 設定\安全性設定\系統服務\Application Identity	自動	CCE-ID：CCE-47123-5
12	Windows Server 2016 DC Server	TWG CB-01-007-0311	系統服務	DFS Namespace	▪ 這項原則設定決定此電腦是否可使用 DFS Namespace 服務 ▪ 此服務可將位在不同伺服器的共用資料夾分組到一或多個邏輯結構命名空間。每個命名空間對使用者而言都是含有一連串子資料夾的單一共用資料夾	電腦設定\Windows 設定\安全性設定\系統服務\DFS Namespace	自動	
13	Windows	TWG	系統	DFS	▪ 這項原則設定決定此電腦是否可使用	電腦設定	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 DC Server	CB-01-007-0312	服務	Replication	DFS Replication 服務 ▪ 此服務可透過本機或廣域網路(WAN)網路連線同步多部伺服器上的資料夾。這個服務使用遠端差異壓縮(RDC)通訊協定，僅更新自從上次複寫之後有變更的檔案	\Windows 設定\安全性設定\系統服務\DFS Replication		
14	Windows Server 2016 DC Server	TWG CB-01-007-0313	系統服務	Distributed Link Tracking Client	這項原則設定決定此電腦是否可使用 Distributed Link Tracking 服務，用以維護電腦中或網路中不同電腦之 NTFS 檔案間的連結	電腦設定\Windows 設定\安全性設定\系統服務\Distributed Link Tracking Client	手動	
15	Windows Server 2016 DC Server	TWG CB-01-007-0314	系統服務	DNS Client	▪ 這項原則設定決定此電腦之 DNS Client 服務是否啟動 ▪ DNS 用戶端服務(dnscache)會為此電腦快取網域名稱系統(DNS)名稱並登	電腦設定\Windows 設定\安全性設定\系統服務\DNS	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					錄完整的電腦名稱 ▪ 如果這個服務被停止，將會繼續解析 DNS 名稱。然而，將不會快取 DNS 名稱查詢的結果，而且不會登錄電腦名稱 ▪ 如果這個服務已停用，所有依存於它的服務都將無法啟動	Client		
16	Windows Server 2016 DC Server	TWG CB-01-007-0315	系統服務	DNS Server	▪ 這項原則設定決定此電腦之 DNS Server 服務是否啟動。讓 DNS 用戶端經由回答 DNS 查詢與動態 DNS 更新要求的方法，解析 DNS 名稱 ▪ 如果此服務停止，DNS 更新將不會發生 ▪ 如果此服務停用，所有明確依存於它的服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\DNS Server	自動	
17	Windows Server	TWG CB-01	系統服務	File Replicatio	▪ 這項原則設定決定此電腦是否使用 File Replication 服務	電腦設定\Windows 設定\	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 DC Server	-007-0316		n	▪如果此服務啟用，就會將資料夾與使用檔案複寫服務(FRS)取代較新之 DFS 複寫技術的檔案伺服器同步處理	安全性設定\系統服務\File Replication		
18	Windows Server 2016 DC Server	TWG CB-01-007-0317	系統服務	Group Policy Client	▪這項原則設定決定此電腦是否使用 Group Policy Client 服務 ▪此服務負責透過「群組原則」元件，將系統管理員所設定的設定值套用在電腦及使用者 ▪如果該服務停用，就不會套用這些設定值，而且也無法透過「群組原則」來管理應用程式及元件 ▪如果該服務停用，需仰賴「群組原則」元件的任何元件或應用程式可能會無法運作	電腦設定\Windows 設定\安全性設定\系統服務\Group Policy Client	自動	
19	Windows Server 2016 DC	TWG CB-01-007-0	系統服務	Intersite Messaging	▪這項原則設定決定此電腦是否使用 Intersite Messaging 服務 ▪此服務讓訊息能夠在執行 Windows	電腦設定\Windows 設定\安全性設定\系	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server	318			Server 站台的電腦間交換 ▪ 如果此服務停止，將無法交換訊息，也將不會計算其他服務的站台路由資訊 ▪ 如果此服務停用，所有明確依存於它的服務都將無法啟動	統服務\Intersite Messaging		
20	Windows Server 2016 DC Server	TWG CB-01-007-0319	系統服務	Kerberos Key Distribution Center	▪ 這項原則設定決定此電腦是否使用 Kerberos Key Distribution Center 服務 ▪ 在網域控制站上執行的這個服務，可以讓使用者使用 Kerberos 驗證通訊協定登入網路 ▪ 如果停止這個服務，使用者將無法登入網路 ▪ 如果此服務停用，所有明確依存於它的服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Kerberos Key Distribution Center	自動	
21	Windows Server	TWG CB-01	系統服務	Netlogon	▪ 這項原則設定決定此電腦是否使用 Netlogon 服務	電腦設定\Windows 設定\	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 DC Server	-007-0320			▪此服務維持這個電腦與網域控制站間用於驗證使用者與服務的安全通道 ▪如果這個服務被停止，電腦可能無法驗證使用者與服務，且網域控制站將無法登錄 DNS 記錄 ▪如果這個服務被停用，任何明確依存於它的服務將無法啟動	安全性設定\系統服務\Netlogon		
22	Windows Server 2016 DC Server	TWG CB-01-007-0321	系統服務	Server	▪這項原則設定決定此電腦是否使用 Server 服務 ▪為這個電腦支援網路上檔案、列印及命名管線的共用 ▪如果停止此服務，將無法使用這些功能 ▪如果這個服務被停用，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Server	自動	
23	Windows Server	TWG CB-01	系統服務	Windows Time	▪這項原則設定決定此電腦是否使用 Windows Time 服務，用以維護在網路	電腦設定\Windows 設定\	自動	

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
	2016 DC Server	-007-0322			上所有用戶端及伺服器的資料及時間同步處理 ▪如果這個服務停止，將無法進行日期與時間同步處理 ▪如果這個服務被停用，所有依存的服務都會停止	安全性設定\系統服務\Windows Time		
24	Windows Server 2016 DC Server	TWGCB-01-007-0323	系統服務	Workstation	▪這項原則設定決定此電腦是否使用 Workstation 服務，用以建立及維護使用 SMB 通訊協定進行的用戶端與遠端伺服器網路連線 ▪如果停止這個服務，將無法使用這些連線 ▪如果停用這個服務，則會停止所有明確依存它的服務	電腦設定\Windows 設定\安全性設定\系統服務\Workstation	自動	
25	Windows Server 2016 DC	TWGCB-01-007-0	進階稽核原則	稽核目錄服務存取	▪這項原則設定決定是否稽核存取 Active Directory 網域服務(AD DS)物件時產生的事件	電腦設定\Windows 設定\安全性設定\進	成功及失敗	CCE-ID：CCE-

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server	324	\DS 存取		▪ 只會記錄具有相符系統存取控制清單(SACL)的 AD DS 物件 ▪ 這個子類別中的事件與舊版 Windows 中的目錄服務存取事件類似 ▪ 伺服器版本的預設值：成功	階稽核原則設定\稽核原則\DS 存取\稽核目錄服務存取		46219-2
26	Windows Server 2016 DC Server	TWG CB-01-007-0325	進階稽核原則\DS 存取	稽核目錄服務變更	▪ 這項原則設定決定是否稽核因 Active Directory 網域服務(AD DS)中物件變更而產生的事件。建立、刪除、修改、移動或解除刪除物件時，會記錄事件 ▪ 如果可能，記錄在這個子類別中的事件會指出物件內容的新舊值 ▪ 只有在網域控制站上才會記錄這個子類別中的事件，而且只會記錄 AD DS 中具有相符系統存取控制清單(SACL)的物件 ▪ 注意：因為結構描述中的物件類別設定，所以部分物件及內容的動作不會	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\DS 存取\稽核目錄服務變更	成功及失敗	CCE-ID：CCE-46701-9

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					產生稽核事件 ▪ 如果設定這項原則設定，則會在嘗試變更 AD DS 中的物件時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在嘗試變更 AD DS 中的物件時產生稽核事件 ▪ 預設值：沒有稽核			
27	Windows Server 2016 DC Server	TWG CB-01-007-0326	進階稽核原則\帳戶管理	稽核電腦帳戶管理	▪ 這項原則設定決定是否稽核因電腦帳戶變更(如建立、變更或刪除電腦帳戶時)而產生的事件 ▪ 如果設定這項原則設定，則會在嘗試變更電腦帳戶時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\帳戶管理\稽核電腦帳戶管理	成功及失敗	CCE-ID：CCE-4590 5-7

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					電腦帳戶變更時產生稽核事件 ▪ 伺服器版本的預設值：成功			
28	Windows Server 2016 DC Server	TWG CB-01-007-0700	安全性選項\網域控制站	網域控制站：LDAP 伺服器通道繫結權杖要求	▪ 這項原則設定決定 LDAP 伺服器是否強制執行在 LDAP 繫結中，要求透過 LDAPS 連線傳送所接收的通道繫結權杖驗證，選項如下： ➢ 永不：不執行任何通道繫結驗證，這是所有尚未更新之伺服器的行為 ➢ 支援時：透過 TLS/SSL 連線進行驗證時，宣告支援通道繫結權杖的用戶端必須提供正確的權杖；未宣告這類支援及/或未使用 TLS/SSL 連線的用戶端不會受到影響，這是允許應用程式相容性的中間選項 ➢ 一律：所有用戶端都必須提供有關 LDAPS 的通道繫結資訊，伺服器拒	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網域控制站：LDAP 伺服器通道繫結權杖要求	一律	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					絕來自不執行此動作之用戶端的 LDAPS 驗證要求 ▪預設值：未定義這項原則，則其效果與「支援時」相同 ▪注意：「支援時」 選項僅保護那些支援驗證擴充保護的用戶端；未支援驗證擴充保護的用戶端仍可能會遭到攻擊，直到修補及/或設定這項原則 ▪若須於本機群組原則編輯器(Gpedit.msc)或群組原則管理(Gpmc.msc)等工具中顯示這項原則設定，請執行以下任一操作： ➢安裝微軟於 2020 年 3 月後所提供之更新，加入這項原則，GPO 設定路徑為「電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網域控制站：LDAP 伺服器通道繫結權杖要求」			

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					➢安裝 1809 以上版本之 SecGuide 系統管理範本，GPO 設定路徑為「電腦設定\系統管理範本\MS Security Guide\Extended Protection for LDAP Authentication (Domain Controllers only)」			

資料來源：本中心整理

表4　Windows Server 2016 DNS Server 政府組態基準列表

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
1	Windows Server 2016 DNS Server	TWGCB-01-007-0327	系統服務	Application Identity	▪這項原則設定決定此電腦是否可使用 Application Identity 之服務，用以判斷並確定應用程式的識別 ▪如果停用此服務將使 AppLocker 無法強制執行	電腦設定\Windows 設定\安全性設定\系統服務\Application Identity	手動	CCE-ID：CCE-47123-5
2	Windows Server 2016 DNS Server	TWGCB-01-007-0328	系統服務	Application Information	▪這項原則設定決定此電腦是否可使用 Application Information 服務，以其他管理權限協助執行互動式應用程式。使用者在執行想要的工作時可能會需要這些權限 ▪如果停止此服務，使用者將無法以其他管理權限來啟動應用程式	電腦設定\Windows 設定\安全性設定\系統服務\Application Information	手動	
3	Windows Server	TWGCB-01	系統服務	Application Layer	這項原則設定決定此電腦是否可使用 Application Layer Gateway Service	電腦設定\Windows 設定	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 DNS Server	-007-0329		Gateway Service	服務，以對網際網路連線共用提供協力廠商通訊協定外掛程式的支援	\安全性設定\系統服務\Application Layer Gateway Service		
4	Windows Server 2016 DNS Server	TWG CB-01-007-0330	系統服務	Application Management	▪ 這項原則設定決定此電腦是否可使用應用程式管理服務 ▪ 針對透過「群組原則」來部署的軟體，處理安裝、移除及列舉要求。若將此服務停用，使用者將無法安裝、移除及列舉透過「群組原則」來部署的軟體，而且與其具有明確相依關係的任何服務，也將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Application Management	手動	
5	Windows Server 2016	TWG CB-01-007-0	系統服務	ASP.NET State Service	▪ 這項原則設定決定此電腦是否可使用 ASP.NET 狀態服務，以提供 ASP.NET 所需跨處理序	電腦設定\Windows 設定\安全性設定\	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	DNS Server	331			(Out-Of-Process)工作階段狀態的支援 ▪ 若停止這項服務，則跨處理序的要求將無法進行 ▪ 如果停用這項服務，與這項服務明確相關的所有其他服務都將無法啟動	系統服務\ASP.NET State Service		
6	Windows Server 2016 DNS Server	TWG CB-01-007-0332	系統服務	Background Intelligent Transfer Service	▪ 這項原則設定決定此電腦是否可使用 Background Intelligent Transfer Service 服務，以使用閒置的網路頻寬在背景傳輸檔案 ▪ 如果停用此服務，所有依存於 BITS 的應用程式(例如，Windows Update 或 MSN Explorer)將無法自動下載程式或其他資訊	電腦設定\Windows 設定\安全性設定\系統服務\Background Intelligent Transfer Service	自動	
7	Windows Server	TWG CB-01	系統服務	Background Tasks	這項原則設定決定此電腦是否可使用 Background Tasks Infrastructure	電腦設定\Windows 設定	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 DNS Server	-007-0333		Infrastructure Service	Service 服務，以控制哪些背景工作可在系統上執行的 Windows 基礎結構服務	\安全性設定\系統服務\Background Tasks Infrastructure Service		
8	Windows Server 2016 DNS Server	TWG CB-01-007-0334	系統服務	Base Filtering Engine	▪ 這項原則設定決定此電腦是否可使用 Base Filtering Engine (BFE)服務 ▪ 基礎篩選引擎(BFE)是管理防火牆與 IP 安全性(IPsec)原則，並執行使用者模式篩選的服務 ▪ 停止或停用 BFE 服務將顯著降低系統的安全性。同時也導致 IPsec 管理與防火牆應用程式意外的行為	電腦設定\Windows 設定\安全性設定\系統服務\Base Filtering Engine	自動	
9	Windows Server 2016	TWG CB-01-007-0	系統服務	Certificate Propagation	▪ 這項原則設定決定此電腦是否可使用 Certificate Propagation 服務 ▪ 從智慧卡將使用者憑證與根憑證複	電腦設定\Windows 設定\安全性設定\	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	DNS Server	335			製到目前使用者的憑證存放區，當智慧卡插入智慧卡讀卡機時進行偵測，(若有需要)並安裝智慧卡隨插即用迷你驅動程式	系統服務\Certificate Propagation		
10	Windows Server 2016 DNS Server	TWG CB-01-007-0336	系統服務	CNG Key Isolation	▪ 這項原則設定決定此電腦是否可使用 CNG key isolation 服務 ▪ CNG 金鑰隔離服務裝載於 LSA 處理程序。該服務可依據一般條件來隔離私密金鑰與相關聯加密編譯操作的金鑰處理程序。該服務會以符合一般條件的安全處理程序來儲存與使用長效金鑰	電腦設定\Windows 設定\安全性設定\系統服務\CNG Key Isolation	手動	
11	Windows Server 2016 DNS	TWG CB-01-007-0337	系統服務	COM+ Event System	▪ 這項原則設定決定此電腦是否可使用 COM+ Event System 服務 ▪ 支援「系統事件通知服務(SENS)」，它可讓事件自動分散到訂閱的 COM	電腦設定\Windows 設定\安全性設定\系統服務	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server				元件。如果服務被停止，SENS 會關閉，並無法提供登入及登出通知。如果此服務被停用，任何明顯依存它的服務都無法啟動	\COM+ Event System		
12	Windows Server 2016 DNS Server	TWG CB-01-007-0338	系統服務	COM+ System Application	▪ 這項原則設定決定此電腦是否可使用 COM+ System Application 服務，以管理 COM+元件的設定及追蹤 ▪ 如果停止此服務，大部分的 COM+元件將無法適當運作 ▪ 如果此服務被停用，任何明確依存它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\COM+ System Application	手動	
13	Windows Server 2016 DNS Server	TWG CB-01-007-0339	系統服務	Computer Browser	▪ 這項原則設定決定是否讓此電腦在網路上之其他使用者進行資源瀏覽 ▪ 維護網路上更新的電腦清單，並將這個清單提供給做為瀏覽器的電腦 ▪ 如果這個服務被停止，這個清單將不會被更新或維護	電腦設定\Windows 設定\安全性設定\系統服務\Computer Browser	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 如果這個服務被停用，任何明確依存於它的服務將無法啟動			
14	Windows Server 2016 DNS Server	TWG CB-01-007-0340	系統服務	Credential Manager	▪ 這項原則設定決定此電腦是否可使用 Credential Manager 服務 ▪ 此項服務提供使用者安全儲存以及擷取認證、應用程式以及安全性服務封裝	電腦設定\Windows 設定\安全性設定\系統服務\Credential Manager	手動	
15	Windows Server 2016 DNS Server	TWG CB-01-007-0341	系統服務	Cryptographic Services	▪ 這項原則設定決定此電腦是否可使用 Cryptographic Services 服務 ▪ Cryptographic Services 提供 3 種管理服務： ➢ 目錄資料庫服務：確認 Windows 檔案的簽章並允許安裝新程式 ➢ 受保護的根目錄服務：從這部電腦新增及移除信任的根憑證授權單位憑證	電腦設定\Windows 設定\安全性設定\系統服務\Cryptographic Services	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					➢自動根憑證更新服務：從 Windows Update 抓取根憑證並啟用案例，例如 SSL ▪如果停止此服務，這些管理服務將無法正常運作 ▪如果停用此服務，任何明確需要它的服務將無法啟動			
16	Windows Server 2016 DNS Server	TWG CB-01-007-0342	系統服務	DCOM Server Process Launcher	▪這項原則設定決定此電腦是否可使用 DCOM Server Process Launcher 服務 ▪DCOMLAUNCH 服務會啟動 COM 與 DCOM 伺服器，以回應物件啟用要求 ▪如果停止或停用此服務，使用 COM 或 DCOM 的程式將無法正常運作。強烈建議持續執行 DCOMLAUNCH 服務	電腦設定\Windows 設定\安全性設定\系統服務\DCOM Server Process Launcher	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
17	Windows Server 2016 DNS Server	TWG CB-01-007-0343	系統服務	Device Association Service	▪這項原則設定決定此電腦是否可使用 Device Association Service 服務 此項服務啟用系統與有線或無線裝置之間的配對	電腦設定\Windows 設定\安全性設定\系統服務\Device Association Service	手動	
18	Windows Server 2016 DNS Server	TWG CB-01-007-0344	系統服務	Device Install Service	▪這項原則設定決定此電腦是否可使用 Device Install Service 服務，以使用者沒有或很少的輸入來識別及適應硬體變更 ▪停止或停用這個服務將導致系統不穩定	電腦設定\Windows 設定\安全性設定\系統服務\Device Install Service	手動	
19	Windows Server 2016 DNS	TWG CB-01-007-0345	系統服務	Device Setup Manager	▪這項原則設定決定此電腦是否可使用 Device Setup Manager 服務，以偵測、下載及安裝裝置相關軟體 ▪如果停用此服務，裝置可能會以過	電腦設定\Windows 設定\安全性設定\系統服務	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server				期的軟體設定，且可能無法正常運作	\Device Setup Manager		
20	Windows Server 2016 DNS Server	TWG CB-01-007-0346	系統服務	DFS Replication	▪ 這項原則設定決定此電腦是否可使用 DFS Replication 服務 ▪ 此服務可透過本機或廣域網路(WAN)網路連線同步多部伺服器上的資料夾。這個服務使用遠端差異壓縮(RDC)通訊協定，僅更新自從上次複寫之後有變更的檔案	電腦設定\Windows 設定\安全性設定\系統服務\DFS Replication	自動	
21	Windows Server 2016 DNS Server	TWG CB-01-007-0347	系統服務	DHCP Client	▪ 這項原則設定決定此電腦是否可使用 DHCP Client 服務，以為這個電腦登錄及更新 IP 位址與 DNS 記錄 ▪ 如果這個服務被停止，這個電腦將會不接收動態 IP 位址與 DNS 更新 ▪ 如果這個服務被停用，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\DHCP Client	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
22	Windows Server 2016 DNS Server	TWG CB-01-007-0348	系統服務	Diagnostic Policy Service	▪ 這項原則設定決定此電腦是否可使用診斷原則服務 ▪ 診斷原則服務能夠偵測 Windows 元件的問題、進行疑難排解及提供解決方案 ▪ 如果停止此服務，便無法再進行診斷	電腦設定\Windows 設定\安全性設定\系統服務\Diagnostic Policy Service	自動	
23	Windows Server 2016 DNS Server	TWG CB-01-007-0349	系統服務	Diagnostic Service Host	▪ 這項原則設定決定此電腦之 Windows 元件錯誤診斷服務之是否啟用 ▪ 診斷原則服務會使用診斷服務裝載，裝載需要在本機服務內容上執行的診斷。如果此服務已停止，其上的任何診斷將不再產生作用	電腦設定\Windows 設定\安全性設定\系統服務\Diagnostic Service Host	手動	
24	Windows Server 2016	TWG CB-01-007-0	系統服務	Diagnostic System Host	▪ 這項原則設定決定此電腦是否可使用 Diagnostic System Host 服務 ▪ 診斷原則服務會使用診斷系統裝	電腦設定\Windows 設定\安全性設定\	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	DNS Server	350			載，裝載需要在本機服務內容上執行的診斷 ▪ 如果此服務已停止，其上的任何診斷將不再產生作用	系統服務\Diagnostic System Host		
25	Windows Server 2016 DNS Server	TWG CB-01-007-0351	系統服務	Distributed Link Tracking Client	這項原則設定決定此電腦是否可使用 Distributed Link Tracking 之服務，以維護電腦中或網路中不同電腦之 NTFS 檔案間的連結	電腦設定\Windows 設定\安全性設定\系統服務\Distributed Link Tracking Client	自動	
26	Windows Server 2016 DNS Server	TWG CB-01-007-0352	系統服務	Distributed Transaction Coordinator	▪ 這項原則設定決定此電腦之候選交易(Coordinates transactions)之管理服務是否啟動，以協調跨越多個資源管理員的交易，比如資料庫、訊息佇列及檔案系統 ▪ 如果此服務被停止，這些交易將會	電腦設定\Windows 設定\安全性設定\系統服務\Distributed Transaction	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					失敗 ▪如果這個服務已停用，所有依存於它的服務都將無法啟動	Coordinator		
27	Windows Server 2016 DNS Server	TWG CB-01-007-0353	系統服務	DNS Client	▪這項原則設定決定此電腦之 DNS Client 服務是否啟動 ▪DNS 用戶端服務(dnscache)會為此電腦快取網域名稱系統(DNS)名稱並登錄完整的電腦名稱 ▪如果這個服務被停止，將會繼續解析 DNS 名稱。然而，將不會快取 DNS 名稱查詢的結果，而且不會登錄電腦名稱 ▪如果這個服務已停用，所有依存於它的服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\DNS Client	自動	
28	Windows Server 2016	TWG CB-01-007-0	系統服務	DNS Server	▪這項原則設定決定此電腦之 DNS Server 服務是否啟動。讓 DNS 用戶端經由回答 DNS 查詢與動態 DNS	電腦設定\Windows 設定\安全性設定\	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	DNS Server	354			更新要求的方法，解析 DNS 名稱 ▪ 如果此服務停止，DNS 更新將不會發生 ▪ 如果此服務停用，所有明確依存於它的服務都將無法啟動	系統服務\DNS Server		
29	Windows Server 2016 DNS Server	TWG CB-01-007-0355	系統服務	Encrypting File System (EFS)	▪ 這項原則設定決定此電腦是否啟用加密檔案系統服務，藉由提供核心檔案加密技術，可以在 NTFS 檔案系統磁碟區上儲存加密的檔案 ▪ 如果此服務停止或停用，應用程式將無法存取加密的檔案	電腦設定\Windows 設定\安全性設定\系統服務\Encrypting File System (EFS)	手動	
30	Windows Server 2016 DNS Server	TWG CB-01-007-0356	系統服務	Extensible Authentication Protocol	▪ 這項原則設定決定此電腦之延伸驗證協定(EAP)之服務是否啟用 ▪ 可延伸的驗證通訊協定(EAP)服務提供例如 802.1x 有線及無線、VPN 以及網路存取保護(NAP)環境中的	電腦設定\Windows 設定\安全性設定\系統服務\Extensible	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					網路驗證 ▪ EAP 在驗證程序期間，也提供網路存取用戶端(包括無線及 VPN 用戶端)使用的應用程式開發介面(API)。如果停用此服務，此電腦將無法存取需要 EAP 驗證的網路	Authentication Protocol		
31	Windows Server 2016 DNS Server	TWG CB-01-007-0357	系統服務	Function Discovery Provider Host	▪ 這項原則設定決定此電腦是否可使用 Function Discovery Provider Host 服務 ▪ FDPHOST 服務裝載功能探索(FD)網路探索提供者。這些 FD 提供者提供 Simple Services Discovery Protocol(SSDP) 與 Web Services-Discovery(WS-D)通訊協定的網路探索服務 ▪ 若停止或停用 FDPHOST 服務，則在使用 FD 時，將停用這些通訊協定的網路探索。無法使用此服務時，	電腦設定\Windows 設定\安全性設定\系統服務\Function Discovery Provider Host	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					利用 FD 及依賴這些探索通訊協定的網路服務將找不到網路裝置或資源			
32	Windows Server 2016 DNS Server	TWG CB-01-007-0358	系統服務	Function Discovery Resource Publication	▪ 這項原則設定決定此電腦是否可進行網路資源發布之服務 ▪ 發布這台電腦與連結至這台電腦的資源，便可在網路上找到它們。如果此服務停止，便不再發布網路資源，網路上的其他電腦將無法找到它們	電腦設定\Windows 設定\安全性設定\系統服務\Function Discovery Resource Publication	手動	
33	Windows Server 2016 DNS Server	TWG CB-01-007-0359	系統服務	Group Policy Client	▪ 這項原則設定決定此電腦是否使用 Group Policy Client 服務 ▪ 此服務負責透過「群組原則」元件，將系統管理員所設定的設定值套用在電腦及使用者 ▪ 如果該服務停用，就不會套用這些	電腦設定\Windows 設定\安全性設定\系統服務\Group Policy Client	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					設定值，而且也無法透過「群組原則」來管理應用程式及元件 ▪ 如果該服務停用，需仰賴「群組原則」元件的任何元件或應用程式可能會無法運作			
34	Windows Server 2016 DNS Server	TWG CB-01-007-0360	系統服務	Human Interface Device Service	▪ 這項原則設定決定此電腦是否啟用 Human Interface Device Service 服務 ▪ 啟用此服務可維護鍵盤、遙控器與其他多媒體裝置上之常用按鈕的使用。建議讓這個服務繼續執行	電腦設定\Windows 設定\安全性設定\系統服務\Human Interface Device Service	手動	
35	Windows Server 2016 DNS Server	TWG CB-01-007-0361	系統服務	Hyper-V Data Exchange Service	▪ 這項原則設定決定此電腦是否可使用 Hyper-V Data Exchange Service 服務 ▪ 此服務提供一種機制，以便在虛擬機器及實體電腦上執行之作業系統	電腦設定\Windows 設定\安全性設定\系統服務\Hyper-V Data	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					間交換資料	Exchange Service		
36	Windows Server 2016 DNS Server	TWG CB-01-007-0362	系統服務	Hyper-V Guest Shutdown Service	▪ 這項原則設定決定此電腦是否可使用 Hyper-V Guest Shutdown Service 服務 ▪ 此服務提供從實體電腦的管理介面關閉這個虛擬機器之作業系統的機制	電腦設定\Windows 設定\安全性設定\系統服務\Hyper-V Guest Shutdown Service	手動	
37	Windows Server 2016 DNS Server	TWG CB-01-007-0363	系統服務	Hyper-V Heartbeat Service	▪ 這項原則設定決定此電腦是否啟用 Hyper-V Heartbeat Service 服務 ▪ 定期報告活動訊號來監視此虛擬機器的狀態。此服務可協助識別已停止回應的執行中虛擬機器	電腦設定\Windows 設定\安全性設定\系統服務\Hyper-V Heartbeat Service	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
38	Windows Server 2016 DNS Server	TWG CB-01-007-0364	系統服務	Hyper-V Remote Desktop Virtualization Service	▪ 這項原則設定決定此電腦是否啟用 Hyper-V Remote Desktop Virtualization Service 服務 ▪ 此服務提供平台，讓虛擬機器與在實體電腦上執行的作業系統彼此通訊	電腦設定\Windows 設定\安全性設定\系統服務\Hyper-V Remote Desktop Virtualization Service	手動	
39	Windows Server 2016 DNS Server	TWG CB-01-007-0365	系統服務	Hyper-V Time Synchronization Service	▪ 這項原則設定決定此電腦是否可使用 Hyper-V Time Synchronization Service 服務 ▪ 此服務同步化這個虛擬機器與實體電腦的系統時間	電腦設定\Windows 設定\安全性設定\系統服務\Hyper-V Time Synchronization Service	手動	
40	Windows	TWG	系統	Hyper-V	▪ 這項原則設定決定此電腦是否啟用	電腦設定	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 DNS Server	CB-01-007-0366	服務	Volume Shadow Copy Requestor	Hyper-V Volume Shadow Copy Requestor 服務 ▪ 此服務協調磁碟區陰影複製服務所需的通訊，以便從實體電腦的作業系統將應用程式與資料備份到這個虛擬機器	\Windows 設定\安全性設定\系統服務\Hyper-V Volume Shadow Copy Requestor		
41	Windows Server 2016 DNS Server	TWG CB-01-007-0367	系統服務	IKE and AuthIP IPsec Keying Modules	▪ 這項原則設定決定此電腦是否啟用 IKE and AuthIP IPsec Keying Modules 服務 ▪ IKEEXT 服務主控 Internet Keying Exchange(IKE)及 Authenticated Internet Protocol(AuthIP)金鑰處理模組 ▪ 這些金鑰處理模組是用來在網際網路通訊協定安全性(IPsec)中進行驗證及金鑰交換 ▪ 停止或停用 IKEEXT 服務將會停用	電腦設定\Windows 設定\安全性設定\系統服務\IKE and AuthIP IPsec Keying Modules	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					與同儕節點電腦間的 IKE 與 AuthIP 金鑰交換 ▪ IPsec 通常會設定為使用 IKE 或 AuthIP，因此如果停止或停用 IKEEXT 服務，將會導致 IPsec 失敗，並危害系統的安全性。強烈建議持續執行 IKEEXT 服務			
42	Windows Server 2016 DNS Server	TWG CB-01-007-0368	系統服務	Interactive Services Detection	▪ 這項原則設定決定使用者於互動式服務之輸入訊息與提示是否可正常使用 ▪ 啟用使用者通知，以通知使用者針對互動服務進行輸入，這樣可在互動服務所建立的對話方塊出現時存取它們 ▪ 如果此服務停止，新互動服務對話方塊的通知功能將無法再運作，而且可能無法存取互動服務對話方塊。如果此服務停用，新互動服務	電腦設定\Windows 設定\安全性設定\系統服務\Interactive Services Detection	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					對話方塊的通知及存取功能都無法再運作			
43	Windows Server 2016 DNS Server	TWG CB-01-007-0369	系統服務	Internet Connection Sharing (ICS)	▪ 這項原則設定決定此電腦是否可使用 Internet Connection Sharing (ICS)之服務 ▪ 此服務可為家用網路或小型辦公室網路提供網路位址轉譯、定址、名稱解析或防止干擾的服務	電腦設定\Windows 設定\安全性設定\系統服務\Internet Connection Sharing (ICS)	已停用	
44	Windows Server 2016 DNS Server	TWG CB-01-007-0370	系統服務	IP Helper	▪ 這項原則設定決定此電腦是否可透過 IPv4 進行 IPv6 之網路連線服務 ▪ 使用 IPv6 轉換技術(6to4、ISATAP、連接埠 Proxy 與 Teredo)與 IP-HTTPS 提供通道連線能力 ▪ 如果停止此服務，電腦將不具有這些技術所提供的增強連線能力效益	電腦設定\Windows 設定\安全性設定\系統服務\IP Helper	自動	
45	Windows	TWG	系統	IPsec Policy	▪ 這項原則設定決定此電腦是否可使	電腦設定	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 DNS Server	CB-01-007-0371	服務	Agent	用 IPsec Policy Agent 之服務 ▪ 網際網路通訊協定安全性(IPsec)支援網路層級的對等驗證、資料來源驗證、資料完整性、資料機密性(加密)及重新執行保護 ▪ 此服務會強制執行透過 IP 安全性原則嵌入式管理單元或命令列工具「netsh ipsec」建立的 IPsec 原則 ▪ 如果停止此服務，當原則需要使用 IPsec 連線時，可能會發生網路連線問題。此外，此服務停止時也無法使用 Windows 防火牆的遠端管理	\Windows 設定\安全性設定\系統服務\IPsec Policy Agent		
46	Windows Server 2016 DNS Server	TWG CB-01-007-0372	系統服務	KDC Proxy Server service (KPS)	▪ 這項原則設定決定此電腦是否可使用 KDC Proxy Server service (KPS)服務 KDC Proxy 伺服器服務會在 Edge Server 上執行，以將 Kerberos 通訊協	電腦設定\Windows 設定\安全性設定\系統服務\KDC Proxy Server service	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					定訊息 Proxy 處理到公司網路上的網域控制站	(KPS)		
47	Windows Server 2016 DNS Server	TWG CB-01-007-0373	系統服務	KtmRm for Distributed Transaction Coordinator	▪ 這項原則設定決定此電腦是否可使用 Kernel Transaction Manager (KTM)之服務 ▪ 協調分散式交易協調器(MSDTC)與核心交易管理員(KTM)之間的交易。如果不需要這樣做，建議讓此服務維持在停止狀態。如果需要這樣做，MSDTC 與 KTM 都會自動啟動此服務 ▪ 如果停用此服務，任何與核心資源管理員互動的 MSDTC 交易都會失敗，且任何明確依存於此服務的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\KtmRm for Distributed Transaction Coordinator	手動	
48	Windows Server	TWG CB-01	系統服務	Link-Layer Topology	▪ 這項原則設定決定此電腦是否可使用 Link-Layer Topology Discovery	電腦設定\Windows 設定	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 DNS Server	-007-0374		Discovery Mapper	Mapper 服務 ▪ 此服務可建立網路圖，其中包含電腦及裝置拓撲(連線能力)資訊以及描述每台電腦與裝置的中繼資料 ▪ 如果這個服務已停用，網路圖將無法正常運作	\安全性設定\系統服務\Link-Layer Topology Discovery Mapper		
49	Windows Server 2016 DNS Server	TWG CB-01-007-0375	系統服務	Local Session Manager	▪ 這項原則設定用於管理本機使用者工作階段的核心 Windows 服務 ▪ 停止或停用此服務將會導致系統不穩定	電腦設定\Windows 設定\安全性設定\系統服務\Local Session Manager	自動	
50	Windows Server 2016 DNS Server	TWG CB-01-007-0376	系統服務	Microsoft iSCSI Initiator Service	▪ 這項原則設定決定此電腦是否可使用 Microsoft iSCSI 服務，用以管理從這部電腦連線至遠端 iSCSI 目標裝置的 Internet SCSI(iSCSI)工作階段	電腦設定\Windows 設定\安全性設定\系統服務\Microsoft	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果此服務停止，這部電腦將無法登入或存取 iSCSI 目標 ▪如果此服務停用，所有明確依存於它的服務都將無法啟動	iSCSI Initiator Service		
51	Windows Server 2016 DNS Server	TWG CB-01-007-0377	系統服務	Microsoft Software Shadow Copy Provider	▪這項原則設定決定此電腦是否可使用 Microsoft Software Shadow Copy Provider 服務，以管理磁碟區陰影複製服務所取得的以軟體為主的磁碟區陰影複製 ▪如果停止這個服務，就無法管理以軟體為主的磁碟區陰影複製 ▪如果停用這個服務，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Microsoft Software Shadow Copy Provider	手動	
52	Windows Server 2016 DNS	TWG CB-01-007-0378	系統服務	Net.Tcp Port Sharing Service	▪這項原則設定決定此電腦是否可使用 Net.Tcp Port Sharing 服務 ▪此服務提供在 net.tcp 通訊協定上共用 TCP 連接埠的能力	電腦設定\Windows 設定\安全性設定\系統服務	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server					\Net.Tcp Port Sharing Service		
53	Windows Server 2016 DNS Server	TWG CB-01-007-0379	系統服務	Netlogon	▪ 這項原則設定決定此電腦是否可使用 Netlogon 服務 ▪ 此服務維持這個電腦與網域控制站間用於驗證使用者與服務的安全通道 ▪ 如果這個服務被停止，電腦可能無法驗證使用者與服務，且網域控制站將無法登錄 DNS 記錄 ▪ 如果這個服務被停用，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Netlogon	自動	
54	Windows Server 2016 DNS	TWG CB-01-007-0380	系統服務	Network Connections	▪ 這項原則設定決定此電腦是否可使用 Network Connections 服務 ▪ 此服務可管理在網路與撥號連線資料夾中的物件，可以在此資料夾中	電腦設定\Windows 設定\安全性設定\系統服務	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server				檢視區域網路與遠端連線	\Network Connections		
55	Windows Server 2016 DNS Server	TWG CB-01-007-0381	系統服務	Network Connectivity Assistant	▪ 這項原則設定決定此電腦是否可使用 Network Connectivity Assistant 服務 ▪ 此服務提供 UI 元件的 DirectAcces 狀態通知	電腦設定\Windows 設定\安全性設定\系統服務\Network Connectivity Assistant	手動	
56	Windows Server 2016 DNS Server	TWG CB-01-007-0382	系統服務	Network List Service	▪ 這項原則設定決定此電腦是否可使用網路識別服務 ▪ 識別電腦已連線的網路、蒐集並儲存這些網路的內容，並在這些內容變更時通知應用程式	電腦設定\Windows 設定\安全性設定\系統服務\Network List Service	手動	
57	Windows Server	TWG CB-01	系統服務	Network Location	▪ 這項原則設定決定此電腦是否可使用 Network Location Awareness 服	電腦設定\Windows 設定	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 DNS Server	-007-0383		Awareness	務，以蒐集及儲存網路的設定資訊，並且在修改此資訊時，通知程式 ▪如果停止此服務，設定資訊就可能會無法使用 ▪如果停用此服務，則明確依賴它的任何服務將會無法啟動	\安全性設定\系統服務\Network Location Awareness		
58	Windows Server 2016 DNS Server	TWG CB-01-007-0384	系統服務	Network Store Interface Service	▪這項原則設定決定此電腦是否可使用 Network Store Interface Service 服務 ▪此服務可將網路通知(例如介面的新增/刪除等)傳遞給使用者模式的用戶端 ▪停止此服務將造成網路連線中斷 ▪如果這個服務被停用，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Network Store Interface Service	自動	
59	Windows	TWG	系統	Optimize	▪這項原則設定決定此電腦是否可使	電腦設定	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 DNS Server	CB-01-007-0385	服務	drives	用 Optimize drives 服務 ▪ 此服務可最佳化存放磁碟機上的檔案，以協助提高電腦執行效率	\Windows 設定\安全性設定\系統服務\Optimize drives		
60	Windows Server 2016 DNS Server	TWG CB-01-007-0386	系統服務	Performance Counter DLL Host	▪ 這項原則設定決定此電腦是否可使用 Performance Counter DLL Host 服務 ▪ 此服務允許遠端使用者與 64 位元處理程序查詢 32 位元 DLL 提供的效能計數器 ▪ 如果這項服務停止，則只有本機使用者與 32 位元處理程序可以查詢 32 位元 DLL 提供的效能計數器	電腦設定\Windows 設定\安全性設定\系統服務\Performance Counter DLL Host	手動	
61	Windows Server 2016	TWG CB-01-007-0	系統服務	Performance Logs & Alerts	▪ 這項原則設定決定此電腦是否可使用 Performance Logs & Alerts 服務 ▪ 效能記錄及警示會根據預先設定的	電腦設定\Windows 設定\安全性設定\	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	DNS Server	387			排程參數，從本機或遠端電腦蒐集效能資料，然後寫入資料到記錄檔或觸發警示 ▪如果停止此服務，將不會蒐集效能資訊 ▪如果這個服務已停用，所有依存於它的服務都將無法啟動	系統服務\Performance Logs & Alerts		
62	Windows Server 2016 DNS Server	TWG CB-01-007-0388	系統服務	Plug and Play	▪這項原則設定決定此電腦是否可識別硬體變更之服務 ▪啟用電腦以使用者沒有或很少的輸入來識別及適應硬體變更，停止或停用這個服務將導致系統不穩定	電腦設定\Windows 設定\安全性設定\系統服務\Plug and Play	手動	
63	Windows Server 2016 DNS Server	TWG CB-01-007-0389	系統服務	Portable Device Enumerator Service	▪這項原則設定決定此電腦之群組原則是否可對卸除式媒體進行管理與強制執行 ▪強制卸除式大型存放裝置使用群組原則。可讓 Windows Media Player	電腦設定\Windows 設定\安全性設定\系統服務\Portable	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					及影像匯入精靈等應用程式，得以使用卸除式大型存放裝置，來傳輸並同步處理內容	Device Enumerator Service		
64	Windows Server 2016 DNS Server	TWG CB-01-007-0390	系統服務	Power	這項原則設定決定此電腦是否可使用 Power 服務，以管理電源原則與電源原則通知傳遞	電腦設定\Windows 設定\安全性設定\系統服務\Power	自動	
65	Windows Server 2016 DNS Server	TWG CB-01-007-0391	系統服務	Print Spooler	▪ 這項原則設定決定此電腦是否啟用 Print Spooler 服務 ▪ 此服務會多工緩衝處理列印工作，並處理與印表機的互動 ▪ 如果關閉此服務，將無法列印或看見印表機	電腦設定\Windows 設定\安全性設定\系統服務\Print Spooler	自動	
66	Windows Server 2016	TWG CB-01-007-0	系統服務	Printer Extensions and	▪ 這項原則設定決定此電腦是否啟用 Printer Extensions and Notifications 服務	電腦設定\Windows 設定\安全性設定\	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	DNS Server	392		Notifications	▪ 此服務會開啟自訂印表機對話方塊，以及處理來自遠端列印伺服器或印表機的通知 ▪ 如果關閉此服務，則無法查看印表機延伸或通知	系統服務\Printer Extensions and Notifications		
67	Windows Server 2016 DNS Server	TWG CB-01-007-0393	系統服務	Problem Reports and Solutions Control Panel Support	▪ 這項原則設定決定此電腦是否可使用問題回報與解法諮詢控制台之服務 ▪ 此服務提供檢視、傳送及刪除「問題報告及解決方案」控制台中之系統等級問題報告的支援	電腦設定\Windows 設定\安全性設定\系統服務\Problem Reports and Solutions Control Panel Support	手動	
68	Windows Server 2016	TWG CB-01-007-0	系統服務	Remote Access Auto Connection	這項原則設定決定此電腦是否可使用遠端自動連線之服務。當程式參照遠端 DNS 或 NetBIOS 名稱或位址	電腦設定\Windows 設定\安全性設定\	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	DNS Server	394		Manager	時，建立遠端網路的連線	系統服務\Remote Access Auto Connection Manager		
69	Windows Server 2016 DNS Server	TWG CB-01-007-0395	系統服務	Remote Access Connection Manager	▪ 這項原則設定決定此電腦是否可使用 VPN 服務，以管理這台電腦到網際網路或其他遠端網路的撥號及虛擬私人網路(VPN)連線 ▪ 如果這個服務已停用，所有依存於它的服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Remote Access Connection Manager	手動	
70	Windows Server 2016 DNS	TWG CB-01-007-0396	系統服務	Remote Desktop Configuration	▪ 這項原則設定決定此電腦是否可使用 Remote Desktop Configuration service (RDCS)服務 ▪ 遠端桌面設定服務(RDCS)負責處理	電腦設定\Windows 設定\安全性設定\系統服務\Remote	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server				與遠端桌面服務及遠端桌面相關的設定及工作階段維護活動(需要系統內容)。這些包括每一工作階段暫存資料夾、遠端桌面主題與遠端桌面憑證	Desktop Configuration		
71	Windows Server 2016 DNS Server	TWG CB-01-007-0397	系統服務	Remote Desktop Services	▪ 這項原則設定決定此電腦是否可使用 Remote Desktop Services 服務，以允許使用者以互動方式連線到遠端電腦 ▪ 遠端桌面及遠端桌面工作階段主機伺服器都需要依賴此服務。若要避免從遠端使用這部電腦，請取清除「系統內容」控制台項目的「遠端」索引標籤上的核取方塊	電腦設定\Windows 設定\安全性設定\系統服務\Remote Desktop Services	手動	
72	Windows Server 2016	TWG CB-01-007-0	系統服務	Remote Desktop Services	▪ 這項原則設定決定此電腦是否可使用 Remote Desktop Services UserMode Port Redirector 服務	電腦設定\Windows 設定\安全性設定\	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	DNS Server	398		UserMode Port Redirector	▪此項服務允許重新導向 RDP 連線的印表機、磁碟機及連接埠	系統服務\Remote Desktop Services UserMode Port Redirector		
73	Windows Server 2016 DNS Server	TWG CB-01-007-0399	系統服務	Remote Procedure Call (RPC)	▪這項原則設定決定此電腦是否可使用 Remote Procedure Call (RPC)服務 ▪RPCSS 服務是 COM 與 DCOM 伺服器的服務控制管理員。該服務會為 COM 與 DCOM 伺服器執行物件啟用要求、物件輸出程式解析，以及分散式記憶體回收 ▪如果停止或停用此服務，使用 COM 或 DCOM 的程式將無法正常運作。強烈建議持續執行 RPCSS 服務	電腦設定\Windows 設定\安全性設定\系統服務\Remote Procedure Call (RPC)	自動	
74	Windows	TWG	系統	Remote	▪這項原則設定決定此電腦是否可使	電腦設定	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 DNS Server	CB-01-007-0400	服務	Procedure Call (RPC) Locator	用 Remote Procedure Call (RPC) Locator 服務 ▪ 在 Windows 2003 以及更舊的 Windows 版本中，遠端程序呼叫(RPC)尋找程式服務負責管理 RPC 名稱服務資料庫 ▪ 在 Windows Vista 與更新的 Windows 版本中，此服務不提供任何功能，只是為了應用程式相容性而保留	\Windows 設定\安全性設定\系統服務\Remote Procedure Call (RPC) Locator		
75	Windows Server 2016 DNS Server	TWG CB-01-007-0401	系統服務	Remote Registry	▪ 這項原則設定決定此電腦是否可使用 Remote Registry 服務，由遠端使用者修改這個電腦上的登錄設定 ▪ 如果這個服務被停止，登錄只能由這個電腦上的使用者修改 ▪ 如果這個服務被停用，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Remote Registry	自動	
76	Windows	TWG	系統	Resultant Set	這項原則設定決定此電腦是否提供	電腦設定	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 DNS Server	CB-01-007-0402	服務	of Policy Provider	網路服務來處理要求，以模擬在各種情況下，將「群組原則」設定值套用至目標使用者或電腦，並推斷「原則結果組」設定值	\Windows 設定\安全性設定\系統服務\Resultant Set of Policy Provider		
77	Windows Server 2016 DNS Server	TWG CB-01-007-0403	系統服務	Routing and Remote Access	這項原則設定決定此電腦是否可於本機區域與網路使用 Routing 之服務。提供連到區域網路及廣域網路的公司的路由服務	電腦設定\Windows 設定\安全性設定\系統服務\Routing and Remote Access	已停用	
78	Windows Server 2016 DNS Server	TWG CB-01-007-0404	系統服務	RPC Endpoint Mapper	▪ 這項原則設定決定此電腦是否可使用 RPC Endpoint Mapper 服務，以解析 RPC 介面識別元為傳輸端點 ▪ 如果此服務停止或停用，使用遠端程序呼叫(RPC)服務的程式將無法	電腦設定\Windows 設定\安全性設定\系統服務\RPC Endpoint	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					正常運作	Mapper		
79	Windows Server 2016 DNS Server	TWG CB-01-007-0405	系統服務	Secondary Logon	▪這項原則設定決定此電腦是否可以在其他認證中啟動處理程序 ▪如果這個服務停止，將無法使用這個登入存取類型。如果這個服務已停用，它的所有依存服務都無法開始	電腦設定\Windows 設定\安全性設定\系統服務\Secondary Logon	手動	
80	Windows Server 2016 DNS Server	TWG CB-01-007-0406	系統服務	Secure Socket Tunneling Protocol Service	▪這項原則設定決定此電腦是否可使用 Secure Socket Tunneling Protocol (SSTP)服務，以提供安全通訊端通道通訊協定(SSTP)使用 VPN 連線到遠端電腦的支援 ▪如果停用此服務，使用者將無法使用 SSTP 存取遠端伺服器	電腦設定\Windows 設定\安全性設定\系統服務\Secure Socket Tunneling Protocol Service	手動	
81	Windows Server	TWG CB-01	系統服務	Security Accounts	▪這項原則設定決定此電腦是否可使用 Security Accounts Manager 服	電腦設定\Windows 設定	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 DNS Server	-007-0407		Manager	務，以告知其他服務，安全性帳戶管理員(SAM)已準備好要接受要求 ▪停用此服務將阻止通知系統中的其他服務 SAM 已經就緒，而導致那些服務無法正確地啟動 ▪此服務不應該停用	\安全性設定\系統服務\Security Accounts Manager		
82	Windows Server 2016 DNS Server	TWG CB-01-007-0408	系統服務	Server	▪這項原則設定決定此電腦是否使用 Server 服務 ▪為這個電腦支援網路上檔案、列印及命名管線的共用 ▪如果停止此服務，將無法使用這些功能 ▪如果這個服務被停用，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Server	自動	
83	Windows Server 2016	TWG CB-01-007-0	系統服務	Shell Hardware Detection	▪這項原則設定決定此電腦是否可使用 Shell Hardware Detection 服務 ▪此項服務為自動播放硬體事件提供	電腦設定\Windows 設定\安全性設定\	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	DNS Server	409			通知	系統服務 \Shell Hardware Detection		
84	Windows Server 2016 DNS Server	TWG CB-01 -007-0 410	系統服務	Smart Card	▪ 這項原則設定決定此電腦是否可使用智慧卡功能 ▪ 管理這個電腦所讀取智慧卡的存取。如果這個服務被停止，這個電腦將無法讀取智慧卡。如果這個服務被停用，任何明確依存於它的服務將無法啟動	電腦設定 \Windows 設定 \安全性設定\ 系統服務 \Smart Card	已停用	
85	Windows Server 2016 DNS Server	TWG CB-01 -007-0 411	系統服務	Smart Card Removal Policy	這項原則設定決定此電腦是否可透過智慧卡移除動作進行使用者電腦鎖定之服務。允許將系統設定為在智慧卡移除時，鎖定使用者桌面	電腦設定 \Windows 設定 \安全性設定\ 系統服務 \Smart Card Removal	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						Policy		
86	Windows Server 2016 DNS Server	TWG CB-01-007-0412	系統服務	SNMP Trap	▪ 這項原則設定決定此電腦是否可使用 SNMP Trap 服務，以接收由本機或遠端簡易網路管理通訊協定(SNMP)代理程式所產生的陷阱訊息，並轉送該訊息給在這個電腦上執行中的 SNMP 管理程式 ▪ 如果這個服務被停止，這個電腦上 SNMP 為主的程式將不接收 SNMP 陷阱訊息。如果這個服務被停用，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\SNMP Trap	手動	
87	Windows Server 2016 DNS Server	TWG CB-01-007-0413	系統服務	Software Protection	▪ 這項原則設定決定此電腦是否可使用 Software Protection 功能，以針對 Window 及 Windows 應用程式，啟用數位授權的下載、安裝及強制執行功能	電腦設定\Windows 設定\安全性設定\系統服務\Software	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果停用該服務，作業系統及已授權的應用程式可能會以通知模式來執行 ▪強烈建議不要停用軟體保護服務	Protection		
88	Windows Server 2016 DNS Server	TWG CB-01-007-0414	系統服務	Special Administration Console Helper	這項原則設定決定是否允取系統管理員使用緊急管理服務，遠端存取命令提示字元	電腦設定\Windows 設定\安全性設定\系統服務\Special Administration Console Helper	手動	
89	Windows Server 2016 DNS Server	TWG CB-01-007-0415	系統服務	Spot Verifier	這項原則設定決定是否檢查可能的檔案系統損毀	電腦設定\Windows 設定\安全性設定\系統服務\Spot Verifier	手動	
90	Windows	TWG	系統	SSDP	▪這項原則設定決定此電腦是否使用	電腦設定	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 DNS Server	CB-01-007-0416	服務	Discovery	SSDP 協定 ▪ 探索使用 SSDP 探索通訊協定且已連上網路的裝置及服務，例如 UPnP 裝置。還會宣告在本機電腦上執行的 SSDP 裝置及服務 ▪ 如果停止此服務，將會無法探索 SSDP 型的裝置。如果這個服務已停用，所有依存於它的服務都將無法啟動	\Windows 設定\安全性設定\系統服務\SSDP Discovery		
91	Windows Server 2016 DNS Server	TWG CB-01-007-0417	系統服務	Superfetch	這項原則設定決定是否維護與改進一段時間後的系統效能	電腦設定\Windows 設定\安全性設定\系統服務\Superfetch	手動	
92	Windows Server 2016	TWG CB-01-007-0	系統服務	System Event Notification Service	▪ 這項原則設定決定此電腦是否可使用系統事件監控與提示服務，以監視系統事件，並通知「COM+事件系	電腦設定\Windows 設定\安全性設定\	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	DNS Server	418			統」的訂閱者有關這些事件的內容	系統服務\System Event Notification Service		
93	Windows Server 2016 DNS Server	TWG CB-01-007-0419	系統服務	Task Scheduler	▪這項原則設定決定此電腦是否可使用 Task Scheduler 服務，讓使用者能夠在這台電腦上設定與排定自動的工作。此服務也主控多個 Windows 系統重要的工作 ▪如果停止或停用這個服務，這些工作將不會在其排定的時間執行 ▪如果停用這個服務，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Task Scheduler	自動	
94	Windows Server 2016 DNS	TWG CB-01-007-0420	系統服務	TCP/IP NetBIOS Helper	▪這項原則設定決定此電腦是否可使用 TCP/IP NetBIOS Helper 服務，以提供對 NetBIOS over TCP/IP 以及網路上用戶端 NetBIOS 名稱解析的支	電腦設定\Windows 設定\安全性設定\系統服務	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server				援，因此讓使用者可以共用檔案、列印以及登入到網路 ▪ 如果這個服務被停止，可能無法使用這些功能 ▪ 如果這個服務被停用，任何明確依存於它的服務將無法啟動	\TCP/IP NetBIOS Helper		
95	Windows Server 2016 DNS Server	TWG CB-01-007-0421	系統服務	Telephony	▪ 這項原則設定決定此電腦是否可使用 Telephony API (TAPI)服務 ▪ 此服務為程式提供電話語音 API(TAPI)支援，讓程式可以控制本機電腦上的電話語音裝置，或透過區域網路控制也同時執行該服務之伺服器上的電話語音裝置	電腦設定 \Windows 設定 \安全性設定\ 系統服務 \Telephony	手動	
96	Windows Server 2016 DNS	TWG CB-01-007-0422	系統服務	Themes	▪ 這項原則設定決定此電腦是否可使用 Themes 服務 ▪ 此服務提供使用者經驗主題管理	電腦設定 \Windows 設定 \安全性設定\ 系統服務	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server					\Themes		
97	Windows Server 2016 DNS Server	TWG CB-01-007-0423	系統服務	UPnP Device Host	▪ 這項原則設定決定此電腦是否可使用 UPnP Device Host 服務，允許在此電腦上裝載 UPnP 裝置 ▪ 如果停止此服務，任何裝載的 UPnP 裝置都將停止運作且無法新增其他裝載的裝置 ▪ 如果停用此服務，明確依存於此服務的任何服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\UPnP Device Host	已停用	
98	Windows Server 2016 DNS Server	TWG CB-01-007-0424	系統服務	User Access Logging Service	▪ 這項原則設定決定此電腦是否可使用 User Access Logging Service 服務 ▪ 此服務會記錄本機伺服器上所安裝產品與角色的唯一用戶端存取要求(形式為 IP 位址與使用者名稱)。當系統管理員需要將伺服器軟體的用戶端需求量化以進行離線用戶端存取授權(CAL)管理時，可以透過	電腦設定\Windows 設定\安全性設定\系統服務\User Access Logging Service	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					Powershell 查詢此資訊 ▪ 如果停用此服務，則用戶端要求不會留下記錄，也無法供人透過 Powershell 查詢抓取。停止此服務並不會影響歷史資料的查詢。本機系統管理員必須參閱其 Windows Server 授權條款，以決定要對伺服器軟體進行適當授權所需的 CAL 數目；使用 UAL 服務與資料並不會變更此義務			
99	Windows Server 2016 DNS Server	TWG CB-01-007-0425	系統服務	User Profile Service	▪ 這項原則設定決定此電腦是否可使用 User Profile Service 服務 ▪ 此服務負責載入及解除載入使用者設定檔 ▪ 如果停止或停用此服務，使用者將無法順利登入或登出，應用程式可能會在取得使用者的資料時發生問題，用來接收設定檔事件通知的已	電腦設定\Windows 設定\安全性設定\系統服務\User Profile Service	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					註冊元件將無法接收通知			
100	Windows Server 2016 DNS Server	TWG CB-01-007-0426	系統服務	Virtual Disk	▪ 這項原則設定決定此電腦是否可使用 Virtual Disk 服務 ▪ 此服務提供磁碟、磁碟區、檔案系統及存放裝置陣列的管理	電腦設定\Windows 設定\安全性設定\系統服務\Virtual Disk	手動	
101	Windows Server 2016 DNS Server	TWG CB-01-007-0427	系統服務	Volume Shadow Copy	▪ 這項原則設定決定此電腦是否可使用硬體空間之 Shadow Copy 服務，以管理及執行用於備份與其他目的的磁碟區陰影複製 ▪ 如果這個服務被停止，陰影複製將無法用於備份，備份可能會失敗。如果這個服務被停用，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Volume Shadow Copy	手動	
102	Windows Server 2016	TWG CB-01-007-0	系統服務	Windows Audio	▪ 這項原則設定決定此電腦是否可使用音訊之服務，以管理 Windows 程式的音訊	電腦設定\Windows 設定\安全性設定\	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	DNS Server	428			▪如果這個服務停止，音訊裝置及效果將無法正常運作 ▪如果停用這個服務，將無法啟動明確依賴此服務的任何服務	系統服務\Windows Audio		
103	Windows Server 2016 DNS Server	TWG CB-01-007-0429	系統服務	Windows Audio Endpoint Builder	▪這項原則設定決定此電腦是否可使用 Windows Audio Endpoint Builder 服務，以管理 Windows 音訊服務的音訊裝置 ▪如果停止此服務，音訊裝置與效果將無法正常運作 ▪如果停用此服務，所有明確依存於它的服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Windows Audio Endpoint Builder	手動	
104	Windows Server 2016 DNS Server	TWG CB-01-007-0430	系統服務	Windows Driver Foundation-User-mode Driver	▪這項原則設定決定此電腦是否可使用 Windows Driver Foundation-User-mode Driver Framework 服務，以建立並管理使用者模式驅動程式處理程序	電腦設定\Windows 設定\安全性設定\系統服務\Windows	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
				Framework	▪ 無法停止此服務	Driver Foundation-User-mode Driver Framework		
105	Windows Server 2016 DNS Server	TWG CB-01-007-0431	系統服務	Windows Error Reporting Service	▪ 這項原則設定決定此電腦是否可使用 Windows Error Reporting Service 服務 ▪ 此服務在程式停止運作或停止回應時，允許回報錯誤，並且允許傳遞現有的解決方案。此外，也允許產生用於診斷與修復服務的記錄檔 ▪ 如果此服務已停止，錯誤報告就可能無法正常運作，並且可能因此無法顯示診斷服務及修復的結果	電腦設定\Windows 設定\安全性設定\系統服務\Windows Error Reporting Service	手動	
106	Windows Server 2016	TWG CB-01-007-0	系統服務	Windows Event Collector	▪ 這項原則設定決定此電腦之 Windows 事件蒐集服務是否啟用 ▪ 此服務管理支援 WS-Management 通	電腦設定\Windows 設定\安全性設定\	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	DNS Server	432			訊協定之遠端來源事件的持續訂閱。這包括 Windows 事件記錄檔、硬體及啟用 IPMI 的事件來源。此服務會將轉送的事件儲存在本機事件記錄檔中 ▪如果此服務停止或停用，將無法建立事件訂閱，也無法接受轉送的事件	系統服務\Windows Event Collector		
107	Windows Server 2016 DNS Server	TWG CB-01-007-0433	系統服務	Windows Event Log	▪這項原則設定決定此電腦是否可使用 Windows Event Log 服務 ▪此服務管理事件與事件記錄檔，支援記錄事件、查詢事件、訂閱事件、封存事件記錄檔，以及管理事件中繼資料 ▪此服務可使用 XML 與純文字格式來顯示事件 ▪停止這個服務可能危害系統的安全	電腦設定\Windows 設定\安全性設定\系統服務\Windows Event Log	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					性與可靠性			
108	Windows Server 2016 DNS Server	TWG CB-01-007-0434	系統服務	Windows Firewall	▪這項原則設定決定此電腦是否可使用 Windows 防火牆服務 ▪Windows 防火牆經由阻止未授權使用者透過網際網路或網路取得對電腦的存取來保護電腦	電腦設定\Windows 設定\安全性設定\系統服務\Windows Firewall	自動	
109	Windows Server 2016 DNS Server	TWG CB-01-007-0435	系統服務	Windows Font Cache Service	▪這項原則設定決定此電腦是否可使用 Windows Font Cache Service 服務，以透過快取常用的字型資料，可以最佳化應用程式效能 ▪如果這個服務尚未執行，應用程式便會啟動該服務。也可以停用此服務，不過這樣做會降低應用程式效能	電腦設定\Windows 設定\安全性設定\系統服務\Windows Font Cache Service	自動	
110	Windows Server	TWG CB-01	系統服務	Windows Installer	▪這項原則設定決定此電腦是否可使用 Windows Installer 服務，以新增、	電腦設定\Windows 設定	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 DNS Server	-007-0436			修改及移除以 Windows Installer (*.msi、*.msp)套件形式提供的應用程式 ▪如果停用此服務，所有明確依存於它的服務都將無法啟動	\安全性設定\系統服務\Windows Installer		
111	Windows Server 2016 DNS Server	TWG CB-01-007-0437	系統服務	Windows Management Instrumentation	▪這項原則設定決定此電腦是否可使用 Windows Management Instrumentation 服務，透過提供公用介面及物件模型，以存取有關作業系統、裝置、應用程式及服務的管理資訊 ▪如果這個服務已停止，大多數的 Windows 軟體將無法正常運作 ▪如果這個服務已停用，所有依存於它的服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Windows Management Instrumentation	自動	
112	Windows Server	TWG CB-01	系統服務	Windows Modules	▪這項原則設定決定此電腦是否可使用 Windows 功能模組安裝服務	電腦設定\Windows 設定	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 DNS Server	-007-0438		Installer	▪ 此服務可以安裝、修改以及移除 Windows 更新與選用的元件 ▪ 如果停用此服務，則此電腦的安裝或解除安裝 Windows 更新可能會失敗	\安全性設定\系統服務\Windows Modules Installer		
113	Windows Server 2016 DNS Server	TWG CB-01-007-0439	系統服務	Windows Remote Management (WS-Management)	▪ 這項原則設定決定此電腦是否可使用 Windows 遠端管理服務 ▪ Windows 遠端管理(WinRM)服務為遠端管理實作 WS-Management 通訊協定 ▪ WS-Management 適用於遠端軟體與硬體管理的標準 Web 服務通訊協定。WinRM 服務會接聽並處理網路上的 WS-Management 要求。必須使用 winrm.cmd 命令列工具或透過群組原則來設定 WinRM 服務搭配接聽程式，它才能接聽網路上的要求	電腦設定\Windows 設定\安全性設定\系統服務\Windows Remote Management (WS-Management)	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪WinRM 服務提供 WMI 資料的存取，並能蒐集事件資料。必須執行此服務，對於事件的事件蒐集與訂閱才能運作。WinRM 訊息使用 HTTP 與 HTTPS 來進行傳輸 ▪WinRM 服務不需依賴 IIS，但它的預先設定會在相同的電腦上與 IIS 共用相同的連接埠。WinRM 服務保留/wsman URL 首碼。為避免與 IIS 衝突，系統管理員應該確定 IIS 上執行的所有網站都不會使用/wsman URL 首碼			
114	Windows Server 2016 DNS Server	TWG CB-01-007-0440	系統服務	Windows Time	▪這項原則設定決定此電腦是否可使用 Windows Time 服務，以維護在網路上所有用戶端及伺服器的資料及時間同步處理 ▪如果這個服務停止，將無法進行日期與時間同步處理	電腦設定\Windows 設定\安全性設定\系統服務\Windows Time	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果這個服務被停用，所有依存的服務都會停止			
115	Windows Server 2016 DNS Server	TWG CB-01-007-0441	系統服務	Windows Update	▪這項原則設定決定此電腦是否可使用 Windows Update 服務，以偵測、下載並安裝 Windows 或其他程式的更新 ▪如果停用此服務，這部電腦的使用者將無法使用 Windows Update 或其自動更新功能。而且程式將無法使用 Windows Update Agent(WUA)API	電腦設定\Windows 設定\安全性設定\系統服務\Windows Update	手動	
116	Windows Server 2016 DNS Server	TWG CB-01-007-0442	系統服務	WinHTTP Web Proxy Auto-Discovery Service	▪這項原則設定決定此電腦是否可使用 WinHTTP Web Proxy Auto-Discovery Service 服務 ▪WinHTTP 會實作用戶端 HTTP 堆疊並提供開發人員 Win32 API 及 COM 自動化元件來傳送 HTTP 要求及接	電腦設定\Windows 設定\安全性設定\系統服務\WinHTTP Web Proxy	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					收回應。此外，WinHTTP 透過實作 Web Proxy Auto-Discovery(WPAD) 通訊協定,提供自動探索 Proxy 設定的支援	Auto-Discovery Service		
117	Windows Server 2016 DNS Server	TWG CB-01-007-0443	系統服務	Wired AutoConfig	▪ 這項原則設定決定此電腦是否可使用 Wired AutoConfig 服務 ▪ 此項服務將於乙太網路卡上執行 IEEE 802.1X 驗證 ▪ 有線自動設定(DOT3SVC)服務負責在乙太網路介面上執行 IEEE 802.1X 驗證。如果目前的有線網路部署強制執行 802.1X 驗證，則應該設定執行 DOT3SVC 服務以建立第二層連線及/或提供網路資源存取。未強制執行 802.1X 驗證的有線網路則不受 DOT3SVC 服務影響	電腦設定\Windows 設定\安全性設定\系統服務\Wired AutoConfig	手動	
118	Windows	TWG	系統	WMI	▪ 這項原則設定決定此電腦是否可使	電腦設定	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 DNS Server	CB-01-007-0444	服務	Performance Adapter	用 WMI Performance Adapter 服務 ▪ 提供來自 Windows Management Instrumentation(WMI)提供者的效能程式庫資訊給網路上的用戶端。只有在啟用效能資料協助程式時，這個服務才會執行	\Windows 設定\安全性設定\系統服務\WMI Performance Adapter		
119	Windows Server 2016 DNS Server	TWG CB-01-007-0445	系統服務	Workstation	▪ 這項原則設定決定此電腦是否使用 Workstation 服務，用以建立及維護使用 SMB 通訊協定進行的用戶端與遠端伺服器網路連線 ▪ 如果停止這個服務，將無法使用這些連線 ▪ 如果停用這個服務，則會停止所有明確依存它的服務	電腦設定\Windows 設定\安全性設定\系統服務\Workstation	自動	

資料來源：本中心整理

表5　Windows Server 2016 File Server 政府組態基準列表

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
1	Windows Server 2016 File Server	TWGCB-01-007-0446	系統服務	Application Identity	▪這項原則設定決定此電腦是否可使用 Application Identity 之服務，用以判斷並確定應用程式的識別 ▪如果停用此服務，將使 AppLocker 無法強制執行	電腦設定\Windows 設定\安全性設定\系統服務\Application Identity	手動	CCE-ID：CCE-47123-5
2	Windows Server 2016 File Server	TWGCB-01-007-0447	系統服務	Application Information	▪這項原則設定決定此電腦是否可使用 Application Information 服務，以其他管理權限協助執行互動式應用程式。使用者在執行想要的工作時可能會需要這些權限 ▪如果停止此服務，使用者將無法以其他管理權限來啟動應用程式	電腦設定\Windows 設定\安全性設定\系統服務\Application Information	手動	
3	Windows Server 2016 File	TWGCB-01-007-0	系統服務	Application Layer Gateway Service	這項原則設定決定此電腦是否可使用 Application Layer Gateway Service 服務，以對網際網路連線共	電腦設定\Windows 設定\安全性設定\系	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server	448			用提供協力廠商通訊協定外掛程式的支援	統服務\Application Layer Gateway Service		
4	Windows Server 2016 File Server	TWG CB-01-007-0449	系統服務	Application Management	▪ 這項原則設定決定此電腦是否可使用應用程式管理服務 ▪ 針對透過「群組原則」來部署的軟體，處理安裝、移除及列舉要求。若將此服務停用，使用者將無法安裝、移除及列舉透過「群組原則」來部署的軟體，而且與其具有明確相依關係的任何服務，也將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Application Management	手動	
5	Windows Server 2016 File Server	TWG CB-01-007-0450	系統服務	Background Intelligent Transfer Service	▪ 這項原則設定決定此電腦是否可使用 Background Intelligent Transfer Service 服務，以使用閒置的網路頻寬在背景傳輸檔案	電腦設定\Windows 設定\安全性設定\系統服務	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 如果停用此服務，所有依存於 BITS 的應用程式(例如，Windows Update 或 MSN Explorer)將無法自動下載程式或其他資訊	\Background Intelligent Transfer Service		
6	Windows Server 2016 File Server	TWG CB-01-007-0451	系統服務	Background Tasks Infrastructure Service	這項原則設定決定此電腦是否可使用 Background Tasks Infrastructure Service 服務，以控制哪些背景工作可在系統上執行的 Windows 基礎結構服務	電腦設定\Windows 設定\安全性設定\系統服務\Background Tasks Infrastructure Service	自動	
7	Windows Server 2016 File Server	TWG CB-01-007-0452	系統服務	Base Filtering Engine	▪ 這項原則設定決定此電腦是否可使用 Base Filtering Engine (BFE)服務 ▪ 基礎篩選引擎(BFE)是管理防火牆與 IP 安全性(IPsec)原則，並執行使	電腦設定\Windows 設定\安全性設定\系統服務\Base Filtering Engine	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					用者模式篩選的服務 ▪停止或停用 BFE 服務將顯著降低系統的安全性。同時也導致 IPsec 管理與防火牆應用程式意外的行為			
8	Windows Server 2016 File Server	TWG CB-01-007-0453	系統服務	Certificate Propagation	▪這項原則設定決定此電腦是否可使用 Certificate Propagation 服務 從智慧卡將使用者憑證與根憑證複製到目前使用者的憑證存放區，當智慧卡插入智慧卡讀卡機時進行偵測，(若有需要)並安裝智慧卡隨插即用迷你驅動程式	電腦設定\Windows 設定\安全性設定\系統服務\Certificate Propagation	手動	
9	Windows Server 2016 File Server	TWG CB-01-007-0454	系統服務	CNG Key Isolation	▪這項原則設定決定此電腦是否可使用 CNG key isolation 服務 ▪CNG 金鑰隔離服務裝載於 LSA 處理程序。該服務可依據一般條件來隔離私密金鑰與相關聯加密編譯	電腦設定\Windows 設定\安全性設定\系統服務\CNG Key Isolation	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					操作的金鑰處理程序。該服務會以符合一般條件的安全處理程序來儲存與使用長效金鑰			
10	Windows Server 2016 File Server	TWG CB-01-007-0455	系統服務	COM+ Event System	▪ 這項原則設定決定此電腦是否可使用 COM+ Event System 服務 ▪ 支援「系統事件通知服務 (SENS)」，它可讓事件自動分散到訂閱的 COM 元件。如果服務被停止，SENS 會關閉，並無法提供登入及登出通知。如果此服務被停用，任何明顯依存它的服務都無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\COM+ Event System	自動	
11	Windows Server 2016 File Server	TWG CB-01-007-0456	系統服務	COM+ System Application	▪ 這項原則設定決定此電腦是否可使用 COM+ System Application 服務，以管理 COM+元件的設定及追蹤 ▪ 如果停止此服務，大部分的 COM+	電腦設定\Windows 設定\安全性設定\系統服務\COM+ System	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					元件將無法適當運作 ▪ 如果此服務被停用，任何明確依存它的服務將無法啟動	Application		
12	Windows Server 2016 File Server	TWG CB-01-007-0457	系統服務	Computer Browser	▪ 這項原則設定決定是否讓此電腦在網路上之其他使用者進行資源瀏覽 ▪ 維護網路上更新的電腦清單，並將這個清單提供給做為瀏覽器的電腦 ▪ 如果這個服務被停止，這個清單將不會被更新或維護 ▪ 如果這個服務被停用，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Computer Browser	已停用	
13	Windows Server 2016 File Server	TWG CB-01-007-0458	系統服務	Credential Manager	▪ 這項原則設定決定此電腦是否可使用 Credential Manager 服務 ▪ 此項服務提供使用者安全儲存以及擷取認證、應用程式以及安全性	電腦設定\Windows 設定\安全性設定\系統服務	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					服務封裝	\Credential Manager		
14	Windows Server 2016 File Server	TWG CB-01-007-0459	系統服務	Cryptographic Services	▪ 這項原則設定決定此電腦是否可使用 Cryptographic Services 服務 ▪ Cryptographic Services 提供 3 種管理服務： ➢ 目錄資料庫服務：確認 Windows 檔案的簽章並允許安裝新程式 ➢ 受保護的根目錄服務：從這部電腦新增及移除信任的根憑證授權單位憑證 ➢ 自動根憑證更新服務：從 Windows Update 抓取根憑證並啟用案例，例如 SSL ▪ 如果停止此服務，這些管理服務將無法正常運作 ▪ 如果停用此服務，任何明確需要它	電腦設定\Windows 設定\安全性設定\系統服務\Cryptographic Services	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					的服務將無法啟動			
15	Windows Server 2016 File Server	TWG CB-01-007-0460	系統服務	Data Deduplication Service	▪ 這項原則設定決定此電腦是否可使用 Data Deduplication Service 服務 ▪ 重複資料刪除服務能夠在選取的磁碟區上進行重複資料刪除與資料壓縮，以便將使用的磁碟空間最佳化 ▪ 如果停止這個服務，將不再進行最佳化，但已最佳化的資料仍可供存取	電腦設定\Windows 設定\安全性設定\系統服務\Data Deduplication Service	手動	
16	Windows Server 2016 File Server	TWG CB-01-007-0461	系統服務	Data Deduplication Volume Shadow Copy Service	▪ 這項原則設定決定此電腦是否可使用 Data Deduplication Volume 服務 ▪ 重複資料刪除 VSS 寫入器引導備份應用程式備份有重複資料刪除的磁碟區	電腦設定\Windows 設定\安全性設定\系統服務\Data Deduplication Volume Shadow	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						Copy Service		
17	Windows Server 2016 File Server	TWG CB-01-007-0462	系統服務	DCOM Server Process Launcher	▪ 這項原則設定決定此電腦是否可使用 DCOM Server Process Launcher 服務 ▪ DCOMLAUNCH 服務會啟動 COM 與 DCOM 伺服器，以回應物件啟用要求 ▪ 如果停止或停用此服務，使用 COM 或 DCOM 的程式將無法正常運作。強烈建議持續執行 DCOMLAUNCH 服務	電腦設定\Windows 設定\安全性設定\系統服務\DCOM Server Process Launcher	自動	
18	Windows Server 2016 File Server	TWG CB-01-007-0463	系統服務	Device Association Service	▪ 這項原則設定決定此電腦是否可使用 Device Association Service 服務 ▪ 此項服務啟用系統與有線或無線裝置之間的配對	電腦設定\Windows 設定\安全性設定\系統服務\Device Association Service	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
19	Windows Server 2016 File Server	TWG CB-01-007-0464	系統服務	Device Install Service	▪ 這項原則設定決定此電腦是否可使用 Device Install Service 服務，以使用者沒有或很少的輸入來識別及適應硬體變更 ▪ 停止或停用這個服務將導致系統不穩定	電腦設定\Windows 設定\安全性設定\系統服務\Device Install Service	手動	
20	Windows Server 2016 File Server	TWG CB-01-007-0465	系統服務	Device Setup Manager	▪ 這項原則設定決定此電腦是否可使用 Device Setup Manager 服務，以偵測、下載及安裝裝置相關軟體 ▪ 如果停用此服務，裝置可能會以過期的軟體設定，且可能無法正常運作	電腦設定\Windows 設定\安全性設定\系統服務\Device Setup Manager	手動	
21	Windows Server 2016 File Server	TWG CB-01-007-0466	系統服務	DFS Namespace	▪ 這項原則設定決定此電腦是否可使用 DFS Namespace 服務 ▪ 此服務可將位在不同伺服器的共用資料夾分組到一或多個邏輯結構命名空間。每個命名空間對使用	電腦設定\Windows 設定\安全性設定\系統服務\DFS Namespace	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					者而言都是含有一連串子資料夾的單一共用資料夾			
22	Windows Server 2016 File Server	TWG CB-01-007-0467	系統服務	DFS Replication	▪ 這項原則設定決定此電腦是否可使用 DFS Replication 服務 ▪ 此服務可透過本機或廣域網路(WAN)網路連線同步多部伺服器上的資料夾。這個服務使用遠端差異壓縮(RDC)通訊協定，僅更新自從上次複寫之後有變更的檔案	電腦設定\Windows 設定\安全性設定\系統服務\DFS Replication	自動	
23	Windows Server 2016 File Server	TWG CB-01-007-0468	系統服務	DHCP Client	▪ 這項原則設定決定此電腦是否可使用 DHCP Client 服務，以為這個電腦登錄及更新 IP 位址與 DNS 記錄 ▪ 如果這個服務被停止，這個電腦將會不接收動態 IP 位址與 DNS 更新 ▪ 如果這個服務被停用，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\DHCP Client	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
24	Windows Server 2016 File Server	TWG CB-01-007-0469	系統服務	Diagnostic Policy Service	▪ 這項原則設定決定此電腦是否可使用診斷原則服務 ▪ 診斷原則服務能夠偵測 Windows 元件的問題、進行疑難排解及提供解決方案 ▪ 如果停止此服務，便無法再進行診斷	電腦設定\Windows 設定\安全性設定\系統服務\Diagnostic Policy Service	自動	
25	Windows Server 2016 File Server	TWG CB-01-007-0470	系統服務	Diagnostic Service Host	▪ 這項原則設定決定此電腦之 Windows 元件錯誤診斷服務之是否啟用 ▪ 診斷原則服務會使用診斷服務裝載，裝載需要在本機服務內容上執行的診斷。如果此服務已停止，其上的任何診斷將不再產生作用	電腦設定\Windows 設定\安全性設定\系統服務\Diagnostic Service Host	手動	
26	Windows Server 2016 File	TWG CB-01-007-0	系統服務	Diagnostic System Host	▪ 這項原則設定決定此電腦是否可使用 Diagnostic System Host 服務 ▪ 診斷原則服務會使用診斷系統裝	電腦設定\Windows 設定\安全性設定\系	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server	471			載，裝載需要在本機服務內容上執行的診斷 ▪如果此服務已停止，其上的任何診斷將不再產生作用	統服務\Diagnostic System Host		
27	Windows Server 2016 File Server	TWG CB-01-007-0472	系統服務	Distributed Link Tracking Client	這項原則設定決定此電腦是否可使用 Distributed Link Tracking 服務，以維護電腦中或網路中不同電腦之 NTFS 檔案間的連結	電腦設定\Windows 設定\安全性設定\系統服務\Distributed Link Tracking Client	自動	
28	Windows Server 2016 File Server	TWG CB-01-007-0473	系統服務	Distributed Transaction Coordinator	▪這項原則設定決定此電腦之候選交易(Coordinates transactions)之管理服務是否啟動，以協調跨越多個資源管理員的交易，比如資料庫、訊息佇列及檔案系統 ▪如果此服務被停止，這些交易將會	電腦設定\Windows 設定\安全性設定\系統服務\Distributed Transaction	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					失敗 ▪ 如果這個服務已停用，所有依存於它的服務都將無法啟動	Coordinator		
29	Windows Server 2016 File Server	TWG CB-01-007-0474	系統服務	DNS Client	▪ 這項原則設定決定此電腦之 DNS Client 服務是否啟動 ▪ DNS 用戶端服務(dnscache)會為此電腦快取網域名稱系統(DNS)名稱並登錄完整的電腦名稱 ▪ 如果這個服務被停止，將會繼續解析 DNS 名稱。然而，將不會快取 DNS 名稱查詢的結果，而且不會登錄電腦名稱 ▪ 如果這個服務已停用，所有依存於它的服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\DNS Client	自動	
30	Windows Server 2016 File	TWG CB-01-007-0	系統服務	Encrypting File System (EFS)	▪ 這項原則設定決定此電腦是否啟用加密檔案系統服務，藉由提供核心檔案加密技術，可以在 NTFS 檔	電腦設定\Windows 設定\安全性設定\系	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server	475			案系統磁碟區上儲存加密的檔案 ▪ 如果此服務停止或停用，應用程式將無法存取加密的檔案	統服務\Encrypting File System (EFS)		
31	Windows Server 2016 File Server	TWG CB-01-007-0476	系統服務	Extensible Authentication Protocol	▪ 這項原則設定決定此電腦之延伸驗證協定(EAP)之服務是否啟用 ▪ 可延伸的驗證通訊協定(EAP)服務提供例如 802.1x 有線及無線、VPN 以及網路存取保護(NAP)環境中的網路驗證 ▪ EAP 在驗證程序期間，也提供網路存取用戶端(包括無線及 VPN 用戶端)使用的應用程式開發介面(API)。如果停用此服務，此電腦將無法存取需要 EAP 驗證的網路	電腦設定\Windows 設定\安全性設定\系統服務\Extensible Authentication Protocol	手動	
32	Windows Server 2016 File	TWG CB-01-007-0	系統服務	File Server Resource Manager	▪ 這項原則設定決定此電腦是否可使用 File Server Resource Manager 服務	電腦設定\Windows 設定\安全性設定\系	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server	477			▪實作檔案伺服器資源管理員通訊協定以管理存放裝置資源。可控制配額、檔案篩選、存放裝置報告、檔案管理工作與檔案分類的管理作業 ▪實作檔案伺服器資源管理員服務可透過可編寫指令碼的 COM 提供者來提供這些功能的存取 ▪當實作檔案伺服器資源管理員服務未執行時，配額、檔案篩選、存放裝置報告、檔案管理工作與分類即無法運作或執行	統服務\File Server Resource Manager		
33	Windows Server 2016 File Server	TWG CB-01-007-0478	系統服務	File Server Storage Reports Manager	▪這項原則設定決定此電腦是否可使用 File Server Storage Reports Manager 服務 ▪檔案伺服器存放裝置報告管理員服務可實作執行階段功能，以執行檔案伺服器存放裝置報告、檔案管	電腦設定\Windows 設定\安全性設定\系統服務\File Server Storage Reports	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					理工作及檔案分類工作 ▪ 此服務會在前述任一工作排定開始時隨即啟動，並在報告或工作完成後關閉	Manager		
34	Windows Server 2016 File Server	TWG CB-01-007-0479	系統服務	Function Discovery Provider Host	▪ 這項原則設定決定此電腦是否可使用 Function Discovery Provider Host 服務 ▪ FDPHOST 服務裝載功能探索(FD)網路探索提供者。這些 FD 提供者提供 Simple Services Discovery Protocol(SSDP) 與 Web Services-Discovery(WS-D)通訊協定的網路探索服務 ▪ 若停止或停用 FDPHOST 服務，則在使用 FD 時，將停用這些通訊協定的網路探索。無法使用此服務時，利用 FD 及依賴這些探索通訊協定的網路服務將找不到網路裝	電腦設定\Windows 設定\安全性設定\系統服務\Function Discovery Provider Host	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					置或資源			
35	Windows Server 2016 File Server	TWG CB-01-007-0480	系統服務	Function Discovery Resource Publication	▪ 這項原則設定決定此電腦是否可進行網路資源發布服務 ▪ 發布這台電腦與連結至這台電腦的資源，便可在網路上找到它們。如果此服務停止，便不再發布網路資源，網路上的其他電腦將無法找到它們	電腦設定\Windows 設定\安全性設定\系統服務\Function Discovery Resource Publication	手動	
36	Windows Server 2016 File Server	TWG CB-01-007-0481	系統服務	Group Policy Client	▪ 這項原則設定決定此電腦是否可使用 Group Policy Client 服務 ▪ 此服務負責透過「群組原則」元件，將系統管理員所設定的設定值套用在電腦及使用者 ▪ 如果該服務停用，就不會套用這些設定值，而且也無法透過「群組原則」來管理應用程式及元件	電腦設定\Windows 設定\安全性設定\系統服務\Group Policy Client	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 如果該服務停用，需仰賴「群組原則」元件的任何元件或應用程式可能會無法運作			
37	Windows Server 2016 File Server	TWG CB-01-007-0482	系統服務	Human Interface Device Service	▪ 這項原則設定決定此電腦是否啟用 Human Interface Device Service 服務 ▪ 啟用此服務可維護鍵盤、遙控器與其他多媒體裝置上之常用按鈕的使用。建議讓這個服務繼續執行	電腦設定\Windows 設定\安全性設定\系統服務\Human Interface Device Service	手動	
38	Windows Server 2016 File Server	TWG CB-01-007-0483	系統服務	Hyper-V Data Exchange Service	▪ 這項原則設定決定此電腦是否可使用 Hyper-V Data Exchange Service 服務 ▪ 此服務提供一種機制，以便在虛擬機器及實體電腦上執行之作業系統間交換資料	電腦設定\Windows 設定\安全性設定\系統服務\Hyper-V Data Exchange Service	手動	
39	Windows	TWG	系統	Hyper-V Guest	▪ 這項原則設定決定此電腦是否可	電腦設定	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 File Server	CB-01-007-0484	服務	Shutdown Service	使用 Hyper-V Guest Shutdown Service 服務 ▪ 此服務提供從實體電腦的管理介面關閉這個虛擬機器之作業系統的機制	\Windows 設定\安全性設定\系統服務\Hyper-V Guest Shutdown Service		
40	Windows Server 2016 File Server	TWG CB-01-007-0485	系統服務	Hyper-V Heartbeat Service	▪ 這項原則設定決定此電腦是否啟用 Hyper-V Heartbeat Service 服務 ▪ 定期報告活動訊號來監視此虛擬機器的狀態。此服務可協助識別已停止回應的執行中虛擬機器	電腦設定\Windows 設定\安全性設定\系統服務\Hyper-V Heartbeat Service	手動	
41	Windows Server 2016 File Server	TWG CB-01-007-0486	系統服務	Hyper-V Remote Desktop Virtualization Service	▪ 這項原則設定決定此電腦是否啟用 Hyper-V Remote Desktop Virtualization Service 服務 ▪ 此服務提供平台，讓虛擬機器與在	電腦設定\Windows 設定\安全性設定\系統服務\Hyper-V	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					實體電腦上執行的作業系統彼此通訊	Remote Desktop Virtualization Service		
42	Windows Server 2016 File Server	TWG CB-01-007-0487	系統服務	Hyper-V Time Synchronization Service	▪ 這項原則設定決定此電腦是否可使用 Hyper-V Time Synchronization Service 服務 ▪ 此服務同步化這個虛擬機器與實體電腦的系統時間	電腦設定\Windows 設定\安全性設定\系統服務\Hyper-V Time Synchronization Service	手動	
43	Windows Server 2016 File Server	TWG CB-01-007-0488	系統服務	Hyper-V Volume Shadow Copy Requestor	▪ 這項原則設定決定此電腦是否可使用 Hyper-V Volume Shadow Copy Requestor 服務 ▪ 此服務協調磁碟區陰影複製服務所需的通訊，以便從實體電腦的作業系統將應用程式與資料備份到這個虛擬機器	電腦設定\Windows 設定\安全性設定\系統服務\Hyper-V Volume Shadow Copy Requestor	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
44	Windows Server 2016 File Server	TWG CB-01-007-0489	系統服務	IKE and AuthIP IPsec Keying Modules	▪ 這項原則設定決定此電腦是否可使用 IKE and AuthIP IPsec Keying Modules 服務 ▪ IKEEXT 服務主控 Internet Keying Exchange(IKE)及 Authenticated Internet Protocol(AuthIP)金鑰處理模組 ▪ 這些金鑰處理模組是用來在網際網路通訊協定安全性(IPsec)中進行驗證及金鑰交換 ▪ 停止或停用 IKEEXT 服務將會停用與同儕節點電腦間的 IKE 與 AuthIP 金鑰交換 ▪ IPsec 通常會設定為使用 IKE 或 AuthIP，因此如果停止或停用 IKEEXT 服務，將會導致 IPsec 失敗，並危害系統的安全性。強烈建	電腦設定\Windows 設定\安全性設定\系統服務\IKE and AuthIP IPsec Keying Modules	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					議持續執行 IKEEXT 服務			
45	Windows Server 2016 File Server	TWG CB-01-007-0490	系統服務	Interactive Services Detection	▪ 這項原則設定決定使用者於互動式服務之輸入訊息與提示是否可正常使用 ▪ 啟用使用者通知，以通知使用者針對互動服務進行輸入，這樣可在互動服務所建立的對話方塊出現時存取它們 ▪ 如果此服務停止，新互動服務對話方塊的通知功能將無法再運作，而且可能無法存取互動服務對話方塊。如果此服務停用，新互動服務對話方塊的通知及存取功能都無法再運作	電腦設定\Windows 設定\安全性設定\系統服務\Interactive Services Detection	手動	
46	Windows Server 2016 File	TWG CB-01-007-0	系統服務	Internet Connection Sharing (ICS)	▪ 這項原則設定決定此電腦是否可使用 Internet Connection Sharing (ICS)之服務	電腦設定\Windows 設定\安全性設定\系	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server	491			▪ 此服務可為家用網路或小型辦公室網路提供網路位址轉譯、定址、名稱解析或防止干擾的服務	統服務\Internet Connection Sharing (ICS)		
47	Windows Server 2016 File Server	TWG CB-01-007-0492	系統服務	IP Helper	▪ 這項原則設定決定此電腦是否可透過 IPv4 進行 IPv6 之網路連線服務 ▪ 使用 IPv6 轉換技術(6to4、ISATAP、連接埠 Proxy 與 Teredo)與 IP-HTTPS 提供通道連線能力 ▪ 如果停止此服務，電腦將不具有這些技術所提供的增強連線能力效益	電腦設定\Windows 設定\安全性設定\系統服務\IP Helper	自動	
48	Windows Server 2016 File Server	TWG CB-01-007-0493	系統服務	IPsec Policy Agent	▪ 這項原則設定決定此電腦是否可使用 IPsec Policy Agent 服務 ▪ 網際網路通訊協定安全性(IPsec)支援網路層級的對等驗證、資料來源驗證、資料完整性、資料機密性(加	電腦設定\Windows 設定\安全性設定\系統服務\IPsec Policy Agent	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					密)及重新執行保護 ▪ 此服務會強制執行透過 IP 安全性原則嵌入式管理單元或命令列工具「netsh ipsec」建立的 IPsec 原則 ▪ 如果停止此服務，當原則需要使用 IPsec 連線時，可能會發生網路連線問題。此外，此服務停止時也無法使用 Windows 防火牆的遠端管理			
49	Windows Server 2016 File Server	TWG CB-01-007-0494	系統服務	KDC Proxy Server service (KPS)	▪ 這項原則設定決定此電腦是否可使用 KDC Proxy Server service (KPS)服務 ▪ KDC Proxy 伺服器服務會在 Edge Server 上執行，以將 Kerberos 通訊協定訊息 Proxy 處理到公司網路上的網域控制站	電腦設定\Windows 設定\安全性設定\系統服務\KDC Proxy Server service (KPS)	手動	
50	Windows	TWG	系統	KtmRm for	▪ 這項原則設定決定此電腦是否可	電腦設定	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 File Server	CB-01-007-0495	服務	Distributed Transaction Coordinator	使用 Kernel Transaction Manager (KTM)服務 ▪ 協調分散式交易協調器(MSDTC)與核心交易管理員(KTM)之間的交易。如果不需要這樣做，建議讓此服務維持在停止狀態。如果需要這樣做，MSDTC 與 KTM 都會自動啟動此服務 ▪ 如果停用此服務，任何與核心資源管理員互動的 MSDTC 交易都會失敗，且任何明確依存於此服務的服務將無法啟動	\Windows 設定\安全性設定\系統服務\KtmRm for Distributed Transaction Coordinator		
51	Windows Server 2016 File Server	TWG CB-01-007-0496	系統服務	Link-Layer Topology Discovery Mapper	▪ 這項原則設定決定此電腦是否可使用 Link-Layer Topology Discovery Mapper 服務，以建立網路圖，其中包含電腦及裝置拓撲(連線能力)資訊以及描述每台電腦與裝置的中繼資料	電腦設定\Windows 設定\安全性設定\系統服務\Link-Layer Topology	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果這個服務已停用，網路圖將無法正常運作	Discovery Mapper		
52	Windows Server 2016 File Server	TWG CB-01-007-0497	系統服務	Local Session Manager	▪這項原則設定用於管理本機使用者工作階段的核心 Windows 服務 ▪停止或停用此服務將會導致系統不穩定	電腦設定\Windows 設定\安全性設定\系統服務\Local Session Manager	自動	
53	Windows Server 2016 File Server	TWG CB-01-007-0498	系統服務	Microsoft File Server Shadow Copy Agent Service	▪這項原則設定決定此電腦是否可使用 Microsoft File Server Shadow Copy Agent Service 服務，以管理 VSS 檔案伺服器代理程式建立的檔案共用陰影複製 ▪如果停止此服務，即無法管理檔案共用陰影複製。如果停用此服務，所有明確依存於它的服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Microsoft File Server Shadow Copy Agent Service	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
54	Windows Server 2016 File Server	TWG CB-01-007-0499	系統服務	Microsoft iSCSI Initiator Service	▪這項原則設定決定此電腦是否可使用 Microsoft iSCSI 服務，用以管理從這部電腦連線至遠端 iSCSI 目標裝置的 Internet SCSI(iSCSI)工作階段 ▪如果此服務停止，這部電腦將無法登入或存取 iSCSI 目標 ▪如果此服務停用，所有明確依存於它的服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Microsoft iSCSI Initiator Service	手動	
55	Windows Server 2016 File Server	TWG CB-01-007-0500	系統服務	Microsoft iSCSI Target Server	這項原則設定決定是否讓這部電腦做為 iSCSI 目標	電腦設定\Windows 設定\安全性設定\系統服務\Microsoft iSCSI Target Server	自動	
56	Windows	TWG	系統	Microsoft	▪這項原則設定決定此電腦是否可	電腦設定	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 File Server	CB-01-007-0501	服務	Software Shadow Copy Provider	使用 Microsoft Software Shadow Copy Provider 服務，以管理磁碟區陰影複製服務所取得的以軟體為主的磁碟區陰影複製 ▪如果停止這個服務，就無法管理以軟體為主的磁碟區陰影複製 ▪如果停用這個服務，任何明確依存於它的服務將無法啟動	\Windows 設定\安全性設定\系統服務\Microsoft Software Shadow Copy Provider		
57	Windows Server 2016 File Server	TWG CB-01-007-0502	系統服務	Net.Tcp Port Sharing Service	▪這項原則設定決定此電腦是否可使用 Net.Tcp Port Sharing 服務 ▪此服務提供在 net.tcp 通訊協定上共用 TCP 連接埠的能力	電腦設定\Windows 設定\安全性設定\系統服務\Net.Tcp Port Sharing Service	已停用	
58	Windows Server 2016 File	TWG CB-01-007-0	系統服務	Netlogon	▪這項原則設定決定此電腦是否可使用 Netlogon 服務 ▪此服務維持這個電腦與網域控制	電腦設定\Windows 設定\安全性設定\系	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server	503			站間用於驗證使用者與服務的安全通道 ▪ 如果這個服務被停止，電腦可能無法驗證使用者與服務，且網域控制站將無法登錄 DNS 記錄 ▪ 如果這個服務被停用，任何明確依存於它的服務將無法啟動	統服務\Netlogon		
59	Windows Server 2016 File Server	TWG CB-01-007-0504	系統服務	Network Connections	▪ 這項原則設定決定此電腦是否可使用 Network Connections 服務 ▪ 此服務可管理在網路與撥號連線資料夾中的物件，可以在此資料夾中檢視區域網路與遠端連線	電腦設定\Windows 設定\安全性設定\系統服務\Network Connections	手動	
60	Windows Server 2016 File Server	TWG CB-01-007-0505	系統服務	Network Connectivity Assistant	▪ 這項原則設定決定此電腦是否可使用 Network Connectivity Assistant 服務 ▪ 此服務提供 UI 元件的 DirectAcces狀態通知	電腦設定\Windows 設定\安全性設定\系統服務\Network Connectivity	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						Assistant		
61	Windows Server 2016 File Server	TWG CB-01-007-0506	系統服務	Network List Service	▪ 這項原則設定決定此電腦是否可使用網路識別服務 ▪ 識別電腦已連線的網路、蒐集並儲存這些網路的內容，並在這些內容變更時通知應用程式	電腦設定\Windows 設定\安全性設定\系統服務\Network List Service	手動	
62	Windows Server 2016 File Server	TWG CB-01-007-0507	系統服務	Network Location Awareness	▪ 這項原則設定決定此電腦是否可使用 Network Location Awareness 服務，以蒐集及儲存網路的設定資訊，並且在修改此資訊時，通知程式 ▪ 如果停止此服務，設定資訊就可能會無法使用 ▪ 如果停用此服務，則明確依賴它的任何服務將會無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Network Location Awareness	自動	
63	Windows Server	TWG CB-01	系統	Network Store	▪ 這項原則設定決定此電腦是否可使用 Network Store Interface	電腦設定\Windows 設定\	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 File Server	-007-0508	服務	Interface Service	Service 服務 ▪ 此服務可將網路通知(例如介面的新增/刪除等)傳遞給使用者模式的用戶端 ▪ 停止此服務將造成網路連線中斷 ▪ 如果這個服務被停用，任何明確依存於它的服務將無法啟動	安全性設定\系統服務\Network Store Interface Service		
64	Windows Server 2016 File Server	TWG CB-01-007-0509	系統服務	Optimize drives	▪ 這項原則設定決定此電腦是否可使用 Optimize drives 服務 ▪ 此服務可最佳化存放磁碟機上的檔案，以協助提高電腦執行效率	電腦設定\Windows 設定\安全性設定\系統服務\Optimize drives	手動	
65	Windows Server 2016 File Server	TWG CB-01-007-0510	系統服務	Performance Counter DLL Host	▪ 這項原則設定決定此電腦是否可使用 Performance Counter DLL Host 服務 ▪ 此服務允許遠端使用者與 64 位元處理程序查詢 32 位元 DLL 提供的	電腦設定\Windows 設定\安全性設定\系統服務\Performance	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					效能計數器 ▪ 如果這項服務停止，則只有本機使用者與 32 位元處理程序可以查詢 32 位元 DLL 提供的效能計數器	Counter DLL Host		
66	Windows Server 2016 File Server	TWG CB-01-007-0511	系統服務	Performance Logs & Alerts	▪ 這項原則設定決定此電腦是否可使用 Performance Logs & Alerts 服務 ▪ 效能記錄及警示會根據預先設定的排程參數，從本機或遠端電腦蒐集效能資料，然後寫入資料到記錄檔或觸發警示 ▪ 如果停止此服務，將不會蒐集效能資訊 ▪ 如果這個服務已停用，所有依存於它的服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Performance Logs & Alerts	手動	
67	Windows Server	TWG CB-01	系統服務	Plug and Play	▪ 這項原則設定決定此電腦是否可識別硬體變更之服務	電腦設定\Windows 設定\	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 File Server	-007-0512			▪啟用電腦以使用者沒有或很少的輸入來識別及適應硬體變更，停止或停用這個服務將導致系統不穩定	安全性設定\系統服務\Plug and Play		
68	Windows Server 2016 File Server	TWG CB-01-007-0513	系統服務	Portable Device Enumerator Service	▪這項原則設定決定此電腦之群組原則是否可對卸除式媒體進行管理與強制執行 ▪強制卸除式大型存放裝置使用群組原則。可讓 Windows Media Player 及影像匯入精靈等應用程式，得以使用卸除式大型存放裝置，來傳輸並同步處理內容	電腦設定\Windows 設定\安全性設定\系統服務\Portable Device Enumerator Service	手動	
69	Windows Server 2016 File Server	TWG CB-01-007-0514	系統服務	Power	這項原則設定決定此電腦是否可使用 Power 服務，以管理電源原則與電源原則通知傳遞	電腦設定\Windows 設定\安全性設定\系統服務\Power	自動	
70	Windows	TWG	系統	Print Spooler	▪這項原則設定決定此電腦是否啟	電腦設定	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 File Server	CB-01-007-0515	服務		用 Print Spooler 服務 ▪ 此服務會多工緩衝處理列印工作，並處理與印表機的互動 ▪ 如果關閉此服務，將無法列印或看見印表機	\Windows 設定\安全性設定\系統服務\Print Spooler		
71	Windows Server 2016 File Server	TWG CB-01-007-0516	系統服務	Printer Extensions and Notifications	▪ 這項原則設定決定此電腦是否可使用 Printer Extensions and Notifications 服務 ▪ 此服務會開啟自訂印表機對話方塊，以及處理來自遠端列印伺服器或印表機的通知 ▪ 如果關閉此服務，則無法查看印表機延伸或通知	電腦設定\Windows 設定\安全性設定\系統服務\Printer Extensions and Notifications	手動	
72	Windows Server 2016 File Server	TWG CB-01-007-0517	系統服務	Problem Reports and Solutions Control Panel Support	▪ 這項原則設定決定此電腦是否可使用問題回報與解法諮詢控制台之服務 ▪ 此服務提供檢視、傳送及刪除「問	電腦設定\Windows 設定\安全性設定\系統服務\Problem	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					題報告及解決方案」控制台中之系統等級問題報告的支援	Reports and Solutions Control Panel Support		
73	Windows Server 2016 File Server	TWG CB-01-007-0518	系統服務	Remote Access Auto Connection Manager	這項原則設定決定此電腦是否可使用遠端自動連線服務。當程式參照遠端 DNS 或 NetBIOS 名稱或位址時，建立遠端網路的連線	電腦設定\Windows 設定\安全性設定\系統服務\Remote Access Auto Connection Manager	手動	
74	Windows Server 2016 File Server	TWG CB-01-007-0519	系統服務	Remote Access Connection Manager	▪ 這項原則設定決定此電腦是否可使用 VPN 服務，以管理這台電腦到網際網路或其他遠端網路的撥號及虛擬私人網路(VPN)連線 ▪ 如果這個服務已停用，所有依存於它的服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Remote Access Connection	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						Manager		
75	Windows Server 2016 File Server	TWG CB-01-007-0520	系統服務	Remote Desktop Configuration	▪ 這項原則設定決定此電腦是否可使用 Remote Desktop Configuration service (RDCS)服務 ▪ 遠端桌面設定服務(RDCS)負責處理與遠端桌面服務及遠端桌面相關的設定及工作階段維護活動(需要系統內容)。這些包括每一工作階段暫存資料夾、遠端桌面主題與遠端桌面憑證	電腦設定\Windows 設定\安全性設定\系統服務\Remote Desktop Configuration	手動	
76	Windows Server 2016 File Server	TWG CB-01-007-0521	系統服務	Remote Desktop Services	▪ 這項原則設定決定此電腦是否可使用 Remote Desktop Services 服務，以允許使用者以互動方式連線到遠端電腦 ▪ 遠端桌面及遠端桌面工作階段主機伺服器都需要依賴此服務。若要避免從遠端使用這部電腦，請取清	電腦設定\Windows 設定\安全性設定\系統服務\Remote Desktop Services	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					除「系統內容」控制台項目的「遠端」索引標籤上的核取方塊			
77	Windows Server 2016 File Server	TWG CB-01-007-0522	系統服務	Remote Desktop Services UserMode Port Redirector	▪ 這項原則設定決定此電腦是否可使用 Remote Desktop Services UserMode Port Redirector 服務 ▪ 此項服務允許重新導向 RDP 連線的印表機、磁碟機及連接埠	電腦設定\Windows 設定\安全性設定\系統服務\Remote Desktop Services UserMode Port Redirector	手動	
78	Windows Server 2016 File Server	TWG CB-01-007-0523	系統服務	Remote Procedure Call (RPC)	▪ 這項原則設定決定此電腦是否可使用 Remote Procedure Call (RPC) 服務 ▪ RPCSS 服務是 COM 與 DCOM 伺服器的服務控制管理員。該服務會為 COM 與 DCOM 伺服器執行物件啟用要求、物件輸出程式解析，以	電腦設定\Windows 設定\安全性設定\系統服務\Remote Procedure Call (RPC)	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					及分散式記憶體回收 ▪ 如果停止或停用此服務，使用 COM 或 DCOM 的程式將無法正常運作。強烈建議持續執行 RPCSS 服務			
79	Windows Server 2016 File Server	TWG CB-01-007-0524	系統服務	Remote Procedure Call (RPC) Locator	▪ 這項原則設定決定此電腦是否可使用 Remote Procedure Call (RPC) Locator 服務 ▪ 在 Windows 2003 以及更舊的 Windows 版本中，遠端程序呼叫(RPC)尋找程式服務負責管理 RPC 名稱服務資料庫 ▪ 在 Windows Vista 與更新的 Windows 版本中，此服務不提供任何功能，只是為了應用程式相容性而保留	電腦設定\Windows 設定\安全性設定\系統服務\Remote Procedure Call (RPC) Locator	手動	
80	Windows	TWG	系統	Remote Registry	▪ 這項原則設定決定此電腦是否可	電腦設定	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 File Server	CB-01-007-0525	服務		使用 Remote Registry 服務，由遠端使用者修改這個電腦上的登錄設定 ▪ 如果這個服務被停止，登錄只能由這個電腦上的使用者修改 ▪ 如果這個服務被停用，任何明確依存於它的服務將無法啟動	\Windows 設定\安全性設定\系統服務\Remote Registry		
81	Windows Server 2016 File Server	TWG CB-01-007-0526	系統服務	Resultant Set of Policy Provider	這項原則設定決定此電腦是否提供網路服務來處理要求，以模擬在各種情況下，將「群組原則」設定值套用至目標使用者或電腦，並推斷「原則結果組」設定值	電腦設定\Windows 設定\安全性設定\系統服務\Resultant Set of Policy Provider	手動	
82	Windows Server 2016 File Server	TWG CB-01-007-0527	系統服務	Routing and Remote Access	這項原則設定決定此電腦是否可於本機區域與網路使用 Routing 服務，以提供連到區域網路及廣域網路的公司的路由服務	電腦設定\Windows 設定\安全性設定\系統服務\Routing	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						and Remote Access		
83	Windows Server 2016 File Server	TWG CB-01-007-0528	系統服務	RPC Endpoint Mapper	▪ 這項原則設定決定此電腦是否可使用 RPC Endpoint Mapper 服務，以解析 RPC 介面識別元為傳輸端點 ▪ 如果此服務停止或停用，使用遠端程序呼叫(RPC)服務的程式將無法正常運作	電腦設定\Windows 設定\安全性設定\系統服務\RPC Endpoint Mapper	自動	
84	Windows Server 2016 File Server	TWG CB-01-007-0529	系統服務	Secondary Logon	▪ 這項原則設定決定此電腦是否可以在其他認證中啟動處理程序 ▪ 如果這個服務停止，將無法使用這個登入存取類型。如果這個服務已停用，它的所有依存服務都無法開始	電腦設定\Windows 設定\安全性設定\系統服務\Secondary Logon	手動	
85	Windows Server	TWG CB-01	系統服務	Secure Socket Tunneling	▪ 這項原則設定決定此電腦是否可使用 Secure Socket Tunneling	電腦設定\Windows 設定\	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 File Server	-007-0530		Protocol Service	Protocol (SSTP)服務，以提供安全通訊端通道通訊協定(SSTP)使用 VPN 連線到遠端電腦的支援 ▪ 如果停用此服務，使用者將無法使用 SSTP 存取遠端伺服器	安全性設定\系統服務\Secure Socket Tunneling Protocol Service		
86	Windows Server 2016 File Server	TWG CB-01-007-0531	系統服務	Security Accounts Manager	▪ 這項原則設定決定此電腦是否可使用 Security Accounts Manager 服務，以告知其他服務，安全性帳戶管理員(SAM)已準備好要接受要求 ▪ 停用此服務將阻止通知系統中的其他服務 SAM 已經就緒，而導致那些服務無法正確地啟動 ▪ 此服務不應該停用	電腦設定\Windows 設定\安全性設定\系統服務\Security Accounts Manager	自動	
87	Windows Server 2016 File Server	TWG CB-01-007-0532	系統服務	Server	▪ 這項原則設定決定此電腦是否使用 Server 服務 ▪ 為這個電腦支援網路上檔案、列印及命名管線的共用	電腦設定\Windows 設定\安全性設定\系統服務\Server	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪ 如果停止此服務，將無法使用這些功能 ▪ 如果這個服務被停用，任何明確依存於它的服務將無法啟動			
88	Windows Server 2016 File Server	TWG CB-01-007-0533	系統服務	Shell Hardware Detection	▪ 這項原則設定決定此電腦是否可使用 Shell Hardware Detection 服務 ▪ 此項服務為自動播放硬體事件提供通知	電腦設定\Windows 設定\安全性設定\系統服務\Shell Hardware Detection	自動	
89	Windows Server 2016 File Server	TWG CB-01-007-0534	系統服務	Smart Card	▪ 這項原則設定決定此電腦是否可使用智慧卡功能 ▪ 管理這個電腦所讀取智慧卡的存取。如果這個服務被停止，這個電腦將無法讀取智慧卡。如果這個服務被停用，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Smart Card	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
90	Windows Server 2016 File Server	TWG CB-01-007-0535	系統服務	Smart Card Removal Policy	這項原則設定決定此電腦是否可透過智慧卡移除動作進行使用者電腦鎖定之服務。允許將系統設定為在智慧卡移除時，鎖定使用者桌面	電腦設定\Windows 設定\安全性設定\系統服務\Smart Card Removal Policy	手動	
91	Windows Server 2016 File Server	TWG CB-01-007-0536	系統服務	SNMP Trap	▪ 這項原則設定決定此電腦是否可使用 SNMP Trap 服務，以接收由本機或遠端簡易網路管理通訊協定(SNMP)代理程式所產生的陷阱訊息，並轉送該訊息給在這個電腦上執行中的 SNMP 管理程式 ▪ 如果這個服務被停止，這個電腦上 SNMP 為主的程式將不接收 SNMP 陷阱訊息。如果這個服務被停用，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\SNMP Trap	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
92	Windows Server 2016 File Server	TWG CB-01-007-0537	系統服務	Software Protection	▪ 這項原則設定決定此電腦是否可使用 Software Protection 功能，以針對 Window 及 Windows 應用程式，啟用數位授權的下載、安裝及強制執行功能 ▪ 如果停用該服務，作業系統及已授權的應用程式可能會以通知模式來執行 ▪ 強烈建議不要停用軟體保護服務	電腦設定\Windows 設定\安全性設定\系統服務\Software Protection	自動	
93	Windows Server 2016 File Server	TWG CB-01-007-0538	系統服務	Special Administration Console Helper	這項原則設定決定是否允取系統管理員使用緊急管理服務，遠端存取命令提示字元	電腦設定\Windows 設定\安全性設定\系統服務\Special Administration Console Helper	手動	
94	Windows Server	TWG CB-01	系統服務	Spot Verifier	這項原則設定決定是否檢查可能的檔案系統損毀	電腦設定\Windows 設定\	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 File Server	-007-0539				安全性設定\系統服務\Spot Verifier		
95	Windows Server 2016 File Server	TWG CB-01-007-0540	系統服務	SSDP Discovery	▪ 這項原則設定決定此電腦是否使用 SSDP 協定 ▪ 探索使用 SSDP 探索通訊協定且已連上網路的裝置及服務，例如 UPnP 裝置。還會宣告在本機電腦上執行的 SSDP 裝置及服務 ▪ 如果停止此服務，將會無法探索 SSDP 型的裝置。如果這個服務已停用，所有依存於它的服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\SSDP Discovery	已停用	
96	Windows Server 2016 File Server	TWG CB-01-007-0541	系統服務	Superfetch	這項原則設定決定是否維護與改進一段時間後的系統效能	電腦設定\Windows 設定\安全性設定\系統服務	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						\Superfetch		
97	Windows Server 2016 File Server	TWG CB-01-007-0542	系統服務	System Event Notification Service	▪ 這項原則設定決定此電腦是否可使用系統事件監控與提示服務，以監視系統事件，並通知「COM+事件系統」的訂閱者有關這些事件的內容	電腦設定\Windows 設定\安全性設定\系統服務\System Event Notification Service	自動	
98	Windows Server 2016 File Server	TWG CB-01-007-0543	系統服務	Task Scheduler	▪ 這項原則設定決定此電腦是否可使用 Task Scheduler 服務，讓使用者能夠在這台電腦上設定與排定自動的工作。此服務也主控多個 Windows 系統重要的工作 ▪ 如果停止或停用這個服務，這些工作將不會在其排定的時間執行 ▪ 如果停用這個服務，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Task Scheduler	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
99	Windows Server 2016 File Server	TWG CB-01-007-0544	系統服務	TCP/IP NetBIOS Helper	▪這項原則設定決定此電腦是否可使用 TCP/IP NetBIOS Helper 服務，以提供對 NetBIOS over TCP/IP 以及網路上用戶端 NetBIOS 名稱解析的支援，因此讓使用者可以共用檔案、列印以及登入到網路 ▪如果這個服務被停止，可能無法使用這些功能 ▪如果這個服務被停用，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\TCP/IP NetBIOS Helper	自動	
100	Windows Server 2016 File Server	TWG CB-01-007-0545	系統服務	Telephony	▪這項原則設定決定此電腦是否可使用 Telephony API (TAPI)服務 ▪此服務為程式提供電話語音 API(TAPI)支援，讓程式可以控制本機電腦上的電話語音裝置，或透過區域網路控制也同時執行該服務之伺服器上的電話語音裝置	電腦設定\Windows 設定\安全性設定\系統服務\Telephony	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
101	Windows Server 2016 File Server	TWG CB-01-007-0546	系統服務	Themes	▪ 這項原則設定決定此電腦是否可使用 Themes 服務 ▪ 此服務提供使用者經驗主題管理	電腦設定\Windows 設定\安全性設定\系統服務\Themes	自動	
102	Windows Server 2016 File Server	TWG CB-01-007-0547	系統服務	UPnP Device Host	▪ 這項原則設定決定此電腦是否可使用 UPnP Device Host 服務，允許在此電腦上裝載 UPnP 裝置 ▪ 如果停止此服務，任何裝載的 UPnP 裝置都將停止運作且無法新增其他裝載的裝置 ▪ 如果停用此服務，明確依存於此服務的任何服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\UPnP Device Host	已停用	
103	Windows Server 2016 File Server	TWG CB-01-007-0548	系統服務	User Access Logging Service	▪ 這項原則設定決定此電腦是否可使用 User Access Logging Service 服務 ▪ 此服務會記錄本機伺服器上所安裝產品與角色的唯一用戶端存取	電腦設定\Windows 設定\安全性設定\系統服務\User Access Logging	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					要求(形式為 IP 位址與使用者名稱)。當系統管理員需要將伺服器軟體的用戶端需求量化以進行離線用戶端存取授權(CAL)管理時，可以透過 Powershell 查詢此資訊 ▪ 如果停用此服務，則用戶端要求不會留下記錄，也無法供人透過 Powershell 查詢抓取。停止此服務並不會影響歷史資料的查詢。本機系統管理員必須參閱其 Windows Server 授權條款，以決定要對伺服器軟體進行適當授權所需的 CAL 數目；使用 UAL 服務與資料並不會變更此義務	Service		
104	Windows Server 2016 File Server	TWG CB-01-007-0549	系統服務	User Profile Service	▪ 這項原則設定決定此電腦是否可使用 User Profile Service 服務 ▪ 此服務負責載入及解除載入使用者設定檔	電腦設定\Windows 設定\安全性設定\系統服務\User	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果停止或停用此服務，使用者將無法順利登入或登出，應用程式可能會在取得使用者的資料時發生問題，用來接收設定檔事件通知的已註冊元件將無法接收通知	Profile Service		
105	Windows Server 2016 File Server	TWG CB-01-007-0550	系統服務	Virtual Disk	▪這項原則設定決定此電腦是否可使用 Virtual Disk 服務 ▪此服務提供磁碟、磁碟區、檔案系統及存放裝置陣列的管理	電腦設定\Windows 設定\安全性設定\系統服務\Virtual Disk	手動	
106	Windows Server 2016 File Server	TWG CB-01-007-0551	系統服務	Volume Shadow Copy	▪這項原則設定決定此電腦是否可使用硬體空間之 Shadow Copy 服務，以管理及執行用於備份與其他目的的磁碟區陰影複製 ▪如果這個服務被停止，陰影複製將無法用於備份，備份可能會失敗 ▪如果這個服務被停用，任何明確依	電腦設定\Windows 設定\安全性設定\系統服務\Volume Shadow Copy	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					存於它的服務將無法啟動			
107	Windows Server 2016 File Server	TWG CB-01-007-0552	系統服務	Windows Audio	▪ 這項原則設定決定此電腦是否可使用音訊之服務，以管理 Windows 程式的音訊 ▪ 如果這個服務停止，音訊裝置及效果將無法正常運作 ▪ 如果停用這個服務，將無法啟動明確依賴此服務的任何服務	電腦設定\Windows 設定\安全性設定\系統服務\Windows Audio	手動	
108	Windows Server 2016 File Server	TWG CB-01-007-0553	系統服務	Windows Audio Endpoint Builder	▪ 這項原則設定決定此電腦是否可使用 Windows Audio Endpoint Builder 服務，以管理 Windows 音訊服務的音訊裝置 ▪ 如果停止此服務，音訊裝置與效果將無法正常運作 ▪ 如果停用此服務，所有明確依存於它的服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Windows Audio Endpoint Builder	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
109	Windows Server 2016 File Server	TWG CB-01-007-0554	系統服務	Windows Driver Foundation-User-mode Driver Framework	▪ 這項原則設定決定此電腦是否可使用 Windows Driver Foundation-User-mode Driver Framework 服務，以建立並管理使用者模式驅動程式處理程序 ▪ 無法停止此服務	電腦設定\Windows 設定\安全性設定\系統服務\Windows Driver Foundation-User-mode Driver Framework	手動	
110	Windows Server 2016 File Server	TWG CB-01-007-0555	系統服務	Windows Error Reporting Service	▪ 這項原則設定決定此電腦是否可使用 Windows Error Reporting Service 服務 ▪ 此服務在程式停止運作或停止回應時，允許回報錯誤，並且允許傳遞現有的解決方案。此外，也允許產生用於診斷與修復服務的記錄檔 ▪ 如果此服務已停止，錯誤報告就可	電腦設定\Windows 設定\安全性設定\系統服務\Windows Error Reporting Service	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					能無法正常運作，並且可能因此無法顯示診斷服務及修復的結果			
111	Windows Server 2016 File Server	TWG CB-01-007-0556	系統服務	Windows Event Collector	▪ 這項原則設定決定此電腦之 Windows 事件蒐集服務是否啟用 ▪ 此服務管理支援 WS-Management 通訊協定之遠端來源事件的持續訂閱。這包括 Windows 事件記錄檔、硬體及啟用 IPMI 的事件來源。此服務會將轉送的事件儲存在本機事件記錄檔中 ▪ 如果此服務停止或停用，將無法建立事件訂閱，也無法接受轉送的事件	電腦設定\Windows 設定\安全性設定\系統服務\Windows Event Collector	手動	
112	Windows Server 2016 File Server	TWG CB-01-007-0557	系統服務	Windows Event Log	▪ 這項原則設定決定此電腦是否可使用 Windows Event Log 服務 ▪ 此服務管理事件與事件記錄檔，支援記錄事件、查詢事件、訂閱事	電腦設定\Windows 設定\安全性設定\系統服務	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					件、封存事件記錄檔，以及管理事件中繼資料 ▪ 此服務可使用 XML 與純文字格式來顯示事件 ▪ 停止這個服務可能危害系統的安全性與可靠性	\Windows Event Log		
113	Windows Server 2016 File Server	TWG CB-01-007-0558	系統服務	Windows Firewall	▪ 這項原則設定決定此電腦是否可使用 Windows 防火牆服務 ▪ Windows 防火牆經由阻止未授權使用者透過網際網路或網路取得對電腦的存取來保護電腦	電腦設定\Windows 設定\安全性設定\系統服務\Windows Firewall	自動	
114	Windows Server 2016 File Server	TWG CB-01-007-0559	系統服務	Windows Font Cache Service	▪ 這項原則設定決定此電腦是否可使用 Windows Font Cache Service 服務，以透過快取常用的字型資料，可以最佳化應用程式效能 ▪ 如果這個服務尚未執行，應用程式	電腦設定\Windows 設定\安全性設定\系統服務\Windows Font	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					便會啟動該服務。也可以停用此服務，不過這樣做會降低應用程式效能	Cache Service		
115	Windows Server 2016 File Server	TWG CB-01-007-0560	系統服務	Windows Installer	▪ 這項原則設定決定此電腦是否可使用 Windows Installer 服務，以新增、修改及移除以 Windows Installer (*.msi、*.msp)套件形式提供的應用程式 ▪ 如果停用此服務，所有明確依存於它的服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Windows Installer	手動	
116	Windows Server 2016 File Server	TWG CB-01-007-0561	系統服務	Windows Management Instrumentation	▪ 這項原則設定決定此電腦是否可使用 Windows Management Instrumentation 服務，透過提供公用介面及物件模型，以存取有關作業系統、裝置、應用程式及服務的管理資訊 ▪ 如果這個服務已停止，大多數的	電腦設定\Windows 設定\安全性設定\系統服務\Windows Management Instrumentation	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					Windows 軟體將無法正常運作 ▪ 如果這個服務已停用，所有依存於它的服務都將無法啟動			
117	Windows Server 2016 File Server	TWG CB-01-007-0562	系統服務	Windows Modules Installer	▪ 這項原則設定決定此電腦是否可使用 Windows 功能模組安裝服務 ▪ 此服務可以安裝、修改以及移除 Windows 更新與選用的元件 ▪ 如果停用此服務，則此電腦的安裝或解除安裝 Windows 更新可能會失敗	電腦設定\Windows 設定\安全性設定\系統服務\Windows Modules Installer	手動	
118	Windows Server 2016 File Server	TWG CB-01-007-0563	系統服務	Windows Remote Management (WS-Management)	▪ 這項原則設定決定此電腦是否可使用 Windows 遠端管理服務 ▪ Windows 遠端管理(WinRM)服務為遠端管理實作 WS-Management 通訊協定 ▪ WS-Management 適用於遠端軟體與硬體管理的標準 Web 服務通訊	電腦設定\Windows 設定\安全性設定\系統服務\Windows Remote Management	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					協定。WinRM 服務會接聽並處理網路上的 WS-Management 要求。必須使用 winrm.cmd 命令列工具或透過群組原則來設定 WinRM 服務搭配接聽程式，它才能接聽網路上的要求 ▪ WinRM 服務提供 WMI 資料的存取，並能蒐集事件資料。必須執行此服務，對於事件的事件蒐集與訂閱才能運作。WinRM 訊息使用 HTTP 與 HTTPS 來進行傳輸 ▪ WinRM 服務不需依賴 IIS，但它的預先設定會在相同的電腦上與 IIS 共用相同的連接埠。WinRM 服務保留/wsman URL 首碼。為避免與 IIS 衝突，系統管理員應該確定 IIS 上執行的所有網站都不會使用 /wsman URL 首碼	(WS-Management)		

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
119	Windows Server 2016 File Server	TWG CB-01-007-0564	系統服務	Windows Time	▪這項原則設定決定此電腦是否可使用 Windows Time 服務，以維護在網路上所有用戶端及伺服器的資料及時間同步處理 ▪如果這個服務停止，將無法進行日期與時間同步處理 ▪如果這個服務被停用，所有依存的服務都會停止	電腦設定\Windows 設定\安全性設定\系統服務\Windows Time	手動	
120	Windows Server 2016 File Server	TWG CB-01-007-0565	系統服務	Windows Update	▪這項原則設定決定此電腦是否可使用 Windows Update 服務，以偵測、下載並安裝 Windows 或其他程式的更新 ▪如果停用此服務，這部電腦的使用者將無法使用 Windows Update 或其自動更新功能。而且程式將無法使用 Windows Update Agent(WUA)API	電腦設定\Windows 設定\安全性設定\系統服務\Windows Update	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
121	Windows Server 2016 File Server	TWG CB-01-007-0566	系統服務	WinHTTP Web Proxy Auto-Discovery Service	▪ 這項原則設定決定此電腦是否可使用 WinHTTP Web Proxy Auto-Discovery Service 服務 ▪ WinHTTP 會實作用戶端 HTTP 堆疊並提供開發人員 Win32 API 及 COM 自動化元件來傳送 HTTP 要求及接收回應。此外，WinHTTP 透過實作 Web Proxy Auto-Discovery(WPAD)通訊協定，提供自動探索 Proxy 設定的支援	電腦設定\Windows 設定\安全性設定\系統服務\WinHTTP Web Proxy Auto-Discovery Service	手動	
122	Windows Server 2016 File Server	TWG CB-01-007-0567	系統服務	Wired AutoConfig	▪ 這項原則設定決定此電腦是否可使用 Wired AutoConfig 服務 ▪ 此項服務將於乙太網路卡上執行 IEEE 802.1X 驗證 ▪ 有線自動設定(DOT3SVC)服務負責在乙太網路介面上執行 IEEE	電腦設定\Windows 設定\安全性設定\系統服務\Wired AutoConfig	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					802.1X 驗證。如果目前的有線網路部署強制執行 802.1X 驗證，則應該設定執行 DOT3SVC 服務以建立第二層連線及/或提供網路資源存取。未強制執行 802.1X 驗證的有線網路則不受 DOT3SVC 服務影響			
123	Windows Server 2016 File Server	TWG CB-01-007-0568	系統服務	WMI Performance Adapter	▪ 這項原則設定決定此電腦是否可使用 WMI Performance Adapter 服務 ▪ 提供來自 Windows Management Instrumentation(WMI)提供者的效能程式庫資訊給網路上的用戶端。只有在啟用效能資料協助程式時，這個服務才會執行	電腦設定\Windows 設定\安全性設定\系統服務\WMI Performance Adapter	手動	
124	Windows Server 2016 File	TWG CB-01-007-0	系統服務	Workstation	▪ 這項原則設定決定此電腦是否使用 Workstation 服務，用以建立及維護使用 SMB 通訊協定進行的用	電腦設定\Windows 設定\安全性設定\系	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server	569			戶端與遠端伺服器網路連線 ▪ 如果停止這個服務，將無法使用這些連線 ▪ 如果停用這個服務，則會停止所有明確依存它的服務	統服務\Workstation		

資料來源：本中心整理

表6　Windows Server 2016 Web Server 政府組態基準列表

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
1	Windows Server 2016 Web Server	TWGCB-01-007-0570	系統服務	Application Host Helper Service	▪這項原則設定決定此電腦是否可使用 Application Host Helper Service 服務，用以為 IIS 提供管理服務，例如設定歷程記錄以及應用程式集區對應 ▪如果停止這項服務，設定歷程記錄以及使用應用程式集區特定存取控制項目鎖定檔案或目錄都將無法運作	電腦設定\Windows 設定\安全性設定\系統服務\Application Host Helper Service	自動	
2	Windows Server 2016 Web Server	TWGCB-01-007-0571	系統服務	Application Identity	▪這項原則設定決定此電腦是否可使用 Application Identity 之服務，用以判斷並確定應用程式的識別 ▪如果停用此服務將使 AppLocker 無法強制執行	電腦設定\Windows 設定\安全性設定\系統服務\Application Identity	手動	CCE-ID：CCE-47123-5
3	Windows	TWG	系統	Application	▪這項原則設定決定此電腦是否可	電腦設定	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Web Server	CB-01-007-0572	服務	Information	使用 Application Information 服務，以其他管理權限協助執行互動式應用程式。使用者在執行想要的工作時可能會需要這些權限 ▪ 如果停止此服務，使用者將無法以其他管理權限來啟動應用程式	\Windows 設定\安全性設定\系統服務\Application Information		
4	Windows Server 2016 Web Server	TWG CB-01-007-0573	系統服務	Application Layer Gateway Service	這項原則設定決定此電腦是否可使用 Application Layer Gateway Service 服務，以對網際網路連線共用提供協力廠商通訊協定外掛程式的支援	電腦設定\Windows 設定\安全性設定\系統服務\Application Layer Gateway Service	手動	
5	Windows Server 2016 Web Server	TWG CB-01-007-0574	系統服務	Application Management	▪ 這項原則設定決定此電腦是否可使用應用程式管理服務 ▪ 針對透過「群組原則」來部署的軟體，處理安裝、移除及列舉要求。	電腦設定\Windows 設定\安全性設定\系統服務	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					若將此服務停用，使用者將無法安裝、移除及列舉透過「群組原則」來部署的軟體，而且與其具有明確相依關係的任何服務，也將無法啟動	\Application Management		
6	Windows Server 2016 Web Server	TWG CB-01-007-0575	系統服務	ASP.NET State Service	▪ 這項原則設定決定此電腦是否可使用 ASP.NET 狀態服務，以提供 ASP.NET 所需跨處理序 (Out-Of-Process)工作階段狀態的支援 ▪ 若停止這項服務，則跨處理序的要求將無法進行 ▪ 如果停用這項服務，與這項服務明確相關的所有其他服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\ASP.NET State Service	手動	
7	Windows Server	TWG CB-01	系統服務	Background Intelligent	▪ 這項原則設定決定此電腦是否可使用 Background Intelligent	電腦設定\Windows 設定\	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 Web Server	-007-0576		Transfer Service	Transfer Service 服務，以使用閒置的網路頻寬在背景傳輸檔案 ▪ 如果停用此服務，所有依存於 BITS 的應用程式(例如，Windows Update 或 MSN Explorer)將無法自動下載程式或其他資訊	安全性設定\系統服務\Background Intelligent Transfer Service		
8	Windows Server 2016 Web Server	TWG CB-01-007-0577	系統服務	Background Tasks Infrastructure Service	這項原則設定決定此電腦是否可使用 Background Tasks Infrastructure Service 服務，以控制哪些背景工作可在系統上執行的 Windows 基礎結構服務	電腦設定\Windows 設定\安全性設定\系統服務\Background Tasks Infrastructure Service	自動	
9	Windows Server 2016 Web	TWG CB-01-007-0	系統服務	Base Filtering Engine	▪ 這項原則設定決定此電腦是否可使用 Base Filtering Engine (BFE)服務	電腦設定\Windows 設定\安全性設定\系	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server	578			▪基礎篩選引擎(BFE)是管理防火牆與 IP 安全性(IPsec)原則，並執行使用者模式篩選的服務 ▪停止或停用 BFE 服務將顯著降低系統的安全性。同時也導致 IPsec 管理與防火牆應用程式意外的行為	統服務\Base Filtering Engine		
10	Windows Server 2016 Web Server	TWG CB-01-007-0579	系統服務	Certificate Propagation	▪這項原則設定決定此電腦是否可使用 Certificate Propagation 服務 ▪從智慧卡將使用者憑證與根憑證複製到目前使用者的憑證存放區，當智慧卡插入智慧卡讀卡機時進行偵測，(若有需要)並安裝智慧卡隨插即用迷你驅動程式	電腦設定\Windows 設定\安全性設定\系統服務\Certificate Propagation	手動	
11	Windows Server 2016 Web	TWG CB-01-007-0	系統服務	CNG Key Isolation	▪這項原則設定決定此電腦是否可使用 CNG key isolation 服務 ▪CNG 金鑰隔離服務裝載於 LSA 處	電腦設定\Windows 設定\安全性設定\系	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server	580			理程序。該服務可依據一般條件來隔離私密金鑰與相關聯加密編譯操作的金鑰處理程序。該服務會以符合一般條件的安全處理程序來儲存與使用長效金鑰	統服務\CNG Key Isolation		
12	Windows Server 2016 Web Server	TWG CB-01-007-0581	系統服務	COM+ Event System	▪ 這項原則設定決定此電腦是否可使用 COM+ Event System 服務 ▪ 支援「系統事件通知服務 (SENS)」，它可讓事件自動分散到訂閱的 COM 元件。如果服務被停止，SENS 會關閉，並無法提供登入及登出通知。如果此服務被停用，任何明顯依存它的服務都無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\COM+ Event System	自動	
13	Windows Server 2016 Web	TWG CB-01-007-0	系統服務	COM+ System Application	▪ 這項原則設定決定此電腦是否可使用 COM+ System Application 服務，以管理 COM+元件的設定及追	電腦設定\Windows 設定\安全性設定\系	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server	582			蹤 ▪ 如果停止此服務，大部分的 COM+ 元件將無法適當運作 ▪ 如果此服務被停用，任何明確依存它的服務將無法啟動	統服務\COM+ System Application		
14	Windows Server 2016 Web Server	TWG CB-01-007-0583	系統服務	Computer Browser	▪ 這項原則設定決定是否讓此電腦在網路上之其他使用者進行資源瀏覽 ▪ 維護網路上更新的電腦清單，並將這個清單提供給做為瀏覽器的電腦 ▪ 如果這個服務被停止，這個清單將不會被更新或維護 ▪ 如果這個服務被停用，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Computer Browser	已停用	
15	Windows Server	TWG CB-01	系統服務	Credential Manager	▪ 這項原則設定決定此電腦是否可使用 Credential Manager 服務	電腦設定\Windows 設定\	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 Web Server	-007-0584			▪ 此項服務提供使用者安全儲存以及擷取認證、應用程式以及安全性服務封裝	安全性設定\系統服務\Credential Manager		
16	Windows Server 2016 Web Server	TWG CB-01-007-0585	系統服務	Cryptographic Services	▪ 這項原則設定決定此電腦是否可使用 Cryptographic Services 服務 ▪ Cryptographic Services 提供 3 種管理服務： ➢ 目錄資料庫服務：確認 Windows 檔案的簽章並允許安裝新程式 ➢ 受保護的根目錄服務：從這部電腦新增及移除信任的根憑證授權單位憑證 ➢ 自動根憑證更新服務：從 Windows Update 抓取根憑證並啟用案例，例如 SSL ▪ 如果停止此服務，這些管理服務將	電腦設定\Windows 設定\安全性設定\系統服務\Cryptographic Services	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					無法正常運作 ▪ 如果停用此服務，任何明確需要它的服務將無法啟動			
17	Windows Server 2016 Web Server	TWG CB-01-007-0586	系統服務	DCOM Server Process Launcher	▪ 這項原則設定決定此電腦是否可使用 DCOM Server Process Launcher 服務 ▪ DCOMLAUNCH 服務會啟動 COM 與 DCOM 伺服器，以回應物件啟用要求 ▪ 如果停止或停用此服務，使用 COM 或 DCOM 的程式將無法正常運作。強烈建議持續執行 DCOMLAUNCH 服務	電腦設定\Windows 設定\安全性設定\系統服務\DCOM Server Process Launcher	自動	
18	Windows Server 2016 Web Server	TWG CB-01-007-0587	系統服務	Device Association Service	▪ 這項原則設定決定此電腦是否可使用 Device Association Service 服務 ▪ 此項服務啟用系統與有線或無線	電腦設定\Windows 設定\安全性設定\系統服務\Device	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					裝置之間的配對	Association Service		
19	Windows Server 2016 Web Server	TWG CB-01-007-0588	系統服務	Device Install Service	▪ 這項原則設定決定此電腦是否可使用 Device Install Service 服務，以使用者沒有或很少的輸入來識別及適應硬體變更 ▪ 停止或停用這個服務將導致系統不穩定	電腦設定\Windows 設定\安全性設定\系統服務\Device Install Service	手動	
20	Windows Server 2016 Web Server	TWG CB-01-007-0589	系統服務	Device Setup Manager	▪ 這項原則設定決定此電腦是否可使用 Device Setup Manager 服務，以偵測、下載及安裝裝置相關軟體 ▪ 如果停用此服務，裝置可能會以過期的軟體設定，且可能無法正常運作	電腦設定\Windows 設定\安全性設定\系統服務\Device Setup Manager	手動	
21	Windows Server 2016 Web	TWG CB-01-007-0	系統服務	DHCP Client	▪ 這項原則設定決定此電腦是否可使用 DHCP Client 服務，以為這個電腦登錄及更新 IP 位址與 DNS 記	電腦設定\Windows 設定\安全性設定\系	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server	590			錄 ▪ 如果這個服務被停止，這個電腦將會不接收動態 IP 位址與 DNS 更新 ▪ 如果這個服務被停用，任何明確依存於它的服務將無法啟動	統服務\DHCP Client		
22	Windows Server 2016 Web Server	TWG CB-01-007-0591	系統服務	Diagnostic Policy Service	▪ 這項原則設定決定此電腦是否可使用診斷原則服務 ▪ 診斷原則服務能夠偵測 Windows 元件的問題、進行疑難排解及提供解決方案 ▪ 如果停止此服務，便無法再進行診斷	電腦設定\Windows 設定\安全性設定\系統服務\Diagnostic Policy Service	自動	
23	Windows Server 2016 Web Server	TWG CB-01-007-0592	系統服務	Diagnostic Service Host	▪ 這項原則設定決定此電腦之 Windows 元件錯誤診斷服務之是否啟用 ▪ 診斷原則服務會使用診斷服務裝載，裝載需要在本機服務內容上執	電腦設定\Windows 設定\安全性設定\系統服務\Diagnostic	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					行的診斷。如果此服務已停止，其上的任何診斷將不再產生作用	Service Host		
24	Windows Server 2016 Web Server	TWG CB-01-007-0593	系統服務	Diagnostic System Host	▪ 這項原則設定決定此電腦是否可使用 Diagnostic System Host 服務 ▪ 診斷原則服務會使用診斷系統裝載，裝載需要在本機服務內容上執行的診斷 ▪ 如果此服務已停止，其上的任何診斷將不再產生作用	電腦設定\Windows 設定\安全性設定\系統服務\Diagnostic System Host	手動	
25	Windows Server 2016 Web Server	TWG CB-01-007-0594	系統服務	Distributed Link Tracking Client	這項原則設定決定此電腦是否可使用 Distributed Link Tracking 服務，以維護電腦中或網路中不同電腦之 NTFS 檔案間的連結	電腦設定\Windows 設定\安全性設定\系統服務\Distributed Link Tracking Client	自動	
26	Windows	TWG	系統	Distributed	▪ 這項原則設定決定此電腦之候選	電腦設定	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Web Server	CB-01-007-0595	服務	Transaction Coordinator	交易(Coordinates transactions)之管理服務是否啟動，以協調跨越多個資源管理員的交易，比如資料庫、訊息佇列及檔案系統 ▪ 如果此服務被停止，這些交易將會失敗 ▪ 如果這個服務已停用，所有依存於它的服務都將無法啟動	\Windows 設定\安全性設定\系統服務\Distributed Transaction Coordinator		
27	Windows Server 2016 Web Server	TWG CB-01-007-0596	系統服務	DNS Client	▪ 這項原則設定決定此電腦之 DNS Client 服務是否啟動 ▪ DNS 用戶端服務(dnscache)會為此電腦快取網域名稱系統(DNS)名稱並登錄完整的電腦名稱 ▪ 如果這個服務被停止，將會繼續解析 DNS 名稱。然而，將不會快取 DNS 名稱查詢的結果，而且不會登錄電腦名稱	電腦設定\Windows 設定\安全性設定\系統服務\DNS Client	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					▪如果這個服務已停用，所有依存於它的服務都將無法啟動			
28	Windows Server 2016 Web Server	TWG CB-01-007-0597	系統服務	Encrypting File System (EFS)	▪這項原則設定決定此電腦是否啟用加密檔案系統服務，藉由提供核心檔案加密技術，可以在 NTFS 檔案系統磁碟區上儲存加密的檔案 ▪如果此服務停止或停用，應用程式將無法存取加密的檔案	電腦設定\Windows 設定\安全性設定\系統服務\Encrypting File System (EFS)	手動	
29	Windows Server 2016 Web Server	TWG CB-01-007-0598	系統服務	Extensible Authentication Protocol	▪這項原則設定決定此電腦之延伸驗證協定(EAP)之服務是否啟用 ▪可延伸的驗證通訊協定(EAP)服務提供例如 802.1x 有線及無線、VPN 以及網路存取保護(NAP)環境中的網路驗證 ▪EAP 在驗證程序期間，也提供網路存取用戶端(包括無線及 VPN 用戶端)使用的應用程式開發介面	電腦設定\Windows 設定\安全性設定\系統服務\Extensible Authentication Protocol	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					(API)。如果停用此服務，此電腦將無法存取需要 EAP 驗證的網路			
30	Windows Server 2016 Web Server	TWG CB-01-007-0599	系統服務	Function Discovery Provider Host	▪ 這項原則設定決定此電腦是否可使用 Function Discovery Provider Host 服務 ▪ FDPHOST 服務裝載功能探索(FD)網路探索提供者。這些 FD 提供者提供 Simple Services Discovery Protocol(SSDP) 與 Web Services-Discovery(WS-D)通訊協定的網路探索服務 ▪ 若停止或停用 FDPHOST 服務，則在使用 FD 時，將停用這些通訊協定的網路探索。無法使用此服務時，利用 FD 及依賴這些探索通訊協定的網路服務將找不到網路裝置或資源	電腦設定\Windows 設定\安全性設定\系統服務\Function Discovery Provider Host	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
31	Windows Server 2016 Web Server	TWG CB-01-007-0600	系統服務	Function Discovery Resource Publication	▪ 這項原則設定決定此電腦是否可進行網路資源發布服務 ▪ 發布這台電腦與連結至這台電腦的資源，便可在網路上找到它們。如果此服務停止，便不再發布網路資源，網路上的其他電腦將無法找到它們	電腦設定\Windows 設定\安全性設定\系統服務\Function Discovery Resource Publication	手動	
32	Windows Server 2016 Web Server	TWG CB-01-007-0601	系統服務	Group Policy Client	▪ 這項原則設定決定此電腦是否可使用 Group Policy Client 服務 ▪ 此服務負責透過「群組原則」元件，將系統管理員所設定的設定值套用在電腦及使用者 ▪ 如果該服務停用，就不會套用這些設定值，而且也無法透過「群組原則」來管理應用程式及元件 ▪ 如果該服務停用，需仰賴「群組原則」元件的任何元件或應用程式可	電腦設定\Windows 設定\安全性設定\系統服務\Group Policy Client	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					能會無法運作			
33	Windows Server 2016 Web Server	TWG CB-01-007-0602	系統服務	Human Interface Device Service	▪ 這項原則設定決定此電腦是否啟用 Human Interface Device Service 服務 ▪ 啟用此服務可維護鍵盤、遙控器與其他多媒體裝置上之常用按鈕的使用。建議讓這個服務繼續執行	電腦設定\Windows 設定\安全性設定\系統服務\Human Interface Device Service	手動	
34	Windows Server 2016 Web Server	TWG CB-01-007-0603	系統服務	Hyper-V Data Exchange Service	▪ 這項原則設定決定此電腦是否可使用 Hyper-V Data Exchange Service 服務 ▪ 此服務提供一種機制，以便在虛擬機器及實體電腦上執行之作業系統間交換資料	電腦設定\Windows 設定\安全性設定\系統服務\Hyper-V Data Exchange Service	手動	
35	Windows Server 2016 Web Server	TWG CB-01-007-0604	系統服務	Hyper-V Guest Shutdown Service	▪ 這項原則設定決定此電腦是否可使用 Hyper-V Guest Shutdown Service 服務 ▪ 此服務提供從實體電腦的管理介	電腦設定\Windows 設定\安全性設定\系統服務\Hyper-V	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					面關閉這個虛擬機器之作業系統的機制	Guest Shutdown Service		
36	Windows Server 2016 Web Server	TWG CB-01-007-0605	系統服務	Hyper-V Heartbeat Service	▪ 這項原則設定決定此電腦是否啟用 Hyper-V Heartbeat Service 服務 ▪ 定期報告活動訊號來監視此虛擬機器的狀態。此服務可協助識別已停止回應的執行中虛擬機器	電腦設定\Windows 設定\安全性設定\系統服務\Hyper-V Heartbeat Service	手動	
37	Windows Server 2016 Web Server	TWG CB-01-007-0606	系統服務	Hyper-V Remote Desktop Virtualization Service	▪ 這項原則設定決定此電腦是否啟用 Hyper-V Remote Desktop Virtualization Service 服務 ▪ 此服務提供平台，讓虛擬機器與在實體電腦上執行的作業系統彼此通訊	電腦設定\Windows 設定\安全性設定\系統服務\Hyper-V Remote Desktop Virtualization Service	手動	
38	Windows Server	TWG CB-01	系統服務	Hyper-V Time Synchronization	▪ 這項原則設定決定此電腦是否可使用 Hyper-V Time Synchronization	電腦設定\Windows 設定\	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 Web Server	-007-0607		Service	Service 服務 ▪ 此服務同步化這個虛擬機器與實體電腦的系統時間	安全性設定\系統服務\Hyper-V Time Synchronization Service		
39	Windows Server 2016 Web Server	TWG CB-01-007-0608	系統服務	Hyper-V Volume Shadow Copy Requestor	▪ 這項原則設定決定此電腦是否可使用 Hyper-V Volume Shadow Copy Requestor 服務 ▪ 此服務協調磁碟區陰影複製服務所需的通訊，以便從實體電腦的作業系統將應用程式與資料備份到這個虛擬機器	電腦設定\Windows 設定\安全性設定\系統服務\Hyper-V Volume Shadow Copy Requestor	手動	
40	Windows Server 2016 Web Server	TWG CB-01-007-0609	系統服務	IKE and AuthIP IPsec Keying Modules	▪ 這項原則設定決定此電腦是否可使用 IKE and AuthIP IPsec Keying Modules 服務 ▪ IKEEXT 服務主控 Internet Keying Exchange(IKE)及 Authenticated	電腦設定\Windows 設定\安全性設定\系統服務\IKE and AuthIP IPsec	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					Internet Protocol(AuthIP)金鑰處理模組 ▪ 這些金鑰處理模組是用來在網際網路通訊協定安全性(IPsec)中進行驗證及金鑰交換 ▪ 停止或停用 IKEEXT 服務將會停用與同儕節點電腦間的 IKE 與 AuthIP 金鑰交換 ▪ IPsec 通常會設定為使用 IKE 或 AuthIP，因此如果停止或停用 IKEEXT 服務，將會導致 IPsec 失敗，並危害系統的安全性。強烈建議持續執行 IKEEXT 服務	Keying Modules		
41	Windows Server 2016 Web Server	TWG CB-01-007-0610	系統服務	Interactive Services Detection	▪ 這項原則設定決定使用者於互動式服務之輸入訊息與提示是否可正常使用 ▪ 啟用使用者通知，以通知使用者針	電腦設定\Windows 設定\安全性設定\系統服務\Interactive	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					對互動服務進行輸入，這樣可在互動服務所建立的對話方塊出現時存取它們 ▪ 如果此服務停止，新互動服務對話方塊的通知功能將無法再運作，而且可能無法存取互動服務對話方塊。如果此服務停用，新互動服務對話方塊的通知及存取功能都無法再運作	Services Detection		
42	Windows Server 2016 Web Server	TWG CB-01-007-0611	系統服務	Internet Connection Sharing (ICS)	▪ 這項原則設定決定此電腦是否可使用 Internet Connection Sharing (ICS)之服務 ▪ 此服務可為家用網路或小型辦公室網路提供網路位址轉譯、定址、名稱解析或防止干擾的服務	電腦設定\Windows 設定\安全性設定\系統服務\Internet Connection Sharing (ICS)	已停用	
43	Windows Server	TWG CB-01	系統服務	IP Helper	▪ 這項原則設定決定此電腦是否可透過 IPv4 進行 IPv6 之網路連線服	電腦設定\Windows 設定\	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 Web Server	-007-0612			務 ▪ 使用 IPv6 轉換技術(6to4、ISATAP、連接埠 Proxy 與 Teredo)與 IP-HTTPS 提供通道連線能力 ▪ 如果停止此服務，電腦將不具有這些技術所提供的增強連線能力效益	安全性設定\系統服務\IP Helper		
44	Windows Server 2016 Web Server	TWG CB-01-007-0613	系統服務	IPsec Policy Agent	▪ 這項原則設定決定此電腦是否可使用 IPsec Policy Agent 服務 ▪ 網際網路通訊協定安全性(IPsec)支援網路層級的對等驗證、資料來源驗證、資料完整性、資料機密性(加密)及重新執行保護 ▪ 此服務會強制執行透過 IP 安全性原則嵌入式管理單元或命令列工具「netsh ipsec」建立的 IPsec 原則 ▪ 如果停止此服務，當原則需要使用	電腦設定\Windows 設定\安全性設定\系統服務\IPsec Policy Agent	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					IPsec 連線時，可能會發生網路連線問題。此外，此服務停止時也無法使用 Windows 防火牆的遠端管理			
45	Windows Server 2016 Web Server	TWG CB-01-007-0614	系統服務	KDC Proxy Server service (KPS)	▪ 這項原則設定決定此電腦是否可使用 KDC Proxy Server service (KPS)服務 ▪ KDC Proxy 伺服器服務會在 Edge Server 上執行，以將 Kerberos 通訊協定訊息 Proxy 處理到公司網路上的網域控制站	電腦設定\Windows 設定\安全性設定\系統服務\KDC Proxy Server service (KPS)	手動	
46	Windows Server 2016 Web Server	TWG CB-01-007-0615	系統服務	KtmRm for Distributed Transaction Coordinator	▪ 這項原則設定決定此電腦是否可使用 Kernel Transaction Manager (KTM)服務 ▪ 協調分散式交易協調器(MSDTC)與核心交易管理員(KTM)之間的交易。如果不需要這樣做，建議讓	電腦設定\Windows 設定\安全性設定\系統服務\KtmRm for Distributed Transaction	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					此服務維持在停止狀態。如果需要這樣做，MSDTC 與 KTM 都會自動啟動此服務 ▪ 如果停用此服務，任何與核心資源管理員互動的 MSDTC 交易都會失敗，且任何明確依存於此服務的服務將無法啟動	Coordinator		
47	Windows Server 2016 Web Server	TWG CB-01-007-0616	系統服務	Link-Layer Topology Discovery Mapper	▪ 這項原則設定決定此電腦是否可使用 Link-Layer Topology Discovery Mapper 服務，以建立網路圖，其中包含電腦及裝置拓撲(連線能力)資訊以及描述每台電腦與裝置的中繼資料 ▪ 如果這個服務已停用，網路圖將無法正常運作	電腦設定\Windows 設定\安全性設定\系統服務\Link-Layer Topology Discovery Mapper	手動	
48	Windows Server	TWG CB-01	系統服務	Local Session Manager	▪ 這項原則設定用於管理本機使用者工作階段的核心 Windows 服務	電腦設定\Windows 設定\	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 Web Server	-007-0617			▪停止或停用此服務將會導致系統不穩定	安全性設定\系統服務\Local Session Manager		
49	Windows Server 2016 Web Server	TWG CB-01-007-0618	系統服務	Microsoft iSCSI Initiator Service	▪這項原則設定決定此電腦是否可使用 Microsoft iSCSI 服務，用以管理從這部電腦連線至遠端 iSCSI 目標裝置的 Internet SCSI(iSCSI)工作階段 ▪如果此服務停止，這部電腦將無法登入或存取 iSCSI 目標 ▪如果此服務停用，所有明確依存於它的服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Microsoft iSCSI Initiator Service	手動	
50	Windows Server 2016 Web Server	TWG CB-01-007-0619	系統服務	Microsoft Software Shadow Copy Provider	▪項原則設定決定此電腦是否可使用 Microsoft Software Shadow Copy Provider 服務，以管理磁碟區陰影複製服務所取得的以軟體為主的	電腦設定\Windows 設定\安全性設定\系統服務	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					磁碟區陰影複製 ▪ 如果停止這個服務，就無法管理以軟體為主的磁碟區陰影複製 ▪ 如果停用這個服務，任何明確依存於它的服務將無法啟動	\Microsoft Software Shadow Copy Provider		
51	Windows Server 2016 Web Server	TWG CB-01-007-0620	系統服務	Net.Tcp Port Sharing Service	▪ 這項原則設定決定此電腦是否可使用 Net.Tcp Port Sharing 服務 ▪ 此服務提供在 net.tcp 通訊協定上共用 TCP 連接埠的能力	電腦設定\Windows 設定\安全性設定\系統服務\Net.Tcp Port Sharing Service	已停用	
52	Windows Server 2016 Web Server	TWG CB-01-007-0621	系統服務	Netlogon	▪ 這項原則設定決定此電腦是否可使用 Netlogon 服務 ▪ 此服務維持這個電腦與網域控制站間用於驗證使用者與服務的安全通道 ▪ 如果這個服務被停止，電腦可能無	電腦設定\Windows 設定\安全性設定\系統服務\Netlogon	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					法驗證使用者與服務，且網域控制站將無法登錄 DNS 記錄 ▪ 如果這個服務被停用，任何明確依存於它的服務將無法啟動			
53	Windows Server 2016 Web Server	TWG CB-01-007-0622	系統服務	Network Connections	▪ 這項原則設定決定此電腦是否可使用 Network Connections 服務 ▪ 此服務可管理在網路與撥號連線資料夾中的物件，可以在此資料夾中檢視區域網路與遠端連線	電腦設定\Windows 設定\安全性設定\系統服務\Network Connections	手動	
54	Windows Server 2016 Web Server	TWG CB-01-007-0623	系統服務	Network Connectivity Assistant	▪ 這項原則設定決定此電腦是否可使用 Network Connectivity Assistant 服務 ▪ 此服務提供 UI 元件的 DirectAcces 狀態通知	電腦設定\Windows 設定\安全性設定\系統服務\Network Connectivity Assistant	手動	
55	Windows Server	TWG CB-01	系統服務	Network List Service	▪ 這項原則設定決定此電腦是否可使用網路識別服務	電腦設定\Windows 設定\	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 Web Server	-007-0624			▪識別電腦已連線的網路、蒐集並儲存這些網路的內容，並在這些內容變更時通知應用程式	安全性設定\系統服務\Network List Service		
56	Windows Server 2016 Web Server	TWG CB-01-007-0625	系統服務	Network Location Awareness	▪這項原則設定決定此電腦是否可使用 Network Location Awareness 服務，以蒐集及儲存網路的設定資訊，並且在修改此資訊時，通知程式 ▪如果停止此服務，設定資訊就可能會無法使用 ▪如果停用此服務，則明確依賴它的任何服務將會無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Network Location Awareness	自動	
57	Windows Server 2016 Web Server	TWG CB-01-007-0626	系統服務	Network Store Interface Service	▪這項原則設定決定此電腦是否可使用 Network Store Interface Service 服務 ▪此服務可將網路通知(例如介面的新增/刪除等)傳遞給使用者模式的	電腦設定\Windows 設定\安全性設定\系統服務\Network Store Interface	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					用戶端 ▪停止此服務將造成網路連線中斷 ▪如果這個服務被停用，任何明確依存於它的服務將無法啟動	Service		
58	Windows Server 2016 Web Server	TWG CB-01-007-0627	系統服務	Optimize drives	▪這項原則設定決定此電腦是否可使用 Optimize drives 服務 ▪此服務可最佳化存放磁碟機上的檔案，以協助提高電腦執行效率	電腦設定\Windows 設定\安全性設定\系統服務\Optimize drives	手動	
59	Windows Server 2016 Web Server	TWG CB-01-007-0628	系統服務	Performance Counter DLL Host	▪這項原則設定決定此電腦是否可使用 Performance Counter DLL Host 服務 ▪此服務允許遠端使用者與 64 位元處理程序查詢 32 位元 DLL 提供的效能計數器 ▪如果這項服務停止，則只有本機使用者與 32 位元處理程序可以查詢	電腦設定\Windows 設定\安全性設定\系統服務\Performance Counter DLL Host	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					32 位元 DLL 提供的效能計數器			
60	Windows Server 2016 Web Server	TWG CB-01-007-0629	系統服務	Performance Logs & Alerts	▪ 這項原則設定決定此電腦是否可使用 Performance Logs & Alerts 服務 ▪ 效能記錄及警示會根據預先設定的排程參數，從本機或遠端電腦蒐集效能資料，然後寫入資料到記錄檔或觸發警示 ▪ 如果停止此服務，將不會蒐集效能資訊 ▪ 如果這個服務已停用，所有依存於它的服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Performance Logs & Alerts	手動	
61	Windows Server 2016 Web Server	TWG CB-01-007-0630	系統服務	Plug and Play	▪ 這項原則設定決定此電腦是否可識別硬體變更之服務 ▪ 啟用電腦以使用者沒有或很少的輸入來識別及適應硬體變更，停止或停用這個服務將導致系統不穩	電腦設定\Windows 設定\安全性設定\系統服務\Plug and Play	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					定			
62	Windows Server 2016 Web Server	TWG CB-01-007-0631	系統服務	Portable Device Enumerator Service	▪ 這項原則設定決定此電腦之群組原則是否可對卸除式媒體進行管理與強制執行 ▪ 強制卸除式大型存放裝置使用群組原則。可讓 Windows Media Player 及影像匯入精靈等應用程式，得以使用卸除式大型存放裝置，來傳輸並同步處理內容	電腦設定\Windows 設定\安全性設定\系統服務\Portable Device Enumerator Service	手動	
63	Windows Server 2016 Web Server	TWG CB-01-007-0632	系統服務	Power	這項原則設定決定此電腦是否可使用 Power 服務，以管理電源原則與電源原則通知傳遞	電腦設定\Windows 設定\安全性設定\系統服務\Power	自動	
64	Windows Server 2016 Web Server	TWG CB-01-007-0633	系統服務	Print Spooler	▪ 這項原則設定決定此電腦是否可使用 Print Spooler 服務 ▪ 此服務會多工緩衝處理列印工作，並處理與印表機的互動。如果	電腦設定\Windows 設定\安全性設定\系統服務\Print	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					關閉此服務，將無法列印或看見印表機	Spooler		
65	Windows Server 2016 Web Server	TWG CB-01-007-0634	系統服務	Printer Extensions and Notifications	▪ 這項原則設定決定此電腦是否可使用 Printer Extensions and Notifications 服務 ▪ 此服務會開啟自訂印表機對話方塊，以及處理來自遠端列印伺服器或印表機的通知 ▪ 如果關閉此服務，則無法查看印表機延伸或通知	電腦設定\Windows 設定\安全性設定\系統服務\Printer Extensions and Notifications	手動	
66	Windows Server 2016 Web Server	TWG CB-01-007-0635	系統服務	Problem Reports and Solutions Control Panel Support	▪ 這項原則設定決定此電腦是否可使用問題回報與解法諮詢控制台之服務 ▪ 此服務提供檢視、傳送及刪除「問題報告及解決方案」控制台中之系統等級問題報告的支援	電腦設定\Windows 設定\安全性設定\系統服務\Problem Reports and Solutions Control Panel	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						Support		
67	Windows Server 2016 Web Server	TWG CB-01-007-0636	系統服務	Remote Access Auto Connection Manager	這項原則設定決定此電腦是否可使用遠端自動連線服務。當程式參照遠端 DNS 或 NetBIOS 名稱或位址時，建立遠端網路的連線	電腦設定\Windows 設定\安全性設定\系統服務\Remote Access Auto Connection Manager	手動	
68	Windows Server 2016 Web Server	TWG CB-01-007-0637	系統服務	Remote Access Connection Manager	▪ 這項原則設定決定此電腦是否可使用 VPN 服務，以管理這台電腦到網際網路或其他遠端網路的撥號及虛擬私人網路(VPN)連線 ▪ 如果這個服務已停用，所有依存於它的服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Remote Access Connection Manager	手動	
69	Windows Server	TWG CB-01	系統服務	Remote Desktop Configuration	▪ 這項原則設定決定此電腦是否可使用 Remote Desktop Configuration	電腦設定\Windows 設定\	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 Web Server	-007-0638			service (RDCS)服務 ▪ 遠端桌面設定服務(RDCS)負責處理與遠端桌面服務及遠端桌面相關的設定及工作階段維護活動(需要系統內容)。這些包括每一工作階段暫存資料夾、遠端桌面主題與遠端桌面憑證	安全性設定\系統服務\Remote Desktop Configuration		
70	Windows Server 2016 Web Server	TWG CB-01-007-0639	系統服務	Remote Desktop Services	▪ 這項原則設定決定此電腦是否可使用 Remote Desktop Services 服務，以允許使用者以互動方式連線到遠端電腦 ▪ 遠端桌面及遠端桌面工作階段主機伺服器都需要依賴此服務。若要避免從遠端使用這部電腦，請取清除「系統內容」控制台項目的「遠端」索引標籤上的核取方塊	電腦設定\Windows 設定\安全性設定\系統服務\Remote Desktop Services	手動	
71	Windows	TWG	系統	Remote Desktop	▪ 這項原則設定決定此電腦是否可	電腦設定	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Web Server	CB-01-007-0640	服務	Services UserMode Port Redirector	使用 Remote Desktop Services UserMode Port Redirector 服務 ▪ 此項服務允許重新導向 RDP 連線的印表機、磁碟機及連接埠	\Windows 設定\安全性設定\系統服務\Remote Desktop Services UserMode Port Redirector		
72	Windows Server 2016 Web Server	TWG CB-01-007-0641	系統服務	Remote Procedure Call (RPC)	▪ 這項原則設定決定此電腦是否可使用 Remote Procedure Call (RPC) 服務 ▪ RPCSS 服務是 COM 與 DCOM 伺服器的服務控制管理員。該服務會為 COM 與 DCOM 伺服器執行物件啟用要求、物件輸出程式解析，以及分散式記憶體回收 ▪ 如果停止或停用此服務，使用 COM 或 DCOM 的程式將無法正常運作。強烈建議持續執行 RPCSS	電腦設定\Windows 設定\安全性設定\系統服務\Remote Procedure Call (RPC)	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					服務			
73	Windows Server 2016 Web Server	TWG CB-01-007-0642	系統服務	Remote Procedure Call (RPC) Locator	▪ 這項原則設定決定此電腦是否可使用 Remote Procedure Call (RPC) Locator 服務 ▪ 在 Windows 2003 以及更舊的 Windows 版本中，遠端程序呼叫(RPC)尋找程式服務負責管理 RPC 名稱服務資料庫 ▪ 在 Windows Vista 與更新的 Windows 版本中，此服務不提供任何功能，只是為了應用程式相容性而保留	電腦設定\Windows 設定\安全性設定\系統服務\Remote Procedure Call (RPC) Locator	手動	
74	Windows Server 2016 Web Server	TWG CB-01-007-0643	系統服務	Remote Registry	▪ 這項原則設定決定此電腦是否可使用 Remote Registry 服務，由遠端使用者修改這個電腦上的登錄設定 ▪ 如果這個服務被停止，登錄只能由	電腦設定\Windows 設定\安全性設定\系統服務\Remote Registry	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					這個電腦上的使用者修改 ▪如果這個服務被停用，任何明確依存於它的服務將無法啟動			
75	Windows Server 2016 Web Server	TWG CB-01-007-0644	系統服務	Resultant Set of Policy Provider	這項原則設定決定此電腦是否提供網路服務來處理要求，以模擬在各種情況下，將「群組原則」設定值套用至目標使用者或電腦，並推斷「原則結果組」設定值	電腦設定\Windows 設定\安全性設定\系統服務\Resultant Set of Policy Provider	手動	
76	Windows Server 2016 Web Server	TWG CB-01-007-0645	系統服務	Routing and Remote Access	這項原則設定決定此電腦是否可於本機區域與網路使用 Routing 服務，以提供連到區域網路及廣域網路的公司的路由服務	電腦設定\Windows 設定\安全性設定\系統服務\Routing and Remote Access	已停用	
77	Windows Server	TWG CB-01	系統服務	RPC Endpoint Mapper	▪這項原則設定決定此電腦是否可使用 RPC Endpoint Mapper 服務，	電腦設定\Windows 設定\	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 Web Server	-007-0646			以解析 RPC 介面識別元為傳輸端點 ▪如果此服務停止或停用，使用遠端程序呼叫(RPC)服務的程式將無法正常運作	安全性設定\系統服務\RPC Endpoint Mapper		
78	Windows Server 2016 Web Server	TWG CB-01-007-0647	系統服務	Secondary Logon	▪這項原則設定決定此電腦是否可以在其他認證中啟動處理程序 ▪如果這個服務停止，將無法使用這個登入存取類型。如果這個服務已停用，它的所有依存服務都無法開始	電腦設定\Windows 設定\安全性設定\系統服務\Secondary Logon	手動	
79	Windows Server 2016 Web Server	TWG CB-01-007-0648	系統服務	Secure Socket Tunneling Protocol Service	▪這項原則設定決定此電腦是否可使用 Secure Socket Tunneling Protocol (SSTP)服務，以提供安全通訊端通道通訊協定(SSTP)使用 VPN 連線到遠端電腦的支援 ▪如果停用此服務，使用者將無法使	電腦設定\Windows 設定\安全性設定\系統服務\Secure Socket Tunneling	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					用 SSTP 存取遠端伺服器	Protocol Service		
80	Windows Server 2016 Web Server	TWG CB-01-007-0649	系統服務	Security Accounts Manager	▪ 這項原則設定決定此電腦是否可使用 Security Accounts Manager 服務，以告知其他服務，安全性帳戶管理員(SAM)已準備好要接受要求 ▪ 停用此服務將阻止通知系統中的其他服務 SAM 已經就緒，而導致那些服務無法正確地啟動 ▪ 此服務不應該停用	電腦設定\Windows 設定\安全性設定\系統服務\Security Accounts Manager	自動	
81	Windows Server 2016 Web Server	TWG CB-01-007-0650	系統服務	Server	▪ 這項原則設定決定此電腦是否使用 Server 服務 ▪ 為這個電腦支援網路上檔案、列印及命名管線的共用 ▪ 如果停止此服務，將無法使用這些功能 ▪ 如果這個服務被停用，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Server	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
82	Windows Server 2016 Web Server	TWG CB-01-007-0651	系統服務	Shell Hardware Detection	▪ 這項原則設定決定此電腦是否可使用 Shell Hardware Detection 服務 ▪ 此項服務為自動播放硬體事件提供通知	電腦設定\Windows 設定\安全性設定\系統服務\Shell Hardware Detection	自動	
83	Windows Server 2016 Web Server	TWG CB-01-007-0652	系統服務	Smart Card	▪ 這項原則設定決定此電腦是否可使用智慧卡功能 ▪ 管理這個電腦所讀取智慧卡的存取。如果這個服務被停止，這個電腦將無法讀取智慧卡。如果這個服務被停用，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Smart Card	已停用	
84	Windows Server 2016 Web Server	TWG CB-01-007-0653	系統服務	Smart Card Removal Policy	這項原則設定決定此電腦是否可透過智慧卡移除動作進行使用者電腦鎖定之服務。允許將系統設定為在智慧卡移除時，鎖定使用者桌面	電腦設定\Windows 設定\安全性設定\系統服務\Smart	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
						Card Removal Policy		
85	Windows Server 2016 Web Server	TWG CB-01-007-0654	系統服務	SNMP Trap	▪ 這項原則設定決定此電腦是否可使用 SNMP Trap 服務，以接收由本機或遠端簡易網路管理通訊協定(SNMP)代理程式所產生的陷阱訊息，並轉送該訊息給在這個電腦上執行中的 SNMP 管理程式 ▪ 如果這個服務被停止，這個電腦上 SNMP 為主的程式將不接收 SNMP 陷阱訊息。如果這個服務被停用，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\SNMP Trap	手動	
86	Windows Server 2016 Web Server	TWG CB-01-007-0655	系統服務	Software Protection	▪ 這項原則設定決定此電腦是否可使用 Software Protection 功能，以針對 Window 及 Windows 應用程式，啟用數位授權的下載、安裝及	電腦設定\Windows 設定\安全性設定\系統服務	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					強制執行功能 ▪ 如果停用該服務，作業系統及已授權的應用程式可能會以通知模式來執行 ▪ 強烈建議不要停用軟體保護服務	\Software Protection		
87	Windows Server 2016 Web Server	TWG CB-01-007-0656	系統服務	Special Administration Console Helper	這項原則設定決定是否允取系統管理員使用緊急管理服務，遠端存取命令提示字元	電腦設定\Windows 設定\安全性設定\系統服務\Special Administration Console Helper	手動	
88	Windows Server 2016 Web Server	TWG CB-01-007-0657	系統服務	Spot Verifier	這項原則設定決定是否檢查可能的檔案系統損毀	電腦設定\Windows 設定\安全性設定\系統服務\Spot Verifier	手動	
89	Windows	TWG	系統	SSDP Discovery	▪ 這項原則設定決定此電腦是否使	電腦設定	已停用	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Web Server	CB-01-007-0658	服務		用 SSDP 協定 ▪ 探索使用 SSDP 探索通訊協定且已連上網路的裝置及服務，例如 UPnP 裝置。還會宣告在本機電腦上執行的 SSDP 裝置及服務 ▪ 如果停止此服務，將會無法探索 SSDP 型的裝置。如果這個服務已停用，所有依存於它的服務都將無法啟動	\Windows 設定\安全性設定\系統服務\SSDP Discovery		
90	Windows Server 2016 Web Server	TWG CB-01-007-0659	系統服務	Superfetch	這項原則設定決定是否維護與改進一段時間後的系統效能	電腦設定\Windows 設定\安全性設定\系統服務\Superfetch	手動	
91	Windows Server 2016 Web	TWG CB-01-007-0	系統服務	System Event Notification Service	▪ 這項原則設定決定此電腦是否可使用系統事件監控與提示服務，以監視系統事件，並通知「COM+事	電腦設定\Windows 設定\安全性設定\系	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server	660			件系統」的訂閱者有關這些事件的內容	統服務\System Event Notification Service		
92	Windows Server 2016 Web Server	TWG CB-01-007-0661	系統服務	Task Scheduler	▪ 這項原則設定決定此電腦是否可使用 Task Scheduler 服務，讓使用者能夠在這台電腦上設定與排定自動的工作。此服務也主控多個 Windows 系統重要的工作 ▪ 如果停止或停用這個服務，這些工作將不會在其排定的時間執行 ▪ 如果停用這個服務，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Task Scheduler	自動	
93	Windows Server 2016 Web Server	TWG CB-01-007-0662	系統服務	TCP/IP NetBIOS Helper	▪ 這項原則設定決定此電腦是否可使用 TCP/IP NetBIOS Helper 服務，以提供對 NetBIOS over TCP/IP 以及網路上用戶端 NetBIOS 名稱	電腦設定\Windows 設定\安全性設定\系統服務\TCP/IP	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					解析的支援，因此讓使用者可以共用檔案、列印以及登入到網路 ▪ 如果這個服務被停止，可能無法使用這些功能 ▪ 如果這個服務被停用，任何明確依存於它的服務將無法啟動	NetBIOS Helper		
94	Windows Server 2016 Web Server	TWG CB-01-007-0663	系統服務	Telephony	▪ 這項原則設定決定此電腦是否可使用 Telephony API (TAPI)服務 ▪ 此服務為程式提供電話語音API(TAPI)支援，讓程式可以控制本機電腦上的電話語音裝置，或透過區域網路控制也同時執行該服務之伺服器上的電話語音裝置	電腦設定\Windows 設定\安全性設定\系統服務\Telephony	手動	
95	Windows Server 2016 Web Server	TWG CB-01-007-0664	系統服務	Themes	▪ 這項原則設定決定此電腦是否可使用 Themes 服務 ▪ 此服務提供使用者經驗主題管理	電腦設定\Windows 設定\安全性設定\系統服務\Themes	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
96	Windows Server 2016 Web Server	TWG CB-01-007-0665	系統服務	UPnP Device Host	▪ 這項原則設定決定此電腦是否可使用 UPnP Device Host 服務，允許在此電腦上裝載 UPnP 裝置 ▪ 如果停止此服務，任何裝載的 UPnP 裝置都將停止運作且無法新增其他裝載的裝置 ▪ 如果停用此服務，明確依存於此服務的任何服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\UPnP Device Host	已停用	
97	Windows Server 2016 Web Server	TWG CB-01-007-0666	系統服務	User Access Logging Service	▪ 這項原則設定決定此電腦是否可使用 User Access Logging Service 服務 ▪ 此服務會記錄本機伺服器上所安裝產品與角色的唯一用戶端存取要求(形式為 IP 位址與使用者名稱)。當系統管理員需要將伺服器軟體的用戶端需求量化以進行離線用戶端存取授權(CAL)管理時，可	電腦設定\Windows 設定\安全性設定\系統服務\User Access Logging Service	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					以透過 Powershell 查詢此資訊 ▪ 如果停用此服務，則用戶端要求不會留下記錄，也無法供人透過 Powershell 查詢抓取。停止此服務並不會影響歷史資料的查詢。本機系統管理員必須參閱其 Windows Server 授權條款，以決定要對伺服器軟體進行適當授權所需的 CAL 數目；使用 UAL 服務與資料並不會變更此義務			
98	Windows Server 2016 Web Server	TWG CB-01-007-0667	系統服務	User Profile Service	▪ 這項原則設定決定此電腦是否可使用 User Profile Service 服務 ▪ 此服務負責載入及解除載入使用者設定檔 ▪ 如果停止或停用此服務，使用者將無法順利登入或登出，應用程式可能會在取得使用者的資料時發生問題，用來接收設定檔事件通知的	電腦設定\Windows 設定\安全性設定\系統服務\User Profile Service	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					已註冊元件將無法接收通知			
99	Windows Server 2016 Web Server	TWG CB-01-007-0668	系統服務	Virtual Disk	▪這項原則設定決定此電腦是否可使用 Virtual Disk 服務 ▪此服務提供磁碟、磁碟區、檔案系統及存放裝置陣列的管理	電腦設定\Windows 設定\安全性設定\系統服務\Virtual Disk	手動	
100	Windows Server 2016 Web Server	TWG CB-01-007-0669	系統服務	Volume Shadow Copy	▪這項原則設定決定此電腦是否可使用硬體空間之 Shadow Copy 服務，以管理及執行用於備份與其他目的的磁碟區陰影複製 ▪如果這個服務被停止，陰影複製將無法用於備份，備份可能會失敗 ▪如果這個服務被停用，任何明確依存於它的服務將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Volume Shadow Copy	手動	
101	Windows Server 2016 Web	TWG CB-01-007-0	系統服務	Web Management Service	▪這項原則設定決定此電腦是否可使用 Web Management Service 服務 ▪Web 管理服務可啟用遠端及委派	電腦設定\Windows 設定\安全性設定\系	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server	670			管理功能，讓系統管理員管理呈現在這部電腦上的網頁伺服器、站台及應用程式	統服務\Web Management Service		
102	Windows Server 2016 Web Server	TWG CB-01-007-0671	系統服務	Windows Audio	▪這項原則設定決定此電腦是否可使用音訊之服務，以管理 Windows 程式的音訊 ▪如果這個服務停止，音訊裝置及效果將無法正常運作 ▪如果停用這個服務，將無法啟動明確依賴此服務的任何服務	電腦設定\Windows 設定\安全性設定\系統服務\Windows Audio	手動	
103	Windows Server 2016 Web Server	TWG CB-01-007-0672	系統服務	Windows Audio Endpoint Builder	▪這項原則設定決定此電腦是否可使用 Windows Audio Endpoint Builder 服務，以管理 Windows 音訊服務的音訊裝置 ▪如果停止此服務，音訊裝置與效果將無法正常運作 ▪如果停用此服務，所有明確依存於	電腦設定\Windows 設定\安全性設定\系統服務\Windows Audio Endpoint Builder	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					它的服務都將無法啟動			
104	Windows Server 2016 Web Server	TWG CB-01-007-0673	系統服務	Windows Driver Foundation-User-mode Driver Framework	▪ 這項原則設定決定此電腦是否可使用 Windows Driver Foundation-User-mode Driver Framework 服務，以建立並管理使用者模式驅動程式處理程序 ▪ 無法停止此服務	電腦設定\Windows 設定\安全性設定\系統服務\Windows Driver Foundation-User-mode Driver Framework	手動	
105	Windows Server 2016 Web Server	TWG CB-01-007-0674	系統服務	Windows Error Reporting Service	▪ 這項原則設定決定此電腦是否可使用 Windows Error Reporting Service 服務 ▪ 此服務在程式停止運作或停止回應時，允許回報錯誤，並且允許傳遞現有的解決方案。此外，也允許產生用於診斷與修復服務的記錄	電腦設定\Windows 設定\安全性設定\系統服務\Windows Error Reporting Service	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					檔 ▪ 如果此服務已停止，錯誤報告就可能無法正常運作，並且可能因此無法顯示診斷服務及修復的結果			
106	Windows Server 2016 Web Server	TWG CB-01-007-0675	系統服務	Windows Event Collector	▪ 這項原則設定決定此電腦之 Windows 事件蒐集服務是否啟用 ▪ 此服務管理支援 WS-Management 通訊協定之遠端來源事件的持續訂閱。這包括 Windows 事件記錄檔、硬體及啟用 IPMI 的事件來源。此服務會將轉送的事件儲存在本機事件記錄檔中 ▪ 如果此服務停止或停用，將無法建立事件訂閱，也無法接受轉送的事件	電腦設定\Windows 設定\安全性設定\系統服務\Windows Event Collector	手動	
107	Windows Server	TWG CB-01	系統服務	Windows Event Log	▪ 這項原則設定決定此電腦是否可使用 Windows Event Log 服務	電腦設定\Windows 設定\	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2016 Web Server	-007-0676			▪ 此服務管理事件與事件記錄檔，支援記錄事件、查詢事件、訂閱事件、封存事件記錄檔，以及管理事件中繼資料 ▪ 此服務可使用 XML 與純文字格式來顯示事件 ▪ 停止這個服務可能危害系統的安全性與可靠性	安全性設定\系統服務\Windows Event Log		
108	Windows Server 2016 Web Server	TWG CB-01-007-0677	系統服務	Windows Firewall	▪ 這項原則設定決定此電腦是否可使用 Windows 防火牆服務 ▪ Windows 防火牆經由阻止未授權使用者透過網際網路或網路取得對電腦的存取來保護電腦	電腦設定\Windows 設定\安全性設定\系統服務\Windows Firewall	自動	
109	Windows Server 2016 Web	TWG CB-01-007-0	系統服務	Windows Font Cache Service	▪ 這項原則設定決定此電腦是否可使用 Windows Font Cache Service 服務，以透過快取常用的字型資	電腦設定\Windows 設定\安全性設定\系	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server	678			料，可以最佳化應用程式效能 ▪ 如果這個服務尚未執行，應用程式便會啟動該服務。也可以停用此服務，不過這樣做會降低應用程式效能	統服務\Windows Font Cache Service		
110	Windows Server 2016 Web Server	TWG CB-01-007-0679	系統服務	Windows Installer	▪ 這項原則設定決定此電腦是否可使用 Windows Installer 服務，以新增、修改及移除以 Windows Installer (*.msi、*.msp)套件形式提供的應用程式 ▪ 如果停用此服務，所有明確依存於它的服務都將無法啟動	電腦設定\Windows 設定\安全性設定\系統服務\Windows Installer	手動	
111	Windows Server 2016 Web Server	TWG CB-01-007-0680	系統服務	Windows Management Instrumentation	▪ 這項原則設定決定此電腦是否可使用 Windows Management Instrumentation 服務，透過提供公用介面及物件模型，以存取有關作業系統、裝置、應用程式及服務的	電腦設定\Windows 設定\安全性設定\系統服務\Windows	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					管理資訊 ▪ 如果這個服務已停止，大多數的 Windows 軟體將無法正常運作 ▪ 如果這個服務已停用，所有依存於它的服務都將無法啟動	Management Instrumentation		
112	Windows Server 2016 Web Server	TWG CB-01-007-0681	系統服務	Windows Modules Installer	▪ 這項原則設定決定此電腦是否可使用 Windows 功能模組安裝服務 ▪ 此服務可以安裝、修改以及移除 Windows 更新與選用的元件 ▪ 如果停用此服務，則此電腦的安裝或解除安裝 Windows 更新可能會失敗	電腦設定\Windows 設定\安全性設定\系統服務\Windows Modules Installer	手動	
113	Windows Server 2016 Web Server	TWG CB-01-007-0682	系統服務	Windows 處理序啟用服務	▪ 這項原則設定決定此電腦是否可使用 Windows 處理序啟用服務 ▪ Windows 處理序啟用服務(WAS)可對訊息啟動的應用程式提供處理序啟用、資源管理及狀況管理服務	電腦設定\Windows 設定\安全性設定\系統服務\Windows 處理	手動	

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值	備註
						序啟用服務		
114	Windows Server 2016 Web Server	TWGCB-01-007-0683	系統服務	Windows Remote Management (WS-Management)	▪ 這項原則設定決定此電腦是否可使用 Windows 遠端管理服務 ▪ Windows 遠端管理(WinRM)服務為遠端管理實作 WS-Management 通訊協定 ▪ WS-Management 適用於遠端軟體與硬體管理的標準 Web 服務通訊協定。WinRM 服務會接聽並處理網路上的 WS-Management 要求。必須使用 winrm.cmd 命令列工具或透過群組原則來設定 WinRM 服務搭配接聽程式，它才能接聽網路上的要求 ▪ WinRM 服務提供 WMI 資料的存取，並能蒐集事件資料。必須執行此服務，對於事件的事件蒐集與訂閱才能運作。WinRM 訊息使用	電腦設定\Windows 設定\安全性設定\系統服務\Windows Remote Management (WS-Management)	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					HTTP 與 HTTPS 來進行傳輸 ▪ WinRM 服務不需依賴 IIS，但它的預先設定會在相同的電腦上與 IIS 共用相同的連接埠。WinRM 服務保留/wsman URL 首碼。為避免與 IIS 衝突，系統管理員應該確定 IIS 上執行的所有網站都不會使用 /wsman URL 首碼			
115	Windows Server 2016 Web Server	TWG CB-01-007-0684	系統服務	Windows Time	▪ 這項原則設定決定此電腦是否可使用 Windows Time 服務，以維護在網路上所有用戶端及伺服器的資料及時間同步處理 ▪ 如果這個服務停止，將無法進行日期與時間同步處理 ▪ 如果這個服務被停用，所有依存的服務都會停止	電腦設定\Windows 設定\安全性設定\系統服務\Windows Time	手動	
116	Windows	TWG	系統	Windows	▪ 這項原則設定決定此電腦是否可	電腦設定	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2016 Web Server	CB-01-007-0685	服務	Update	使用 Windows Update 服務，以偵測、下載並安裝 Windows 或其他程式的更新 ▪ 如果停用此服務，這部電腦的使用者將無法使用 Windows Update 或其自動更新功能。而且程式將無法使用 Windows Update Agent(WUA)API	\Windows 設定\安全性設定\系統服務\Windows Update		
117	Windows Server 2016 Web Server	TWG CB-01-007-0686	系統服務	WinHTTP Web Proxy Auto-Discovery Service	▪ 這項原則設定決定此電腦是否可使用 WinHTTP Web Proxy Auto-Discovery Service 服務 ▪ WinHTTP 會實作用戶端 HTTP 堆疊並提供開發人員 Win32 API 及 COM 自動化元件來傳送 HTTP 要求及接收回應。此外，WinHTTP 透過實作 Web Proxy Auto-Discovery(WPAD)通訊協定，提供自動探索 Proxy 設定的支	電腦設定\Windows 設定\安全性設定\系統服務\WinHTTP Web Proxy Auto-Discovery Service	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					援			
118	Windows Server 2016 Web Server	TWG CB-01-007-0687	系統服務	Wired AutoConfig	▪ 這項原則設定決定此電腦是否可使用 Wired AutoConfig 服務 ▪ 此項服務將於乙太網路卡上執行 IEEE 802.1X 驗證 ▪ 有線自動設定(DOT3SVC)服務負責在乙太網路介面上執行 IEEE 802.1X 驗證。如果目前的有線網路部署強制執行 802.1X 驗證，則應該設定執行 DOT3SVC 服務以建立第二層連線及/或提供網路資源存取。未強制執行 802.1X 驗證的有線網路則不受 DOT3SVC 服務影響	電腦設定\Windows 設定\安全性設定\系統服務\Wired AutoConfig	手動	
119	Windows Server 2016 Web Server	TWG CB-01-007-0688	系統服務	WMI Performance Adapter	▪ 這項原則設定決定此電腦是否可使用 WMI Performance Adapter 服務 ▪ 提供來自 Windows Management	電腦設定\Windows 設定\安全性設定\系統服務\WMI	手動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					Instrumentation(WMI)提供者的效能程式庫資訊給網路上的用戶端。只有在啟用效能資料協助程式時，這個服務才會執行	Performance Adapter		
120	Windows Server 2016 Web Server	TWG CB-01-007-0689	系統服務	Workstation	▪ 這項原則設定決定此電腦是否使用 Workstation 服務，用以建立及維護使用 SMB 通訊協定進行的用戶端與遠端伺服器網路連線 ▪ 如果停止這個服務，將無法使用這些連線 ▪ 如果停用這個服務，則會停止所有明確依存它的服務	電腦設定\Windows 設定\安全性設定\系統服務\Workstation	自動	
121	Windows Server 2016 Web Server	TWG CB-01-007-0690	系統服務	World Wide Web Publishing 服務	▪ 這項原則設定決定此電腦是否可使用 World Wide Web Publishing 服務 ▪ 此服務經由 Internet Information Services 管理員可提供網頁的連接	電腦設定\Windows 設定\安全性設定\系統服務\World Wide Web	自動	

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
					及管理能力	Publishing 服務		

資料來源：本中心整理

3. 參考文獻

[1]Common Configuration Enumeration(CCE)List.

http://cce.mitre.org/lists/cce_list.htm

[2]Center for Internet Security, CIS Microsoft Windows Server 2016 RTM (Release 1607) Benchmark v1.0.0.

https://benchmarks.cisecurity.org

[3]Center for Internet Security, CIS Microsoft Windows Server 2016 RTM (Release 1607) Benchmark v1.3.0.

https://benchmarks.cisecurity.org

[4]Windows Server 2016 Security Guide, Version 1.0. Microsoft Security Compliance Manager.

https://technet.microsoft.com/zh-tw/library/cc677002.aspx

[5]Defense Information Systems Agency (DISA), Microsoft Windows Server 2016 STIG MS DC Version: 1 Release: 3.

https://iase.disa.mil/stigs/os/windows/Pages/2016.aspx

[6]Defense Information Systems Agency (DISA), Microsoft Windows Server 2016 STIG Version: 2 Release: 1.

https://public.cyber.mil/stigs/downloads/

4. 附件

附件 1 版次 1.2 異動設定項目列表

附件1 版次 1.2 異動設定項目列表

●新增列表

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
1	Windows Server 2016 Common Settings	TWGCB-01-007-0691	系統管理範本\MS Security Guide	Enable Structured Exception Handling Overwrite Protection (SEHOP)	▪ 這項原則設定決定是否啟用結構化例外處理覆防寫(SEHOP)之保護機制 ▪ SEHOP 保護機制用於封鎖運用結構化例外處理常式(SEH)覆寫技術之入侵，由於此保護機制是在執行階段提供，因此無論應用程式是否已使用最新的改進功能進行編譯，都有助於保護應用程式 ▪ 如果啟用這項原則設定，將啟用 SEHOP 保護機制 ▪ 如果停用或未設定這項原則設定，將停用 SEHOP 保護機制 ▪ 若須於本機群組原則編輯器(Gpedit.msc)或群組原則管理(Gpmc.msc)等工具中顯示這項原則設定，請安裝 1703 以上版本	電腦設定\系統管理範本\MS Security Guide\Enable Structured Exception Handling Overwrite Protection (SEHOP)	已啟用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					之 SecGuide 系統管理範本		
2	Windows Server 2016 Common Settings	TWGCB-01-007-0692	系統管理範本\Microsoft 帳戶	封鎖所有消費者 Microsoft 帳戶使用者驗證	▪ 這項原則設定控制使用者是否能透過提供 Microsoft 帳戶，進行應用程式或服務的身分驗證 ▪ 如果啟用這項設定，此裝置上所有應用程式與服務，將無法透過 Microsoft 帳戶進行身分驗證 ▪ 這項設定同時適用於裝置目前的使用者以及可能新增的新使用者，但是對於已驗證使用者的應用程式或服務，在身分快取驗證過期前，啟用這項設定將不會造成任何影響 ▪ 建議在任何使用者登入裝置前啟用這項設定，可避免快取權杖出現 ▪ 如果停用或未設定這項設定，應用程式與服務可以使用 Microsoft 帳戶進行身分驗證	電腦設定\系統管理範本\Windows 元件\Microsoft 帳戶\封鎖所有消費者 Microsoft 帳戶使用者驗證	已啟用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					▪在預設情況下，這項設定將被停用 ▪注意：這項設定不影響使用者是否能透過 Microsoft 帳戶登入裝置，或使用者透過瀏覽器提供 Microsoft 帳戶以進行 Web 架構應用程式身分驗證之能力 ▪若須於本機群組原則編輯器(Gpedit.msc)或群組原則管理(Gpmc.msc)等工具中顯示這項原則設定，請安裝 1703 以上版本之 MSAPolicy 系統管理範本		
3	Windows Server 2016 Common Settings	TWGCB-01-007-0693	系統管理範本\訊息中心	允許簡訊服務雲端同步	▪這項原則設定決定是否允許將行動數據簡訊備份及還原到 Microsoft 雲端服務 ▪如果啟用這項設定，則允許簡訊服務雲端同步 ▪如果停用這項設定，則不允許簡訊服務雲端同步 ▪若須於本機群組原則編輯器(Gpedit.msc)或群組原則管理(Gpmc.msc)等工具中顯	電腦設定\系統管理範本\Windows 元件\訊息中心\允許簡訊服務雲端同步	已停用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					示這項原則設定，請安裝 1709 以上版本之 Messaging 系統管理範本		
4	Windows Server 2016 Common Settings	TWGCB-01-007-0694	系統管理範本/遠端桌面服務	需要對遠端(RDP)連線使用特定的安全層	▪ 這項原則設定決定在遠端桌面通訊協定(RDP)連線期間，是否必須使用特定的安全性階層，來確保用戶端與遠端桌面工作階段主機伺服器之間的通訊安全 ▪ 如果啟用這項原則設定，在遠端連線期間，用戶端與遠端桌面工作階段主機伺服器之間的所有通訊都必須使用這項設定中指定的安全性方法，可用之安全性方法如下： ➢ 交涉：交涉方法會強制執行用戶端支援的最安全方法。如果支援傳輸層安全性(TLS)，就使用 TLS 來驗證遠端桌面工作階段主機伺服器。如果不支援 TLS，則使用原始遠端桌面通訊協定(RDP)加密來確保通訊安全，但不會驗證遠端桌面工作階段主機伺服	電腦設定\系統管理範本\Windows 元件\遠端桌面服務\遠端桌面工作階段主機\安全性\需要對遠端(RDP)連線使用特定的安全層	已啟用：SSL

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					器 ➢RDP：RDP 方法會使用原始 RDP 加密，確保用戶端與遠端桌面工作階段主機伺服器之間的通訊安全。如果選取這項設定，就不會驗證遠端桌面工作階段主機伺服器 ➢SSL：必須使用 TLS 來驗證遠端桌面工作階段主機伺服器。如果不支援 TLS，連線會失敗 ▪如果停用或未設定這項原則設定，則不會在群組原則層級指定遠端桌面工作階段主機伺服器在遠端連線所要使用的安全性方法		
5	Windows Server 2016 Common	TWGCB-01-007-0695	系統管理範本/遠端桌面服務	透過使用網路層級驗證以要求對遠端連線進行	▪這項原則設定決定是否要使用網路層級驗證來對連至遠端桌面工作階段主機伺服器的遠端連線要求使用者驗證。此原則設定要求使用者驗證在遠端連線處理	電腦設定\系統管理範本\Windows 元件\遠端桌面服務\遠端桌	已啟用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	Settings			使用者驗證	程序初期執行，以增強安全性 ▪ 如果啟用這項原則設定，只有支援網路層級驗證的用戶端電腦能夠連線到遠端桌面工作階段主機伺服器，若要判斷用戶端電腦是否支援網路層級驗證，請在用戶端電腦上啟動「遠端桌面連線」，按一下「遠端桌面連線」對話方塊左上角的圖示，然後按一下「關於」。在「關於遠端桌面連線」對話方塊中，尋找是否出現「支援網路層級驗證」 ▪ 如果停用這項原則設定，則在允許遠端連線到遠端桌面工作階段主機伺服器之前，不必使用網路層級驗證進行使用者驗證 ▪ 如果未設定這項原則設定，則將強制執行目標電腦上的本機設定 ▪ 注意：停用這項原則設定將提供較低的安全性，因為使用者驗證將在遠端連線	面工作階段主機\安全性\透過使用網路層級驗證以要求對遠端連線進行使用者驗證	

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					處理程序後期執行		
6	Windows Server 2016 Common Settings	TWGCB-01-007-0696	系統管理範本/認證委派	加密預示修復	▪ 這項原則設定適用於使用 CredSSP 元件(例如：遠端桌面連線)之應用程式 ▪ CredSSP 通訊協定某些版本有弱點，容易受到針對用戶端的加密 Oracle 攻擊所威脅 ▪ 這項原則會控制易受攻擊的用戶端與伺服器之相容性，可讓使用者設定加密 Oracle 弱點所需的保護層級 ▪ 如果啟用這項原則設定，就會依據下列選項來選取 CredSSP 版本支援： ➢ 強制使用更新的用戶端：使用 CredSSP 的用戶端應用程式將無法回復成不安全的版本，並且使用 CredSSP 的服務將不會接受未修補的用戶端 ➢ 已降低影響：使用 CredSSP 的用戶端	電腦設定\系統管理範本\系統\認證委派\加密預示修復	已啟用：強制使用更新的用戶端

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					應用程式將無法回復成不安全的版本，但使用 CredSSP 的服務可接受未修補的用戶端 ➢易受攻擊：使用 CredSSP 的用戶端應用程式可支援回復成不安全的版本，且使用 CredSSP 的服務可接受未修補的用戶端，進而導致遠端伺服器容易遭受攻擊 ▪注意：除非所有遠端主機都已支援最新的版本，否則不應該使用「強制使用更新的用戶端」選項 ▪若須於本機群組原則編輯器(Gpedit.msc)或群組原則管理(Gpmc.msc)等工具中顯示這項原則設定，請安裝 1803 以上版本之 CredSsp 系統管理範本		
7	Windows Server 2016	TWGCB-01-007-0	系統管理範本/認證	遠端主機允許委派不可匯出	▪這項原則設定決定遠端主機是否允許委派不可匯出的認證	電腦設定\系統管理範本\系統\認證委	已啟用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	Common Settings	697	委派	的認證	▪使用認證委派時，裝置會將可匯出版本的認證提供給遠端主機，這會讓使用者暴露在遠端主機上攻擊者偷取認證的風險下 ▪如果啟用這項原則設定，主機支援「受限的系統管理」或「Remote Credential Guard」模式 ▪如果停用或未設定這項原則設定，則不支援「受限的系統管理」與「Remote Credential Guard」模式，使用者一律需要將其認證傳遞給主機 ▪若須於本機群組原則編輯器(Gpedit.msc)或群組原則管理(Gpmc.msc)等工具中顯示這項原則設定，請安裝 1703 以上版本之 CredSsp 系統管理範本	派\遠端主機允許委派不可匯出的認證	
8	Windows Server 2016	TWGCB-01-007-0	系統管理範本/檔案總管框架	開啟或關閉詳細資	▪這項原則設定決定是否在「檔案總管」中顯示或隱藏「詳細資料」窗格	使用者設定\系統管理範本\Windows	已啟用：一律

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	Common Settings	698	窗格	料窗格	▪如果啟用這項原則設定並設定為隱藏窗格，就會隱藏「檔案總管」中的「詳細資料」窗格，且使用者無法將其開啟 ▪如果啟用這項原則設定並設定為顯示窗格，就一律會顯示「檔案總管」中的「詳細資料」窗格，且使用者無法將其隱藏。這項設定的副作用是無法切換成「預覽」窗格，因為「詳細資料」窗格不能與「預覽」窗格同時顯示 ▪如果停用或未設定這項原則設定，則會依預設隱藏「詳細資料」窗格，且使用者可以將其顯示，這是預設的原則設定	元件\檔案總管\檔案總管框架窗格\開啟或關閉詳細資料窗格	隱藏
9	Windows Server 2016 Common Settings	TWGCB-01-007-0699	系統管理範本/檔案總管框架窗格	關閉預覽窗格	▪這項原則設定決定是否隱藏「檔案總管」中的「預覽」窗格 ▪如果啟用這項原則設定，就會隱藏「檔案總管」中的「預覽」窗格，且使用者無法將其開啟	使用者設定\系統管理範本\Windows 元件\檔案總管\檔案總管框架窗格\關	已啟用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					▪如果停用或未設定這項原則設定，則會依預設隱藏「預覽」窗格，但使用者可以將其顯示	閉預覽窗格	
10	Windows Server 2016 DC Server	TWGCB-01-007-0700	安全性選項\網域控制站	網域控制站：LDAP 伺服器通道繫結權杖要求	▪這項原則設定決定 LDAP 伺服器是否強制執行在 LDAP 繫結中，要求透過 LDAPS 連線傳送所接收的通道繫結權杖驗證，選項如下： ➢永不：不執行任何通道繫結驗證，這是所有尚未更新之伺服器的行為 ➢支援時：透過 TLS/SSL 連線進行驗證時，宣告支援通道繫結權杖的用戶端必須提供正確的權杖；未宣告這類支援及/或未使用 TLS/SSL 連線的用戶端不會受到影響，這是允許應用程式相容性的中間選項 ➢一律：所有用戶端都必須提供有關 LDAPS 的通道繫結資訊，伺服器拒絕來自不執行此動作之用戶端的	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網域控制站：LDAP 伺服器通道繫結權杖要求	一律

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					LDAPS 驗證要求 ▪ 預設值：未定義這項原則，則其效果與「支援時」相同 ▪ 注意：「支援時」選項僅保護那些支援驗證擴充保護的用戶端；未支援驗證擴充保護的用戶端仍可能會遭到攻擊，直到修補及/或設定這項原則 ▪ 若須於本機群組原則編輯器(Gpedit.msc)或群組原則管理(Gpmc.msc)等工具中顯示這項原則設定，請執行以下任一操作： ➢ 安裝微軟於 2020 年 3 月後所提供之更新，加入這項原則，GPO 設定路徑為「電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網域控制站：LDAP 伺服器通道繫結權杖要求」 ➢ 安裝 1809 以上版本之 SecGuide 系統管理範本，GPO 設定路徑為「電腦設定\系統管理範本\MS Security		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					Guide\Extended Protection for LDAP Authentication (Domain Controllers only)」		

資料來源：本中心整理

●刪除列表

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
1	Windows Server 2016 Common Settings	TWGCB-01-007-0096	安全性選項\網路安全性	網路安全性：強制限制登入時數	▪ 這項原則設定決定使用者連線至本機電腦若超過其使用者帳戶有效的登入時數時，是否要中斷連線。此設定會影響伺服器訊息區(SMB)元件 ▪ 啟用此設定時，若用戶端登入時數到期，會強制中斷用戶端工作階段與 SMB 伺服器的連線 ▪ 若停用此設定，當用戶端登錄時數到期	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路安全性：強制限制登入時數	已停用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					之後,可以允許保留已建立的用戶端工作階段		

資料來源：本中心整理

●修改列表

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
1	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0002	密碼原則	密碼最長使用期限	▪ 這項原則設定決定系統要求使用者變更密碼之前，密碼可以使用的期限(天數)。使用者可以設定密碼在 1 至 999 天之後到期；或將天數設為 0，表示密碼永遠不會到期。如果「密碼最長使用期限」介於 1 到 999 天之間，則「密碼最短使用期限」不得超過「密碼最長使用期限」的天數。如果「密碼最長使用期限」設定為 0，則「密碼最短使用期限」可以是介於 0 到 998 天之	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則\密碼最長使用期限	90 天以下

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						間的任何數值 ▪根據環境而定，「密碼最長使用期限」若設定密碼每 30 至 90 天到期。如此一來，攻擊者破解使用者密碼及存取網路資源的時間便很有限 ▪「密碼最長使用期限」預設值為 42		
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0002	密碼原則	密碼最長使用期限	▪這項原則設定決定系統要求使用者變更密碼之前，密碼可以使用的期限(天數)。使用者可以設定密碼在 1 至 999 天之後到期；或將天數設為 0，表示密碼永遠不會到期。如果「密碼最長使用期限」介於 1 到 999 天之間，則「密碼最短使用期限」不得超過「密碼最長使用期限」的天數。如果「密碼最長使用期限」設定為 0，則「密碼最短使用期限」可以是介於 0 到 998 天之間的任何數值 ▪根據環境而定，「密碼最長使用期限」	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則\密碼最長使用期限	90 天以下，但須大於 0 天

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						若設定密碼每 30 至 90 天到期。如此一來，攻擊者破解使用者密碼及存取網路資源的時間便很有限 ▪「密碼最長使用期限」預設值為 42		
2	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0003	密碼原則	最小密碼長度	▪這項原則設定決定使用者帳戶的密碼可包含的最少字元數 ▪使用者可以設定介於 1 到 20 個字元之間的值，或是將字元數設為 0，如此便不需要密碼 ▪最小密碼長度在網域控制站上預設值為 7，在獨立伺服器上預設值為 0	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則\最小密碼長度	12 個字元
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0003	密碼原則	最小密碼長度	▪這項原則設定決定使用者帳戶的密碼可包含的最少字元數 ▪使用者可以設定介於 1 到 14 個字元之間的值，或是將字元數設為 0，如此便不需要密碼 ▪最小密碼長度在網域控制站上預設值	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則\最小密碼長度	12 個字元以上

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						為 7，在獨立伺服器上預設值為 0		
3	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0007	帳戶鎖定原則	帳戶鎖定閾值	▪ 這項原則設定決定導致使用者帳戶被鎖定的嘗試登入失敗次數。除非由系統管理員重設或該帳戶的鎖定期間已到期，否則無法使用該鎖定帳戶。失敗的登入嘗試值可設定為介於 0 到 999 之間。如果將值設定為 0，將永遠不會鎖定該帳戶 ▪ 對使用 CTRL+ALT+DELETE 或受密碼保護的螢幕保護裝置來鎖定的工作站或成員伺服器輸入密碼失敗，也算是失敗的登入嘗試 ▪ 預設值為 0	電腦設定\Windows 設定\安全性設定\帳戶原則\帳戶鎖定原則\帳戶鎖定閾值	5 次不正確的登入嘗試
	修改後	Windows Server 2016 Common	TWGCB-01-007-0007	帳戶鎖定原則	帳戶鎖定閾值	▪ 這項原則設定決定導致使用者帳戶被鎖定的嘗試登入失敗次數。除非由系統管理員重設或該帳戶的鎖定時間已到期，否則無法使用該鎖定帳戶。失	電腦設定\Windows 設定\安全性設定\帳戶原則\帳戶	5 次以下不正確的登入嘗試，但須

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings				敗的登入嘗試值可設定為介於 0 到 999 之間。如果將值設定為 0，將永遠不會鎖定該帳戶 ▪ 對使用 CTRL+ALT+DELETE 或受密碼保護的螢幕保護裝置來鎖定的工作站或成員伺服器輸入密碼失敗，也算是失敗的登入嘗試 ▪ 預設值為 0	鎖定原則\帳戶鎖定閾值	大於 0 次
4	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0008	帳戶鎖定原則	重設帳戶鎖定計數器的時間間隔	▪ 這項原則設定決定在登入嘗試失敗之後必須經過幾分鐘，才會將失敗的登入嘗試計數器重設為 0 次失敗。可用的範圍是從 1 分鐘到 99,999 分鐘 ▪ 如果已定義帳戶鎖定閾值，此重設時間必須小於或等於帳戶鎖定期間	電腦設定\Windows 設定\安全性設定\帳戶原則\帳戶鎖定原則\重設帳戶鎖定計數器的時間間隔	15 分鐘
	修改後	Windows Server	TWGCB-01-007-	帳戶鎖定	重設帳戶鎖定計數	▪ 這項原則設定決定在登入嘗試失敗之後必須經過幾分鐘，才會將失敗的登	電腦設定\Windows 設定	15 分鐘以上

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		2016 Common Settings	0008	原則	器的時間間隔	入嘗試計數器重設為 0 次失敗。可用的範圍是從 1 分鐘到 99,999 分鐘 ▪ 如果已定義帳戶鎖定閾值，此重設時間必須小於或等於帳戶鎖定時間	\安全性設定\帳戶原則\帳戶鎖定原則\重設帳戶鎖定計數器的時間間隔	
5	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0009	帳戶鎖定原則	帳戶鎖定時間	▪ 這項原則設定決定在鎖定帳戶自動解除鎖定之前，還會繼續鎖定的分鐘數。可用的範圍是從 0 分鐘到 99,999 分鐘。如果將帳戶鎖定期間設定為 0，將會繼續鎖定帳戶，直到系統管理員明確將該帳戶解除鎖定 ▪ 如果已定義帳戶鎖定閾值，帳戶鎖定期間必須大於或等於重設時間	電腦設定\Windows 設定\安全性設定\帳戶原則\帳戶鎖定原則\帳戶鎖定時間	15 分鐘
	修改後	Windows Server 2016 Common	TWGCB-01-007-0009	帳戶鎖定原則	帳戶鎖定時間	▪ 這項原則設定決定在鎖定帳戶自動解除鎖定之前，還會繼續鎖定的分鐘數。可用的範圍是從 0 分鐘到 99,999 分鐘。如果將帳戶鎖定時間設定為 0，	電腦設定\Windows 設定\安全性設定\帳戶原則\帳戶	15 分鐘以上

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings				將會繼續鎖定帳戶，直到系統管理員明確將該帳戶解除鎖定 ▪ 如果已定義帳戶鎖定閾值，帳戶鎖定時間必須大於或等於重設時間	鎖定原則\帳戶鎖定時間	
6	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0016	安全性選項\Microsoft 網路伺服器	Microsoft 網路伺服器：暫停工作階段前，要求的閒置時間	▪ 這項原則設定決定伺服器訊息區(SMB)工作階段的連續閒置時間長度超過多少時，工作階段會因為處於非使用狀態而暫停 ▪ 系統管理員可使用此原則，控制電腦於何時暫停非使用中的 SMB 工作階段。若用戶端活動繼續，則會自動重新建立工作階段 ▪ 對於這項原則設定，零值表示在合理的時間範圍內儘速中斷工作階段的連線。最大值是 99,999，即 208 天；實際上，此值會停用此設定	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\Microsoft 網路伺服器：暫停工作階段前，要求的閒置時間	15 分鐘
	修改	Windows	TWGCB	安全	Microsoft	▪ 這項原則設定決定伺服器訊息區	電腦設定	15 分鐘

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	後	Server 2016 Common Settings	-01-007-0016	性選項\Microsoft 網路伺服器	網路伺服器：暫停工作階段前，要求的閒置時間	(SMB)工作階段的連續閒置時間長度超過多少時，工作階段會因為處於非使用狀態而暫停 ▪ 系統管理員可使用此原則，控制電腦於何時暫停非使用中的 SMB 工作階段。若用戶端活動繼續，則會自動重新建立工作階段 ▪ 對於這項原則設定，零值表示在合理的時間範圍內儘速中斷工作階段的連線。最大值是 99,999，實際上，此值會停用此設定	\Windows 設定\安全性設定\本機原則\安全性選項\Microsoft 網路伺服器：暫停工作階段前，要求的閒置時間	以下，但須大於 0 分鐘
7	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0018	安全性選項\MSS	MSS：(NoDefaultExempt)Configure IPSec exemptions for various	▪ 這項原則設定決定是否啟用 IPSec 篩選器的預設豁免項目 ▪ 選項如下： (1)Allow all exemptions (least secure)：代表「多點傳送廣播，RSVP、Kerberos 及 ISAKMP 流量	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：(NoDefaultExempt)Configure	Multicast, broadcast, and ISAKMP are exempt(Best for

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					types of network traffic.	不受限於 IPSec 篩選功能」 (2)Multicast, broadcast, & ISAKMP exempt (best for Windows XP)：代表「Kerberos 及 RSVP 流量不能免除 IPSec 篩選，但多點傳播、廣播及 ISAKMP 流量都是豁免」 (3)RSVP, Kerberos, and ISAKMP are exempt：代表「多點傳播和廣播流量不能免除 IPSec 篩選，但 RSVP、Kerberos 及 ISAKMP 流量被豁免」 (4)Only ISAKMP is exempt (recommended for Windows Server 2003)：代表「只有 ISAKMP 流量是免除 IPSec 篩選功能」	IPSec exemptions for various types of network traffic	Windows XP)
	修改後	Windows Server 2016 Common	TWGCB-01-007-0018	安全性選項\MS	MSS：(NoDefaultExempt)Configure	▪ 這項原則設定決定是否啟用 IPSec 篩選器的預設豁免項目 ▪ 選項如下：	電腦設定\Windows 設定\安全性設定\本機原則\安全	Multicast, broadcast, & ISAKMP

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings		S	IPSec exemptions for various types of network traffic.	(1)Allow all exemptions (least secure)：代表「多點傳送廣播，RSVP、Kerberos 及 ISAKMP 流量不受限於 IPSec 篩選功能」 (2)Multicast, broadcast, & ISAKMP exempt (best for Windows XP)：代表「Kerberos 及 RSVP 流量不能免除 IPSec 篩選，但多點傳播、廣播及 ISAKMP 流量都是豁免」 (3)RSVP, Kerberos, and ISAKMP are exempt：代表「多點傳播和廣播流量不能免除 IPSec 篩選，但 RSVP、Kerberos 及 ISAKMP 流量被豁免」 (4)Only ISAKMP is exempt (recommended for Windows Server 2003)：代表「只有 ISAKMP 流量是免除 IPSec 篩選功能」	性選項\MSS：(NoDefaultExempt)Configure IPSec exemptions for various types of network traffic.	exempt (best for Windows XP)

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
8	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0020	安全性選項\MSS	MSS：(TcpMaxDataRetransmissions)How many times unacknowledged data is retransmitted(3 recommended, 5 is default)	▪ 這項原則設定決定在放棄連線之前，透過 TCP 重傳未獲回應之資料的次數 ▪ 建議值設為 3 次，預設值設為 5 次	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：(TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted(3 recommended, 5 is default)	3
	修改後	Windows Server 2016 Common	TWGCB-01-007-0020	安全性選項\MS	MSS：(TcpMaxDataRetransmissions)H	▪ 這項原則設定決定在放棄連線之前，透過 TCP 重傳未獲回應之資料的次數 ▪ 建議值設為 3 次，預設值設為 5 次	電腦設定\Windows 設定\安全性設定\本機原則\安全	3 以下，但須大於 0

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings		S	ow many times unacknowledged data is retransmitted(3 recommended, 5 is default)		性選項\MSS：(TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted(3 recommended, 5 is default)	
9	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0026	安全性選項\MSS	MSS：(TcpMaxDataRetransmissions IPv6)How many times unacknowledged data	▪ 這項原則設定決定在放棄連線之前，透過 TCP 重傳未獲回應之資料的次數 ▪ 建議值設為 3 次，預設值設為 5 次	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：(TcpMaxDataRetransmissions IPv6)How	3

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					is retransmitted(3 recommended, 5 is default)		many times unacknowledged data is retransmitted(3 recommended, 5 is default)	
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0026	安全性選項\MSS	MSS：(TcpMaxDataRetransmissions IPv6)How many times unacknowledged data is retransmitted(3 recommend	▪ 這項原則設定決定在放棄連線之前，透過 TCP 重傳未獲回應之資料的次數 ▪ 建議值設為 3 次，預設值設為 5 次	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\MSS：(TcpMaxDataRetransmissions IPv6)How many times unacknowledged data is retransmitted(3	3 以下，但須大於 0

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					ed, 5 is default)		recommended, 5 is default)	
10	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0034	安全性選項\互動式登入	互動式登入：在密碼到期前提示使用者變更密碼	▪ 這項原則設定決定在使用者的密碼即將到期時，要提前多久(天數)事先警告使用者，讓使用者有時間建構密碼強度高的密碼 ▪ 預設值為 5 天	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：在密碼到期前提示使用者變更密碼	14 天
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0034	安全性選項\互動式登入	互動式登入：在密碼到期前提示使用者變更密碼	▪ 這項原則設定決定在使用者的密碼即將到期時，要提前多久(天數)事先警告使用者，讓使用者有時間建構密碼強度高的密碼 ▪ 預設值為 5 天	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：在密碼到期前提示使	14 天<u>以上</u>

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
							用者變更密碼	
11	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0036	安全性選項\互動式登入	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	▪ 每個唯一使用者的登入資訊會存放於本機快取，因此，若網域控制站在後續登入嘗試期間無法使用，他們仍然可以登入。快取的登入資訊是從先前的登入工作階段儲存。若網域控制站無法使用且未快取使用者的登入資訊，則會以「目前無可用的登入伺服器來服務登入請求」訊息提示使用者 ▪ 在這項原則設定中，0 值會停用登入快取。超過 50 的任何值只會快取 50 個登入嘗試。Windows 最多支援 50 個快取項目，而每一使用者耗用的項目數目取決於認證。舉例來說，在 Windows 系統中最多可以快取 50 個唯一密碼使用者帳戶，但只能快取 25 個智慧卡使用者帳戶，因為會同時儲存密碼資訊與智慧卡資訊。當擁有快取登入資訊	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：網域控制站無法使用時，要快取的先前登入次數	4 次

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						的使用者再次登入時，會取代該使用者個人的快取資訊		
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0036	安全性選項\互動式登入	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	▪ 每個唯一使用者的登入資訊會存放於本機快取，因此，若網域控制站在後續登入嘗試期間無法使用，他們仍然可以登入。快取的登入資訊是從先前的登入工作階段儲存。若網域控制站無法使用且未快取使用者的登入資訊，則會以「目前無可用的登入伺服器來服務登入請求」訊息提示使用者 ▪ 在這項原則設定中，0 值會停用登入快取。超過 50 的任何值只會快取 50 個登入嘗試。Windows 最多支援 50 個快取項目，而每一使用者耗用的項目數目取決於認證。舉例來說，在 Windows 系統中最多可以快取 50 個唯一密碼使用者帳戶，但只能快取 25 個智慧卡使用者帳戶，因為會同時儲存密碼資訊	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：網域控制站無法使用時，要快取的先前登入次數	4 次<u>以下</u>

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						與智慧卡資訊。當擁有快取登入資訊的使用者再次登入時，會取代該使用者個人的快取資訊		
12	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0041	安全性選項\互動式登入	互動式登入：電腦未使用時間限制	▪ 這項原則設定決定 Windows 是否會監控登入工作階段的未使用時間，而且會在未使用時間超過未使用時間限制時執行螢幕保護裝置並鎖定該工作階段 ▪ 數值必須介於 0 及 599,940 之間	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：電腦未使用時間限制	900 秒
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0041	安全性選項\互動式登入	互動式登入：電腦未使用時間限制	▪ 這項原則設定決定 Windows 是否會監控登入工作階段的未使用時間，而且會在未使用時間超過未使用時間限制時，執行螢幕保護裝置並鎖定該工作階段 ▪ 數值必須介於 0 及 599,940 之間	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：電腦未使用時間限制	900 秒以下，但須大於 0 秒

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
13	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0049	安全性選項\使用者帳戶控制	使用者帳戶控制：允許 UIAccess 應用程式不使用安全桌面來提升權限	▪ 這項原則設定控制使用者介面協助工具(UIAccess 或 UIA)程式在標準使用者使用提升權限提示時，是否自動停用安全桌面 ▪ 已啟用：UIA 程式，包括 Windows 遠端協助在內的 UIA 程式，可自動停用提升權限提示的安全桌面。如果未停用「使用者帳戶控制：提示提升權限時切換到安全桌面」原則設定，提示會出現在互動式使用者的桌面上，而非安全桌面 ▪ 已停用：(預設值)只有互動式桌面的使用者才能停用安全桌面，或是停用「使用者帳戶控制：提示提升權限時切換到安全桌面」原則設定才能停用安全桌面	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\使用者帳戶控制：允許 UIAccess 應用程式不使用安全桌面來提升權限	已停用
	修改	Windows Server	TWGCB-01-007-	安全性選	使用者帳戶控制：允	▪ 這項原則設定控制使用者介面協助工具(UIAccess 或 UIA)程式在標準使用	電腦設定\Windows 設定	已停用

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	後	2016 Common Settings	0049	項\使用者帳戶控制	許 UIAccess 應用程式不使用安全桌面來提示提升權限	者使用提升權限提示時，是否自動停用安全桌面 ▪ 已啟用：UIA 程式，包括 Windows 遠端協助在內的 UIA 程式，可自動停用提升權限提示的安全桌面。如果未停用「使用者帳戶控制：提示提升權限時切換到安全桌面」原則設定，提示會出現在互動式使用者的桌面上，而非安全桌面 ▪ 已停用：(預設值)只有互動式桌面的使用者才能停用安全桌面，或是停用「使用者帳戶控制：提示提升權限時切換到安全桌面」原則設定才能停用安全桌面	\安全性設定\本機原則\安全性選項\使用者帳戶控制：允許 UIAccess 應用程式不使用安全桌面來提示提升權限	
14	修改前	Windows Server 2016 Common	TWGCB-01-007-0051	安全性選項\使用	使用者帳戶控制：僅針對已簽署與驗證	▪ 這項原則設定會強制公開金鑰基礎結構(PKI)簽章檢查任何要求提升權限的互動式應用程式。系統管理員可透過將憑證新增至本機電腦的受信任的發	電腦設定\Windows 設定\安全性設定\本機原則\安全	已停用

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings		者帳戶控制	過的可執行檔，提高其權限	行者憑證存放區，來控制允許執行哪些應用程式 ▪ 選項如下： ➢ 已啟用：允許指定的可執行檔執行之前，強制執行 PKI 憑證路徑驗證 ➢ 已停用：(預設值)允許指定的可執行檔執行之前，不強制執行 PKI 憑證路徑驗證	性選項\使用者帳戶控制：僅針對已簽署與驗證過的可執行檔，提高其權限	
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0051	安全性選項\使用者帳戶控制	使用者帳戶控制：僅針對已簽章與驗證過的可執行檔，提高其權限	▪ 這項原則設定會強制公開金鑰基礎結構(PKI)簽章檢查任何要求提升權限的互動式應用程式。系統管理員可透過將憑證新增至本機電腦的受信任的發行者憑證存放區，來控制允許執行哪些應用程式 ▪ 選項如下： ➢ 已啟用：允許指定的可執行檔執行之前，強制執行 PKI 憑證路徑驗證	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\使用者帳戶控制：僅針對已簽章與驗證過的可執行檔，提高其	已停用

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						➢已停用：(預設值)允許指定的可執行檔執行之前，不強制執行 PKI 憑證路徑驗證	權限	
15	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0071	安全性選項\網域成員	網域成員：最長電腦帳戶密碼有效期	這項原則設定決定網域成員嘗試變更其電腦帳戶密碼的頻率	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網域成員：最長電腦帳戶密碼有效期	30 天
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0071	安全性選項\網域成員	網域成員：最長電腦帳戶密碼有效期	這項原則設定決定網域成員嘗試變更其電腦帳戶密碼的頻率	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網域成員：最長電腦帳戶密碼有效	30 天以下，但須大於 0 天

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
							期	
16	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0094	安全性選項\網路安全性	網路安全性：設定 Kerberos 允許的加密類型	▪ 這項原則設定允許使用者設定允許 Kerberos 使用的加密類型 ▪ 如果未選取，則不允許加密類型。這項設定可能會影響與用戶端電腦或者服務和應用程式的相容性。允許選取多個項目	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路安全性：設定 Kerberos 允許的加密類型	RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, 未來的加密類型
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0094	安全性選項\網路安全	網路安全性：設定 Kerberos 允許的加密類型	▪ 這項原則提供使用者設定允許 Kerberos 使用的加密類型 ▪ 如果未選取，則不允許加密類型。這項設定可能會影響與用戶端電腦或者服務與應用程式的相容性。允許選取	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\網路安全性：設定	AES128_HMAC_SHA1, AES256_HMAC_SHA1, 未

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
				性		多個項目	Kerberos 允許的加密類型	來的加密類型
17	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0100	安全性選項\稽核	稽核：強制執行稽核原則子類別設定 (Windows Vista 或更新版本)以覆寫稽核原則類別設定	▪ Windows Vista 及更新版本的 Windows 允許使用稽核原則子類別，以更精確的方式來管理稽核原則。在類別層級設定稽核原則，將會覆寫新的子類別稽核原則功能。群組原則只允許稽核原則可以在類別層級設定，而且因為新機器會加入網域或者升級至 Windows Vista 或更新的版本，所以現有的群組原則可以覆寫新機器的子類別設定。為了讓稽核原則不需變更群組原則即可使用子類別來管理，在 Windows Vista 與更新版本中有新的登錄值 SCENoApplyLegacyAuditPolicy，可防止將類別層級稽核原則套用到群組原則及「本機安全性原則」系統管理工	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\稽核：強制執行稽核原則子類別設定(Windows Vista 或更新版本)以覆寫稽核原則類別設定	已啟用

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						具 ▪ 如果在這裡設定的類別層級稽核原則與目前產生的事件不一致，其原因可能是已設定此登錄機碼		
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0100	安全性選項\稽核	稽核：強制執行稽核原則子類別設定(Windows Vista 或更新的版本)以覆寫稽核原則類別設定	▪ Windows Vista 及更新版本的 Windows 允許使用稽核原則子類別，以更精確的方式來管理稽核原則。在類別層級設定稽核原則，將會覆寫新的子類別稽核原則功能。群組原則只允許稽核原則可以在類別層級設定，而且因為新機器會加入網域或者升級至 Windows Vista 或更新的版本，所以現有的群組原則可以覆寫新機器的子類別設定。為了讓稽核原則不需變更群組原則即可使用子類別來管理，在 Windows Vista 與更新版本中有新的登錄值 SCENoApplyLegacyAuditPolicy，可防	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\稽核：強制執行稽核原則子類別設定(Windows Vista 或更新的版本)以覆寫稽核原則類別設定	已啟用

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						止將類別層級稽核原則套用到群組原則及「本機安全性原則」系統管理工具 ▪ 如果在這裡設定的類別層級稽核原則與目前產生的事件不一致，其原因可能是已設定此登錄機碼		
18	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0158	事件記錄服務/安全性	指定記錄檔大小上限(KB)	▪ 這項原則設定可指定記錄檔的大小上限(以 KB 為單位) ▪ 如果啟用這項原則設定，即可將記錄檔大小上限設定為介於 1 MB(1,024 KB)至 2TB(2,147,483,647 KB)之間(以 KB 為遞增單位) ▪ 如果停用或未設定這項原則設定，則記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更這個值，此值預設為 20 MB	電腦設定\系統管理範本\Windows 元件\事件記錄服務\安全性\指定記錄檔大小上限(KB)	已啟用：196608KB

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0158	事件記錄服務/安全性	指定記錄檔大小上限(KB)	▪ 這項原則設定可指定記錄檔的大小上限(以 KB 為單位) ▪ 如果啟用這項原則設定，即可將記錄檔大小上限設定為介於 1 MB(1,024 KB)至 2TB(2,147,483,647 KB)之間(以 KB 為遞增單位) ▪ 如果停用或未設定這項原則設定，則記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更這個值，此值預設為 20 MB	電腦設定\系統管理範本\Windows 元件\事件記錄服務\安全性\指定記錄檔大小上限(KB)	已啟用：196,608KB 以上
19	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0160	事件記錄服務/系統	指定記錄檔大小上限(KB)	▪ 這項原則設定可指定記錄檔的大小上限(以 KB 為單位) ▪ 如果啟用這項原則設定，即可將記錄檔大小上限設定為介於 1 MB(1,024 KB)至 2TB(2,147,483,647 KB)之間(以 KB 為遞增單位)	電腦設定\系統管理範本\Windows 元件\事件記錄服務\系統\指定記錄檔大小上限	已啟用：32768KB

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						▪ 如果停用或未設定這項原則設定，則記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更這個值，此值預設為 20 MB	(KB)	
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0160	事件記錄服務/系統	指定記錄檔大小上限(KB)	▪ 這項原則設定可指定記錄檔的大小上限(以 KB 為單位) ▪ 如果啟用這項原則設定，即可將記錄檔大小上限設定為介於 1 MB(1,024 KB)至 2TB(2,147,483,647 KB)之間(以 KB 為遞增單位) ▪ 如果停用或未設定這項原則設定，則記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更這個值，此值預設為 20 MB	電腦設定\系統管理範本\Windows 元件\事件記錄服務\系統\指定記錄檔大小上限(KB)	已啟用：32,768KB 以上
20	修改	Windows	TWGCB	事件	指定記錄	▪ 這項原則設定可指定記錄檔的大小上	電腦設定\系統	已啟用：

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	前	Server 2016 Common Settings	-01-007-0162	記錄服務/應用程式	檔大小上限(KB)	限(以 KB 為單位) ▪ 如果啟用這項原則設定，即可將記錄檔大小上限設定為介於 1 MB(1,024 KB)至 2TB(2,147,483,647 KB)之間(以 KB 為遞增單位) ▪ 如果停用或未設定這項原則設定，則記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更這個值，此值預設為 20 MB	管理範本\Windows 元件\事件記錄服務\應用程式\指定記錄檔大小上限(KB)	32768KB
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0162	事件記錄服務/應用程式	指定記錄檔大小上限(KB)	▪ 這項原則設定可指定記錄檔的大小上限(以 KB 為單位) ▪ 如果啟用這項原則設定，即可將記錄檔大小上限設定為介於 1 MB(1,024 KB)至 2TB(2,147,483,647 KB)之間(以 KB 為遞增單位) ▪ 如果停用或未設定這項原則設定，則	電腦設定\系統管理範本\Windows 元件\事件記錄服務\應用程式\指定記錄檔大小上限(KB)	已啟用：32,768KB 以上

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						記錄檔大小上限將會設定為本機設定值。本機系統管理員可使用「記錄內容」對話方塊來變更這個值，此值預設為 20 MB		
21	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0179	系統管理範本/網際網路通訊管理	關閉檔案和資料夾的「發佈到網站」工作	▪ 這項原則設定指定「Windows」資料夾的檔案和資料夾工作是否有「將此檔案發佈到網站」、「將此資料夾發佈到網站」或「將選取項目發佈到網站」選項 ▪ 網頁發佈精靈可以用來下載提供者清單，並讓使用者發佈內容到網站 ▪ 如果啟用這項原則設定，將會從「Windows」資料夾的檔案和資料夾工作中移除這些工作 ▪ 如果停用或未設定這項原則設定，將顯示該工作	電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉檔案和資料夾的「發佈到網站」工作	已啟用
	修改	Windows	TWGCB	系統	關閉檔案	▪ 這項原則設定指定「Windows」資料夾	電腦設定\系統	已啟用

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	後	Server 2016 Common Settings	-01-007-0179	管理範本/網際網路通訊管理	及資料夾的[發佈到網站]工作	的檔案及資料夾工作是否有「將此檔案發佈到網站」、「將此資料夾發佈到網站」或「將選取項目發佈到網站」選項 ▪ 網頁發佈精靈可以用來下載提供者清單，並讓使用者發佈內容到網站 ▪ 如果啟用這項原則設定，將會從「Windows」資料夾的檔案及資料夾工作中移除這些工作 ▪ 如果停用或未設定這項原則設定，將顯示該工作	管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉檔案及資料夾的[發佈到網站]工作	
22	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0190	系統管理範本\MS Security Guid	Configure SMB v1 client driver	▪ 這項原則設定決定 SMBv1 用戶端驅動程式的啟動類型 ▪ 要停用 SMBv1 協定的用戶端處理，請選擇「啟用」選項按鈕，然後從下拉式功能表中選擇「停用驅動程式」 ▪ 警告：在任何情況下，不要選擇「停	電腦設定\系統管理範本\MS Security Guide\Configure SMB v1 client driver	啟用：停用驅動程式

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
				e		用」選項按鈕 ▪對此設定的更改需要重新開機才能生效		
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0190	系統管理範本\MS Security Guide	Configure SMB v1 client driver	▪這項原則設定決定 SMBv1 用戶端驅動程式的啟動類型 ▪要停用 SMBv1 協定的用戶端處理，請選擇「啟用」選項按鈕，然後從下拉式功能表中選擇「停用驅動程式」 ▪注意：在任何情況下，不要選擇「停用」選項按鈕 ▪對此設定的更改需要重新開機才能生效 ▪若須於本機群組原則編輯器(Gpedit.msc)或群組原則管理(Gpmc.msc)等工具中顯示這項原則設定，請安裝 1703 以上版本之 SecGuide 系統管理範本	電腦設定\系統管理範本\MS Security Guide\Configure SMB v1 client driver	已啟用：Disable driver (recommended)

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
23	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0191	系統管理範本\MS Security Guide	Configure SMB v1 server	▪ 這項原則設定決定啟用或停用 SMBv1 協定的伺服器端處理 ▪ 停用此設定，將停用 SMBv1 協定的伺服器端處理 ▪ 啟用此設定，將啟用 SMBv1 協定的伺服器端處理 ▪ 對此設定的更改需要重新開機才能生效	電腦設定\系統管理範本\MS Security Guide\Configure SMB v1 server	已停用
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0191	系統管理範本\MS Security Guide	Configure SMB v1 server	▪ 這項原則設定決定啟用或停用 SMBv1 協定的伺服器端處理 ▪ 停用此設定，將停用 SMBv1 協定的伺服器端處理 ▪ 啟用此設定，將啟用 SMBv1 協定的伺服器端處理 ▪ 對此設定的更改需要重新開機才能生效 ▪ 若須於本機群組原則編輯器	電腦設定\系統管理範本\MS Security Guide\Configure SMB v1 server	已停用

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						(Gpedit.msc)或群組原則管理(Gpmc.msc)等工具中顯示這項原則設定，請安裝 1703 以上版本之 SecGuide 系統管理範本		
24	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0199	進階稽核原則\系統	稽核其他系統事件	▪ 這項原則設定決定是否稽核下列任一事件： ➢Windows 防火牆服務及驅動程式的啟動及關閉 ➢Windows 防火牆服務的安全性原則處理 ➢加密編譯金鑰檔案及移轉操作 ▪ 預設值：成功，失敗	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\系統\稽核其他系統事件	沒有稽核
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0199	進階稽核原則\系統	稽核其他系統事件	▪ 這項原則設定決定是否稽核下列任一事件： ➢Windows 防火牆服務及驅動程式的啟動及關閉 ➢Windows 防火牆服務的安全性原則	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則	成功與失敗

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						處理 ➢加密編譯金鑰檔案及移轉操作 ▪ 預設值：成功，失敗	\系統\稽核其他系統事件	
25	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0201	進階稽核原則\物件存取	稽核其他物件存取事件	▪ 這項原則設定決定是否稽核因管理工作排程器物件或 COM+物件而產生的事件 ▪ 如果是排程器工作，則會稽核下列項目： ➢建立工作 ➢刪除工作 ➢啟用工作 ➢停用工作 ➢更新工作 ▪ 如果是 COM+物件，則會稽核下列項目： ➢新增類別目錄物件	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\物件存取\稽核其他物件存取事件	沒有稽核

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						➢更新類別目錄物件 ➢刪除類別目錄物件		
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0201	進階稽核原則\物件存取	稽核其他物件存取事件	▪這項原則設定決定是否稽核因管理工作排程器物件或 COM+物件而產生的事件 ▪如果是排程器工作，則會稽核下列項目： ➢建立工作 ➢刪除工作 ➢啟用工作 ➢停用工作 ➢更新工作 ▪如果是 COM+物件，則會稽核下列項目： ➢新增類別目錄物件 ➢更新類別目錄物件	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\物件存取\稽核其他物件存取事件	成功與失敗

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						➢刪除類別目錄物件		
26	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0203	進階稽核原則\物件存取	稽核檔案共用	▪這項原則設定決定是否稽核存取共用資料夾的嘗試 ▪如果設定這項原則設定，則會在嘗試存取共用資料夾時產生稽核事件。如果定義這項原則設定，則系統管理員可以指定只稽核成功、只稽核失敗，或同時稽核兩者 ▪注意：共用資料夾沒有系統存取控制清單(SACL)。如果啟用這項原則設定，則會稽核系統上所有共用資料夾的存取	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\物件存取\稽核檔案共用	沒有稽核
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0203	進階稽核原則\物件存	稽核檔案共用	▪這項原則設定決定是否稽核存取共用資料夾的嘗試 ▪如果設定這項原則設定，則會在嘗試存取共用資料夾時產生稽核事件。如果定義這項原則設定，則系統管理員	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則	成功與失敗

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
				取		可以指定只稽核成功、只稽核失敗，或同時稽核兩者 ▪ 注意：共用資料夾沒有系統存取控制清單(SACL)。如果啟用這項原則設定，則會稽核系統上所有共用資料夾的存取	\物件存取\稽核檔案共用	
27	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0211	進階稽核原則\物件存取	稽核詳細的檔案共用	▪ 這項原則設定決定是否稽核存取共用資料夾中之檔案及資料夾的嘗試。「詳細的檔案共用」設定記錄每次存取檔案或資料夾的事件，而「檔案共用」設定對於用戶端和檔案共用之間建立的任何連線只會記錄一次事件。「詳細的檔案共用」稽核的事件，包括關於權限或用來授與或拒絕存取之其他條件的詳細資訊 ▪ 如果設定這項原則設定，當嘗試存取共用上的檔案或資料夾時，就會產生稽核事件。系統管理員可以指定只稽	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\物件存取\稽核詳細的檔案共用	沒有稽核

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						核成功、只稽核失敗，或同時稽核兩者 ▪ 注意：共用資料夾沒有系統存取控制清單(SACL)。如果啟用這項原則設定，則會稽核系統上所有共用檔案與資料夾的存取		
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0211	進階稽核原則\物件存取	稽核詳細的檔案共用	▪ 這項原則設定決定是否稽核存取共用資料夾中之檔案及資料夾的嘗試。「詳細的檔案共用」設定記錄每次存取檔案或資料夾的事件，而「檔案共用」設定對於用戶端與檔案共用之間建立的任何連線只會記錄一次事件。「詳細的檔案共用」稽核的事件，包括關於權限或用來授與或拒絕存取之其他條件的詳細資訊 ▪ 如果設定這項原則設定，當嘗試存取共用上的檔案或資料夾時，就會產生稽核事件。系統管理員可以指定只稽	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\物件存取\稽核詳細的檔案共用	失敗

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						核成功、只稽核失敗，或同時稽核兩者 ▪ 注意：共用資料夾沒有系統存取控制清單(SACL)。如果啟用這項原則設定，則會稽核系統上所有共用檔案與資料夾的存取		
28	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0215	進階稽核原則\原則變更	稽核授權原則變更	▪ 這項原則設定決定是否稽核因授權原則變更而產生的事件，例如： ➢指派未透過「驗證原則變更」子類別稽核的使用者權限(如 SeCreateTokenPrivilege) ➢移除未透過「驗證原則變更」子類別稽核的使用者權限(如 SeCreateTokenPrivilege) ➢加密檔案系統(EFS)原則的變更 ➢物件之資源屬性的變更 ➢套用至物件之集中存取原則(CAP)	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\原則變更\稽核授權原則變更	沒有稽核

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						的變更 ▪ 如果設定這項原則設定，則會在嘗試變更授權原則時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在變更授權原則時產生稽核事件 ▪ 預設值：沒有稽核		
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0215	進階稽核原則\原則變更	稽核授權原則變更	▪ 這項原則設定決定是否稽核因授權原則變更而產生的事件，例如： ➢ 指派未透過「驗證原則變更」子類別稽核的使用者權限(如 SeCreateTokenPrivilege) ➢ 移除未透過「驗證原則變更」子類別稽核的使用者權限(如 SeCreateTokenPrivilege) ➢ 加密檔案系統(EFS)原則的變更	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\原則變更\稽核授權原則變更	成功

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						➢物件之資源屬性的變更 ➢套用至物件之集中存取原則(CAP)的變更 ▪ 如果設定這項原則設定，則會在嘗試變更授權原則時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在變更授權原則時產生稽核事件 ▪ 預設值：沒有稽核		
29	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0217	進階稽核原則\原則變更	稽核 MPSSVC 規則層級原則變更	▪ 這項原則設定決定是否稽核因 Microsoft 保護服務(MPSSVC)使用之原則規則變更而產生的事件。這個服務是供 Windows 防火牆使用。包含下列事件： ➢報告 Windows 防火牆服務啟動時的使用中原則	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\原則變更\稽核 MPSSVC 規	沒有稽核

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						➢Windows 防火牆規則的變更 ➢Windows 防火牆例外清單的變更 ➢Windows 防火牆設定的變更 ➢Windows 防火牆服務忽略或未套用的規則 ➢Windows 防火牆群組原則設定的變更 ▪ 如果設定這項原則設定，則會在嘗試變更 MPSSVC 所使用的原則規則時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，在 MPSSVC 使用的原則規則變更時則不會產生稽核事件 ▪ 預設值：沒有稽核	則層級原則變更	
	修改後	Windows Server	TWGCB-01-007-	進階稽核	稽核 MPSSVC	▪ 這項原則設定決定是否稽核因 Microsoft 保護服務(MPSSVC)使用之	電腦設定\Windows 設定	成功與失敗

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		2016 Common Settings	0217	原則\原則變更	規則層級原則變更	原則規則變更而產生的事件。這個服務是供 Windows 防火牆使用。包含下列事件： ➢報告 Windows 防火牆服務啟動時的使用中原則 ➢Windows 防火牆規則的變更 ➢Windows 防火牆例外清單的變更 ➢Windows 防火牆設定的變更 ➢Windows 防火牆服務忽略或未套用的規則 ➢Windows 防火牆群組原則設定的變更 ▪如果設定這項原則設定，則會在嘗試變更 MPSSVC 所使用的原則規則時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪如果未設定這項原則設定，在	\安全性設定\進階稽核原則設定\稽核原則\原則變更\稽核 MPSSVC 規則層級原則變更	

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						MPSSVC 使用的原則規則變更時則不會產生稽核事件 ▪ 預設值：沒有稽核		
30	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0218	進階稽核原則\原則變更	稽核其他原則變更事件	▪ 這項原則設定決定是否稽核原則變更類別未稽核之其他安全性原則變更所產生的事件，例如： ➢信賴平台模組(TPM)組態變更 ➢核心模式密碼編譯自我測試 ➢密碼編譯提供者操作 ➢密碼編譯內容操作或修改 ➢已套用的集中存取原則(CAP)變更 ➢開機設定資料(BCD)修改 ▪ 預設值：沒有稽核	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\原則變更\稽核其他原則變更事件	沒有稽核
	修改後	Windows Server 2016	TWGCB-01-007-0218	進階稽核原則	稽核其他原則變更事件	▪ 這項原則設定決定是否稽核原則變更類別未稽核之其他安全性原則變更所產生的事件，例如：	電腦設定\Windows 設定\安全性設定\	失敗

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Common Settings		\原則變更		➢信賴平台模組(TPM)組態變更 ➢核心模式密碼編譯自我測試 ➢密碼編譯提供者操作 ➢密碼編譯內容操作或修改 ➢已套用的集中存取原則(CAP)變更 ➢開機設定資料(BCD)修改 ▪ 預設值：沒有稽核	進階稽核原則設定\稽核原則\原則變更\稽核其他原則變更事件	
31	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0222	進階稽核原則\帳戶登入	稽核 Kerberos 驗證服務	▪ 這項原則設定決定是否稽核因 Kerberos 驗證票證授權票證(TGT)要求而產生的事件。 ▪ 如果設定這項原則設定，則會在 Kerberos 驗證 TGT 要求之後產生稽核事件。成功稽核會記錄成功要求，而失敗稽核則會記錄失敗要求 ▪ 如果未設定這項原則設定，則不會在 Kerberos 驗證 TGT 要求之後產生稽核	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\帳戶登入\稽核 Kerberos 驗證服務	沒有稽核

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						事件 ▪ 用戶端版本的預設值：沒有稽核 ▪ 伺服器版本的預設值：成功		
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0222	進階稽核原則\帳戶登入	稽核 Kerberos 驗證服務	▪ 這項原則設定決定是否稽核因 Kerberos 驗證票證授權票證(TGT)要求而產生的事件 ▪ 如果設定這項原則設定，則會在 Kerberos 驗證 TGT 要求之後產生稽核事件。成功稽核會記錄成功要求，而失敗稽核則會記錄失敗要求 ▪ 如果未設定這項原則設定，則不會在 Kerberos 驗證 TGT 要求之後產生稽核事件 ▪ 伺服器版本的預設值：成功	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\帳戶登入\稽核 Kerberos 驗證服務	成功與失敗
32	修改前	Windows Server 2016	TWGCB-01-007-0224	進階稽核原則	稽核 Kerberos 服務票證操	▪ 這項原則設定決定是否稽核因針對使用者帳戶提交 Kerberos 驗證票證授權票證(TGT)要求而產生的事件	電腦設定\Windows 設定\安全性設定\	沒有稽核

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Common Settings		\帳戶登入	作	▪ 如果設定這項原則設定，則會在針對使用者帳戶要求 Kerberos 驗證 TGT 之後產生稽核事件。成功稽核會記錄成功要求，而失敗稽核則會記錄失敗要求 ▪ 如果未設定這項原則設定，則不會在針對使用者帳戶要求 Kerberos 驗證 TGT 之後產生稽核事件 ▪ 用戶端版本的預設值：沒有稽核 ▪ 伺服器版本的預設值：成功	進階稽核原則設定\稽核原則\帳戶登入\稽核 Kerberos 服務票證操作	
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0224	進階稽核原則\帳戶登入	稽核 Kerberos 服務票證操作	▪ 這項原則設定決定是否稽核因針對使用者帳戶提交 Kerberos 驗證票證授權票證(TGT)要求而產生的事件 ▪ 如果設定這項原則設定，則會在針對使用者帳戶要求 Kerberos 驗證 TGT 之後產生稽核事件。成功稽核會記錄成功要求，而失敗稽核則會記錄失敗要	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\帳戶登入\稽核 Kerberos 服	成功與失敗

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						求 ▪ 如果未設定這項原則設定，則不會在針對使用者帳戶要求 Kerberos 驗證 TGT 之後產生稽核事件 ▪ 伺服器版本的預設值：成功	務票證操作	
33	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0230	進階稽核原則\帳戶管理	稽核發佈群組管理	▪ 這項原則設定決定是否稽核因發佈群組變更而產生的事件，例如： ➢建立、變更或刪除發佈群組 ➢在發佈群組中新增或移除成員 ➢變更發佈群組類型 ▪ 如果設定這項原則設定，則會在嘗試變更發佈群組時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在發佈群組變更時產生稽核事件 ▪ 注意：這個子類別中的事件只會記錄	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\帳戶管理\稽核發佈群組管理	沒有稽核

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						在網域控制站上 ▪ 預設值：沒有稽核		
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0230	進階稽核原則\帳戶管理	稽核發佈群組管理	▪ 這項原則設定決定是否稽核因發佈群組變更而產生的事件，例如： ➢建立、變更或刪除發佈群組 ➢在發佈群組中新增或移除成員 ➢變更發佈群組類型 ▪ 如果設定這項原則設定，則會在嘗試變更發佈群組時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 ▪ 如果未設定這項原則設定，則不會在發佈群組變更時產生稽核事件 ▪ 注意：這個子類別中的事件只會記錄在網域控制站上 ▪ 預設值：沒有稽核	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\帳戶管理\稽核發佈群組管理	成功

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
34	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0232	進階稽核原則\登入/登出	稽核帳戶鎖定	▪ 這項原則設定決定是否稽核因嘗試登入的帳戶被鎖定而失敗所產生的事件 ▪ 若設定這項原則設定，則會在帳戶因鎖定而無法登入電腦時產生稽核事件。成功稽核會記錄成功的嘗試，而失敗稽核則會記錄不成功的嘗試 ▪ 預設值：成功	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\登入/登出\稽核帳戶鎖定	沒有稽核
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0232	進階稽核原則\登入/登出	稽核帳戶鎖定	▪ 這項原則設定決定是否稽核因嘗試登入的帳戶被鎖定而失敗所產生的事件 ▪ 若設定這項原則設定，則會在帳戶因鎖定而無法登入電腦時產生稽核事件。成功稽核會記錄成功的嘗試，而失敗稽核則會記錄不成功的嘗試 ▪ 預設值：成功	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\登入/登出\稽核帳戶鎖定	失敗
35	修改前	Windows Server 2016	TWGCB-01-007-0248	Windows 防火	Windows 防火牆：網域設定	這項原則設定決定是否允許套用本機系統管理員所建立的本機防火牆規則	電腦設定\Windows 設定\安全性設定\	是(預設)

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Common Settings		牆/網域設定檔	檔：套用本機防火牆規則		具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\網域設定檔：套用本機防火牆規則	
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0248	Windows 防火牆/網域設定檔	Windows 防火牆：網域設定檔：套用本機防火牆規則	這項原則設定決定是否允許套用本機系統管理員所建立的本機防火牆規則	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\網域	是(預設)

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
							設定檔\設定\套用本機防火牆規則	
36	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0249	Windows 防火牆/網域設定檔	Windows 防火牆：網域設定檔：顯示通知	這項原則設定決定當程式因為接收輸入連線而被封鎖時，是否為使用者顯示通知	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\網域設定檔\顯示通知	是
	修改後	Windows Server 2016 Common	TWGCB-01-007-0249	Windows 防火牆/	Windows 防火牆：網域設定檔：顯示通	這項原則設定決定當程式因為接收輸入連線而被封鎖時，是否為使用者顯示通知	電腦設定\Windows 設定\安全性設定\具有進階安全	是

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings		網域設定檔	知		性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\網域設定檔\設定\顯示通知	
37	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0250	Windows 防火牆/網域設定檔	Windows 防火牆：網域設定檔：套用本機連線安全性規則	這項原則設定決定是否允許套用本機系統管理員所建立的本機連線安全性規則	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\網域設定檔：套用本機連線安全	是(預設)

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
							性規則	
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0250	Windows 防火牆/網域設定檔	Windows 防火牆：網域設定檔：套用本機連線安全性規則	這項原則設定決定是否允許套用本機系統管理員所建立的本機連線安全性規則	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\網域設定檔\設定\套用本機連線安全性規則	是(預設)
38	修改前	Windows Server 2016 Common	TWGCB-01-007-0251	Windows 防火牆/網域	Windows 防火牆：網域設定檔：允許單點傳播回	這項原則設定決定此電腦是否接收其傳出之多點傳送或廣播訊息的單點傳送回應	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows	否

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings		設定檔	應		防火牆\具有進階安全性的 Windows 防火牆\內容\網域設定檔\允許單點傳播回應	
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0251	Windows 防火牆/網域設定檔	Windows 防火牆：網域設定檔：允許單點傳播回應	這項原則設定決定此電腦是否接收其傳出之多點傳送或廣播訊息的單點傳送回應	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\網域設定檔\設定\允許單點傳播回應	否

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
39	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0254	Windows 防火牆/私人設定檔	Windows 防火牆：私人設定檔：套用本機防火牆規則	▪ 這項原則設定決定是否允許套用本機系統管理員所建立的本機防火牆規則	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\私人設定檔：套用本機防火牆規則	是(預設)
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0254	Windows 防火牆/私人設定	Windows 防火牆：私人設定檔：套用本機防火牆規則	這項原則設定決定是否允許套用本機系統管理員所建立的本機防火牆規則	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進	是(預設)

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
				檔			階安全性的 Windows 防火牆\內容\私人設定檔\設定\套用本機防火牆規則	
40	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0255	Windows 防火牆/私人設定檔	Windows 防火牆：私人設定檔：顯示通知	這項原則設定決定當程式因為接收輸入連線而被封鎖時，是否為使用者顯示通知	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\私人設定檔\顯示通知	是

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0255	Windows 防火牆/私人設定檔	Windows 防火牆：私人設定檔：顯示通知	這項原則設定決定當程式因為接收輸入連線而被封鎖時，是否為使用者顯示通知	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\私人設定檔\設定\顯示通知	是
41	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0256	Windows 防火牆/私人設定檔	Windows 防火牆：私人設定檔：允許單點傳播回應	這項原則設定決定此電腦是否接收其傳出之多點傳送或廣播訊息的單點傳送回應	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的	否

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
							Windows 防火牆\內容\私人設定檔\允許單點傳播回應	
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0256	Windows 防火牆/私人設定檔	Windows 防火牆：私人設定檔：允許單點傳播回應	這項原則設定決定此電腦是否接收其傳出之多點傳送或廣播訊息的單點傳送回應	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\私人設定檔\設定\允許單點傳播回應	否
42	修改	Windows Server	TWGCB-01-007-	Windows	Windows 防火牆：私	這項原則設定決定是否允許套用本機系統管理員所建立的本機連線安全性	電腦設定\Windows 設定	是(預設)

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	前	2016 Common Settings	0257	防火牆/私人設定檔	人設定檔：套用本機連線安全性規則	規則	\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\私人設定檔：套用本機連線安全性規則	
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0257	Windows 防火牆/私人設定檔	Windows 防火牆：私人設定檔：套用本機連線安全性規則	這項原則設定決定是否允許套用本機系統管理員所建立的本機連線安全性規則	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火	是(預設)

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
							牆\內容\私人設定檔\設定\套用本機連線安全性規則	
43	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0259	Windows 防火牆/公用設定檔	Windows 防火牆：公用設定檔：允許單點傳播回應	這項原則設定決定此電腦是否接收其傳出之多點傳送或廣播訊息的單點傳送回應	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\公用設定檔\允許單點傳播回應	否
	修改後	Windows Server 2016	TWGCB-01-007-	Windows 防火	Windows 防火牆：公用設定	這項原則設定決定此電腦是否接收其傳出之多點傳送或廣播訊息的單點傳	電腦設定\Windows 設定\安全性設定\	否

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Common Settings	0259	牆/公用設定檔	檔：允許單點傳播回應	送回應	具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\公用設定檔\設定\允許單點傳播回應	
44	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0260	Windows 防火牆/公用設定檔	Windows 防火牆：公用設定檔：顯示通知	這項原則設定決定當程式因為接收輸入連線而被封鎖時，是否為使用者顯示通知	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\公用	是

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
							設定檔\顯示通知	
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0260	Windows 防火牆/公用設定檔	Windows 防火牆：公用設定檔：顯示通知	這項原則設定決定當程式因為接收輸入連線而被封鎖時，是否為使用者顯示通知	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\公用設定檔\設定\顯示通知	是
45	修改前	Windows Server 2016 Common	TWGCB-01-007-0261	Windows 防火牆/公用	Windows 防火牆：公用設定檔：套用本機連線安	這項原則設定決定是否允許套用本機系統管理員所建立的本機連線安全性規則	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows	是(預設)

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings		設定檔	全性規則		防火牆\具有進階安全性的 Windows 防火牆\內容\公用設定檔：套用本機連線安全性規則	
	修改後	Windows Server 2016 Common Settings	TWGCB-01-007-0261	Windows 防火牆/公用設定檔	Windows 防火牆：公用設定檔：套用本機連線安全性規則	這項原則設定決定是否允許套用本機系統管理員所建立的本機連線安全性規則	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\公用設定檔\設定\套用本機連線	是(預設)

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
							安全性規則	
46	修改前	Windows Server 2016 Common Settings	TWGCB-01-007-0263	Windows 防火牆/公用設定檔	Windows 防火牆：公用設定檔：套用本機防火牆規則	這項原則設定決定是否允許套用本機系統管理員所建立的本機防火牆規則	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows 防火牆\具有進階安全性的 Windows 防火牆\內容\公用設定檔：套用本機防火牆規則	是(預設)
	修改後	Windows Server 2016 Common	TWGCB-01-007-0263	Windows 防火牆/公用	Windows 防火牆：公用設定檔：套用本機防火牆	這項原則設定決定是否允許套用本機系統管理員所建立的本機防火牆規則	電腦設定\Windows 設定\安全性設定\具有進階安全性的 Windows	是(預設)

項次	修改對照	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings		設定檔	規則		防火牆\具有進階安全性的 Windows 防火牆\內容\公用設定檔\設定\套用本機防火牆規則	

資料來源：本中心整理