



政府組態基準
Microsoft Windows Server 2012 R2
TWGCB-01-006
(V1.2)

行政院國家資通安全會報技術服務中心
中華民國110年10月

修訂歷史紀錄表

項次	版次	修訂日期	說明
1	1.0	107/1/29	新編
2	1.1	108/12/17	<ul style="list-style-type: none"> ▪ 刪除「CCE-ID」欄位，將 CCE-ID 資料移至「備註」欄位 ▪ 新增「TWGCB-ID」欄位與資料 ▪ 表 2 項次 145 之錯別字由「高等及」修改為「高等級」 ▪ 表 2 項次 146~151 共 6 項之類別與設定路徑由「事件日誌服務」修改為「事件記錄服務」 ▪ 表 2 項次 153 之設定路徑由「電腦設定\系統管理範本\Windows 元件\Windows 遠端殼層\」修改為「電腦設定\系統管理範本\Windows 元件\Windows 遠端殼層\」 ▪ 表 2 項次 158 之設定路徑由「電腦設定\系統管理範本\Windows 元件\系統\登入\」修改為「電腦設定\系統管理範本\系統\登入\」 ▪ 表 2 項次 159 之設定路徑由「電腦設定\系統管理範本\Windows 元件\系統\稽核建立處理程序\」修改為「電腦設定\系統管理範本\系統\稽核建立處理程序\」 ▪ 表 2 項次 163 之原則名稱與設定路徑由「關閉 Windows 客戶經驗改進計畫」修改為「關閉 Windows Messenger 客戶經驗改進計畫」 ▪ 表 3 項次 64 之原則名稱與設定路徑由「關閉 Windows Messenger 客戶經驗改進計畫」修改為「關閉 Windows 客戶經驗改進計畫」 ▪ 表 3 項次 84 之原則名稱由「強制特定螢幕保護裝置：Screen saver executable name」修改為「強制特定螢幕保護裝置」 ▪ 表 4 項次 1、43、49、61、67、76、83、113、123

項次	版次	修訂日期	說明
			<p>及 124 之設定值由「自動」修改為「手動」</p> <ul style="list-style-type: none"> ▪ 表 4 項次 7 與 26 之設定值由「手動」修改為「自動」 ▪ 表 4 項次 89 之設定值由「手動」修改為「已停用」
3	1.2	110/10/5	<ul style="list-style-type: none"> ▪ 表 2~表 6 部分項次說明內容修改用語，包含： <ul style="list-style-type: none"> i. 「這項安全性設定」、「此安全性設定」、「這個原則設定」、「此原則設定」及「此設定」修改為「這項原則設定」 ii. 「您」與「他們」修改為「使用者」 iii. 「警告：」、「重要：」及「重要事項：」修改為「注意：」 iv. 「和」修改為「與」或「及」 v. 「收集」修改為「蒐集」 vi. 「這個設定」修改為「這項設定」 vii. 「和/或」修改為「或」 viii. 移除多餘之說明文字、空格、標點符號及贅字(如會、的、您、它、以及、不) ix. 刪除對 Windows Server 2012 R2 前之舊版作業系統與非伺服器版本提醒事項 ▪ 表 2 項次 8 與 9 之說明內容，由「鎖定期間」修改為「鎖定時間」 ▪ 表 2 項次 12 之說明內容，由「停用此原則」修改為「停用此設定」 ▪ 表 2 項次 27 之說明內容，依照使用者介面選項名稱將「停用」修改為「已停用」，「啟用」修改為「已啟用」 ▪ 表 2 項次 28 之說明內容，由「啟用此設定後，將允許」修改為「這項原則設定決定是否允許」 ▪ 表 2 項次 32、41、68、90、141、154、155、156

項次	版次	修訂日期	說明
			<p>及 159，表 3 項次 50、52、56 及 75，表 4 項次 16，說明內容第一句句首補充「這項原則設定」、「這項原則設定決定」、「這項原則設定決定是否」、「這項原則設定控制」或「此服務」，並調整文字段落與標點符號</p> <ul style="list-style-type: none"> ▪ 表 2 項次 36 與表 3 項次 1 之說明內容，由「以下列訊息提示使用者：目前無可用的登入伺服器來服務登入請求」修改為「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」 ▪ 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 56 之說明內容，由「會控制要求」修改為「控制是否要求」 ▪ 表 2 項次 71 說明內容之錯別字「篡改」修改為「竄改」 ▪ 表 2 項次 93 之說明內容，由「如下：」修改為「選項如下：」 ▪ 表 2 項次 102 之說明內容，由「造成拒絕服務中斷」修改為「造成拒絕服務」 ▪ 表 2 項次 107、109、132 及 133 之說明內容，由「阻止」修改為「禁止」 ▪ 表 2 項次 127 之說明內容，由「如果啟用此原則」修改為「如果啟用此權限」 ▪ 表 3 項次 50 之說明內容，由「控制能否」修改為「決定能否」 ▪ 表 3 項次 52 之說明內容，由「損毀時停用」修改為「損毀時關閉」 ▪ 表 3 項次 56 之說明內容，由「這項原則設定可以」修改為「這項原則設定決定是否」

項次	版次	修訂日期	說明
			<ul style="list-style-type: none"> ▪ 新增 4 項、刪除 2 項及修改 57 項設定項目，異動內容詳見附件 1
4			
5			

目次

1. 前言	1
1.1 適用環境	1
1.2 項數統計	1
1.3 文件發行	2
2.Windows Server 2012 R2 政府組態基準列表	3
3. 參考文獻	371
4. 附件	372
附件 1 版次 1.2 異動設定項目列表	附件 1-1

表 目 次

表 1	Windows Server 2012 R2 組態基準項目統計	1
表 2	Windows Server 2012 R2 政府組態基準列表	3
表 3	Windows Server 2012 R2 DC Server 政府組態基準列表	170
表 4	Windows Server 2012 R2 DNS Server 政府組態基準列表	226
表 5	Windows Server 2012 R2 File Server 政府組態基準列表	277
表 6	Windows Server 2012 R2 Web Server 政府組態基準列表	325

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)的一致性安全設定(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疑慮。

1.1 適用環境

本文件適用於微軟公司所發行之 Windows Server 2012 R2 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安全基準與實作指引，供政府機關透過建立安全組態，提升資安防護能力。Windows Server 2012 R2 組態基準計有 242 項設定項目(表 1 項次 1)，如有安裝其他伺服器角色，Domain Controller Server(以下簡稱 DC Server)組態基準計有 83 項設定項目(表 1 項次 2)，DNS Server 組態基準計有 128 項設定項目(表 1 項次 3)，File Server 組態基準計有 132 項設定項目(表 1 項次 4)，Web Server 組態基準計有 129 項設定項目(表 1 項次 5)，項目統計詳見表 1，異動設定項目詳見附件 1。

表1 Windows Server 2012 R2 組態基準項目統計

項次	類別	項數	小計	合計
1	Windows Server 2012 R2 Account Settings	9	242	714
	Windows Server 2012 R2 Computer Settings	233		
2	Windows Server 2012 R2 DC Server	83	83	
3	Windows Server 2012 R2 DNS Server	128	128	
4	Windows Server 2012 R2 File Server	132	132	
5	Windows Server 2012 R2 Web Server	129	129	

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 2012 R2 政府組態基準列表

表2 Windows Server 2012 R2 政府組態基準列表

項次	GPO	TWG CB-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 2012 R2 Account Settings	TWG CB-01 -006-0 001	密碼 原則	密碼最短 使用期限	<ul style="list-style-type: none"> ▪ 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 	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-I D： CCE-3 7073-4

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
					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。因此，根據預設，「強制執行密碼歷程記錄」設定為 1			
2	Windows Server 2012 R2 Account Settings	TWG CB-01 -006-0 002	密碼 原則	密碼最長 使用期限	<ul style="list-style-type: none"> ▪ 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 ▪ 注意：根據使用者的環境而定，安全性的最佳作法是讓密碼每 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 	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-I D： CCE-3 7167-4

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
3	Windows Server 2012 R2 Account Settings	TWG CB-01-006-0003	密碼原則	最小密碼長度	<ul style="list-style-type: none"> ▪ 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 	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-36534-6
4	Windows Server 2012 R2 Account Settings	TWG CB-01-006-0004	密碼原則	密碼必須符合複雜性需求	<ul style="list-style-type: none"> ▪ 這項原則設定決定密碼是否必須符合複雜性需求 ▪ 如果啟用了此原則，則密碼必須符合下列最小需求： <ul style="list-style-type: none"> ➢ 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： <ol style="list-style-type: none"> (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) 	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則\密碼必須符合複雜性需求	已啟用	CCE-ID: CCE-37063-5

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
					(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			
5	Windows Server 2012 R2 Account Settings	TWG CB-01-006-005	密碼原則	強制執行密碼歷程記錄	<ul style="list-style-type: none"> ▪ 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 ▪ 注意：依預設，成員電腦會遵循其網域控制站的設定 	電腦設定 \\Windows 設定\\ 安全性設定\\帳 戶原則\\密碼原 則\\強制執行密 碼歷程記錄	3 個以上 記憶的密 碼	CCE-I D： CCE-3 7166-6
6	Windows Server 2012 R2 Account Settings	TWG CB-01-006-006	密碼原則	使用可還原的加密來存放密碼	<ul style="list-style-type: none"> ▪ 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，否則絕不應該啟用這項原則 	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-I D： CCE-3 6286-3

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
					<ul style="list-style-type: none"> 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 			
7	Windows Server 2012 R2 Account Settings	TWG CB-01 -006-0 007	帳戶 鎖定 原則	帳戶鎖定 閾值	<ul style="list-style-type: none"> 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。可以將失敗的登入嘗試值設定為介於 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 	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-I D： CCE-3 6008-1
8	Windows Server 2012 R2 Account	TWG CB-01 -006-0 008	帳戶 鎖定 原則	重設帳戶 鎖定計數 器的時間 間隔	<ul style="list-style-type: none"> 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 	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	15 分鐘以 上	CCE-I D： CCE-3 6883-7

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
	Settings				<ul style="list-style-type: none"> ▪ 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 	戶鎖定計數器的時間間隔		
9	Windows Server 2012 R2 Account Settings	TWG CB-01 -006-0 009	帳戶 鎖定 原則	帳戶鎖定 時間	<ul style="list-style-type: none"> ▪ 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-I D： CCE-3 7034-6
10	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 010	安全 性選 項 \\Micr osoft 網路 用戶 端	Microsoft 網路用戶 端：傳送未 加密的密 碼到其他 廠商的 SMB 伺服 器	<ul style="list-style-type: none"> ▪ 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 ▪ 傳送未經加密的密碼會有安全性風險 	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：傳 送未加密的密碼 到其他廠商的	已停用	CCE-I D： CCE-3 7863-8

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
						SMB 伺服器		
11	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 011	安全 性選 項 \ Micr o s o f t 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)	<ul style="list-style-type: none"> ▪ 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。此原則設定決定 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 ▪ 若停用此原則，SMB 用戶端將不會交涉 SMB 封包簽章 	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-I D： CCE-3 6269-9
12	Windows	TWG	安全	Microsoft	<ul style="list-style-type: none"> ▪ 這項原則設定決定 SMB 用戶端元件是否需 	電腦設定	已啟用	CCE-I

項次	GPO	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 2012 R2 Computer Settings	CB-01 -006-0 012	性選 項 \ Microsoft 網路 用戶 端	網路用戶 端：數位簽 章用戶端 的通訊(自 動)	<p>要封包簽章</p> <ul style="list-style-type: none"> ▪ 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。此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 	\ 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)		D： CCE-3 6325-9
13	Windows Server 2012 R2 Computer	TWG CB-01 -006-0 013	安全 性選 項 \ Microsoft	Microsoft 網路伺 服器：伺 服器 SPN 目 標名 稱驗 證	<ul style="list-style-type: none"> ▪ 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，選項如下： (1)關閉：SMB 伺服器不需要或不會驗證 	電腦設定 \ Windows 設定\ 安全性設定\ 本機原則\ 安全性選 項\ Microsoft	關閉	CCE-I D： CCE-3 6170-9

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
	Settings		網路 伺服器	層級	<p>SMB 用戶端的 SPN</p> <p>(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</p> <p>(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</p> <ul style="list-style-type: none"> 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 	網路伺服器：伺服器 SPN 目標名稱驗證層級		

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
14	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 014	安全 性選 項 \ Micr osoft 網路 伺服器	Microsoft 網路伺服 器：數位簽 章伺服器 的通訊(自 動)	<ul style="list-style-type: none"> ▪ 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。此原則設定決定允許與 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 	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(自動)	已啟用	CCE-I D： CCE-3 7864-6
15	Windows Server 2012 R2	TWG CB-01 -006-0	安全 性選 項	Microsoft 網路伺服 器：數位簽	<ul style="list-style-type: none"> ▪ 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 	電腦設定 \ Windows 設定\ 安全性設定\ 本	已啟用	CCE-I D： CCE-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
	Computer Settings	015	\Micro soft 網路 伺服器	章伺服器的通訊(如果用戶端同意)	<p>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。此原則設定決定 SMB 伺服器是否將在 SMB 用戶端要求 SMB 封包簽章時進行交涉</p> <ul style="list-style-type: none"> ▪ 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 ▪ 若停用此原則，SMB 用戶端將不會交涉 SMB 封包簽章 	機原則\安全性 選項\Microsoft 網路伺服器：數 位簽章伺服器的 通訊(如果用戶 端同意)		5988-5
16	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 016	安全 性選 項 \Micro soft 網路	Microsoft 網路伺服 器：暫停工 作階段 前，要求的 閒置時間	<ul style="list-style-type: none"> ▪ 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 	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	15 分鐘以 下，但須大 於 0 分鐘	CCE-I D： CCE-3 8046-9

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
			伺服器		<p>動繼續，則會自動重新建立工作階段</p> <ul style="list-style-type: none"> 對於此原則設定，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，此值會停用此原則 	停工作階段前，要求的閒置時間		
17	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0017	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	<ul style="list-style-type: none"> 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 啟用此原則時，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 如果停用此原則，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-37972-7
18	Windows Server 2012 R2	TWG CB-01-006-0	安全性選項	MSS：(NoDefault Exempt)	<ul style="list-style-type: none"> 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	Multicast, broadcast, &	CCE-ID： CCE-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
	Computer Settings	018	\MS S	Configure IPsec exemptions for various types of network traffic.	<p>(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」</p> <p>(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」</p> <p>(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」</p> <p>(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」</p>	機原則\安全性選項\MSS：(NoDefaultExempt) Configure IPsec exemptions for various types of network traffic	ISAKMP exempt (best for Windows XP)	6922-3
19	Windows Server 2012 R2 Computer	TWG CB-01-006-0	安全性選項 \MS	MSS：(KeepAliveTime) How often	<ul style="list-style-type: none"> 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是否仍然不變 	電腦設定 \Windows 設定\安全性設定\本機原則\安全性	300000 or 5 minutes (recommen	CCE-ID：CCE-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
	Settings	019	S	keep-alive packets are sent in milliseconds	<ul style="list-style-type: none"> ▪ 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 	選項\MSS：(KeepAliveTime) How often keep-alive packets are sent in milliseconds	ded)	6868-8
20	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-020	安全性選項\MS S	<p>MSS：(TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended</p>	<ul style="list-style-type: none"> ▪ 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	3 以下，但須大於 0	CCE-ID：CCE-36051-1

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
				ded, 5 is default)		is default)		
21	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0021	安全性選項 MS S	MSS : (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes	<ul style="list-style-type: none"> ▪ 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 : (EnableICMPRed irect) Allow ICMP redirects to override OSPF generated routes	已啟用	CCE-ID : CCE-3 7988-3
22	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0022	安全性選項 MS S	MSS : (Hidden) Hide Computer From the	<ul style="list-style-type: none"> ▪ 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 	電腦設定 \\Windows 設定\\ 安全性設定\\本 機原則\\安全性 選項\\MSS :	已啟用	CCE-ID : CCE-3 6862-1

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
				Browse List (not recommended except for highly secure environments)	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	(Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments)		
23	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0023	安全性選項 MS S	MSS : (DisableIP SourceRouting) IP source routing protection level (protects against	<ul style="list-style-type: none"> ▪ 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 ▪ 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： <ul style="list-style-type: none"> (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 	電腦設定 \\Windows 設定\ 安全性設定\ 本機原則\ 安全性選項\ MSS : (DisableIPSourceRouting) IP source routing protection level (protects against	Highest protection, source routing is completely disabled	CCE-ID : CCE-36535-3

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
				packet spoofing)	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	packet spoofing)		
24	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0024	安全性選項 MS S	MSS：(DisableIP SourceRouting IPv6) IP source routing protection level (protects against packet spoofing)	<ul style="list-style-type: none"> 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： <ul style="list-style-type: none"> (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 	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 routing protection level(protects against packet spoofing)	Highest protection, source routing is completely disabled	CCE-ID：CCE-36871-2
25	Windows Server 2012 R2	TWG CB-01-006-0	安全性選項	MSS：(NoNameReleaseOn	<ul style="list-style-type: none"> 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 	電腦設定 \\Windows 設定\\安全性設定\\本	已啟用	CCE-ID：CCE-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
	Computer Settings	025	\MS S	Demand) Allow the computer to ignore NetBIOS name release requests except from WINS servers	NetBIOS 名稱解析為這些系統所設定的 IP 位址 <ul style="list-style-type: none"> ▪ 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。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 	機原則\安全性 選項\MSS： (NoNameRelease OnDemand)Allo w the computer to ignore NetBIOS name release requests except from WINS servers		6879-5
26	Windows Server 2012 R2	TWG CB-01 -006-0	安全 性選 項	MSS： (TcpMaxD ataRetrans	<ul style="list-style-type: none"> ▪ 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 	電腦設定 \Windows 設定\ 安全性設定\本	3 以下，但 須大於 0	CCE-I D： CCE-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
	Computer Settings	026	\MS S	missions IPv6) How many times unacknowl edged data is retransmitt ed (3 recommen ded, 5 is default)	<ul style="list-style-type: none"> 建議值設為 3 次，預設值設為 5 次 	機原則\安全性 選項\MSS： (TcpMaxDataRet ransmissions IPv6)How many times unacknowledged data is retransmitted(3 recommended，5 is default)		7846-3
27	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 027	安全 性選 項 \MS S	MSS： (PerformR outerDisco very) Allow IRDP to	<ul style="list-style-type: none"> 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 	電腦設定 \Windows 設定\ 安全性設定\本 機原則\安全性 選項\MSS： (PerformRouterD	已啟用	CCE-I D： CCE-3 8065-9

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
				detect and configure Default Gateway addresses (could lead to DoS)	(2)已啟用 (3)僅在 DHCP 傳送路由器探查選項時啟用	iscovery)Allow IRDP to detect and configure Default Gateway addresses(could lead to DoS)		
28	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0028	安全性選項 MS S	MSS : (AutoReboot) Allow Windows to automatically restart after a system crash (recommen	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	已啟用	CCE-ID : CCE-38250-7

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
				ded except for highly secure environme nts)		except for highly secure environments)		
29	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 029	安全 性選 項 MS S	MSS： (WarningL evel) Percentage threshold for the security event log at which the system will generate a warning	<ul style="list-style-type: none"> ▪ 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-I D： CCE-3 6880-3

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
30	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 030	安全 性選 項 MS S	MSS： (SafeDllSe archMode) Enable Safe DLL search mode (recommen ded)	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➢ 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： <ul style="list-style-type: none"> ➢ 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 	電腦設定 \\Windows 設定\ 安全性設定\本 機原則\安全性 選項\MSS： (SafeDllSearchM ode) Enable Safe DLL search mode (recommended)	已啟用	CCE-I D： CCE-3 6351-5

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
31	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 031	安全 性選 項 MS S	MSS： (AutoAdm inLogon) Enable Automatic Logon (not recommen ded)	<ul style="list-style-type: none"> ▪ 這項原則設定決定電腦是否採取自動登入方式 ▪ 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 	電腦設定 \\Windows 設定\ 安全性設定\本 機原則\安全性 選項\MSS： (AutoAdminLog on)Enable Automatic Logon(not recommended)	已停用	CCE-I D： CCE-3 7067-6
32	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 032	安全 性選 項 MS S	MSS： (AutoShar eServer) Enable Administra tive Shares (recommen ded except	<ul style="list-style-type: none"> ▪ 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」工具來檢視它們 	電腦設定 \\Windows 設定\ 安全性設定\本 機原則\安全性 選項\MSS： (AutoShareServe r) Enable Administrative	已啟用	CCE-I D： CCE-3 5932-3

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
				for highly secure environments)	<ul style="list-style-type: none"> ▪ 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資料夾中： <ul style="list-style-type: none"> ➤ 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：這是在網域控制站的資源 ➤ SYSVOL：這是在網域控制站的資源 ➤ 列印\$：這是印表機的遠端管理期間所使用的資源 ➤ 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 	Shares (recommended except for highly secure environments)		

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
33	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0033	安全性選項\MS S	MSS : (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)	<ul style="list-style-type: none"> ▪ 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-37993-3
34	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0034	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。有了這個事先警告，使用者便有時間建構一個強式密碼	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	14 天以上	CCE-ID : CCE-37622-8

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
			入			入：在密碼到期前提示使用者變更密碼		
35	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-035	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	<ul style="list-style-type: none"> ▪ 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-38240-8
36	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-036	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	<ul style="list-style-type: none"> ▪ 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 	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	4 次以下	CCE-ID： CCE-37439-7

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
				數	<p>務登入請求」訊息提示使用者</p> <ul style="list-style-type: none"> ▪ 在此原則設定中，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取資訊 	無法使用時，要快取的先前登入次數		
37	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 037	安全 性選 項\ 互動 式登 入	互動式登 入：智慧卡 移除操作	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➤ 無動作 ➤ 鎖定工作站 ➤ 強制登出 	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-I D： CCE-3 8333-1

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
					<p>➤ 如果是遠端桌面服務工作階段則中斷連線</p> <ul style="list-style-type: none"> ▪ 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 2012 R2	TWG CB-01 -006-0	安全 性選 項\	互動式登 入：須有智	<ul style="list-style-type: none"> ▪ 這項原則設定需要使用者使用智慧卡來登入電腦 	電腦設定 \Windows 設定\ 安全性設定\本	已停用	CCE-I D： CCE-3

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Computer Settings	038	互動式登入	慧卡	<ul style="list-style-type: none"> ▪ 選項如下： <ul style="list-style-type: none"> ➢ 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 	機原則\安全性選項\互動式登入：須有智慧卡		8045-1
39	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0039	安全性選項\互動式登入	互動式登入：不要求按 CTRL+ALT+DEL 鍵	<ul style="list-style-type: none"> ▪ 這項原則設定決定使用者是否需要按 CTRL+ALT+DEL 才能登入 ▪ 如果在電腦上啟用了此原則，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，這可確保使用者輸入密碼時，以受信任的路徑進行通訊 ▪ 如果停用了此原則，則任何使用者都需要按 CTRL+ALT+DEL 才能登入 Windows 	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：不要求按 CTRL+ALT+DEL 鍵	已停用	CCE-ID：CCE-37637-6
40	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0040	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	<ul style="list-style-type: none"> ▪ 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 ▪ 如果啟用此原則，登入畫面不會顯示上次順利登入的使用者名稱 	電腦設定\Windows 設定\安全性設定\本機原則\安全性	已啟用	CCE-ID：CCE-36056-0

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
	Settings		式登 入	者名稱	<ul style="list-style-type: none"> ▪ 如果停用此原則，便會顯示上次登入的使用者名稱 	選項\互動式登 入：不要顯示上 次登入的使用者 名稱		
41	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 041	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	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-I D： CCE-3 8235-8
42	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 042	安全 性選 項\ 系統 加密 編譯	系統加密 編譯：對使 用者儲存 在電腦上 的金鑰強 制使用增 強式金鑰	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➢ 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 	電腦設定 \Windows 設定\ 安全性設定\本 機原則\安全性 選項\系統加密 編譯：對使用者 儲存在電腦上的	當新金鑰 被儲存及 使用時，不 要求使用 者的輸入	CCE-I D： CCE-3 6327-5

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
				保護	<ul style="list-style-type: none"> 使用者必須在每次使用金鑰時輸入密碼 	金鑰強制使用增強式金鑰保護		
43	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-043	安全性選項\系統加密編譯	系統加密編譯:使用 FIPS 相容演算法於加密, 雜湊, 以及簽章	<ul style="list-style-type: none"> 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 與 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 	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\系統加密編譯: 使用 FIPS 相容演算法於加密, 雜湊, 以及簽章	已啟用	CCE-ID: CCE-36110-5

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
					<ul style="list-style-type: none"> 對於遠端桌面服務，它只支援使用三重 DES 加密演算法來加密遠端桌面服務網路通訊 			
44	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 044	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)	<ul style="list-style-type: none"> 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 若啟用此原則，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-I D： CCE-3 7644-2
45	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 045	安全 性選 項\ 系統 物件	系統物 件：要求不 區分大小 寫用於非 Windows	<ul style="list-style-type: none"> 這項原則設定決定是否要強制所有子系統區分大小寫。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、 	電腦設定 \Windows 設定\ 安全性設定\ 本機原則\ 安全性選 項\ 系統物	已啟用	CCE-I D： CCE-3 7885-1

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
				子系統	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	件：要求不區分大小寫用於非 Windows 子系統		
46	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0046	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-35921-6
47	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0047	安全性選項\系統設定	系統設定：於軟體限制原則對 Windows 可執行檔使用憑證	▪ 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，可以建立憑證規則，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	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：於軟體限制原則對 Windows	已啟用	CCE-ID：CCE-37172-4

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
				規則	<p>效，必須啟用這項原則設定</p> <ul style="list-style-type: none"> 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 	可執行檔使用憑證規則		
48	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0048	安全性選項\ 使用者帳戶控制	使用者帳戶控制：提示提升權限時切換到安全桌面	<ul style="list-style-type: none"> 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 選項如下： <ul style="list-style-type: none"> 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 	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：提示提升權限時切換到安全桌面	已啟用	CCE-ID： CCE-36866-2
49	Windows Server 2012 R2 Computer	TWG CB-01-006-0049	安全性選項\ 使用	使用者帳戶控制：允許 UIAccess	<ul style="list-style-type: none"> 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 	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-36863-9

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
	Settings		者帳戶控制	應用程式不使用安全桌面來提示提升權限	<p>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</p> <ul style="list-style-type: none"> 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 	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		
50	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 050	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	<ul style="list-style-type: none"> 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： <ul style="list-style-type: none"> 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 	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-37029-6

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
					<p>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的認證，操作會以使用者的最高可用權限繼續</p> <ul style="list-style-type: none"> ➤ 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 ➤ 認證提示：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 ➤ 同意提示：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 ➤ 非 Windows 二進位檔案的同意提示：(預 			

項次	GPO	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 2012 R2 Computer Settings	TWG CB-01 -006-0 051	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	<ul style="list-style-type: none"> ▪ 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。企業的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： <ul style="list-style-type: none"> ➢ 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 	電腦設定 \ <windows 設定\<br=""></windows> 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-I D： CCE-3 6865-4
52	Windows Server	TWG CB-01	安全 性選	使用者帳 戶控制:所	<ul style="list-style-type: none"> ▪ 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。如果變更此原則設 	電腦設定 \ <windows 設定\<br=""></windows>	已啟用	CCE-I D：

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 Computer Settings	-006-0 052	項\ 使用者帳 戶控 制	有系統管 理員均以 管理員核 准模式執 行	<p>定，必須重新啟動電腦</p> <ul style="list-style-type: none"> ▪ 選項如下： <ul style="list-style-type: none"> ➢ 已啟用：(預設值)啟用管理員核准模式。必須啟用此原則，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：如果停用此原則設定，資訊安全中心會通知作業系統的整體安全性已降低 	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		CCE-3 6869-6
53	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 053	安全 性選 項\ 使用 者帳	使用者帳 戶控制：偵 測應用程 式安裝，並 提示提升	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➢ 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 	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	已啟用	CCE-I D： CCE-3 6533-8

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
			戶控制	權限	<p>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</p> <p>➤ 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，應該停用此原則設定。在此情況下，不需要進行安裝程式偵測</p>	戶控制：偵測應用程式安裝，並提示提升權限		
54	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0054	安全性選項\使用者帳戶控制	使用者帳戶控制：內建的 Administrator 帳戶的管理員核准模式	<ul style="list-style-type: none"> ▪ 這項原則設定會控制內建的 Administrator 帳戶的管理員核准模式行為 ▪ 選項如下： <ul style="list-style-type: none"> ➤ 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 	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：內建的 Administrator 帳戶的管理員核准模式	已啟用	CCE-ID：CCE-36494-3

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
					程式			
55	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 055	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	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➤ 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 ➤ 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 	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 的行為	提示輸入 認證	CCE-I D： CCE-3 6864-7

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
					執行			
56	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0056	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 應用程式，提高其權限	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➢ ...\Program Files\，包含子目錄 ➢ ...\Windows\system32\ ➢ ...\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： <ul style="list-style-type: none"> ➢ 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 	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：僅針對在安全位置安裝的 UIAccess 應用程式，提高其權限	已啟用	CCE-ID：CCE-37057-7

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
					<ul style="list-style-type: none"> ➤ 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 			
57	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 057	安全 性選 項\ 使用 者帳 戶控 制	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	<ul style="list-style-type: none"> ▪ 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。此原則設定可減少那些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： <ul style="list-style-type: none"> ➤ 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 	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：將 檔案及登 錄寫入失 敗虛擬化 並儲存至 每一使用 者位置	已啟用	CCE-ID： CCE-3 7064-3
58	Windows Server	TWG CB-01	安全 性選	修復主控台：允許軟	<ul style="list-style-type: none"> ▪ 這項原則設定決定是否允許使用修復主控台 SET 命令 	電腦設定 \Windows 設定\ 安全性選 項\ 修復主控 台	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
	2012 R2 Computer Settings	-006-0 058	項\ 修復 主控 台	碟複製以 及存取所 有磁碟和 所有資料 夾	<ul style="list-style-type: none"> ▪ 啟用此安全性選項便可以使用修復主控台 SET 命令，此命令可讓使用者設定下列修復主控台環境變數： <ul style="list-style-type: none"> ➤ AllowWildCards：對某些命令啟用萬用字元支援(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 	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 以及存取 所有磁碟 和所有資 料夾		CCE-3 7307-6
59	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 059	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	<ul style="list-style-type: none"> ▪ 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	已停用	CCE-I D： CCE-3 7624-4

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
						統管理登入		
60	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 060	安全 性選 項\ 帳戶	帳戶：限制 使用空白 密碼的本 機帳戶僅 能登入到 主控台	<ul style="list-style-type: none"> ▪ 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 ▪ 注意：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」 	電腦設定 \ Windows 設定\ 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	已啟用	CCE-I D： CCE-3 7615-2

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
61	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0061	安全性選項\ 帳戶	帳戶：重新命名來賓帳戶名稱	<ul style="list-style-type: none"> 這項原則設定決定不同的帳戶名稱是否與「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 	電腦設定\ \Windows 設定\ 安全性設定\ 本機原則\ 安全性選項\ 帳戶：重新命名來賓帳戶名稱	Renamed_Guest	CCE-ID： CCE-38027-9
62	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0062	安全性選項\ 帳戶	帳戶：重新命名系統管理員帳戶	<ul style="list-style-type: none"> 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 	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-38233-3
63	Windows Server 2012 R2 Computer	TWG CB-01-006-0063	安全性選項\ 裝置	裝置：防止使用者安裝印表機	<ul style="list-style-type: none"> 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 	電腦設定\ \Windows 設定\ 安全性設定\ 本機原則\ 安全性	已啟用	CCE-ID： CCE-38027-9

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
	Settings	063	裝置	驅動程式	<p>安裝印表機驅動程式</p> <ul style="list-style-type: none"> ▪ 如果啟用此設定，只有 Administrators 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 ▪ 注意： <ul style="list-style-type: none"> ➢ 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 	選項\裝置：防止使用者安裝印表機驅動程式		7942-0
64	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 064	安全性選項\ 裝置	裝置：允許卸除而不須登入	<ul style="list-style-type: none"> ▪ 這項原則設定決定是否可卸除可攜式電腦而不須登入 ▪ 如果已啟用此原則，則不須登入即可使用外部硬體的退出按鈕來卸除電腦 ▪ 如果停用此原則，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 ▪ 注意：停用此原則可能會讓使用者使用外部硬體退出按鈕以外的方法，嘗試並實際從銜 	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-35908-3

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
					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			
65	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 065	安全 性選 項\ 裝置	裝置：允許 格式化以 及退出卸 除式媒體	<ul style="list-style-type: none"> ▪ 這項原則設定決定允許哪些人格式化與退出卸除式 NTFS 媒體 ▪ 此功能可指定給： <ul style="list-style-type: none"> ➤ Administrators ➤ Administrators 與 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 退出卸 除式媒 體	Administra tors	CCE-I D： CCE-3 7701-0
66	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 066	安全 性選 項\ 裝置	裝置： CD-ROM 存取只限 於登入本 機的使用 者	<ul style="list-style-type: none"> ▪ 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 ▪ 如果啟用此原則，便只允許以互動方式登入的使用者存取卸除式 CD-ROM 媒體。如果啟用此原則但無人以互動方式登入，便能從網路存取該 CD-ROM 	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 存取只 限於登 入本機 的使用 者	已停用	CCE-I D： CCE-3 5971-1

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
67	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 067	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	<ul style="list-style-type: none"> ▪ 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 ▪ 如果啟用此原則，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。如果啟用此原則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-I D： CCE-3 7529-5
68	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 068	安全 性選 項\ 網域 成員	網域成 員：停用電 腦帳戶密 碼變更	<ul style="list-style-type: none"> ▪ 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 ▪ 如果啟用了此設定，網域成員便不會嘗試變更其電腦帳戶密碼 ▪ 如果停用了此設定，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，預設為每隔 30 天 ▪ 注意： <ul style="list-style-type: none"> ➢ 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 	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-I D： CCE-3 7508-9

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
					<p>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</p> <p>➤ 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</p>			
69	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 069	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 天以 下，但須大 於 0 天	CCE-I D： CCE-3 7431-4
70	Windows Server 2012 R2 Computer	TWG CB-01 -006-0	安全 性選 項\ 網域	網域成 員：安全通 道資料加 以數位加	<ul style="list-style-type: none"> ▪ 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， 	電腦設定 \ Windows 設定\ 安全性設定\ 本機原則\ 安全性	已啟用	CCE-I D： CCE-3

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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	070	成員	密或簽章 (自動)	<p>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</p> <ul style="list-style-type: none"> ▪ 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 ▪ 如果已啟用這項原則，那麼將不會建立安全通道，除非已交涉所有安全通道傳輸的簽章或加密 ▪ 如果停用了這項原則，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： <ul style="list-style-type: none"> ➤ 網域成員：安全通道資料加以數位加密(可能的話) 	選項\網域成員：安全通道資料加以數位加密或簽章(自動)		6142-8

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
					<ul style="list-style-type: none"> ➤ 網域成員：安全通道資料加以數位簽章(自動) ▪ 注意： <ul style="list-style-type: none"> ➤ 如果啟用了此原則，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 ➤ 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 			
71	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0071	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)	<ul style="list-style-type: none"> ▪ 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 	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	已啟用	CCE-ID： CCE-37222-7

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
					<p>LSA SID/名稱查詢的操作</p> <ul style="list-style-type: none"> ▪ 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，如此能確保它不會在傳送時遭到竄改 ▪ 注意： <ul style="list-style-type: none"> ➢ 如果啟用了原則「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 	(自動)		
72	Windows	TWG	安全	網域成	<ul style="list-style-type: none"> ▪ 這項原則設定決定加密的安全通道資料是否 	電腦設定	已啟用	CCE-I

項次	GPO	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 2012 R2 Computer Settings	CB-01 -006-0 072	性選 項\ 網域 成員	員：要求增 強式 (Windows 2000 或更 新)工作階 段金鑰	<p>需要 128 位元的金鑰長度</p> <ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➢ 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 	\\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) 工作階 段金鑰		D： CCE-3 7614-5

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
					<ul style="list-style-type: none"> ▪ 如果停用這項設定，則會與網域控制站交涉金鑰長度 ▪ 注意： <ul style="list-style-type: none"> ➤ 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 			
73	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-073	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)	<ul style="list-style-type: none"> ▪ 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、 	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	已啟用	CCE-ID： CCE-37130-2

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
					<p>LSA SID/名稱查詢之類的操作</p> <ul style="list-style-type: none"> ▪ 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加密 ▪ 如果已啟用，則網域成員將要求所有安全通道傳輸的加密。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 ▪ 注意：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 	(可能的話)		

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
					的網域控制站建立安全通道			
74	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 074	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	<ul style="list-style-type: none"> ▪ 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到匿名使用者。若設定此選項，匿名使用者只能存取他們已明確取得權限的資源 ▪ 若啟用此原則，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-I D： CCE-3 6148-5
75	Windows	TWG	安全	網路存	<ul style="list-style-type: none"> ▪ 這項原則設定決定如何驗證使用本機帳戶的 	電腦設定	傳統-本機	CCE-I

項次	GPO	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 2012 R2 Computer Settings	CB-01 -006-0 075	性選 項\ 網路 存取	取：共用和 安全性模 式用於本 機帳戶	<p>網路登入</p> <ul style="list-style-type: none"> ▪ 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 	\\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	使用者以 自身身分 驗證	D： CCE-3 7623-6

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
					則任何人都可使用那些使用者帳戶存取共用系統資源			
76	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 076	安全 性選 項\ 網路 存取	網路存 取：不允許 SAM 帳戶 的匿名列 舉	<ul style="list-style-type: none"> ▪ 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，如下： <ul style="list-style-type: none"> ➤ 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 Everyone 取代之為 Authenticated Users ➤ 已停用：沒有其他限制。視預設權限而定 	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-I D： CCE-3 6316-8
77	Windows Server	TWG CB-01	安全 性選	網路存 取：限制匿	<ul style="list-style-type: none"> ▪ 這項原則設定決定是否限制匿名存取具名管道和共用 	電腦設定 \Windows 設定\ 	已啟用	CCE-I D：

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 Computer Settings	-006-0077	項\ 網路存取	名存取具名管道和共用	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➤ 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 	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		CCE-36021-4
78	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0078	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	<ul style="list-style-type: none"> ▪ 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，請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及子路徑	System\Cu rrentContr olSet\Cont rol\Print\Pr inters System\Cu rrentContr olSet\Servi ces\Eventl og Software\ Microsoft\	CCE-ID： CCE-36347-3

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
							OLAP Server Software\ Microsoft\ Windows NT\Curren tVersion\ Print Software\ Microsoft\ Windows NT\Curren tVersion\ Windows System\Cu rrentContr olSet\ Control\ Content Index	

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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\Terminal Server\System\CurrentControlSet\Control\Terminal Server\UserConfig\System\CurrentControlSet\Control\Terminal Server\DefaultUserCo	

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
							nfiguration Software\ Microsoft\ Windows NT\Curren tVersion\ Perflib System\ CurrentContr olSet\ Services\ SysmonLog	
79	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 079	安全 性選 項\ 網路 存取	網路存 取：允許匿 名 SID/名 稱轉譯	<ul style="list-style-type: none"> ▪ 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(SID)屬性 ▪ 如果啟用此原則，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原則的電腦，且能使用該 SID 來取得系統管理員的名稱。 	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：允許匿名	已停用	CCE-I D： CCE-3 6065-1

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
					<p>此設定會影響 SID 轉譯為名稱以及名稱轉譯為 SID</p> <ul style="list-style-type: none"> ▪ 如果已停用此原則設定，匿名使用者將無法為其他使用者要求 SID 屬性 	SID/名稱轉譯		
80	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 080	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-I D： CCE-3 8095-6
81	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 081	安全 性選 項\ 網路 存取	網路存 取：可以匿 名存取的 具名管道	這項原則設定決定哪個通訊工作階段(管道)將 擁有允許匿名存取的屬性與權限	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	無	CCE-I D： CCE-3 8258-0

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
						取的具名管道		
82	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 082	安全 性選 項\ 網路 存取	網路存 取：可遠端 存取的登 錄路徑	<ul style="list-style-type: none"> ▪ 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) ▪ 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\Cu rrentContr olSet\Cont rol\Product Options System\Cu rrentContr olSet\Cont rol\Server Applicatio ns Software\ Microsoft\ Windows NT\Curren tVersion	CCE-I D： CCE-3 7194-8
83	Windows	TWG	安全	網路存	<ul style="list-style-type: none"> ▪ 這項原則設定決定認證管理員取得網域驗證 	電腦設定	已停用	CCE-I

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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 2012 R2 Computer Settings	CB-01 -006-0 083	性選 項\ 網路 存取	取：不允許 存放網路 驗證的密 碼與認證	<p>時，是否儲存密碼與認證，以供稍後使用</p> <ul style="list-style-type: none"> ▪ 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 ▪ 如果停用或未設定此原則設定，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 	\\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		D： CCE-3 8119-4
84	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 084	安全 性選 項\ 網路 存取	網路存 取：不允 許 SAM 帳戶 和共用 的匿名 列舉	<ul style="list-style-type: none"> ▪ 這項原則設定決定是否允許 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，請啟用此原則 	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 帳戶和 共用的 匿名列 舉	已啟用	CCE-I D： CCE-3 6077-6
85	Windows	TWG	安全	網路安全	<ul style="list-style-type: none"> ▪ 這項原則設定決定在下次密碼變更時，是否 	電腦設定	已啟用	CCE-I

項次	GPO	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 2012 R2 Computer Settings	CB-01 -006-0 085	性選 項\ 網路 安全 性	性：下次密碼變更時不儲存 LAN Manager 雜湊數值	要儲存新密碼的 LAN Manager 雜湊數值。和加密編譯較強的 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，密碼可能會被破解	\\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		D： CCE-3 6326-7
86	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 086	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	<ul style="list-style-type: none"> ▪ 這項原則設定允許使用交涉的 Local System 服務在還原使用 NTLM 驗證時，使用電腦身分識別 ▪ 如果啟用這項原則設定，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 ▪ 如果停用這項原則設定，則以 Local System 執行且使用交涉的服務在還原為 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-I D： CCE-3 8341-4

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
87	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 087	安全 性選 項\ 網路 安全 性	網路安全 性：LAN Manager 驗證等級	<p>▪ 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，如下：</p> <p>➤ 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</p> <p>➤ 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</p> <p>➤ 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</p>	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 驗證等 級	只傳送 NTLMv2 回應\ 拒絕 LM 和 NTLM	CCE-I D： CCE-3 6173-3

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
					<p>受 LM、NTLM 及 NTLMv2 驗證</p> <ul style="list-style-type: none"> ➤ 只傳送 NTLMv2 回應：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) 			
88	Windows Server 2012 R2	TWG CB-01 -006-0	安全 性選 項\	網路安全 性：允許對 此電腦的	<ul style="list-style-type: none"> ▪ 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 	電腦設定 \Windows 設定\ 安全性設定\本	已停用	CCE-I D： CCE-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
	Computer Settings	088	網路安全性	PKU2U 驗證要求使用線上身分識別	<ul style="list-style-type: none"> 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別來向已加入網域的電腦驗證 	機原則\安全性選項\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		8047-7
89	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0089	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	<p>這項原則設定允許伺服器要求 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：</p> <ul style="list-style-type: none"> 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-37835-6
90	Windows Server	TWG CB-01	安全性選項	網路安全性：允許	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\	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
	2012 R2 Computer Settings	-006-0 090	項\ 網路 安全 性	LocalSystem NULL 工作階段 回復		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		CCE-3 7035-3
91	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 091	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 段安全性	這項原則設定允許用戶端要求 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： <ul style="list-style-type: none"> ➤ 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)用戶端 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-I D： CCE-3 7553-5
92	Windows	TWG	安全	網路安全	▪ 這項原則提供使用者設定允許 Kerberos 使用	電腦設定	AES128_	CCE-I

項次	GPO	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 2012 R2 Computer Settings	CB-01 -006-0 092	性選 項\ 網路 安全 性	性：設定 Kerberos 允許的加 密類型	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。允許多個選取項目	\\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	HMAC_S HA1, AES256_ HMAC_S HA1, 未 來的加密 類型	D： CCE-3 7755-6
93	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 093	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：這和交涉簽章相同。不過，若 LDAP 伺服器的中繼 saslBindInProgress 回	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 求	交涉簽章	CCE-I D： CCE-3 6858-9

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
					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			
94	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 095	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	<ul style="list-style-type: none"> ▪ 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有項目，但已啟用此安全性選項，則會出現下列停止錯誤： <ul style="list-style-type: none"> ➤ 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 	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-3 5907-5

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
					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			
95	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 096	安全 性選 項\ 稽核	稽核：稽核 通用系統 物件的存 取	<ul style="list-style-type: none"> ▪ 這項原則設定決定是否稽核通用系統物件的存取 ▪ 如果啟用此原則，會導致系統物件(如 Mutex(互斥)、事件、信號和 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 	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-I D： CCE-3 6319-2
96	Windows Server 2012 R2 Computer	TWG CB-01 -006-0 097	安全 性選 項\ 稽核	稽核：稽核 備份與還 原權限的 使用	<ul style="list-style-type: none"> ▪ 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 	電腦設定 \ Windows 設定\ 安全性設定\ 本機原則\ 安全性	已停用	CCE-I D： CCE-3 6262-4

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
	Settings				還原的每個檔案產生一個稽核事件 <ul style="list-style-type: none"> ▪ 如果停用此原則，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 	選項\稽核：稽核備份與還原權限的使用		
97	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0098	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) 可以覆寫稽核原則類別設定	<ul style="list-style-type: none"> ▪ 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 	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	CCE-ID： CCE-37850-5

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
					登錄機碼			
98	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 099	安全 性選 項\ 關機	關機：允許 不登入就 將系統關 機	<ul style="list-style-type: none"> ▪ 這項原則設定決定是否無需登入 Windows 便能夠將電腦關機 ▪ 啟用此原則時，Windows 登入畫面上可以使用「關機」命令 ▪ 停用此原則時，Windows 登入畫面上不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 	電腦設定 \ Windows 設定\ 安全性設定\ 本機原則\ 安全性選 項\ 關機：允 許不登 入就將 系統關 機	已停用	CCE-I D： CCE-3 6788-8
99	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 100	安全 性選 項\ 關機	關機：清除 虛擬記憶 體分頁檔	<ul style="list-style-type: none"> ▪ 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 	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-I D： CCE-3 8335-6

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
					<p>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</p> <ul style="list-style-type: none"> 當啟用此原則時，在正常關機時會清除系統分頁檔。若啟用此安全性選項，當停用休眠時，也會清除休眠檔案(hiberfil.sys) 			
100	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0101	使用者權限指派	鎖定記憶體中的分頁	<ul style="list-style-type: none"> 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-36495-0
101	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0102	使用者權限指派	增加處理程序工作組	<ul style="list-style-type: none"> 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 	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-38026-1

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
					<p>影響處理程序的虛擬記憶體分頁行為</p> <ul style="list-style-type: none"> 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 			
102	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 103	使用者權 限指 派	關閉系統	<ul style="list-style-type: none"> 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	Administra tors	CCE-I D： CCE-3 8328-1
103	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 104	使用者權 限指 派	調整處理 程序的記 憶體配額	<ul style="list-style-type: none"> 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	Administra tors, Local Service, Network Service	CCE-I D： CCE-3 7071-8
104	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呼叫	電腦設定	Local	CCE-I

項次	GPO	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 2012 R2 Computer Settings	CB-01 -006-0 105	者權 限指 派	程序等級 權杖	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	D : CCE-3 7430-6
105	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 106	使用 者權 限指 派	取得檔案 或其他物 件的擁有 權	<ul style="list-style-type: none"> ▪ 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、處理程序和執行緒 ▪ 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	Administra tors	CCE-I D : CCE-3 8325-7
106	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 107	使用 者權 限指 派	拒絕透過 遠端桌面 服務登入	這項原則設定決定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\\本 機原則\\使用者 權限指派\\拒絕	Guests,本 機帳戶	CCE-I D : CCE-3 6867-0

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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					透過遠端桌面服務登入		
107	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 108	使用者權 限指 派	拒絕從網 路存取這 台電腦	這項原則設定決定禁止哪些使用者從網路存取電腦。此原則設定會取代「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 Administra tors 群組 的成員	CCE-I D: CCE-3 7954-5
108	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 109	使用者權 限指 派	載入及解 除載入裝 置驅動程 式	<ul style="list-style-type: none"> ▪ 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 	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 及解除載入裝置 驅動程式	Administra tors	CCE-I D: CCE-3 6318-4

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
109	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 110	使用者權 限指 派	拒絕以服 務方式登 入	<ul style="list-style-type: none"> ▪ 這項原則設定決定禁止哪些服務帳戶以服務方式登錄處理程序。此原則設定會取代「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-I D： CCE-3 6877-9
110	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 111	使用者權 限指 派	讓電腦及 使用者帳 戶受信 賴，以進行 委派	<ul style="list-style-type: none"> ▪ 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 ▪ 此使用者權限會定義在「預設網域控制站群組原則」物件(GPO)及工作站、伺服器的本機 	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，以進行 委派	No One	CCE-I D： CCE-3 6860-5

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
					<p>安全性原則中</p> <ul style="list-style-type: none"> 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 			
111	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 112	使用 者權 限指 派	備份檔案 及目錄	<ul style="list-style-type: none"> 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： <ul style="list-style-type: none"> ➤ 周遊資料夾/執行檔案 ➤ 列出資料夾/讀取資料 ➤ 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 	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	Administra tors	CCE-I D： CCE-3 5912-5

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
					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			
112	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 113	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-I D： CCE-3 6054-5
113	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 114	使用 者權 限指 派	當成作業 系統的一 部分	<ul style="list-style-type: none"> ▪ 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 	電腦設定 \\Windows 設定\ 安全性設定\\本 機原則\\使用者 權限指派\\當成 作業系統的一部 分	No One	CCE-I D： CCE-3 6876-1

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
					<ul style="list-style-type: none"> 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 			
114	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 115	使用 者權 限指 派	變更系統 時間	<ul style="list-style-type: none"> 此使用者權限決定哪些使用者和群組能夠變更電腦內部時鐘的時間和日期。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 此使用者權限定義在「預設網域控制站群組原則」物件(GPO)及工作站、伺服器的本機安全性原則中 	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, Administra tors	CCE-I D： CCE-3 7452-0
115	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 116	使用 者權 限指 派	允許透過 遠端桌面 服務登入	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\ 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	Administra tors	CCE-I D： CCE-3 7072-6

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
						務登入		
116	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 117	使用 者權 限指 派	修改韌體 環境值	<ul style="list-style-type: none"> ▪ 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 ▪ 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」 	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	Administra tors	CCE-I D： CCE-3 8113-7

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
					的「進階」索引標籤)的使用者			
117	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 118	使用 者權 限指 派	建立通用 物件	<ul style="list-style-type: none"> 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	Administra tors, SERVICE, LOCAL SERVICE, NETWOR K SERVICE	CCE-I D : CCE-3 7453-8
118	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 119	使用 者權 限指 派	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\ 安全性設定\ 本機原則\ 使用者 權限指派\ 監視 系統效能	Administra tors,NT SERVICE\ WdiServic eHost	CCE-I D : CCE-3 6052-9
119	Windows	TWG	使用	產生安全	<ul style="list-style-type: none"> 這項原則設定決定處理程序可使用哪些帳戶 	電腦設定	Local	CCE-I

項次	GPO	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 2012 R2 Computer Settings	CB-01 -006-0 120	者權 限指 派	性稽核	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 <ul style="list-style-type: none"> ▪ 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 	\\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	Service, Network Service	D： CCE-3 7639-2
120	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 121	使用 者權 限指 派	以服務方 式登入	<ul style="list-style-type: none"> ▪ 這項原則設定可以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，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 	電腦設定 \\Windows 設定\ 安全性設定\本 機原則\使用者 權限指派\以服 務方式登入	No One	CCE-I D： CCE-3 6165-9
121	Windows Server 2012 R2 Computer	TWG CB-01 -006-0 122	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	No One	CCE-I D： CCE-3 7056-9

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
	Settings					權限指派\存取 認證管理員做為 信任的呼叫者		
122	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 123	使用 者權 限指 派	變更時區	<ul style="list-style-type: none"> 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, Administra tors	CCE-I D : CCE-3 7700-2
123	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 124	使用 者權 限指 派	執行磁碟 區維護工 作	<ul style="list-style-type: none"> 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和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，使用者能夠讀取和修改取得的資料 	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	Administra tors	CCE-I D : CCE-3 6143-6
124	Windows Server	TWG CB-01	使用 者權	建立權杖 物件	<ul style="list-style-type: none"> 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 	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	No One	CCE-I D :

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 Computer Settings	-006-0 125	限指 派		<p>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</p> <ul style="list-style-type: none"> 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 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 	安全性設定\本機原則\使用者權限指派\建立權杖物件		CCE-3 6861-3
125	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 126	使用 者權 限指 派	強制從遠端系統進行關閉	<ul style="list-style-type: none"> 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	Administra tors	CCE-I D： CCE-3 7877-8
126	Windows Server	TWG CB-01	使用 者權	建立符號連結	<ul style="list-style-type: none"> 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 	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	Administra tors	CCE-I D：

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 Computer Settings	-006-0 127	限指 派		<ul style="list-style-type: none"> ▪ 注意： <ul style="list-style-type: none"> ➤ 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 ➤ 此設定可搭配 symlink filesystem 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 	安全性設定\本機原則\使用者權限指派\建立符號連結		CCE-3 5823-4
127	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 128	使用 者權 限指 派	從銜接站 移除電腦	<ul style="list-style-type: none"> ▪ 這項原則設定決定使用者是否無需登入便可從銜接站卸除可攜式電腦 ▪ 如果啟用此權限，使用者必須先登入，才能從銜接站移除可攜式電腦 ▪ 如果停用此權限，使用者無需登入便可從銜接站移除可攜式電腦 	電腦設定 \Windows 設定\ 安全性設定\本 機原則\使用者 權限指派\從銜 接站移除電腦	Administra tors	CCE-I D： CCE-3 6064-4
128	Windows Server 2012 R2 Computer	TWG CB-01 -006-0 129	使用 者權 限指 派	略過周遊 檢查	<ul style="list-style-type: none"> ▪ 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	Administra tors, Authentica ted Users,	CCE-I D： CCE-3 6284-8

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
	Settings					權限指派\略過周遊檢查	Local Service, Network Service	
129	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0130	使用者權限指派	建立分頁檔	<ul style="list-style-type: none"> 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-35821-8
130	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0131	使用者權限指派	增加排程優先順序	<ul style="list-style-type: none"> 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-38326-5
131	Windows	TWG	使用	管理稽核	<ul style="list-style-type: none"> 此安全設定決定哪些使用者能夠指定個別資 	電腦設定	Administrators	CCE-I

項次	GPO	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 2012 R2 Computer Settings	CB-01 -006-0 132	者權 限指 派	及安全性 記錄檔	<p>源(例如檔案、Active Directory 物件及登錄機碼)的物件存取稽核選項</p> <ul style="list-style-type: none"> ▪ 這項原則設定不允許使用者啟用檔案和物件存取稽核。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和清除安全性記錄檔 	<p>\Windows 設定\ 安全性設定\本 機原則\使用者 權限指派\管理 稽核及安全性記 錄檔</p>	tors	D : CCE-3 5906-7
132	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 133	使用 者權 限指 派	拒絕以批 次工作登 入	<ul style="list-style-type: none"> ▪ 這項原則設定決定會禁止哪些帳戶以批次工作登入 ▪ 此原則設定會取代「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 	<p>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</p>	Guests	CCE-I D : CCE-3 6923-1
133	Windows Server	TWG CB-01	使用 者權	拒絕本機 登入	<ul style="list-style-type: none"> ▪ 這項原則設定決定會禁止哪些使用者登入電腦。此原則設定會取代「允許本機登入」原 	<p>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</p>	Guests	CCE-I D :

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 Computer Settings	-006-0 134	限指 派		則設定，如果帳戶同時受限於這兩種原則 <ul style="list-style-type: none"> 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 	安全性設定\本 機原則\使用者 權限指派\拒絕 本機登入		CCE-3 7146-8
134	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 135	使用 者權 限指 派	偵錯程式	<ul style="list-style-type: none"> 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	Administra tors	CCE-I D： CCE-3 7075-9
135	Windows Server 2012 R2 Computer	TWG CB-01 -006-0 136	使用 者權 限指 派	建立永久 共用物件	<ul style="list-style-type: none"> 此使用者權限決定哪些帳戶處理程序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 	電腦設定 \Windows 設定\ 安全性設定\本 機原則\使用者	No One	CCE-I D： CCE-3 6532-0

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
	Settings				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	權限指派\建立永久共用物件		
136	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 137	使用者權 限指 派	還原檔案 及目錄	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➤ 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 	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	Administra tors	CCE-I D： CCE-3 7613-7

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
137	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 138	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	Administra tors	CCE-I D : CCE-3 7131-0
138	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 139	使用者權 限指 派	以批次工 作登入	<ul style="list-style-type: none"> ▪ 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	Administra tors	CCE-I D : CCE-3 8080-8
139	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 140	使用者權 限指 派	在驗證後 模擬用戶 端	<ul style="list-style-type: none"> ▪ 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 	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	Administra tors, SERVICE, Local Service, Network	CCE-I D : CCE-3 7106-2

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
					<p>權限提升到管理或系統層級</p> <ul style="list-style-type: none"> 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 	證後模擬用戶端	Service	
140	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 141	使用 者權 限指 派	從網路存取這台電腦	<ul style="list-style-type: none"> 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 路存取這台電腦	Administra tors, Authentica ted Users	CCE-I D : CCE-3 5818-4
141	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 142	使用 者權 限指 派	允許本機 登入	<ul style="list-style-type: none"> 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	Administra tors	CCE-I D : CCE-3 7659-0
142	Windows	TWG	系統	永遠以較	<ul style="list-style-type: none"> 這項原則設定會指定 Windows Installer 在安 	電腦設定\ 系統	已停用	CCE-I

項次	GPO	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 2012 R2 Computer Settings	CB-01 -006-0 143	管理 範本 /Win dows Instal ler	高的特殊 權限安裝	<p>裝任何程式到系統時應使用較高的權限</p> <ul style="list-style-type: none"> ▪ 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 	管理範本 \\Windows 元件 \\Windows Installer\\永遠以 較高的特殊權限 安裝		D： CCE-3 6919-9

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
143	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 144	系統 管理 範本 /自 動播 放原 則	關閉自動 播放	<ul style="list-style-type: none"> ▪ 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，程式的安裝檔案和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 	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-I D： CCE-3 6875-3

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
144	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0145	系統管理範本/遠端桌面服務	設定用戶端連線加密層級	<ul style="list-style-type: none"> ▪ 這項原則設定指定在遠端桌面通訊協定 (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 ▪ 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： <ul style="list-style-type: none"> ➤ 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 	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\設定用戶端連線加密層級	已啟用：高等級	CCE-ID：CCE-36627-8

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
					<p>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</p> <p>➤ 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</p>			
145	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0146	事件記錄服務/安全性	指定記錄檔大小上限(KB)	<ul style="list-style-type: none"> ▪ 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 2 TB(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-37695-4
146	Windows Server	TWG CB-01	事件記錄	控制記錄檔達到其	<ul style="list-style-type: none"> ▪ 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 	電腦設定\系統管理範本	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
	2012 R2 Computer Settings	-006-0 147	服務 /安 全性	大小上限 時的事件 記錄檔行 為	失 <ul style="list-style-type: none"> ▪ 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 	\\Windows 元件\ 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 錄檔行為		CCE-3 7145-0
147	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 148	事件 記錄 服務 /系 統	指定記錄 檔大小上 限(KB)	<ul style="list-style-type: none"> ▪ 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 2 TB(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-I D： CCE-3 6092-5
148	Windows	TWG	事件	控制記錄	<ul style="list-style-type: none"> ▪ 如果啟用這項原則設定，且記錄檔達到其大 	電腦設定\系統	已停用	CCE-I

項次	GPO	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 2012 R2 Computer Settings	CB-01 -006-0 149	記錄 服務 /系 統	檔達到其 大小上限 時的事件 記錄檔行 為	<p>小上限時，新事件將不會寫入記錄檔且會遺失</p> <ul style="list-style-type: none"> ▪ 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		D： CCE-3 6160-0
149	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 150	事件 記錄 服務 /應 用程 式	指定記錄 檔大小上 限(KB)	<ul style="list-style-type: none"> ▪ 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 2 TB(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\ 應用程式\指定 記錄檔大小上限 (KB)	已啟用： 32,768KB 以上	CCE-I D： CCE-3 7948-7

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
150	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 151	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	<ul style="list-style-type: none"> ▪ 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-I D： CCE-3 7775-4
151	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 152	Wind ows 元件 \One Drive	防止使用 OneDrive 儲存檔案	<ul style="list-style-type: none"> ▪ 這項原則設定可防止應用程式和功能使用 OneDrive 上的檔案 ▪ 如果啟用這項原則設定： <ul style="list-style-type: none"> ➢ 使用者不能從 OneDrive 應用程式和檔案選擇器存取 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 	電腦設定\系統 管理範本 \Windows 元件 \OneDrive\防止 使用 OneDrive 儲 存檔案	已啟用	CCE-I D： CCE-3 6939-7

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
					<ul style="list-style-type: none"> ➢ 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和影片 ▪ 如果停用或未設定這項原則設定，應用程式和功能就可以使用 OneDrive 檔案儲存空間 			
152	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0153	系統管理範本 / Windows 遠端殼層	允許遠端殼層存取	<ul style="list-style-type: none"> ▪ 這項原則設定可設定遠端殼層的存取權 ▪ 如果啟用這項原則設定，伺服器會允許新的遠端殼層連線 ▪ 如果停用或未設定這項原則設定，則伺服器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-36499-2
153	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0154	系統管理範本 / Windows	系統起始的重新啟動之後自動登入最後一個互	<ul style="list-style-type: none"> ▪ 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 	電腦設定\系統管理範本 \Windows 元件 \Windows 登入選項\系統起始	已停用	CCE-ID: CCE-36977-7

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
			登入 選項	動式使用者	<p>域和加密的密碼)，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</p> <ul style="list-style-type: none"> ▪ 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 	的重新啟動之後自動登入最後一個互動式使用者		
154	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0155	系統管理範本/市集	關閉市集應用程式	<ul style="list-style-type: none"> ▪ 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-38363-8
155	Windows	TWG	系統	關閉自動	<ul style="list-style-type: none"> ▪ 這項原則設定決定啟用或停用自動下載和安 	電腦設定\系統	已啟用	CCE-I

項次	GPO	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 2012 R2 Computer Settings	CB-01 -006-0 156	管理 範本 /市 集	下載和安 裝更新	<p>裝應用程式更新</p> <ul style="list-style-type: none"> ▪ 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 	管理範本 \\Windows 元件\ 市集\關閉自動 下載和安裝更新		D： CCE-3 8360-4
156	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 157	系統 管理 範本 /市 集	關閉更新 至最新版 Windows 的服務	<ul style="list-style-type: none"> ▪ 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-I D： CCE-3 8362-0
157	Windows Server 2012 R2	TWG CB-01 -006-0	系統 管理 範本	不要顯示 網路選取 UI	<ul style="list-style-type: none"> ▪ 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 	電腦設定\系統 管理範本\系統\ 登入\不要顯示	已啟用	CCE-I D： CCE-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
	Computer Settings	158	/登 入		後才能變更電腦的網路連線狀態 <ul style="list-style-type: none"> ▪ 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 	網路選取 UI		8353-9
158	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 159	系統 管理 範本 /稽 核建 立處 理程 序	在建立處理程序事件中包含命令列	<ul style="list-style-type: none"> ▪ 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，做為套用此原則設定之工作站和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 	電腦設定\系統 管理範本\系統\ 稽核建立處理程 序\在建立處理 程序事件中包含 命令列	已停用	CCE-I D： CCE-3 6925-6

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
					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			
159	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 160	系統 管理 範本 /搜 尋	允許加密 檔案索引	<ul style="list-style-type: none"> ▪ 這項原則設定決定是否允許對加密項目編製索引 ▪ 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 	電腦設定\系統 管理範本 \Windows 元件\ 搜尋\允許加密 檔案索引	已停用	CCE-I D： CCE-3 8277-0

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
					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			
160	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 161	系統 管理 範本 /搜 尋	設定「搜尋」中可以分享的資訊	<ul style="list-style-type: none"> ▪ 這項原則設定可以控制在「搜尋」中使用 Bing 分享哪些資訊 ▪ 如果啟用這項原則設定, 則可以指定四個設定的其中一個, 而且使用者不能變更這些設定: <ul style="list-style-type: none"> ➢ 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和某些 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 	電腦設定\系統管理範本 \\Windows 元件\\搜尋\設定「搜尋」中可以分享的資訊	已啟用: 匿名資訊	CCE-ID: CCE-36937-1

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
					選擇「搜尋」中要分享哪些資訊			
161	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0162	系統管理範本/應用程式執行階段	允許選用 Microsoft 帳戶	<ul style="list-style-type: none"> ▪ 這項原則設定可控制需要帳戶登入的 Windows 市集應用程式是否可以選用 Microsoft 帳戶 ▪ 這項原則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 	電腦設定\系統管理範本\Windows 元件\應用程式執行階段\允許選用 Microsoft 帳戶	已啟用	CCE-ID: CCE-38354-7
162	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0163	系統管理範本/網際網路通	關閉 Windows Messenger 客戶經驗改進計畫	<ul style="list-style-type: none"> ▪ 這項原則設定指定 Windows Messenger 是否蒐集關於 Windows Messenger 軟體和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	已啟用	CCE-ID: CCE-36628-6

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
			訊管 理		<ul style="list-style-type: none"> ▪ 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 	Messenger 客戶 經驗改進計畫		
163	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 164	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	<ul style="list-style-type: none"> ▪ 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和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 	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-I D： CCE-3 6884-5

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
					<p>者使用的是傳統搜尋，否則搜尋小幫手將會下載內容更新</p> <ul style="list-style-type: none"> 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 及選用的搜尋提供者。選擇傳統搜尋將會完全關閉搜尋小幫手的功能 			
164	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 165	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	<ul style="list-style-type: none"> 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 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 案及資料夾的 「發佈到網站」 工作	已啟用	CCE-I D： CCE-3 7090-8
165	Windows	TWG	系統	防止啟用	<ul style="list-style-type: none"> 這項原則設定決定是否停用「電腦設定」中 	電腦設定\系統	已啟用	CCE-I

項次	GPO	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 2012 R2 Computer Settings	CB-01 -006-0 166	管理 範本 /個 人化	鎖定畫面 投影片放 映	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 <ul style="list-style-type: none"> ▪ 如果啟用這項設定，使用者將無法修改「電腦設定」中投影片放映設定，也不會開始任何投影片放映 	管理範本\控制台\個人化\防止 啟用鎖定畫面投 影片放映		D： CCE-3 8348-9
166	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 167	系統 管理 範本 /個 人化	防止啟用 鎖定畫面 相機	<ul style="list-style-type: none"> ▪ 這項原則設定決定是否停用「電腦設定」中鎖定畫面相機切換開關，防止在鎖定畫面上叫用相機 ▪ 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叫用相機 	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-I D： CCE-3 8347-1
167	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 168	進階 稽核 原則 \DS 存取	稽核詳細 目錄服務 複寫	<ul style="list-style-type: none"> ▪ 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	沒有稽核	CCE-I D： CCE-3 7361-3

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
						錄服務複寫		
168	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 169	進階 稽核 原則 \ DS 存取	稽核目錄 服務複寫	<ul style="list-style-type: none"> ▪ 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-I D： CCE-3 8234-1
169	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 170	進階 稽核 原則 \ 系 統	稽核系統 完整性	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➢ 因稽核系統發生問題而無法寫入事件記錄檔的事件 ➢ 使用本機程序呼叫(LPC)連接埠的處理程 	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\ 系統	成功與失 敗	CCE-I D： CCE-3 7132-8

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
					<p>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</p> <ul style="list-style-type: none"> ➤ 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 <p>▪ 預設值：成功，失敗</p>	稽核系統完整性		
170	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 171	進階 稽核 原則 \ 系統	稽核 IPSEC 驅 動程式	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➤ 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 ➤ 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 	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-I D： CCE-3 7853-9

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
					<p>作，或需要更新驅動程式</p> <ul style="list-style-type: none"> ➤ 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 			
171	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 172	進階 稽核 原則 \ 系統	稽核安全 性系統延 伸	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➤ 載入安全性系統延伸(如驗證、通知或安全性封裝)，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 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 	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\ 稽核安全性系統 延伸	成功與失 敗	CCE-I D： CCE-3 6144-4

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
					<p>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</p> <ul style="list-style-type: none"> ▪ 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 			
172	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 173	進階 稽核 原則 \ 系統	稽核其他 系統事件	<ul style="list-style-type: none"> ▪ 這項原則設定決定是否稽核下列任一事件： <ul style="list-style-type: none"> ➢ 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-I D： CCE-3 8030-3
173	Windows	TWG	進階	稽核安全	<ul style="list-style-type: none"> ▪ 這項原則設定決定是否稽核因電腦安全性狀 	電腦設定	成功與失	CCE-I

項次	GPO	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 2012 R2 Computer Settings	CB-01 -006-0 174	稽核 原則 \系 統	性狀態變 更	<p>態變更而產生的事件，例如下列事件：</p> <ul style="list-style-type: none"> ➤ 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 登錄項目時於系統重新啟動之後記錄 <p>▪ 預設值：成功</p>	<p>\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</p>	敗	D： CCE-3 8114-5
174	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 175	進階 稽核 原則 \物 件存 取	稽核其他 物件存取 事件	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➤ 建立工作 ➤ 刪除工作 ➤ 啟用工作 ➤ 停用工作 ➤ 更新工作 	<p>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</p>	成功與失 敗	CCE-I D： CCE-3 7620-2

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
					<ul style="list-style-type: none"> ▪ 如果是 COM+物件，則會稽核下列項目： <ul style="list-style-type: none"> ➢ 新增類別目錄物件 ➢ 更新類別目錄物件 ➢ 刪除類別目錄物件 			
175	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 176	進階 稽核 原則 \物 件存 取	稽核控制 代碼操作	<ul style="list-style-type: none"> ▪ 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 	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-I D： CCE-3 7511-3

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
					未啟用登錄物件存取，則不會產生控制代碼操作安全性稽核事件			
176	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 177	進階 稽核 原則 物件存 取	稽核檔案 共用	<ul style="list-style-type: none"> ▪ 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-I D： CCE-3 7026-2
177	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 178	進階 稽核 原則 物件存 取	稽核篩選 平台連線	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➤ 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 ➤ WFP 封鎖連線 	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\\稽核篩選	沒有稽核	CCE-I D： CCE-3 8116-0

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
					<ul style="list-style-type: none"> ➢ 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 	平台連線		
178	Windows Server 2012 R2	TWG CB-01 -006-0	進階 稽核 原則	稽核憑證 服務	<ul style="list-style-type: none"> ▪ 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： 	電腦設定 \\Windows 設定\ 安全性設定\\進	沒有稽核	CCE-I D： CCE-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
	Computer Settings	179	\物件 存取		<ul style="list-style-type: none"> ➤ 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佈是針對 Active Directory 網域服務 ➤ AD CS 的安全性權限變更 ➤ 金鑰的封存 ➤ 金鑰的匯入 ➤ 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 	階稽核原則設定 \稽核原則\物件 存取\稽核憑證 服務		8037-8

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
					➤ 線上憑證狀態通訊協定(OCSP)回應程式服務的停止			
179	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 180	進階 稽核 原則 物件存 取	稽核檔案 系統	<ul style="list-style-type: none"> ▪ 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 	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-I D： CCE-3 7384-5

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 SACL			
180	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 181	進階 稽核 原則 物件存 取	稽核 SAM	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➢ 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) 	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-I D： CCE-3 8039-4

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
181	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 182	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-I D: CCE-3 7225-0
182	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 183	進階 稽核 原則 \物 件存 取	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，會使用這個子類別來記錄與其功能相關的 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\物件 存取\稽核產生 的應用程式	沒有稽核	CCE-I D: CCE-3 7857-0
183	Windows Server 2012 R2 Computer	TWG CB-01 -006-0	進階 稽核 原則 \物	稽核登錄	<ul style="list-style-type: none"> 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 	電腦設定 \Windows 設定\ 安全性設定\進 階稽核原則設定	沒有稽核	CCE-I D: CCE-3

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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	184	物件存取		<p>定時，才會產生安全性稽核事件</p> <ul style="list-style-type: none"> ▪ 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 	\\稽核原則\物件存取\稽核登錄		7193-0
184	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 185	進階 稽核 原則 \物 件存 取	稽核詳細 的檔案共 用	<ul style="list-style-type: none"> ▪ 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 	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-I D： CCE-3 6878-7

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
					<p>的詳細資訊</p> <ul style="list-style-type: none"> ▪ 如果設定此原則設定，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)。如果啟用此原則設定，則會稽核系統上所有共用檔案和資料夾的存取 			
185	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 186	進階 稽核 原則 \物件 存取	稽核核心 物件	<ul style="list-style-type: none"> ▪ 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-I D： CCE-3 7437-1
186	Windows Server	TWG CB-01	進階 稽核	稽核篩選 平台原則	<ul style="list-style-type: none"> ▪ 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： 	電腦設定 \Windows 設定\ 	沒有稽核	CCE-I D：

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 Computer Settings	-006-0 187	原則 \原 則變 更	變更	<ul style="list-style-type: none"> ➢ IPsec 服務狀態 ➢ 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 	安全性設定\進 階稽核原則設定 \稽核原則\原則 變更\稽核篩選 平台原則變更		CCE-3 6856-3
187	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 188	進階 稽核 原則 \原 則變 更	稽核驗證 原則變更	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➢ 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：電腦設定 	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 原則變更	成功	CCE-I D： CCE-3 8327-3

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
					\Windows 設定\安全性設定\帳戶原則 \Kerberos 原則 <ul style="list-style-type: none"> ▪ 將下列任何使用者權限授與使用者或群組： <ul style="list-style-type: none"> ➤ 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 ▪ 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 			

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
					<ul style="list-style-type: none"> ▪ 預設值：成功 			
188	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 189	進階 稽核 原則 \原 則變 更	稽核授權 原則變更	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➢ 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 	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-I D： CCE-3 6320-0

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
189	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 190	進階 稽核 原則 \原 則變 更	稽核「稽核 原則變更」	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➢ 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 	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-I D： CCE-3 8028-7

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
					<p>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</p> <ul style="list-style-type: none"> ▪ 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 			
190	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0191	進階稽核原則\原則變更	稽核 MPSSVC 規則層級原則變更	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➢ 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 	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 規則層級原則變更	成功與失敗	CCE-ID：CCE-37852-1

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
					<p>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</p> <ul style="list-style-type: none"> ▪ 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 			
191	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 192	進階 稽核 原則 \原 則變 更	稽核其他 原則變更 事件	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➢ 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 ▪ 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-I D： CCE-3 8029-5
192	Windows	TWG	進階	稽核機密	<ul style="list-style-type: none"> ▪ 這項原則設定決定是否稽核使用機密特殊權 	電腦設定	成功與失	CCE-I

項次	GPO	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 2012 R2 Computer Settings	CB-01 -006-0 193	稽核 原則 \特 殊權 限使 用	特殊權限 使用	<p>限(使用者權限)時產生的事件，例如：</p> <ul style="list-style-type: none"> ➤ 呼叫特許服務 ➤ 呼叫下列其中一種權限： <ul style="list-style-type: none"> (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 	\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 機密特殊權限使 用	敗	D： CCE-3 6267-3

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
					<p>(13)取得檔案或其他物件的擁有權</p> <ul style="list-style-type: none"> ▪ 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 			
193	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0194	進階稽核原則\特殊權限使用	稽核非機密特殊權限使用	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➢ 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 ➢ 略過周遊檢查 	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-38331-5

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
					<ul style="list-style-type: none"> ➤ 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 ➤ 以批次工作登入 ➤ 以服務方式登入 			

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
					<ul style="list-style-type: none"> ➤ 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 <ul style="list-style-type: none"> ▪ 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 			
194	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 195	進階 稽核 原則 \特 殊權	稽核其他 特殊權限 使用事件	<ul style="list-style-type: none"> ▪ 這項原則設定決定是否稽核其他特殊權限(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 	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	沒有稽核	CCE-I D： CCE-3 6536-1

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
			限使用		功呼叫，而失敗稽核則會記錄失敗呼叫 <ul style="list-style-type: none"> ▪ 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 	權限使用\稽核 其他特殊權使用事件		
195	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 196	進階 稽核 原則 \帳 戶登 入	稽核 Kerberos 驗證服務	<ul style="list-style-type: none"> ▪ 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	CCE-I D： CCE-3 8140-0
196	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 197	進階 稽核 原則 \帳 戶登	稽核認證 驗證	<ul style="list-style-type: none"> ▪ 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 	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	成功與失 敗	CCE-I D： CCE-3 7741-6

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
			入		<ul style="list-style-type: none"> ▪ 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 	登入\稽核認證 驗證		
197	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 198	進階 稽核 原則 \帳 戶登 入	稽核 Kerberos 服務票證 操作	<ul style="list-style-type: none"> ▪ 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 ▪ 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 	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 服務票 證操作	成功與失 敗	CCE-I D： CCE-3 7975-0
198	Windows Server 2012 R2	TWG CB-01 -006-0	進階 稽核 原則	稽核其他 帳戶登入 事件	<ul style="list-style-type: none"> ▪ 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 	電腦設定 \Windows 設定\ 安全性設定\進	沒有稽核	CCE-I D： CCE-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
	Computer Settings	199	\帳 戶登 入		<ul style="list-style-type: none"> 預設值：沒有稽核 	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		7888-5
199	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 200	進階 稽核 原則 \帳 戶管 理	稽核應用 程式群組 管理	<ul style="list-style-type: none"> 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： <ul style="list-style-type: none"> 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 	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\ 稽核應用 程式群組管理	沒有稽核	CCE-I D： CCE-3 8329-9
200	Windows Server 2012 R2	TWG CB-01 -006-0	進階 稽核 原則	稽核電腦 帳戶管理	<ul style="list-style-type: none"> 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 	電腦設定 \Windows 設定\ 安全性設定\ 進	成功	CCE-I D： CCE-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
	Computer Settings	201	\帳戶管理		<ul style="list-style-type: none"> ▪ 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 	階稽核原則設定 \稽核原則\帳戶管理\稽核電腦帳戶管理		8004-8
201	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 202	進階稽核原則 \帳戶管理	稽核其他帳戶管理事件	<ul style="list-style-type: none"> ▪ 這項原則設定決定是否稽核因這個類別未涵蓋的其他使用者帳戶變更而產生的事件，例如： <ul style="list-style-type: none"> ➤ 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： 	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\稽核其他 帳戶管理事件	成功與失敗	CCE-ID： CCE-3 7855-4

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
					<p>(1)電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則</p> <p>(2)電腦設定\Windows 設定\安全性設定\帳戶原則\帳戶鎖定原則</p> <ul style="list-style-type: none"> ▪ 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，則不會發生該事件 ▪ 預設值：沒有稽核 			
202	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 203	進階 稽核 原則 \帳 戶管 理	稽核安全 性群組管 理	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➢ 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 	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-I D： CCE-3 8034-5

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
					<ul style="list-style-type: none"> ▪ 預設值：成功 			
203	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 204	進階 稽核 原則 \帳 戶管 理	稽核發佈 群組管理	<ul style="list-style-type: none"> ▪ 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： <ul style="list-style-type: none"> ➢ 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	CCE-I D： CCE-3 6265-7
204	Windows Server	TWG CB-01	進階 稽核	稽核使用 者帳戶管	<ul style="list-style-type: none"> ▪ 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： 	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	成功與失 敗	CCE-I D：

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 Computer Settings	-006-0 205	原則 帳戶管理	理	<ul style="list-style-type: none"> ➤ 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 ➤ 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 	安全性設定\進階稽核原則設定\稽核原則\帳戶管理\稽核使用者帳戶管理		CCE-3 7856-2
205	Windows Server 2012 R2	TWG CB-01 -006-0	進階 稽核 原則	稽核帳戶 鎖定	<ul style="list-style-type: none"> ▪ 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 ▪ 若設定此原則設定，則會在帳戶因鎖定而無 	電腦設定 \Windows 設定\ 安全性設定\進	失敗	CCE-I D： CCE-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
	Computer Settings	206	\登入/ 登出		<p>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</p> <ul style="list-style-type: none"> ▪ 預設值：成功 	階稽核原則設定 \稽核原則\ 登入/ 登出\ 稽核帳戶 鎖定		7133-6
206	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0207	進階稽核原則 \登入/ 登出	稽核 IPsec 延伸模式	<ul style="list-style-type: none"> ▪ 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-36060-2
207	Windows Server 2012 R2 Computer	TWG CB-01-006-0208	進階稽核原則 \登	稽核網路原則伺服器	<ul style="list-style-type: none"> ▪ 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。這些要求可以是授與、拒絕、捨棄、隔離、鎖定及解除鎖定 	電腦設定 \Windows 設定\ 安全性設定\ 進階稽核原則設定	成功	CCE-ID： CCE-38330-7

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
	Settings		入/ 登出		<ul style="list-style-type: none"> ▪ 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 	\\稽核原則\登入/ 登出\稽核網路 原則伺服器		
208	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 209	進階 稽核 原則 \登 入/ 登出	稽核 IPsec 主要模式	<ul style="list-style-type: none"> ▪ 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 ▪ 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 	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-I D： CCE-3 7436-3
209	Windows	TWG	進階	稽核其他	<ul style="list-style-type: none"> ▪ 這項原則設定決定是否稽核「登入/登出」原 	電腦設定	沒有稽核	CCE-I

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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 2012 R2 Computer Settings	CB-01 -006-0 210	稽核 原則 \登 入/ 登出	登入/登出 事件	<p>則設定未涵蓋的其他登入/登出相關事件，例如：</p> <ul style="list-style-type: none"> ➤ 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帳戶 ➤ 將有線 802.1x 網路存取權限授與使用者或電腦帳戶 <p>▪ 預設值：沒有稽核</p>	\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		D： CCE-3 6322-6

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
210	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 211	進階 稽核 原則 \登 入/ 登出	稽核登出	<ul style="list-style-type: none"> ▪ 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-I D： CCE-3 8237-4
211	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 212	進階 稽核 原則 \登 入/ 登出	稽核登入	<ul style="list-style-type: none"> ▪ 這項原則設定決定是否稽核因電腦上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 	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\稽核登入	成功與失 敗	CCE-I D： CCE-3 8036-0

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
					<p>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：</p> <ul style="list-style-type: none"> ➤ 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) <p>▪ 伺服器版本的預設值：成功，失敗</p>			
212	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 213	進階 稽核 原則 \ 登入/ 登出	稽核 IPsec 快速模式	<ul style="list-style-type: none"> ▪ 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 	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 快速模式	沒有稽核	CCE-I D： CCE-3 7619-4

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
					快速模式交涉期間產生稽核事件 <ul style="list-style-type: none"> 預設值：沒有稽核 			
213	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 214	進階 稽核 原則 \ 登入/ 登出	稽核特殊 登入	<ul style="list-style-type: none"> 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： <ul style="list-style-type: none"> ➢ 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 	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-I D： CCE-3 6266-5
214	Windows Server 2012 R2 Computer	TWG CB-01 -006-0 215	進階 稽核 原則 \ 詳	稽核 RPC 事件	<ul style="list-style-type: none"> 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 	電腦設定 \ Windows 設定\ 安全性設定\ 進 階稽核原則設定	沒有稽核	CCE-I D： CCE-3 6145-1

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
	Settings		細追 蹤		成功嘗試，而失敗稽核則會記錄失敗嘗試 <ul style="list-style-type: none"> ▪ 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 	\稽核原則\詳細 追蹤\稽核 RPC 事件		
215	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 216	進階 稽核 原則 \詳 細追 蹤	稽核 DPAPI 活 動	<ul style="list-style-type: none"> ▪ 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) ▪ 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 	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 DPAPI 活動	沒有稽核	CCE-I D： CCE-3 8035-2
216	Windows Server 2012 R2 Computer	TWG CB-01 -006-0 217	進階 稽核 原則 \詳	稽核建立 處理程序	<ul style="list-style-type: none"> ▪ 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 	電腦設定 \Windows 設定\ 安全性設定\進 階稽核原則設定	成功	CCE-I D： CCE-3 6059-4

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
	Settings		細追 蹤		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 <ul style="list-style-type: none"> ▪ 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 	\稽核原則\詳細 追蹤\稽核建立 處理程序		
217	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 218	進階 稽核 原則 \詳 細追 蹤	稽核終止 處理程序	<ul style="list-style-type: none"> ▪ 這項原則設定決定是否稽核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 	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\稽核終止 處理程序	沒有稽核	CCE-I D: CCE-3 8115-2
218	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 219	Wind ows 防火 牆/ 網域 設定	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	允許(預 設)	CCE-I D: CCE-3 6146-9

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
			檔			性的 Windows 防火牆\內容\網域設定檔\輸出連線		
219	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0220	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-36062-8
220	Windows Server 2012 R2 Computer	TWG CB-01-006-0221	Windows 防火牆/	Windows 防火牆:網域設定檔:輸入連	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	封鎖(預設)	CCE-ID: CCE-38117-8

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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		網域 設定 檔	線		Windows 防火牆 \具有進階安全 性的 Windows 防 火牆\內容\網域 設定檔\輸入連 線		
221	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 222	Wind ows 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 用本機防火牆規 則	是(預設)	CCE-I D: CCE-3 7860-4
222	Windows	TWG	Wind	Windows	這項原則設定決定當程式因為接收輸入連線	電腦設定	是	CCE-I

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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 2012 R2 Computer Settings	CB-01 -006-0 223	ows 防火 牆/ 網域 設定 檔	防火牆：網 域設定 檔：顯示通 知	而被封鎖時，是否為使用者顯示通知	\\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\\顯 示通知		D： CCE-3 8041-0
223	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 224	Wind ows 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	是(預設)	CCE-I D： CCE-3 8040-2

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
						用本機連線安全性規則		
224	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 225	Wind ows 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-I D： CCE-3 7859-6
225	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 226	Wind ows 防火 牆/ 私人 設定	Windows 防火牆：私 人設定 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	開啟(建議 選項)	CCE-I D： CCE-3 8239-0

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
			檔			性的 Windows 防火牆\內容\私人設定檔\防火牆狀態		
226	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0227	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\輸入連線	封鎖(預設)	CCE-ID: CCE-38042-8
227	Windows Server 2012 R2 Computer	TWG CB-01-006-0228	Windows 防火牆/	Windows 防火牆:私人設定檔:套用本	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	是(預設)	CCE-ID: CCE-37438-9

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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		私人 設定 檔	機防火牆 規則		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		
228	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 229	Wind ows 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	CCE-I D: CCE-3 7621-0
229	Windows	TWG	Wind	Windows	這項原則設定決定此電腦是否接收其傳出之	電腦設定	否	CCE-I

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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 2012 R2 Computer Settings	CB-01 -006-0 230	ows 防火 牆/ 私人 設定 檔	防火牆:私 人設定 檔:允許單 點傳播回 應	多點傳送或廣播訊息的單點傳送回應	\\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		D: CCE-3 7134-4
230	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 231	Wind ows 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	是(預設)	CCE-I D: CCE-3 6063-6

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
						用本機連線安全性規則		
231	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 232	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 \\具有進階安全 性的 Windows 防 火牆\\內容\\私人 設定檔\\輸出連 線	允許(預 設)	CCE-I D： CCE-3 8332-3
232	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 233	Windows 防火牆/ 公用 設定	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	否	CCE-I D： CCE-3 6324-2

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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			性的 Windows 防火牆\內容\公用設定檔\設定\允許單點傳播回應		
233	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0234	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-38043-6
234	Windows Server 2012 R2 Computer	TWG CB-01-006-0235	Windows 防火牆/	Windows 防火牆:公用設定檔:套用本	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	是(預設)	CCE-ID: CCE-36268-1

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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		公用 設定 檔	機連線安 全性規則		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 用本機連線安全 性規則		
235	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 236	Wind ows 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-I D: CCE-3 6057-8
236	Windows	TWG	Wind	Windows	這項原則設定決定是否允許套用本機系統管	電腦設定	是(預設)	CCE-I

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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 2012 R2 Computer Settings	CB-01 -006-0 237	ows 防火 牆/ 公用 設定 檔	防火牆：公 用設定 檔：套用本 機防火牆 規則	理員所建立的本機連線安全性規則	\\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 用本機防火牆規 則		D： CCE-3 7861-2
237	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 238	Wind ows 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 火牆\\內容\\公用	允許(預 設)	CCE-I D： CCE-3 7434-8

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
						設定檔\輸出連線		
238	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 239	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-I D： CCE-3 7862-0
239	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 713	系統 管理 範本 /遠 端桌 面服	需要對遠 端(RDP) 連線使用 特定的安 全層	<ul style="list-style-type: none"> ▪ 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 	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\	已啟用： SSL(TLS 1.0)	

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
			務		<p>的所有通訊都必須使用這項設定中指定的安全性方法，可用的安全性方法如下：</p> <ul style="list-style-type: none"> ➤ 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(TLS 1.0)：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 <p>▪ 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</p>	需要對遠端 (RDP)連線使用特定的安全層		

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
					伺服器在遠端連線所要使用的安全性方法			
240	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 714	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	<ul style="list-style-type: none"> ▪ 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 	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
					<p>標電腦上的本機設定</p> <ul style="list-style-type: none"> 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 			
241	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 715	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	<ul style="list-style-type: none"> 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」窗格不能和「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 	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
242	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 716	系統 管理 範本 /檔 案總 管框 架窗 格	關閉預覽 窗格	<ul style="list-style-type: none"> ▪ 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 2012 R2 DC Server 政府組態基準列表

項次	GPO	TWG CB-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 2012 R2 DC Server	TWG CB-01-006-0240	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	<ul style="list-style-type: none"> ▪ 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 ▪ 在此原則設定中，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 	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-37439-7

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
					人的快取資訊			
2	Windows Server 2012 R2 DC Server	TWG CB-01-006-0241	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	<ul style="list-style-type: none"> ▪ 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-36921-5
3	Windows Server 2012 R2 DC Server	TWG CB-01-006-0242	安全性選項\網域控制站	網域控制站：允許伺服器操作者排程工作	<ul style="list-style-type: none"> ▪ 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設備 	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：允許伺服器操作者排程工作	已停用	CCE-ID：CCE-37848-9
4	Windows Server	TWG CB-01	安全性選	網域控制站：LDAP 伺	<ul style="list-style-type: none"> ▪ 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： 	電腦設定\Windows 設定\	要求簽章	CCE-ID：CCE-35904

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 DC Server	-006-0 243	項\ 網域 控制 站	伺服器簽章要 求	<ul style="list-style-type: none"> ➤ 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：未定義此原則，相當於設定為「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 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 簡單繫結和透過 SSL 進行的 LDAP 簡單繫結 	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		-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
5	Windows Server 2012 R2 DC Server	TWG CB-01-006-0244	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。此原則設定會取代「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-37954-5
6	Windows Server 2012 R2 DC Server	TWG CB-01-006-0246	使用者權限指派	將工作站新增至網域	<ul style="list-style-type: none"> ▪ 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 中的帳戶和群組 ▪ 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 	電腦設定 \\Windows 設定\\ 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	Administrators	CCE-ID : CCE-36282-2

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
					<p>立 10 個電腦帳戶的限制</p> <ul style="list-style-type: none"> 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 2012 R2 DC Server	TWG CB-01 -006-0 247	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-36099 -0
8	Windows Server	TWG CB-01	使用 者權	從網路存取 這台電腦	<ul style="list-style-type: none"> 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 	電腦設定 \ Windows 設定\ 	Admini strators	CCE-ID： CCE-35818

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 DC Server	-006-0 248	限指 派		<ul style="list-style-type: none"> ▪ 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」 	安全性設定\本機原則\使用者權限指派\從網路存取這台電腦	, Authen ticated Users, ENTE RPRIS E DOMA IN CONT ROLL ERS	-4
9	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 249	系統 服務	Active Directory Domain Services	AD DS 網域控制站服務。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	CCE-ID： CCE-36681 -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
10	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 250	系統 服務	Active Directory Web Services	這個服務提供 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 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	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Active Directory Web Services	自動	CCE-ID： CCE-37038 -7
11	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 251	系統 服務	Application Identity	判斷並確定應用程式的識別。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-36892 -8
12	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 252	系統 服務	DFS Namespace	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	CCE-ID： CCE-36692 -2
13	Windows	TWG	系統	DFS	透過本機或廣域網路(WAN)網路連線同步	電腦設定	自動	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
	Server 2012 R2 DC Server	CB-01 -006-0 253	服務	Replication	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		CCE-36870 -4
14	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 254	系統 服務	Distributed Link Tracking Client	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	CCE-ID : CCE-36992 -6
15	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 255	系統 服務	DNS Client	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	CCE-ID : CCE-36697 -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
16	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 256	系統 服務	DNS Server	讓 DNS 用戶端經由回答 DNS 查詢和動態 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	CCE-ID： CCE-36768 -0
17	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 257	系統 服務	File Replication	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	電腦設定 \Windows 設定\ 安全性設定\系統 服務\File Replication	已停用	CCE-ID： CCE-36700 -3
18	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 258	系統 服務	Group Policy Client	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	CCE-ID： CCE-36702 -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
19	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 259	系統 服務	Intersite Messaging	讓訊息能夠在執行 Windows 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	電腦設定 \\Windows 設定\ 安全性設定\\系統 服務\\Intersite Messaging	自動	CCE-ID： CCE-36708 -6
20	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 260	系統 服務	Kerberos Key Distribution Center	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	CCE-ID： CCE-36710 -2
21	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 261	系統 服務	Netlogon	維持這個電腦和網域控制站間用於驗證使用者和服務的安全通道。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	CCE-ID： CCE-36717 -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
22	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 262	系統 服務	Server	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	CCE-ID： CCE-36736 -7
23	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 263	系統 服務	Windows Time	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，將無法進行日期和時間同步處理。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	自動	CCE-ID： CCE-37047 -8
24	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 264	系統 服務	Workstation	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	CCE-ID： CCE-36905 -8
25	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 265	進階 稽核 原則 \\DS	稽核目錄服 務存取	<ul style="list-style-type: none"> ▪ 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 ▪ 只會記錄具有相符系統存取控制清單 	電腦設定 \Windows 設定\ 安全性設定\進階 稽核原則設定\稽	成功及 失敗	CCE-ID： CCE-37433 -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
			存取		<p>(SACL)的 AD DS 物件</p> <ul style="list-style-type: none"> ▪ 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 	核原則\DS 存取\ 稽核目錄服務存取		
26	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 266	進階 稽核 原則 \DS 存取	稽核目錄服 務變更	<ul style="list-style-type: none"> ▪ 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產生稽核事件 ▪ 如果設定這項原則設定，則會在嘗試變更 	電腦設定 \Windows 設定\ 安全性設定\進階 稽核原則設定\稽 核原則\DS 存取\ 稽核目錄服務變 更	成功及 失敗	CCE-ID： CCE-37616 -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
					<p>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</p> <ul style="list-style-type: none"> ▪ 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 2012 R2 DC Server	TWG CB-01 -006-0 267	進階 稽核 原則 \ 帳 戶 管 理	稽核電腦帳 戶管理	<ul style="list-style-type: none"> ▪ 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	成功及 失敗	CCE-ID： CCE-38004 -8
28	Windows	TWG	安全	帳戶：	<ul style="list-style-type: none"> ▪ 這項原則設定決定要啟用或停用本機 	電腦設定	已停用	CCE-ID：

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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 2012 R2 DC Server	CB-01 -006-0 268	性選 項\ 帳戶	Administrator 帳戶狀態	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 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	\\Windows 設定\ 安全性設定\\本機 原則\\安全性選項 \\帳戶： Administrator 帳 戶狀態		CCE-37953 -7
29	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 269	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-37432 -2
30	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 270	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，使用者將無法透過「摘要」內容頁將 Feed Sync Engine 設成	電腦設定\\系統管 理範本\\Windows 元件\\RSS 摘要\ 防止下載隨函附	已啟用	CCE-ID： CCE-37126 -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
			摘要		<p>下載隨函附件。開發人員無法透過「摘要」API 來變更下載設定</p> <ul style="list-style-type: none"> ▪ 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 	件		
31	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 271	系統 管理 範本 /Win dows Defe nder	加入 Microsoft MAPS	<ul style="list-style-type: none"> ▪ 這項原則設定可加入 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和傳送。在某些情況下，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 	電腦設定\系統管理範本\Windows 元件\Windows Defender\MAPS\ 加入 Microsoft MAPS	已停用	CCE-ID： CCE-33833 -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
					<p>的身分或與使用者聯繫</p> <ul style="list-style-type: none"> ▪ 可能的選項為： <ul style="list-style-type: none"> ➢ (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 ▪ 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 			

項次	GPO	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 MAPS			
32	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 272	系統 管理 範本 /Win dows Instal ler	允許使用者 控制安裝	<ul style="list-style-type: none"> ▪ 這項原則設定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。它能让安裝完成，不因安全性違規而暫停安裝 ▪ 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 	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-36400 -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
					計。它可以用來規避安裝程式中防止軟體被安裝的錯誤			
33	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 273	系統 管理 範本 /Win dows Instal ler	防止出現 Windows Installer 指令 碼的 Internet Explorer 安全 性提示	<ul style="list-style-type: none"> ▪ 這項原則設定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 ▪ 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佈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 	電腦設定\系統管理範本\Windows 元件\Windows Installer\防止出現 Windows Installer 指令碼的 Internet Explorer 安全性提示	已停用	CCE-ID： CCE-37524 -6
34	Windows Server 2012 R2	TWG CB-01 -006-0	系統 管理 範本	不允許摘要 式驗證	<ul style="list-style-type: none"> ▪ 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 	電腦設定\系統管理範本\Windows 元件\Windows 遠	已啟用	CCE-ID： CCE-38318 -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
	DC Server	274	/Windows 遠端管理 (WinRM)		會使用摘要式驗證 <ul style="list-style-type: none"> ▪ 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 	端管理 (WinRM)\WinRM 用戶端\不允許摘要式驗證		
35	Windows Server 2012 R2 DC Server	TWG CB-01-006-0 275	系統管理範本 /Windows 遠端管理 (WinRM)	允許未加密的流量	<ul style="list-style-type: none"> ▪ 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和接收未加密的訊息 ▪ 如果啟用這項原則設定，WinRM 用戶端會透過網路傳送和接收未加密的訊息 ▪ 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 	電腦設定\系統管理範本\Windows 遠端管理 (WinRM)\WinRM 用戶端\允許未加密的流量	已停用	CCE-ID : CCE-37726-7
36	Windows Server 2012 R2	TWG CB-01-006-0	系統管理範本	允許基本驗證	<ul style="list-style-type: none"> ▪ 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 	電腦設定\系統管理範本\Windows 遠	已停用	CCE-ID : CCE-36310-1

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
	DC Server	276	/Win dows 遠端 管理 (Win RM)		<p>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</p> <ul style="list-style-type: none"> ▪ 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 	端管理 (WinRM)\WinR M 用戶端\允許基 本驗證		
37	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 277	系統 管理 範本 /Win dows 遠端 管理 (Win RM)	不允許 WinRM 儲存 RunAs 認證	<ul style="list-style-type: none"> ▪ 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 ▪ 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 和 RunAsPassword 設定值，而且可安全地儲存 	電腦設定\系統管 理範本\Windows 元件\Windows 遠 端管理 (WinRM)\WinR M 服務\不允許 WinRM 儲存 RunAs 認證	已啟用	CCE-ID： CCE-36000 -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
					RunAsPassword 值 <ul style="list-style-type: none"> ▪ 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 			
38	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 278	系統 管理 範本 /Win dows 遠端 管理 (Win RM)	允許未加密 的流量	<ul style="list-style-type: none"> ▪ 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 	電腦設定\系統管理範本\Windows 元件\Windows 遠端管理 (WinRM)\WinRM 服務\允許未加密的流量	已停用	CCE-ID： CCE-38223 -4
39	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 279	系統 管理 範本 /Win dows 遠端	允許基本驗 證	<ul style="list-style-type: none"> ▪ 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 	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	已停用	CCE-ID： CCE-36254 -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
			管理 (Win RM)		<ul style="list-style-type: none"> ▪ 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 	驗證		
40	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 280	系統 管理 範本 /自 動播 放原 則	不允許非磁 碟區裝置的 自動播放	<ul style="list-style-type: none"> ▪ 這項原則設定不允許 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 ▪ 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 	電腦設定\系統管理範本\Windows 元件\自動播放原則\不允許非磁碟區裝置的自動播放	已啟用	CCE-ID： CCE-37636 -8
41	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 281	系統 管理 範本 /自 動播 放原 則	設定 AutoRun 的預設行為	<ul style="list-style-type: none"> ▪ 這項原則設定可設定 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 Vista 或更新版本的 AutoRun 預設行為變更為下列行為： 	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-38217 -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
					<ul style="list-style-type: none"> ➤ 完全停用 AutoRun 命令，或者 ➤ 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 			
42	Windows Server 2012 R2 DC Server	TWG CB-01-006-0282	系統管理範本/定位和感應器	關閉定位	<ul style="list-style-type: none"> ▪ 這項原則設定會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 	電腦設定\系統管理範本\Windows 元件\定位和感應器\關閉定位	已啟用	CCE-ID： CCE-36886-0
43	Windows Server 2012 R2 DC Server	TWG CB-01-006-0283	系統管理範本/認	不要顯示密碼顯示按鈕	<ul style="list-style-type: none"> ▪ 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 	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	已啟用	CCE-ID： CCE-37534-5

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
			證使用者 介面		<p>密碼顯示按鈕</p> <ul style="list-style-type: none"> ▪ 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 	碼顯示按鈕		
44	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 284	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	<ul style="list-style-type: none"> ▪ 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和密碼 	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	CCE-ID： CCE-36512 -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
45	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 285	系統 管理 範本 /遠 端桌 面服 務	連線時永遠 提示密碼	<ul style="list-style-type: none"> ▪ 這項原則設定指定遠端桌面服務是否總是在連線時，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，即使他們已經在遠端桌面連線用戶端中提供過密碼 ▪ 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。他們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 	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 \連線時永遠提示 密碼	已啟用	CCE-ID： CCE-37929 -7
46	Windows	TWG	系統	需要安全的	<ul style="list-style-type: none"> ▪ 指定遠端桌面工作階段主機伺服器與所有 	電腦設定\系統管	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
	Server 2012 R2 DC Server	CB-01 -006-0 286	管理 範本 /遠 端桌 面服 務	RPC 通訊	<p>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</p> <ul style="list-style-type: none"> ▪ 可以使用這項設定，藉由只允許已驗證及已加密的要求，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 	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 \需要安全的 RPC 通訊		CCE-37567 -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
47	Windows Server 2012 R2 DC Server	TWG CB-01-006-0287	系統管理範本/遠端桌面服務	不允許磁碟重新導向	<ul style="list-style-type: none"> ▪ 這項原則設定指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) ▪ 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和剪 	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\裝置及資源重新導向\不允許磁碟重新導向	已啟用	CCE-ID : CCE-36509-8

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
					貼簿檔案複製重新導向			
48	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 288	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	<ul style="list-style-type: none"> ▪ 這項原則設定可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 	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	CCE-ID： CCE-38180 -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
					<p>理員指定了不一樣的設定</p> <ul style="list-style-type: none"> ▪ 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 			
49	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 289	系統 管理 範本 /遠 端桌 面服 務	結束後不刪除暫存資料夾	<ul style="list-style-type: none"> ▪ 這項原則設定會指定在使用者登出時，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 	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	CCE-ID： CCE-37946 -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
					<p>員指定了不一樣的設定</p> <ul style="list-style-type: none"> ▪ 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 			
50	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 290	系統 管理 範本 /遠 端桌 面服 務	不允許儲存 密碼	<ul style="list-style-type: none"> ▪ 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 	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-36223 -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
					<ul style="list-style-type: none"> ▪ 如果停用或未做這項設定，則使用者能夠使用遠端桌面連線儲存密碼 			
51	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 291	系統 管理 範本 /檔 案總 管	設定 Windows SmartScreen 篩選工具	<ul style="list-style-type: none"> ▪ 這項原則設定可管理 Windows SmartScreen 篩選工具的行為 Windows SmartScreen 篩選工具會在從網際網路執行無法辨識的程式下載之前警告使用者，使電腦更加安全。啟用這個功能時，會將檔案以及在電腦上執行之程式的相關資訊傳送給 Microsoft ▪ 如果啟用這項原則設定，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： <ul style="list-style-type: none"> ➢ 在執行不明軟體下載之前需要系統管理員核准 ➢ 在執行不明軟體下載之前警告使用者 ➢ 關閉 SmartScreen ▪ 如果停用或未設定這項原則設定，則電腦的系統管理員可以使用「行動作業中心」 	電腦設定\系統管理範本\Windows 元件\檔案總管\設定 Windows SmartScreen 篩選工具	已啟用：在執行不明軟體下載之前需要系統管理員核准	CCE-ID： CCE-35859 -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
					<p>的「Windows SmartScreen 篩選工具設定」 管理 Windows SmartScreen 篩選工具的行為</p> <ul style="list-style-type: none"> ▪ 選項： <ul style="list-style-type: none"> ➢ 在執行不明軟體下載之前需要系統管理員核准 ➢ 在執行不明軟體下載之前警告使用者 ➢ 關閉 SmartScreen 篩選工具 			
52	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 292	系統 管理 範本 /檔 案總 管	損毀時關閉 終止堆集	這項原則設定決定是否損毀時關閉終止堆集可讓特定的舊版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	電腦設定\系統管理範本\Windows 元件\檔案總管\ 損毀時關閉終止 堆集	已停用	CCE-ID： CCE-36660 -9
53	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 293	系統 管理 範本 /檔	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	電腦設定\系統管理範本\Windows 元件\檔案總管\ 關閉殼層通訊協	已停用	CCE-ID： CCE-36809 -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
			案總 管		<p>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</p> <ul style="list-style-type: none"> ▪ 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 	定受保護模式		
54	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 294	系統 管理 範本 /檔 案總	關閉檔案總 管的資料執 行防止	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	已停用	CCE-ID： CCE-37809 -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
			管			資料執行防止		
55	Windows Server 2012 R2 DC Server	TWG CB-01-006-0295	系統管理範本/登入	列舉加入網域電腦上的本機使用者	<ul style="list-style-type: none"> ▪ 這項原則設定會允許列舉加入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 	電腦設定\系統管理範本\系統\登入\列舉加入網域電腦上的本機使用者	已停用	CCE-ID：CCE-35894-5
56	Windows Server 2012 R2 DC Server	TWG CB-01-006-0296	系統管理範本/登入	關閉鎖定畫面上的應用程式通知	<ul style="list-style-type: none"> ▪ 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	CCE-ID：CCE-35893-7
57	Windows Server	TWG CB-01	系統管理	開機啟動驅動程式初始	<ul style="list-style-type: none"> ▪ 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 	電腦設定\系統管理範本\系統\開	已啟用：良	CCE-ID：CCE-37912

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 DC Server	-006-0 297	範本 /開 機初 期啟 動的 反惡 意程 式碼	化原則	<p>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：</p> <ul style="list-style-type: none"> ➤ 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 <p>▪ 如果啟用這項原則設定，可以選擇下次電</p>	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	好和不明	-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
					<p>腦啟動時要初始的啟動開機驅動程式</p> <ul style="list-style-type: none"> ▪ 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 			
58	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 298	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)	<ul style="list-style-type: none"> ▪ 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	CCE-ID： CCE-37066 -8
59	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 299	系統 管理 範本 /睡 眠設	喚醒電腦時 必須使用密 碼(使用電池)	<ul style="list-style-type: none"> ▪ 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 	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	已啟用	CCE-ID： CCE-36881 -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
			定		<ul style="list-style-type: none"> ▪ 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 	電池)		
60	Windows Server 2012 R2 DC Server	TWG CB-01-006-0300	系統管理範本/疑難排解與診斷	Microsoft 支援服務診斷工具：開啟 MSDT 與支援提供者的互動式通訊	<ul style="list-style-type: none"> ▪ 這項原則設定會設定 Microsoft 支援服務診斷工具(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 	電腦設定\系統管理範本\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	已停用	CCE-ID： CCE-38161-6

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
61	Windows Server 2012 R2 DC Server	TWG CB-01-006-0301	系統管理範本/疑難排解與診斷	啟用/停用 PerfTrack	<ul style="list-style-type: none"> ▪ 這項原則設定會指定要啟用或停用回應事件的追蹤 ▪ 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，DPS 會預設啟用 Windows 效能 PerfTrack 	電腦設定\系統管理範本\系統\疑難排解與診斷\Windows 效能 PerfTrack\啟用/停用 PerfTrack	已停用	CCE-ID : CCE-36648-4
62	Windows Server 2012 R2 DC Server	TWG CB-01-006-0302	系統管理範本/網際網路通訊管理	關閉 HTTP 上的列印	<ul style="list-style-type: none"> ▪ 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及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 	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	CCE-ID : CCE-36920-7

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
					<ul style="list-style-type: none"> ▪ 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 			
63	Windows Server 2012 R2 DC Server	TWG CB-01-006-0303	系統管理範本/網際網路通訊管理	關閉 Windows 客戶經驗改進計畫	<ul style="list-style-type: none"> ▪ 這項原則設定會關閉 Windows 客戶經驗改進計畫。「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和服務的資訊，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，使用者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」 	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 客戶經驗改進計畫	已啟用	CCE-ID： CCE-36174-1

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
64	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 304	系統 管理 範本 /網 際網 路通 訊管 理	關閉手寫辨識錯誤報告	<ul style="list-style-type: none"> ▪ 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 ▪ 如果啟用這項原則，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 ▪ 如果停用這項原則，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 Microsoft 	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	CCE-ID： CCE-36203 -8
65	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 305	系統 管理 範本 /網	關閉市集的存取權	<ul style="list-style-type: none"> ▪ 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	已啟用	CCE-ID： CCE-37904 -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
			際網路通訊管理		<p>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</p> <ul style="list-style-type: none"> ▪ 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 	定\關閉市集的存取權		
66	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 306	系統管理範本/際網路通訊管理	關閉透過 HTTP 下載印表機驅動程式	<ul style="list-style-type: none"> ▪ 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 ▪ 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 	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\關閉透過 HTTP 下載印表機驅動程式	已啟用	CCE-ID： CCE-36625 -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
					裝的驅動程式 <ul style="list-style-type: none"> ▪ 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 			
67	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 307	系統 管理 範本 /遠 端協 助	設定提供遠 端協助	<ul style="list-style-type: none"> ▪ 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 ▪ 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 	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	CCE-ID： CCE-36388 -7
68	Windows	TWG	系統	設定請求遠	<ul style="list-style-type: none"> ▪ 這項原則設定可以在這部電腦上開啟或關 	電腦設定\系統管	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
	Server 2012 R2 DC Server	CB-01 -006-0 308	管理 範本 /遠 端協 助	端協助	<p>閉「請求(要求)遠端協助」</p> <ul style="list-style-type: none"> ▪ 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」 	理範本\系統\遠端協助\設定請求遠端協助		CCE-37281 -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
					<ul style="list-style-type: none"> ▪ 「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 ▪ 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 			
69	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 309	系統 管理 範本 /Micro soft	關閉 Microsoft 對 等網路服務	<ul style="list-style-type: none"> ▪ 這項原則設定會完全關閉 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 	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	已啟用	CCE-ID： CCE-37699 -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
			對等 網路 服務		<p>發佈和分散式處理等領域的應用程式</p> <ul style="list-style-type: none"> ▪ 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 	路服務		
70	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 310	系統 管理 範本 /Win dows Conn ect Now	使用 Windows Connect Now 進行無線設 定	<ul style="list-style-type: none"> ▪ 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)和 USB 快閃磁碟機，尋找與設定 Ethernet(UPnP)和 In-band 802.11 Wi-Fi 上的裝置 ▪ 其他選項則允許在指定的媒體上進行搜索與設定 ▪ 如果啟用這項原則設定，會有額外選項可以關閉特定媒體上的操作 ▪ 如果停用這項原則設定，會停用所有媒體上的操作 ▪ 如果未設定這項原則設定，會啟用所有媒 	電腦設定\系統管 理範本\網路 \Windows Connect Now\使 用 Windows Connect Now 進 行無線設定	已停用	CCE-ID： CCE-37481 -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
					<p>體上的操作</p> <ul style="list-style-type: none"> ▪ 這項原則設定的預設值可允許所有媒體上的操作 			
71	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 311	系統 管理 範本 /Win dows Conn ect Now	禁止存取 Windows Connect Now 精靈	<ul style="list-style-type: none"> ▪ 這項原則設定會禁止存取 Windows Connect Now(WCN)精靈 ▪ 如果啟用這項原則設定，就會關閉精靈，而使用者會無法存取任何精靈工作。所有和設定相關的工作，包含「設定無線路由器或存取點」與「新增無線裝置」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 	電腦設定\系統管理範本\網路\Windows Connect Now\禁止存取 Windows Connect Now 精靈	已啟用	CCE-ID： CCE-36109 -7
72	Windows Server	TWG CB-01	系統 管理	開啟 Mapper I/O(LLTDIO)	<ul style="list-style-type: none"> ▪ 這項原則設定會變更 Mapper I/O 網路通訊協定驅動程式的操作行為 	電腦設定\系統管理範本\網路\連	已停用	CCE-ID： CCE-38170

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 DC Server	-006-0 312	範本 /連 結階 層拓 樸搜 索	驅動程式	<ul style="list-style-type: none"> ▪ 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 	結階層拓樸搜索\ 開啟 Mapper I/O(LLTDIO)驅 動程式		-7
73	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 313	系統 管理 範本 /連 結階	開啟 Responder (RSPNDR)驅 動程式	<ul style="list-style-type: none"> ▪ 這項原則設定會變更 Responder 網路通訊協定驅動程式的操作行為 ▪ Responder 允許電腦加入「連結階層拓樸搜索」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 	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	已停用	CCE-ID： CCE-37959 -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
			層拓 樸搜 索		<p>(Quality-of-Service)活動，例如頻寬估計和網路狀態分析</p> <ul style="list-style-type: none"> ▪ 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 	程式		
74	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 314	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	<ul style="list-style-type: none"> ▪ 這項原則設定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 	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	CCE-ID： CCE-38188 -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
					置			
75	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 315	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	<ul style="list-style-type: none"> ▪ 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 	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、設定及使用網路橋接	已啟用	CCE-ID： CCE-38002 -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
76	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 316	系統 管理 範本 /通 知	在鎖定畫面上關閉快顯通知	<ul style="list-style-type: none"> ▪ 這項原則設定可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 ▪ 這項原則設定不需重新開機或重新啟動服務就會生效 	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	CCE-ID： CCE-36332 -5
77	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 317	系統 管理 範本 /Win dows Medi a Playe	防止轉碼器下載	<ul style="list-style-type: none"> ▪ 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 	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	CCE-ID： CCE-37445 -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
			r		<p>方塊</p> <ul style="list-style-type: none"> ▪ 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 			
78	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 318	系統 管理 範本 /附 件管 理員	不要保留檔案附件的區域資訊	<ul style="list-style-type: none"> ▪ 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)。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 	使用者設定\系統 管理範本 \Windows 元件\ 附件管理員\不要 保留檔案附件的 區域資訊	已停用	CCE-ID： CCE-37424 -9
79	Windows Server	TWG CB-01	系統 管理	開啟附件時 通知防毒程	<ul style="list-style-type: none"> ▪ 這項原則設定可管理已登錄防毒程式的通行行為。如果已登錄多種程式，將會全部 	使用者設定\系統 管理範本	已啟用	CCE-ID： CCE-36622

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 DC Server	-006-0 319	範本 / 附件 管理員	式	<p>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</p> <ul style="list-style-type: none"> ▪ 如果啟用這項原則設定，Windows 會命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 ▪ 如果停用這項原則設定，Windows 就不會在開啟附件檔案時呼叫已登錄防毒程式 ▪ 如果未設定這項原則設定，Windows 就不會在開啟附件檔案時呼叫已登錄防毒程式 	\\Windows 元件\ 附件管理員\ 開啟 附件時通知防毒 程式		-9
80	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 320	系統 管理 範本 / 網路共	防止使用者 共用其設定 檔內的檔案	<ul style="list-style-type: none"> ▪ 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 	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	已啟用	CCE-ID： CCE-38070 -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
			用		<p>內的檔案</p> <ul style="list-style-type: none"> ▪ 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，共用精靈也不會在此%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 	檔內的檔案		
81	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 321	系統 管理 範本 /個 人化	以密碼保護 螢幕保護裝 置	<ul style="list-style-type: none"> ▪ 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 ▪ 這項原則設定也會停用「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 	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-37658 -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
					<p>用者變更密碼保護設定</p> <ul style="list-style-type: none"> ▪ 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 			
82	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 322	系統 管理 範本 /個 人化	啟用螢幕保護裝置	<ul style="list-style-type: none"> ▪ 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」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 	使用者設定\系統 管理範本\控制台 \個人化\啟用螢 幕保護裝置	已啟用	CCE-ID： CCE-37970 -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
					立，螢幕保護裝置就會執行：第一，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。第二，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			
83	Windows Server 2012 R2 DC Server	TWG CB-01 -006-0 323	系統 管理 範本 /個 人化	強制特定螢幕保護裝置	<ul style="list-style-type: none"> ▪ 這項原則設定指定使用者桌面的螢幕保護裝置 ▪ 如果啟用這項設定，系統會在使用者的桌面上顯示指定的螢幕保護裝置。此外，這項設定會停用「個人化」或「顯示」控制台的「螢幕保護裝置」對話方塊中的螢幕保護裝置下拉式清單，以防止使用者變更螢幕保護裝置 ▪ 如果停用或未設定這項設定，則使用者可以選取任一螢幕保護裝置 ▪ 如果啟用這項設定，請輸入含有螢幕保護裝置的檔案名稱(包括.scr 副檔名)。如果螢 	使用者設定\系統 管理範本\控制台 \個人化\強制特 定螢幕保護裝置	已啟 用： scrnsav e.scr	CCE-ID： CCE-37907 -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
					<p>幕保護裝置檔案不在 %Systemroot%\System32 目錄中，請輸入檔 案的完整路徑</p> <ul style="list-style-type: none"> ▪ 如果指定的螢幕保護裝置未安裝在套用這 項設定的電腦上，就會略過這項設定 ▪ 注意：這項設定可能已被「啟用螢幕保護 裝置」設定所取代。如果「啟用螢幕保護 裝置」設定已停用，就會略過這項設定， 而且螢幕保護裝置不會執行 			

資料來源：本中心整理

表4 Windows Server 2012 R2 DNS Server 政府組態基準列表

項次	GPO	TWG CB-I D	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
1	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 324	系統 服務	Application Experience	在應用程式啟動時，處理應用程式的相容性 快取要求	電腦設定 \\Windows 設定\ 安全性設定\\系 統服務 \\Application Experience	手動	CCE-ID： CCE-3689 1-0
2	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 325	系統 服務	Application Identity	判斷並確定應用程式的識別。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-3689 2-8
3	Windows Server 2012 R2	TWG CB-01 -006-0	系統 服務	Application Information	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	電腦設定 \\Windows 設定\ 安全性設定\\系	手動	CCE-ID： CCE-3668 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
	DNS Server	326			以其他管理權限來啟動應用程式	統服務 \Application Information		
4	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 327	系統 服務	Application Layer Gateway Service	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	CCE-ID： CCE-3698 8-4
5	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 328	系統 服務	Application Management	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	CCE-ID： CCE-3668 5-6

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
6	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 329	系統 服務	ASP.NET State Service	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	CCE-ID： CCE-3668 6-4
7	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 330	系統 服務	Background Intelligent Transfer Service	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	CCE-ID： CCE-3590 1-8
8	Windows Server 2012 R2 DNS	TWG CB-01 -006-0	系統 服務	Background Tasks Infrastructure	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	自動	CCE-ID： CCE-3678 1-3

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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	331		Service		\Background Tasks Infrastructure Service		
9	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 332	系統 服務	Base Filtering Engine	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	CCE-ID： CCE-3682 7-4
10	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 333	系統 服務	Certificate Propagation	從智慧卡將使用者憑證和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	CCE-ID： CCE-3698 9-2
11	Windows	TWG	系統	CNG Key	CNG 金鑰隔離服務裝載於 LSA 處理程序。	電腦設定	手動	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
	Server 2012 R2 DNS Server	CB-01 -006-0 334	服務	Isolation	該服務可依據一般條件來隔離私密金鑰和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	\\Windows 設定\ 安全性設定\系 統服務\CNG Key Isolation		CCE-3668 9-8
12	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 335	系統 服務	COM+ Event System	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	CCE-ID： CCE-3699 0-0
13	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 336	系統 服務	COM+ System Application	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	CCE-ID： CCE-3669 0-6
14	Windows	TWG	系統	Computer	維護網路上更新的電腦清單，並將這個清單	電腦設定	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
	Server 2012 R2 DNS Server	CB-01 -006-0 337	服務	Browser	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	\\Windows 設定\ 安全性設定\系 統服務 \\Computer Browser		CCE-3703 9-5
15	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 338	系統 服務	Credential Manager	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	CCE-ID : CCE-3676 7-2
16	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 339	系統 服務	Cryptographic Services	<ul style="list-style-type: none"> ▪ 此服務提供三種管理服務： <ul style="list-style-type: none"> ➢ 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	CCE-ID : CCE-3669 1-4

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-I D	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
					<ul style="list-style-type: none"> ➤ 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 			
17	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 340	系統 服務	DCOM Server Process Launcher	COMLAUNCH 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	CCE-ID： CCE-3689 3-6
18	Windows Server 2012 R2 DNS	TWG CB-01 -006-0 341	系統 服務	Device Association Service	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	手動	CCE-ID： CCE-3651 7-1

項次	GPO	TWG CB-I D	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server					Service		
19	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 342	系統 服務	Device Install Service	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\Device Install Service	手動	CCE-ID： CCE-3683 3-2
20	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 343	系統 服務	Device Setup Manager	啟用裝置相關軟體的偵測、下載及安裝。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	CCE-ID： CCE-3678 3-9
21	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 344	系統 服務	DFS Replication	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	CCE-ID： CCE-3687 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
22	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 345	系統 服務	DHCP Client	為這個電腦登錄及更新 IP 位址和 DNS 記錄。如果這個服務被停止，這個電腦將會不接收動態 IP 位址和 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	CCE-ID： CCE-3669 3-0
23	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 346	系統 服務	Diagnostic Policy Service	診斷原則服務能夠偵測 Windows 元件的問題、進行疑難排解和提供解決方案。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	CCE-ID： CCE-3699 1-8
24	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 347	系統 服務	Diagnostic Service Host	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	手動	CCE-ID： CCE-2515 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
						Service Host		
25	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 348	系統 服務	Diagnostic System Host	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	CCE-ID： CCE-3704 0-3
26	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 349	系統 服務	Distributed Link Tracking Client	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	CCE-ID： CCE-3699 2-6
27	Windows Server	TWG CB-01	系統 服務	Distributed Transaction	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	電腦設定 \Windows 設定\ 安全性設定\系 統服務 \Distributed Transaction	自動	CCE-ID： CCE-3685

項次	GPO	TWG CB-I D	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 DNS Server	-006-0 350		Coordinator	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	安全性設定\系統服務 \Distributed Transaction Coordinator		9-7
28	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 351	系統 服務	DNS Client	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	CCE-ID： CCE-3669 7-1
29	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 352	系統 服務	DNS Server	讓 DNS 用戶端經由回答 DNS 查詢和動態 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	CCE-ID： CCE-3676 8-0

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-I D	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
30	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 353	系統 服務	Encrypting File System (EFS)	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	CCE-ID： CCE-3682 8-2
31	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 354	系統 服務	Extensible Authentication Protocol	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	CCE-ID： CCE-3669 8-9
32	Windows Server 2012 R2 DNS	TWG CB-01 -006-0	系統 服務	Function Discovery Provider Host	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)和 Web Services - Discovery(WS-D)通訊協定的網路探索服	電腦設定 \\Windows 設定\ 安全性設定\系 統服務	手動	CCE-ID： CCE-3704 1-1

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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	355			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 以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	\Function Discovery Provider Host		
33	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 356	系統 服務	Function Discovery Resource Publication	發佈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，便不再發佈網路資源，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	CCE-ID： CCE-3676 9-8
34	Windows Server 2012 R2 DNS	TWG CB-01 -006-0 357	系統 服務	Group Policy Client	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	電腦設定 \Windows 設定\ 安全性設定\ 系統服務\Group	自動	CCE-ID： CCE-3670 2-9

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
	Server				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	Policy Client		
35	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 358	系統 服務	Health Key and Certificate Management	提供網路存取保護代理程式(NAPAgent)的 X.509 憑證和金鑰管理服務。不使用此服務，使用 X.509 憑證的強制隔離技術將無法正常運作	電腦設定 \\Windows 設定\ 安全性設定\\系 統服務\\Health Key and Certificate Management	手動	CCE-ID： CCE-3689 5-1
36	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 359	系統 服務	Human Interface Device Service	啟用並維護鍵盤、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	CCE-ID： CCE-3670 3-7

項次	GPO	TWG CB-I D	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
37	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 360	系統 服務	Hyper-V Data Exchange Service	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	CCE-ID： CCE-3834 2-2
38	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 361	系統 服務	Hyper-V Guest Shutdown Service	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	CCE-ID： CCE-3723 1-8
39	Windows Server 2012 R2	TWG CB-01 -006-0	系統 服務	Hyper-V Heartbeat	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	電腦設定 \\Windows 設定\ 安全性設定\系	手動	CCE-ID： CCE-3806

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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	362		Service	虛擬機器	統服務 \Hyper-V Heartbeat Service		6-7
40	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 363	系統 服務	Hyper-V Remote Desktop Virtualization Service	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	CCE-ID： CCE-3718 3-1
41	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 364	系統 服務	Hyper-V Time Synchronizati on Service	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	手動	CCE-ID： CCE-3815 7-4

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
						Synchronization Service		
42	Windows Server 2012 R2 DNS Server	TWG CB-01-006-0365	系統服務	Hyper-V Volume Shadow Copy Requestor	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	CCE-ID： CCE-3588 1-2
43	Windows Server 2012 R2 DNS Server	TWG CB-01-006-0366	系統服務	IKE and AuthIP IPsec Keying Modules	IKEEXT 服務主控 Internet KeyingExchange(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 和 AuthIP 金鑰交換。IPsec 通常會設定為使用 IKE 或 AuthIP，因此如	電腦設定 \\Windows 設定\\ 安全性設定\\系 統服務\\IKE and AuthIP IPsec Keying Modules	手動	CCE-ID： CCE-3677 0-6

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
					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			
44	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 367	系統 服務	Interactive Services Detection	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	CCE-ID： CCE-3682 9-0
45	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 368	系統 服務	Internet Connection Sharing (ICS)	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	CCE-ID： CCE-3670 7-8

項次	GPO	TWG CB-I D	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
46	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 369	系統 服務	IP Helper	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	CCE-ID： CCE-3670 9-4
47	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 370	系統 服務	IPsec Policy Agent	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)，以及重新執行保護。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	電腦設定 \Windows 設定\ 安全性設定\系 統服務\IPsec Policy Agent	手動	CCE-ID： CCE-3699 6-7
48	Windows Server 2012 R2	TWG CB-01 -006-0	系統 服務	KDC Proxy Server service	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	電腦設定 \Windows 設定\ 安全性設定\系	手動	CCE-ID： CCE-3700

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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	371		(KPS)	理到公司網路上的網域控制站	統服務\KDC Proxy Server service (KPS)		9-8
49	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 372	系統 服務	KtmRm for Distributed Transaction Coordinator	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	CCE-ID： CCE-3639 2-9
50	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 373	系統 服務	Link-Layer Topology Discovery Mapper	<ul style="list-style-type: none"> ▪ 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及裝置的中繼資料 ▪ 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	手動	CCE-ID： CCE-3677 1-4

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
						Mapper		
51	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 374	系統 服務	Local Session Manager	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	CCE-ID : CCE-3701 0-6
52	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 375	系統 服務	Microsoft .NE T Framework NGEN v2.0.50727_I6 4	這項原則設定決定此電腦是否可使用 Microsoft .NET Framework NGEN 之服務	電腦設定 \Windows 設定\ 安全性設定\系 統服務 \Microsoft .NET Framework NGEN v2.0.50727_I64	手動	CCE-ID : CCE-3689 8-5
53	Windows	TWG	系統	Microsoft	管理從這部電腦連線至遠端 iSCSI 目標裝置	電腦設定	手動	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
	Server 2012 R2 DNS Server	CB-01 -006-0 376	服務	iSCSI Initiator Service	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	\\Windows 設定\ 安全性設定\系 統服務 \\Microsoft iSCSI Initiator Service		CCE-3671 3-6
54	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 377	系統 服務	Microsoft Software Shadow Copy Provider	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	CCE-ID： CCE-3671 4-4
55	Windows Server 2012 R2	TWG CB-01 -006-0	系統 服務	Multimedia Class Scheduler	根據整個系統的工作優先順序啟用相關的工作優先順序。主要的目標是多媒體應用程式。如果這個服務停止，個別的工作會回復	電腦設定 \\Windows 設定\ 安全性設定\系	手動	CCE-ID： CCE-3671 5-1

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
	DNS Server	378			為預設的優先順序	統服務 \Multimedia Class Scheduler		
56	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 379	系統 服務	Net.Tcp Port Sharing Service	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	CCE-ID： CCE-3671 6-9
57	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 380	系統 服務	Netlogon	維持這個電腦與網域控制站間用於驗證使 用者及服務的安全通道。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	CCE-ID： CCE-3671 7-7
58	Windows	TWG	系統	Network	網路存取保護(NAP)代理程式服務會蒐集與	電腦設定	手動	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
	Server 2012 R2 DNS Server	CB-01 -006-0 381	服務	Access Protection Agent	管理網路上之用戶端電腦的健康情況資訊。NAP 代理程式蒐集的資訊是用來確定用戶端電腦具有必要的軟體與設定。如果用戶端電腦與健康原則不相容，則用戶端電腦在其設定更新之前，只會具有有限的網路存取權。而根據健康原則的設定，可能會自動更新用戶端電腦，這樣使用者就可以快速重新取得完整的網路存取權，而不需要手動更新他們的電腦	\\Windows 設定\ 安全性設定\系 統服務\Network Access Protection Agent		CCE-3699 9-1
59	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 382	系統 服務	Network Connections	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	CCE-ID : CCE-3671 8-5
60	Windows Server 2012 R2	TWG CB-01 -006-0	系統 服務	Network Connectivity Assistant	提供 UI 元件的 DirectAccess 狀態通知	電腦設定 \\Windows 設定\ 安全性設定\系	手動	CCE-ID : CCE-3678 6-2

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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	383				統服務\Network Connectivity Assistant		
61	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 384	系統 服務	Network List Service	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	CCE-ID： CCE-3704 3-7
62	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 385	系統 服務	Network Location Awareness	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	CCE-ID： CCE-3677 3-0
63	Windows Server	TWG CB-01	系統 服務	Network Store Interface	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	電腦設定 \Windows 設定\ 安全性設定\系 統服務\Network Store Interface	自動	CCE-ID： CCE-3689

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 DNS Server	-006-0 386		Service	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		9-3
64	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 387	系統 服務	Optimize drives	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	CCE-ID： CCE-3704 8-6
65	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 388	系統 服務	Performance Counter DLL Host	允許遠端使用者和 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	CCE-ID： CCE-3672 2-7

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
66	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 389	系統 服務	Performance Logs & Alerts	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	CCE-ID： CCE-3672 3-5
67	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 390	系統 服務	Plug and Play	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	CCE-ID： CCE-3677 4-8
68	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 391	系統 服務	Portable Device Enumerator Service	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	手動	CCE-ID： CCE-3672 4-3

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-I D	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
						Service		
69	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 392	系統 服務	Power	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	CCE-ID： CCE-3672 5-0
70	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 393	系統 服務	Print Spooler	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	CCE-ID： CCE-3672 6-8
71	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 394	系統 服務	Printer Extensions and 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	電腦設定 \Windows 設定\ 安全性設定\系 統服務\Printer Extensions and	手動	CCE-ID： CCE-3678 7-0

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
						Notifications		
72	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 395	系統 服務	Problem Reports and Solutions Control Panel Support	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	CCE-ID： CCE-3700 1-5
73	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 396	系統 服務	Remote Access Auto Connection Manager	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	CCE-ID： CCE-3704 4-5

項次	GPO	TWG CB-I D	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
74	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 397	系統 服務	Remote Access Connection Manager	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	CCE-ID： CCE-3677 5-5
75	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 398	系統 服務	Remote Desktop Configuration	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	CCE-ID： CCE-3690 1-7
76	Windows Server 2012 R2 DNS	TWG CB-01 -006-0	系統 服務	Remote Desktop Services	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	電腦設定 \\Windows 設定\ 安全性設定\系 統服務\Remote	手動	CCE-ID： CCE-3673 0-0

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-I D	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server	399			「遠端」索引標籤上的核取方塊	Desktop Services		
77	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 400	系統 服務	Remote Desktop Services UserMode Port Redirector	允許重新導向 RDP 連線的印表機/磁碟機/ 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	CCE-ID : CCE-3752 2-0
78	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 401	系統 服務	Remote Procedure Call (RPC)	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	CCE-ID : CCE-3700 2-3

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
79	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 402	系統 服務	Remote Procedure Call (RPC) Locator	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	CCE-ID： CCE-3673 1-8
80	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 403	系統 服務	Remote Registry	啟用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	CCE-ID： CCE-3673 2-6
81	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 404	系統 服務	Resultant Set of Policy Provider	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	手動	CCE-ID： CCE-3673 3-4

項次	GPO	TWG CB-I D	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
						Policy Provider		
82	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 405	系統 服務	Routing and Remote Access	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	CCE-ID : CCE-3673 4-2
83	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 406	系統 服務	RPC Endpoint Mapper	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	CCE-ID : CCE-3700 4-9
84	Windows Server 2012 R2	TWG CB-01 -006-0	系統 服務	Secondary Logon	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	電腦設定 \Windows 設定\ 安全性設定\系	手動	CCE-ID : CCE-3673 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
	DNS Server	407			無法開始	統服務 \Secondary Logon		
85	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 408	系統 服務	Secure Socket Tunneling Protocol Service	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	CCE-ID： CCE-3704 5-2
86	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 409	系統 服務	Security Accounts Manager	啟動此服務即告知其他服務，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	CCE-ID： CCE-3677 6-3

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
87	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 410	系統 服務	Server	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	CCE-ID： CCE-3673 6-7
88	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 411	系統 服務	Shell Hardware Detection	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	CCE-ID： CCE-3666 4-1
89	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 412	系統 服務	Smart Card	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	CCE-ID： CCE-3676 1-5

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
90	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 413	系統 服務	Smart Card Removal Policy	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	CCE-ID： CCE-3666 6-6
91	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 414	系統 服務	SNMP Trap	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	CCE-ID： CCE-3666 7-4
92	Windows Server 2012 R2 DNS	TWG CB-01 -006-0	系統 服務	Software Protection	針對 Windows 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	電腦設定 \\Windows 設定\ 安全性設定\\系 統服務	自動	CCE-ID： CCE-3666 8-2

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-I D	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server	415			停用軟體保護服務	\Software Protection		
93	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 416	系統 服務	Special Administratio n Console Helper	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	CCE-ID： CCE-3698 3-5
94	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 417	系統 服務	Spot Verifier	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	CCE-ID： CCE-3651 8-9
95	Windows Server 2012 R2	TWG CB-01 -006-0	系統 服務	SSDP Discovery	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	電腦設定 \Windows 設定\ 安全性設定\系	已停用	CCE-ID： CCE-3676 2-3

項次	GPO	TWG CB-I D	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	DNS Server	418			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	統服務\SSDP Discovery		
96	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 419	系統 服務	Superfetch	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	CCE-ID： CCE-3682 5-8
97	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 420	系統 服務	System Event Notification Service	可監視系統事件，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	CCE-ID： CCE-3698 4-3
98	Windows	TWG	系統	Task	讓使用者能夠在這台電腦上設定與排定自	電腦設定	自動	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
	Server 2012 R2 DNS Server	CB-01 -006-0 421	服務	Scheduler	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	\\Windows 設定\\ 安全性設定\\系 統服務\\Task Scheduler		CCE-3667 0-8
99	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 422	系統 服務	TCP/IP NetBIOS Helper	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	CCE-ID： CCE-3667 1-6
100	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 423	系統 服務	Telephony	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	CCE-ID： CCE-3667 2-4

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
101	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 424	系統 服務	Themes	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	CCE-ID : CCE-3676 3-1
102	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 425	系統 服務	Thread Ordering Server	在指定的時段中依順序執行一組執行緒	電腦設定 \Windows 設定\ 安全性設定\系 統服務\Thread Ordering Server	手動	CCE-ID : CCE-3667 3-2
103	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 426	系統 服務	UPnP Device Host	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	CCE-ID : CCE-3688 9-4
104	Windows	TWG	系統	User Access	此服務會記錄本機伺服器上所安裝產品與	電腦設定	自動	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
	Server 2012 R2 DNS Server	CB-01 -006-0 427	服務	Logging Service	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 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	\\Windows 設定\ 安全性設定\ 系統服務\User Access Logging Service		CCE-3678 2-1
105	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 428	系統 服務	User Profile Service	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註冊元件將無法接收通知	電腦設定 \\Windows 設定\ 安全性設定\ 系統服務\User Profile Service	自動	CCE-ID： CCE-3667 4-0

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
106	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 429	系統 服務	Virtual Disk	提供磁碟、磁碟區、檔案系統與存放裝置陣列的管理服務	電腦設定 \Windows 設定\ 安全性設定\系 統服務\Virtual Disk	手動	CCE-ID： CCE-3689 0-2
107	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 430	系統 服務	Volume Shadow Copy	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	CCE-ID： CCE-3667 5-7
108	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 431	系統 服務	Windows All-User Install Agent	為所有授權使用者安裝 AppX 套件	電腦設定 \Windows 設定\ 安全性設定\系 統服務 \Windows All-User Install	手動	CCE-ID： CCE-3678 4-7

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
						Agent		
109	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 432	系統 服務	Windows Audio	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	CCE-ID： CCE-3667 7-3
110	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 433	系統 服務	Windows Audio Endpoint Builder	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	CCE-ID： CCE-3676 4-9
111	Windows Server	TWG CB-01	系統 服務	Windows Color System	WcsPlugInService 服務主控協力廠商的 Windows 色彩系統色彩裝置模型，以及色域	電腦設定 \Windows 設定\ 安全性設定\系 統服務 \Windows Color System	手動	CCE-ID： CCE-3667

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 DNS Server	-006-0 434			圖對應模型外掛程式模組。這些外掛程式模組是 Windows 色彩系統基準線色彩裝置及色域圖對應模型的廠商特定延伸。停止或停用 WcsPlugInService 服務將停用此延伸功能，並且 Windows 色彩系統將使用其基準線模組處理，而不會使用廠商想要的處理。這可能會導致色彩呈現方式不正確	安全性設定\系統服務 \Windows Color System		8-1
112	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 435	系統 服務	Windows Driver Foundation-User-mode Driver Framework	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	CCE-ID： CCE-3668 0-7
113	Windows	TWG	系統	Windows	在程式停止運作或停止回應時，允許回報錯	電腦設定	手動	CCE-ID：

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-I D	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	Server 2012 R2 DNS Server	CB-01 -006-0 436	服務	Error Reporting Service	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	\\Windows 設定\ 安全性設定\系 統服務 \\Windows Error Reporting Service		CCE-3673 7-5
114	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 437	系統 服務	Windows Event Collector	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 Vista 事件記錄檔、硬體與啟用 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	CCE-ID： CCE-3677 7-1
115	Windows Server 2012 R2 DNS	TWG CB-01 -006-0 438	系統 服務	Windows Event Log	這個服務管理事件與事件記錄檔。它支援記錄事件、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。它可以使用 XML 與純文字格式來顯示事件。停止這個	電腦設定 \\Windows 設定\ 安全性設定\系 統服務	自動	CCE-ID： CCE-3683 2-4

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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				服務可能危害系統的安全性與可靠性	\Windows Event Log		
116	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 439	系統 服務	Windows Firewall	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	CCE-ID： CCE-3673 8-3
117	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 440	系統 服務	Windows Font Cache Service	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	CCE-ID： CCE-3673 9-1
118	Windows Server	TWG CB-01	系統 服務	Windows Installer	新增、修改及移除以 Windows Installer(*.msi、*.msp)套件形式提供的應用	電腦設定 \Windows 設定\ 	手動	CCE-ID： CCE-3708

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 DNS Server	-006-0 441			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		4-1
119	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 442	系統 服務	Windows Management Instrumentation	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	CCE-ID： CCE-3700 6-4
120	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 443	系統 服務	Windows Modules Installer	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	手動	CCE-ID： CCE-3674 2-5

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
						Installer		
121	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 444	系統 服務	Windows Remote Management (WS-Management)	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 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	電腦設定 \\Windows 設定\\ 安全性設定\\系 統服務 \\Windows Remote Management (WS-Management)	自動	CCE-ID： CCE-3674 5-8

項次	GPO	TWG CB-I D	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
					不會使用/wsman URL 首碼			
122	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 445	系統 服務	Windows Store Service (WSService)	提供「Windows 市集」的基礎結構支援。此服務會視需要啟動，而且若停用此服務，使用「Windows 市集」購買的應用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 \\Windows Store Service (WSService)	手動	CCE-ID： CCE-3678 5-4
123	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 446	系統 服務	Windows Time	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	CCE-ID： CCE-3704 7-8
124	Windows Server 2012 R2	TWG CB-01 -006-0	系統 服務	Windows Update	啟用偵測、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	電腦設定 \\Windows 設定\ 安全性設定\系	手動	CCE-ID： CCE-3703 3-8

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
	DNS Server	447			更新功能。而且程式將無法使用 Windows Update Agent(WUA) API	統服務 \Windows Update		
125	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 448	系統 服務	WinHTTP Web Proxy Auto-Discover y Service	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	CCE-ID： CCE-3651 6-3
126	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 449	系統 服務	Wired AutoConfig	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	電腦設定 \Windows 設定\ 安全性設定\系 統服務\Wired AutoConfig	手動	CCE-ID： CCE-3690 4-1

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
					務影響			
127	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 450	系統 服務	WMI Performance Adapter	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	CCE-ID： CCE-3677 9-7
128	Windows Server 2012 R2 DNS Server	TWG CB-01 -006-0 451	系統 服務	Workstation	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	CCE-ID： CCE-3690 5-8

資料來源：本中心整理

表5 Windows Server 2012 R2 File Server 政府組態基準列表

項次	GPO	TWG CB-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 2012 R2 File Server	TWG CB-01 -006-0 452	系統 服務	Application Experience	在應用程式啟動時，處理應用程式的相容性 快取要求	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Application Experience	手動	CCE-ID： CCE-3689 1-0
2	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 453	系統 服務	Application Identity	判斷並確定應用程式的識別。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-3689 2-8
3	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 454	系統 服務	Application Information	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	CCE-ID： CCE-3668 4-9
4	Windows	TWG	系統	Application	對網際網路連線共用提供協力廠商通訊協	電腦設定	手動	CCE-ID：

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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 2012 R2 File Server	CB-01 -006-0 455	服務	Layer Gateway Service	定外掛程式的支援	\\Windows 設定\ 安全性設定\\系統 服務\\Application Layer Gateway Service		CCE-3698 8-4
5	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 456	系統 服務	Application Management	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	CCE-ID： CCE-3668 5-6
6	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 457	系統 服務	Background Intelligent Transfer Service	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	CCE-ID： CCE-3590 1-8
7	Windows	TWG	系統	Background	控制哪些背景工作可在系統上執行的	電腦設定	自動	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
	Server 2012 R2 File Server	CB-01 -006-0 458	服務	Tasks Infrastructure Service	Windows 基礎結構服務	\\Windows 設定\ 安全性設定\\系統 服務\\Background Tasks Infrastructure Service		CCE-3678 1-3
8	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 459	系統 服務	Base Filtering Engine	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	CCE-ID： CCE-3682 7-4
9	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 460	系統 服務	Certificate Propagation	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	CCE-ID： CCE-3698 9-2
10	Windows	TWG	系統	CNG Key	CNG 金鑰隔離服務裝載於 LSA 處理程序。	電腦設定	手動	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
	Server 2012 R2 File Server	CB-01 -006-0 461	服務	Isolation	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	\\Windows 設定\ 安全性設定\系統 服務\CNG Key Isolation		CCE-3668 9-8
11	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 462	系統 服務	COM+ Event System	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	CCE-ID： CCE-3699 0-0
12	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 463	系統 服務	COM+ System Application	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	CCE-ID： CCE-3669 0-6
13	Windows Server	TWG CB-01	系統 服務	Computer Browser	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	電腦設定 \\Windows 設定\ 	已停用	CCE-ID： CCE-3703

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 File Server	-006-0 464			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	安全性設定\系統 服務\Computer Browser		9-5
14	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 465	系統 服務	Credential Manager	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	CCE-ID： CCE-3676 7-2
15	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 466	系統 服務	Cryptographic Services	<ul style="list-style-type: none"> ▪ 此服務提供三種管理服務： <ul style="list-style-type: none"> ➢ 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 	電腦設定 \Windows 設定\ 安全性設定\系統 服務 \Cryptographic Services	自動	CCE-ID： CCE-3669 1-4

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
					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 2012 R2 File Server	TWG CB-01 -006-0 467	系統 服務	Data Deduplication Service	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	CCE-ID： CCE-3796 6-9
17	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 468	系統 服務	Data Deduplication Volume Shadow Copy Service	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 Copy Service	自動	CCE-ID： CCE-3767 7-2
18	Windows Server	TWG CB-01	系統 服務	DCOM Server	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	電腦設定 \Windows 設定\ 	自動	CCE-ID： CCE-3689

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 File Server	-006-0 469		Process Launcher	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	安全性設定\系統 服務\DCOM Server Process Launcher		3-6
19	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 470	系統 服務	Device Association Service	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	CCE-ID： CCE-3651 7-1
20	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 471	系統 服務	Device Install Service	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\Device Install Service	手動	CCE-ID： CCE-3683 3-2
21	Windows Server	TWG CB-01	系統 服務	Device Setup Manager	啟用裝置相關軟體的偵測、下載及安裝。如果停用此服務，裝置可能會以過期的軟體設	電腦設定 \Windows 設定\ 	手動	CCE-ID： CCE-3678

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 File Server	-006-0 472			定，且可能無法正常運作	安全性設定\系統 服務\Device Setup Manager		3-9
22	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 473	系統 服務	DFS Namespace	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	CCE-ID： CCE-3669 2-2
23	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 474	系統 服務	DFS Replication	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	CCE-ID： CCE-3687 0-4
24	Windows Server 2012 R2 File	TWG CB-01 -006-0 475	系統 服務	DHCP Client	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	電腦設定 \Windows 設定\ 安全性設定\系統 服務\DHCP	自動	CCE-ID： CCE-3669 3-0

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
	Server				啟動	Client		
25	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 476	系統 服務	Diagnostic Policy Service	▪ 診斷原則服務能夠偵測 Windows 元件的問題、進行疑難排解與提供解決方案。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	CCE-ID： CCE-3699 1-8
26	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 477	系統 服務	Diagnostic Service Host	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	CCE-ID： CCE-2515 8-7
27	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 478	系統 服務	Diagnostic System Host	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	CCE-ID： CCE-3704 0-3
28	Windows	TWG	系統	Distributed	維護電腦中或網路中不同電腦之 NTFS 檔案	電腦設定	自動	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
	Server 2012 R2 File Server	CB-01 -006-0 479	服務	Link Tracking Client	間的連結	\\Windows 設定\ 安全性設定\\系統 服務\\Distributed Link Tracking Client		CCE-3699 2-6
29	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 480	系統 服務	Distributed Transaction Coordinator	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	電腦設定 \\Windows 設定\ 安全性設定\\系統 服務\\Distributed Transaction Coordinator	自動	CCE-ID： CCE-3685 9-7
30	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 481	系統 服務	DNS Client	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	CCE-ID： CCE-3669 7-1

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
31	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 482	系統 服務	Encrypting File System (EFS)	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	CCE-ID： CCE-3682 8-2
32	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 483	系統 服務	Extensible Authenticatio n Protocol	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	CCE-ID： CCE-3669 8-9
33	Windows Server 2012 R2 File	TWG CB-01 -006-0 484	系統 服務	File Server Resource Manager	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。它可控制配額、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	電腦設定 \\Windows 設定\ 安全性設定\\系統 服務\\File Server Resource	自動	CCE-ID： CCE-3699 4-2

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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				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	Manager		
34	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 485	系統 服務	File Server Storage Reports Manager	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	電腦設定 \Windows 設定\ 安全性設定\系統 服務\File Server Storage Reports Manager	手動	CCE-ID： CCE-3670 1-1
35	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 486	系統 服務	Function Discovery Provider Host	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 以及依賴這些探索通訊協定的網路服務將找不到網	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Function Discovery Provider Host	手動	CCE-ID： CCE-3704 1-1

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
					路裝置或資源			
36	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 487	系統 服務	Function Discovery Resource Publication	發佈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，便不再發佈網路資源，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	CCE-ID： CCE-3676 9-8
37	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 488	系統 服務	Group Policy Client	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	CCE-ID： CCE-3670 2-9
38	Windows Server	TWG CB-01	系統 服務	Health Key and	提供網路存取保護代理程式(NAPAagent)的X.509 憑證與金鑰管理服務。不使用此服	電腦設定 \Windows 設定\ 	手動	CCE-ID： CCE-3689

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 File Server	-006-0 489		Certificate Management	務，使用 X.509 憑證的強制隔離技術將無法 正常運作	安全性設定\系統 服務\Health Key and Certificate Management		5-1
39	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 490	系統 服務	Human Interface Device Service	啟用並維護鍵盤、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	CCE-ID： CCE-3670 3-7
40	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 491	系統 服務	Hyper-V Data Exchange Service	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	CCE-ID： CCE-3834 2-2
41	Windows	TWG	系統	Hyper-V	提供從實體電腦的管理介面關閉這個虛擬	電腦設定	手動	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
	Server 2012 R2 File Server	CB-01 -006-0 492	服務	Guest Shutdown Service	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		CCE-3723 1-8
42	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 493	系統 服務	Hyper-V Heartbeat Service	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	CCE-ID : CCE-3806 6-7
43	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 494	系統 服務	Hyper-V Remote Desktop Virtualization Service	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	CCE-ID : CCE-3718 3-1

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
44	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 495	系統 服務	Hyper-V Time Synchronizati on Service	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	CCE-ID : CCE-3815 7-4
45	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 496	系統 服務	Hyper-V Volume Shadow Copy Requestor	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	CCE-ID : CCE-3588 1-2
46	Windows Server 2012 R2 File	TWG CB-01 -006-0 497	系統 服務	IKE and AuthIP IPsec Keying Modules	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	電腦設定 \Windows 設定\ 安全性設定\系統 服務\IKE and AuthIP IPsec	手動	CCE-ID : CCE-3677 0-6

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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				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		
47	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 498	系統 服務	Interactive Services Detection	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	CCE-ID： CCE-3682 9-0
48	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 499	系統 服務	Internet Connection Sharing (ICS)	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	已停用	CCE-ID： CCE-3670 7-8

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
						Sharing (ICS)		
49	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 500	系統 服務	IP Helper	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	CCE-ID： CCE-3670 9-4
50	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 501	系統 服務	IPsec Policy Agent	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)，以及重新執行保護。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	電腦設定 \Windows 設定\ 安全性設定\系統 服務\IPsec Policy Agent	手動	CCE-ID： CCE-3699 6-7
51	Windows Server	TWG CB-01	系統 服務	KDC Proxy Server service	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	電腦設定 \Windows 設定\ 安全性設定\系統 服務\KDC Proxy Server service	手動	CCE-ID： CCE-3700

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 File Server	-006-0 502		(KPS)	理到公司網路上的網域控制站	安全性設定\系統 服務\KDC Proxy Server service (KPS)		9-8
52	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 503	系統 服務	KtmRm for Distributed Transaction Coordinator	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	CCE-ID： CCE-3639 2-9
53	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 504	系統 服務	Link-Layer Topology Discovery Mapper	<ul style="list-style-type: none"> ▪ 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及裝置的中繼資料 ▪ 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	CCE-ID： CCE-3677 1-4

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
54	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 505	系統 服務	Local Session Manager	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	CCE-ID： CCE-3701 0-6
55	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 506	系統 服務	Microsoft File Server Shadow Copy Agent Service	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	CCE-ID： CCE-3781 9-0
56	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 507	系統 服務	Microsoft iSCSI Initiator Service	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	手動	CCE-ID： CCE-3671 3-6

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
						Service		
57	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 508	系統 服務	Microsoft iSCSI Software Target	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 Software Target	自動	CCE-ID： CCE-3685 4-8
58	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 509	系統 服務	Microsoft Software Shadow Copy Provider	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	CCE-ID： CCE-3671 4-4
59	Windows Server 2012 R2 File	TWG CB-01 -006-0 510	系統 服務	Multimedia Class Scheduler	根據整個系統的工作優先順序啟用相關的工作優先順序。主要的目標是多媒體應用程式。如果這個服務停止，個別的工作會回復為預設的優先順序	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Multimedia	手動	CCE-ID： CCE-3671 5-1

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
	Server					Class Scheduler		
60	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 511	系統 服務	Net.Tcp Port Sharing Service	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	CCE-ID： CCE-3671 6-9
61	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 512	系統 服務	Netlogon	維持這個電腦與網域控制站間用於驗證使用者及服務的安全通道。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	CCE-ID： CCE-3671 7-7
62	Windows Server 2012 R2 File	TWG CB-01 -006-0 513	系統 服務	Network Access Protection Agent	網路存取保護(NAP)代理程式服務會蒐集與管理網路上之用戶端電腦的健康情況資訊。NAP 代理程式蒐集的資訊是用來確定用戶端電腦具有必要的軟體與設定。如果用戶	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Network	手動	CCE-ID： CCE-3699 9-1

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
	Server				端電腦與健康原則不相容，則用戶端電腦在其設定更新之前，只會具有有限的網路存取權。而根據健康原則的設定，可能會自動更新用戶端電腦，這樣使用者就可以快速重新取得完整的網路存取權，而不需要手動更新他們的電腦	Access Protection Agent		
63	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 514	系統 服務	Network Connections	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	CCE-ID： CCE-3671 8-5
64	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 515	系統 服務	Network Connectivity Assistant	提供 UI 元件的 DirectAccess 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	CCE-ID： CCE-3678 6-2

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
65	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 516	系統 服務	Network List Service	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	CCE-ID： CCE-3704 3-7
66	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 517	系統 服務	Network Location Awareness	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	CCE-ID： CCE-3677 3-0
67	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 518	系統 服務	Network Store Interface Service	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	CCE-ID： CCE-3689 9-3

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
68	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 519	系統 服務	Optimize drives	<ul style="list-style-type: none"> 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	CCE-ID： CCE-3704 8-6
69	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 520	系統 服務	Performance Counter DLL Host	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	CCE-ID： CCE-3672 2-7
70	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 521	系統 服務	Performance Logs & Alerts	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	手動	CCE-ID： CCE-3672 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
						Logs & Alerts		
71	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 522	系統 服務	Plug and Play	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	CCE-ID： CCE-3677 4-8
72	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 523	系統 服務	Portable Device Enumerator Service	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	CCE-ID： CCE-3672 4-3
73	Windows Server 2012 R2 File	TWG CB-01 -006-0 524	系統 服務	Power	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	CCE-ID： CCE-3672 5-0

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
	Server							
74	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 525	系統 服務	Print Spooler	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	CCE-ID： CCE-3672 6-8
75	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 526	系統 服務	Printer Extensions and 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	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Printer Extensions and Notifications	手動	CCE-ID： CCE-3678 7-0
76	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 527	系統 服務	Problem Reports and Solutions Control Panel Support	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	手動	CCE-ID： CCE-3700 1-5

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
						Solutions Control Panel Support		
77	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 528	系統 服務	Remote Access Auto Connection Manager	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	CCE-ID： CCE-3704 4-5
78	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 529	系統 服務	Remote Access Connection Manager	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	CCE-ID： CCE-3677 5-5
79	Windows	TWG	系統	Remote	遠端桌面設定服務(RDCS)負責處理與遠端	電腦設定	手動	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
	Server 2012 R2 File Server	CB-01 -006-0 530	服務	Desktop Configuration	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	\\Windows 設定\ 安全性設定\系統 服務\Remote Desktop Configuration		CCE-3690 1-7
80	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 531	系統 服務	Remote Desktop Services	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	CCE-ID： CCE-3673 0-0
81	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 532	系統 服務	Remote Desktop Services UserMode Port Redirector	允許重新導向 RDP 連線的印表機/磁碟機/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	CCE-ID： CCE-3752 2-0

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
82	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 533	系統 服務	Remote Procedure Call (RPC)	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	CCE-ID： CCE-3700 2-3
83	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 534	系統 服務	Remote Procedure Call (RPC) Locator	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	CCE-ID： CCE-3673 1-8
84	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 535	系統 服務	Remote Registry	啟用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	自動	CCE-ID： CCE-3673 2-6

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
	Server					Registry		
85	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 536	系統 服務	Resultant Set of Policy Provider	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	CCE-ID： CCE-3673 3-4
86	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 537	系統 服務	Routing and Remote Access	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	CCE-ID： CCE-3673 4-2
87	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 538	系統 服務	RPC Endpoint Mapper	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	CCE-ID： CCE-3700 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
88	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 539	系統 服務	Secondary Logon	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	CCE-ID： CCE-3673 5-9
89	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 540	系統 服務	Secure Socket Tunneling Protocol Service	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	CCE-ID： CCE-3704 5-2
90	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 541	系統 服務	Security Accounts Manager	啟動此服務即告知其他服務，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	CCE-ID： CCE-3677 6-3

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
91	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 542	系統 服務	Server	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	CCE-ID： CCE-3673 6-7
92	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 543	系統 服務	Shell Hardware Detection	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	CCE-ID： CCE-3666 4-1
93	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 544	系統 服務	Smart Card	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	CCE-ID： CCE-3676 1-5
94	Windows	TWG	系統	Smart Card	允許將系統設定為在智慧卡移除時，鎖定使	電腦設定	手動	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
	Server 2012 R2 File Server	CB-01 -006-0 545	服務	Removal Policy	用者桌面	\\Windows 設定\ 安全性設定\系統 服務\Smart Card Removal Policy		CCE-3666 6-6
95	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 546	系統 服務	SNMP Trap	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	CCE-ID： CCE-3666 7-4
96	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 547	系統 服務	Software Protection	針對 Windows 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	CCE-ID： CCE-3666 8-2
97	Windows	TWG	系統	Special	允取系統管理員使用緊急管理服務，遠端存	電腦設定	手動	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
	Server 2012 R2 File Server	CB-01 -006-0 548	服務	Administratio n Console Helper	取命令提示字元	\\Windows 設定\ 安全性設定\\系統 服務\\Special Administration Console Helper		CCE-3698 3-5
98	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 549	系統 服務	Spot Verifier	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	CCE-ID : CCE-3651 8-9
99	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 550	系統 服務	SSDP Discovery	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	CCE-ID : CCE-3676 2-3
100	Windows	TWG	系統	Superfetch	維護與改進一段時間後的系統效能	電腦設定	手動	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
	Server 2012 R2 File Server	CB-01 -006-0 551	服務			\Windows 設定\ 安全性設定\系統 服務\Superfetch		CCE-3682 5-8
101	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 552	系統 服務	System Event Notification Service	可監視系統事件，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	CCE-ID： CCE-3698 4-3
102	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 553	系統 服務	Task Scheduler	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	CCE-ID： CCE-3667 0-8

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
103	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 554	系統 服務	TCP/IP NetBIOS Helper	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	CCE-ID： CCE-3667 1-6
104	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 555	系統 服務	Telephony	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	CCE-ID： CCE-3667 2-4
105	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 556	系統 服務	Themes	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	CCE-ID： CCE-3676 3-1
106	Windows	TWG	系統	Thread	在指定的時段中依順序執行一組執行緒	電腦設定	手動	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
	Server 2012 R2 File Server	CB-01 -006-0 557	服務	Ordering Server		\\Windows 設定\ 安全性設定\系統 服務\Thread Ordering Server		CCE-3667 3-2
107	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 558	系統 服務	UPnP Device Host	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	CCE-ID： CCE-3688 9-4
108	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 559	系統 服務	User Access Logging Service	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 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	電腦設定 \\Windows 設定\ 安全性設定\系統 服務\User Access Logging Service	自動	CCE-ID： CCE-3678 2-1

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
					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			
109	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 560	系統 服務	User Profile Service	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註冊元件將無法接收通知	電腦設定 \Windows 設定\ 安全性設定\系統 服務\User Profile Service	自動	CCE-ID： CCE-3667 4-0
110	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 561	系統 服務	Virtual Disk	提供磁碟、磁碟區、檔案系統與存放裝置陣列的管理服務	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Virtual Disk	手動	CCE-ID： CCE-3689 0-2
111	Windows Server 2012 R2	TWG CB-01 -006-0	系統 服務	Volume Shadow Copy	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	電腦設定 \Windows 設定\ 安全性設定\系統	手動	CCE-ID： CCE-3667 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
	File Server	562			個服務被停用，任何明確依存於它的服務將無法啟動	服務\Volume Shadow Copy		
112	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 563	系統 服務	Windows All-User Install Agent	為所有授權使用者安裝 AppX 套件	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Windows All-User Install Agent	手動	CCE-ID： CCE-3678 4-7
113	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 564	系統 服務	Windows Audio	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	CCE-ID： CCE-3667 7-3
114	Windows Server 2012 R2 File	TWG CB-01 -006-0 565	系統 服務	Windows Audio Endpoint Builder	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	手動	CCE-ID： CCE-3676 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
	Server					Audio Endpoint Builder		
115	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 566	系統 服務	Windows Color System	WcsPlugInService 服務主控協力廠商的 Windows 色彩系統色彩裝置模型，以及色域圖對應模型外掛程式模組。這些外掛程式模組是 Windows 色彩系統基準線色彩裝置及色域圖對應模型的廠商特定延伸。停止或停用 WcsPlugInService 服務將停用此延伸功能，並且 Windows 色彩系統將使用其基準線模組處理，而不會使用廠商想要的處理。這可能會導致色彩呈現方式不正確	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Windows Color System	手動	CCE-ID： CCE-3667 8-1
116	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 567	系統 服務	Windows Driver Foundation-U ser-mode Driver Framework	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	手動	CCE-ID： CCE-3668 0-7

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
						Framework		
117	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 568	系統 服務	Windows Error Reporting Service	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	CCE-ID： CCE-3673 7-5
118	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 569	系統 服務	Windows Event Collector	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 Vista 事件記錄檔、硬體與啟用 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	CCE-ID： CCE-3677 7-1
119	Windows Server 2012 R2	TWG CB-01 -006-0	系統 服務	Windows Event Log	這個服務管理事件與事件記錄檔。它支援記錄事件、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。它可以使用	電腦設定 \Windows 設定\ 安全性設定\系統	自動	CCE-ID： CCE-3683 2-4

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
	File Server	570			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	服務\Windows Event Log		
120	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 571	系統 服務	Windows Firewall	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	CCE-ID : CCE-3673 8-3
121	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 572	系統 服務	Windows Font Cache Service	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	CCE-ID : CCE-3673 9-1
122	Windows Server 2012 R2 File	TWG CB-01 -006-0 573	系統 服務	Windows Installer	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	手動	CCE-ID : CCE-3708 4-1

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
	Server					Installer		
123	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 574	系統 服務	Windows Management Instrumentation	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	CCE-ID： CCE-3700 6-4
124	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 575	系統 服務	Windows Modules Installer	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	CCE-ID： CCE-3674 2-5
125	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 576	系統 服務	Windows Remote Management (WS-Management)	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	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Windows Remote	自動	CCE-ID： CCE-3674 5-8

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
					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	Management (WS-Management)		
126	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 577	系統 服務	Windows Store Service (WSService)	提供「Windows 市集」的基礎結構支援。此服務會視需要啟動，而且若停用此服務，使用「Windows 市集」購買的應用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\Windows Store Service (WSService)	手動	CCE-ID： CCE-3678 5-4

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
127	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 578	系統 服務	Windows Time	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	CCE-ID： CCE-3704 7-8
128	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 579	系統 服務	Windows Update	啟用偵測、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	CCE-ID： CCE-3703 3-8
129	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 580	系統 服務	WinHTTP Web Proxy Auto-Discover y Service	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	CCE-ID： CCE-3651 6-3

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
130	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 581	系統 服務	Wired AutoConfig	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	CCE-ID： CCE-3690 4-1
131	Windows Server 2012 R2 File Server	TWG CB-01 -006-0 582	系統 服務	WMI Performance Adapter	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	CCE-ID： CCE-3677 9-7
132	Windows Server 2012 R2 File	TWG CB-01 -006-0 583	系統 服務	Workstation	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	CCE-ID： CCE-3690 5-8

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
	Server							

資料來源：本中心整理

表6 Windows Server 2012 R2 Web Server 政府組態基準列表

項次	GPO	TWG CB-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 2012 R2 Web Server	TWG CB-01-006-0584	系統服務	Application Experience	在應用程式啟動時，處理應用程式的相容性快取要求	電腦設定\ Windows 設定\ 安全性設定\系統服務\Application Experience	手動	CCE-ID : CCE-3689 1-0
2	Windows Server 2012 R2 Web Server	TWG CB-01-006-0585	系統服務	Application Host Helper Service	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	CCE-ID : CCE-3668 3-1
3	Windows Server 2012 R2 Web Server	TWG CB-01-006-0586	系統服務	Application Identity	判斷並確定應用程式的識別。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-3689 2-8

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
4	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 587	系統 服務	Application Information	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	CCE-ID： CCE-3668 4-9
5	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 588	系統 服務	Application Layer Gateway Service	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	CCE-ID： CCE-3698 8-4
6	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 589	系統 服務	Application Management	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	CCE-ID： CCE-3668 5-6
7	Windows	TWG	系統	ASP.NET	提供 ASP.NET 所需跨處理序	電腦設定	手動	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
	Server 2012 R2 Web Server	CB-01 -006-0 590	服務	State Service	(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	\\Windows 設定\ 安全性設定\系統 服務\ASP.NET State Service		CCE-3668 6-4
8	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 591	系統 服務	Background Intelligent Transfer Service	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	CCE-ID： CCE-3590 1-8
9	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 592	系統 服務	Background Tasks Infrastructure Service	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	CCE-ID： CCE-3678 1-3

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
10	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 593	系統 服務	Base Filtering Engine	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	CCE-ID： CCE-3682 7-4
11	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 594	系統 服務	Certificate Propagation	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	CCE-ID： CCE-3698 9-2
12	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 595	系統 服務	CNG Key Isolation	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	CCE-ID： CCE-3668 9-8
13	Windows Server	TWG CB-01	系統 服務	COM+ Event System	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	電腦設定 \Windows 設定\ 	自動	CCE-ID： CCE-3699

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 Web Server	-006-0 596			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	安全性設定\系統 服務\COM+ Event System		0-0
14	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 597	系統 服務	COM+ System Application	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	CCE-ID： CCE-3669 0-6
15	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 598	系統 服務	Computer Browser	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	CCE-ID： CCE-3703 9-5
16	Windows Server 2012 R2	TWG CB-01 -006-0	系統 服務	Credential Manager	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	手動	CCE-ID： CCE-3676 7-2

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
	Web Server	599				服務\Credential Manager		
17	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 600	系統 服務	Cryptographi c Services	<ul style="list-style-type: none"> ▪ 此服務提供三種管理服務： <ul style="list-style-type: none"> ➢ 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，任何明確需要它的服務將無法啟動 	電腦設定 \Windows 設定\ 安全性設定\系統 服務 \Cryptographic Services	自動	CCE-ID： CCE-3669 1-4
18	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 601	系統 服務	DCOM Server Process Launcher	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	自動	CCE-ID： CCE-3689 3-6

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
						Launcher		
19	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 602	系統 服務	Device Association Service	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	CCE-ID： CCE-3651 7-1
20	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 603	系統 服務	Device Install Service	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\Device Install Service	手動	CCE-ID： CCE-3683 3-2
21	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 604	系統 服務	Device Setup Manager	啟用裝置相關軟體的偵測、下載及安裝。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	CCE-ID： CCE-3678 3-9

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
22	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 605	系統 服務	DHCP Client	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	CCE-ID： CCE-3669 3-0
23	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 606	系統 服務	Diagnostic Policy Service	診斷原則服務能夠偵測 Windows 元件的問題、進行疑難排解與提供解決方案。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	CCE-ID： CCE-3699 1-8
24	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 607	系統 服務	Diagnostic Service Host	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	CCE-ID： CCE-2515 8-7
25	Windows Server	TWG CB-01	系統 服務	Diagnostic System Host	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	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Diagnostic System Host	手動	CCE-ID： CCE-3704

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 Web Server	-006-0 608			務已停止，其上的任何診斷將不再產生作用	安全性設定\系統 服務\Diagnostic System Host		0-3
26	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 609	系統 服務	Distributed Link Tracking Client	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	CCE-ID： CCE-3699 2-6
27	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 610	系統 服務	Distributed Transaction Coordinator	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	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Distributed Transaction Coordinator	自動	CCE-ID： CCE-3685 9-7
28	Windows Server	TWG CB-01	系統 服務	DNS Client	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	電腦設定 \Windows 設定\ 	自動	CCE-ID： CCE-3669

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 Web Server	-006-0 611			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	安全性設定\系統 服務\DNS Client		7-1
29	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 612	系統 服務	Encrypting File System (EFS)	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	CCE-ID： CCE-3682 8-2
30	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 613	系統 服務	Extensible Authenticatio n Protocol	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	CCE-ID： CCE-3669 8-9

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
31	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 614	系統 服務	Function Discovery Provider Host	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 以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	CCE-ID： CCE-3704 1-1
32	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 615	系統 服務	Function Discovery Resource Publication	發佈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，便不再發佈網路資源，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	CCE-ID： CCE-3676 9-8
33	Windows Server	TWG CB-01	系統	Group Policy	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	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Function Discovery Resource Publication	自動	CCE-ID： CCE-3670

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 Web Server	-006-0 616	服務	Client	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	安全性設定\系統 服務\Group Policy Client		2-9
34	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 617	系統 服務	Health Key and Certificate Management	提供網路存取保護代理程式(NAPAgent)的 X.509 憑證與金鑰管理服務。不使用此服務，使用 X.509 憑證的強制隔離技術將無法正常運作	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Health Key and Certificate Management	手動	CCE-ID： CCE-3689 5-1
35	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 618	系統 服務	Human Interface Device Service	啟用並維護鍵盤、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	CCE-ID： CCE-3670 3-7

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
36	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 619	系統 服務	Hyper-V Data Exchange Service	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	CCE-ID： CCE-3834 2-2
37	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 620	系統 服務	Hyper-V Guest Shutdown Service	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	CCE-ID： CCE-3723 1-8
38	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 621	系統 服務	Hyper-V Heartbeat Service	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	CCE-ID： CCE-3806 6-7

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
39	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 622	系統 服務	Hyper-V Remote Desktop Virtualization Service	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	CCE-ID： CCE-3718 3-1
40	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 623	系統 服務	Hyper-V Time Synchronizati on Service	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	CCE-ID： CCE-3815 7-4
41	Windows Server 2012 R2 Web	TWG CB-01 -006-0	系統 服務	Hyper-V Volume Shadow Copy	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	手動	CCE-ID： CCE-3588 1-2

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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	624		Requestor		Volume Shadow Copy Requestor		
42	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 625	系統 服務	IKE and AuthIP IPsec Keying Modules	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。強烈建議持續執行 IKEEXT 服務	電腦設定 \Windows 設定\ 安全性設定\系統 服務\IKE and AuthIP IPsec Keying Modules	手動	CCE-ID： CCE-3677 0-6
43	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 626	系統 服務	Interactive Services Detection	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。	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Interactive Services	手動	CCE-ID： CCE-3682 9-0

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
					如果此服務停用，新互動服務對話方塊的通知及存取功能都無法再運作	Detection		
44	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 627	系統 服務	Internet Connection Sharing (ICS)	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	CCE-ID： CCE-3670 7-8
45	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 628	系統 服務	IP Helper	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	CCE-ID： CCE-3670 9-4
46	Windows Server 2012 R2 Web	TWG CB-01 -006-0 629	系統 服務	IPsec Policy Agent	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)，以及重新執行保護。此服務會強制執行透過 IP 安全性原則嵌入式	電腦設定 \Windows 設定\ 安全性設定\系統 服務\IPsec Policy	手動	CCE-ID： CCE-3699 6-7

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
	Server				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	Agent		
47	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 630	系統 服務	KDC Proxy Server service (KPS)	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	CCE-ID： CCE-3700 9-8
48	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 631	系統 服務	KtmRm for Distributed Transaction Coordinator	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	CCE-ID： CCE-3639 2-9

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
49	Windows Server 2012 R2 Web Server	TWG CB-01-006-0632	系統服務	Link-Layer Topology Discovery Mapper	<ul style="list-style-type: none"> ▪ 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及裝置的中繼資料 ▪ 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	CCE-ID : CCE-3677 1-4
50	Windows Server 2012 R2 Web Server	TWG CB-01-006-0633	系統服務	Local Session Manager	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	CCE-ID : CCE-3701 0-6
51	Windows Server 2012 R2 Web Server	TWG CB-01-006-0634	系統服務	Microsoft iSCSI Initiator Service	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	手動	CCE-ID : CCE-3671 3-6

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
						Service		
52	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 635	系統 服務	Microsoft Software Shadow Copy Provider	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	CCE-ID： CCE-3671 4-4
53	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 636	系統 服務	Multimedia Class Scheduler	根據整個系統的工作優先順序啟用相關的工作優先順序。主要的目標是多媒體應用程式。如果這個服務停止，個別的工作會回復為預設的優先順序	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Multimedia Class Scheduler	手動	CCE-ID： CCE-3671 5-1
54	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 637	系統 服務	Net.Tcp Port Sharing Service	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	已停用	CCE-ID： CCE-3671 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
						Service		
55	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 638	系統 服務	Netlogon	維持這個電腦與網域控制站間用於驗證使用者及服務的安全通道。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	CCE-ID： CCE-3671 7-7
56	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 639	系統 服務	Network Access Protection Agent	網路存取保護(NAP)代理程式服務會蒐集與管理網路上之用戶端電腦的健康情況資訊。NAP 代理程式蒐集的資訊是用來確定用戶端電腦具有必要的軟體與設定。如果用戶端電腦與健康原則不相容，則用戶端電腦在其設定更新之前，只會具有有限的網路存取權。而根據健康原則的設定，可能會自動更新用戶端電腦，這樣使用者就可以快速重新取得完整的網路存取權，而不需要手動更新他們的電腦	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Network Access Protection Agent	手動	CCE-ID： CCE-3699 9-1

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
57	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 640	系統 服務	Network Connections	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	CCE-ID： CCE-3671 8-5
58	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 641	系統 服務	Network Connectivity Assistant	提供 UI 元件的 DirectAccess 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	CCE-ID： CCE-3678 6-2
59	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 642	系統 服務	Network List Service	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	CCE-ID： CCE-3704 3-7
60	Windows	TWG	系統	Network	蒐集及儲存網路的設定資訊，並且在修改此	電腦設定	自動	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
	Server 2012 R2 Web Server	CB-01 -006-0 643	服務	Location Awareness	資訊時，通知程式。如果停止此服務，設定資訊就可能無法使用。如果停用此服務，則明確依賴它的任何服務將會無法啟動	\\Windows 設定\ 安全性設定\\系統 服務\\Network Location Awareness		CCE-3677 3-0
61	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 644	系統 服務	Network Store Interface Service	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	CCE-ID： CCE-3689 9-3
62	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 645	系統 服務	Optimize drives	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	CCE-ID： CCE-3704 8-6
63	Windows	TWG	系統	Performance	允許遠端使用者與 64 位元處理程序查詢 32	電腦設定	手動	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
	Server 2012 R2 Web Server	CB-01 -006-0 646	服務	Counter DLL Host	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	\\Windows 設定\ 安全性設定\\系統 服務 \\Performance Counter DLL Host		CCE-3672 2-7
64	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 647	系統 服務	Performance Logs & Alerts	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	CCE-ID： CCE-3672 3-5
65	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 648	系統 服務	Plug and Play	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	CCE-ID： CCE-3677 4-8

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
66	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 649	系統 服務	Portable Device Enumerator Service	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	CCE-ID： CCE-3672 4-3
67	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 650	系統 服務	Power	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	CCE-ID： CCE-3672 5-0
68	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 651	系統 服務	Print Spooler	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	CCE-ID： CCE-3672 6-8

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
69	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 652	系統 服務	Printer Extensions and 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	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Printer Extensions and Notifications	手動	CCE-ID： CCE-3678 7-0
70	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 653	系統 服務	Problem Reports and Solutions Control Panel Support	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	CCE-ID： CCE-3700 1-5
71	Windows Server 2012 R2 Web	TWG CB-01 -006-0 654	系統 服務	Remote Access Auto Connection Manager	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	手動	CCE-ID： CCE-3704 4-5

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	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					Connection Manager		
72	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 655	系統 服務	Remote Access Connection Manager	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	CCE-ID： CCE-3677 5-5
73	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 656	系統 服務	Remote Desktop Configuration	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	CCE-ID： CCE-3690 1-7
74	Windows Server	TWG CB-01	系統 服務	Remote Desktop	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	電腦設定 \Windows 設定\ 	手動	CCE-ID： CCE-3673

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 Web Server	-006-0 657		Services	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	安全性設定\系統 服務\Remote Desktop Services		0-0
75	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 658	系統 服務	Remote Desktop Services UserMode Port Redirector	允許重新導向 RDP 連線的印表機/磁碟機/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	CCE-ID： CCE-3752 2-0
76	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 659	系統 服務	Remote Procedure Call (RPC)	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	CCE-ID： CCE-3700 2-3
77	Windows	TWG	系統	Remote	在 Windows 2003 以及更舊的 Windows 版本	電腦設定	手動	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
	Server 2012 R2 Web Server	CB-01 -006-0 660	服務	Procedure Call (RPC) Locator	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		CCE-3673 1-8
78	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 661	系統 服務	Remote Registry	啟用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	CCE-ID： CCE-3673 2-6
79	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 662	系統 服務	Resultant Set of Policy Provider	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	CCE-ID： CCE-3673 3-4
80	Windows	TWG	系統	Routing and	提供連到區域網路及廣域網路的公司的路由	電腦設定	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
	Server 2012 R2 Web Server	CB-01 -006-0 663	服務	Remote Access	服務	\\Windows 設定\ 安全性設定\\系統 服務\\Routing and Remote Access		CCE-3673 4-2
81	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 664	系統 服務	RPC Endpoint Mapper	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	CCE-ID： CCE-3700 4-9
82	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 665	系統 服務	Secondary Logon	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	CCE-ID： CCE-3673 5-9
83	Windows Server 2012 R2	TWG CB-01 -006-0	系統 服務	Secure Socket Tunneling	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	手動	CCE-ID： CCE-3704 5-2

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
	Web Server	666		Protocol Service	器	服務\Secure Socket Tunneling Protocol Service		
84	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 667	系統 服務	Security Accounts Manager	啟動此服務即告知其他服務，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	CCE-ID： CCE-3677 6-3
85	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 668	系統 服務	Server	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	CCE-ID： CCE-3673 6-7
86	Windows Server 2012 R2	TWG CB-01 -006-0	系統 服務	Shell Hardware Detection	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	自動	CCE-ID： CCE-3666 4-1

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
	Web Server	669				服務\Shell Hardware Detection		
87	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 670	系統 服務	Smart Card	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	CCE-ID： CCE-3676 1-5
88	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 671	系統 服務	Smart Card Removal Policy	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	CCE-ID： CCE-3666 6-6
89	Windows Server 2012 R2 Web	TWG CB-01 -006-0 672	系統 服務	SNMP Trap	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	電腦設定 \Windows 設定\ 安全性設定\系統 服務\SNMP Trap	手動	CCE-ID： CCE-3666 7-4

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
	Server				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			
90	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 673	系統 服務	Software Protection	針對 Windows 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	CCE-ID： CCE-3666 8-2
91	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 674	系統 服務	Special Administratio n Console Helper	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	CCE-ID： CCE-3698 3-5
92	Windows Server 2012 R2	TWG CB-01 -006-0	系統 服務	Spot Verifier	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	手動	CCE-ID： CCE-3651 8-9

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
	Web Server	675				服務\Spot Verifier		
93	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 676	系統 服務	SSDP Discovery	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	CCE-ID： CCE-3676 2-3
94	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 677	系統 服務	Superfetch	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	CCE-ID： CCE-3682 5-8
95	Windows Server 2012 R2 Web	TWG CB-01 -006-0 678	系統 服務	System Event Notification Service	可監視系統事件，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	自動	CCE-ID： CCE-3698 4-3

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
	Server					Event Notification Service		
96	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 679	系統 服務	Task Scheduler	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	CCE-ID： CCE-3667 0-8
97	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 680	系統 服務	TCP/IP NetBIOS Helper	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	CCE-ID： CCE-3667 1-6
98	Windows Server	TWG CB-01	系統 服務	Telephony	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	電腦設定 \Windows 設定\ 	手動	CCE-ID： CCE-3667

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 Web Server	-006-0 681			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	安全性設定\系統 服務\Telephony		2-4
99	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 682	系統 服務	Themes	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	CCE-ID : CCE-3676 3-1
100	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 683	系統 服務	Thread Ordering Server	在指定的時段中依順序執行一組執行緒	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Thread Ordering Server	手動	CCE-ID : CCE-3667 3-2
101	Windows Server 2012 R2 Web	TWG CB-01 -006-0 684	系統 服務	UPnP Device Host	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	電腦設定 \Windows 設定\ 安全性設定\系統 服務\UPnP	已停用	CCE-ID : CCE-3688 9-4

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
	Server				法啟動	Device Host		
102	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 685	系統 服務	User Access Logging Service	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 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	電腦設定 \Windows 設定\ 安全性設定\系統 服務\User Access Logging Service	自動	CCE-ID : CCE-3678 2-1
103	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 686	系統 服務	User Profile Service	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註冊元件將無法接收通知	電腦設定 \Windows 設定\ 安全性設定\系統 服務\User Profile Service	自動	CCE-ID : CCE-3667 4-0

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
104	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 687	系統 服務	Virtual Disk	提供磁碟、磁碟區、檔案系統與存放裝置陣列的管理服務	電腦設定 \\Windows 設定\ 安全性設定\\系統 服務\\Virtual Disk	手動	CCE-ID： CCE-3689 0-2
105	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 688	系統 服務	Volume Shadow Copy	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	CCE-ID： CCE-3667 5-7
106	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 689	系統 服務	Web Management Service	Web 管理服務可啟用遠端及委派管理功能，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	電腦設定 \\Windows 設定\ 安全性設定\\系統 服務\\Web Management Service	手動	CCE-ID： CCE-3698 6-8
107	Windows	TWG	系統	Windows	為所有授權使用者安裝 AppX 套件	電腦設定	手動	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
	Server 2012 R2 Web Server	CB-01 -006-0 690	服務	All-User Install Agent		\\Windows 設定\ 安全性設定\\系統 服務\\Windows All-User Install Agent		CCE-3678 4-7
108	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 691	系統 服務	Windows Audio	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	CCE-ID： CCE-3667 7-3
109	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 692	系統 服務	Windows Audio Endpoint Builder	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	CCE-ID： CCE-3676 4-9
110	Windows	TWG	系統	Windows	WcsPlugInService 服務主控協力廠商的	電腦設定	手動	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
	Server 2012 R2 Web Server	CB-01 -006-0 693	服務	Color System	Windows 色彩系統色彩裝置模型，以及色域圖對應模型外掛程式模組。這些外掛程式模組是 Windows 色彩系統基準線色彩裝置及色域圖對應模型的廠商特定延伸。停止或停用 WcsPlugInService 服務將停用此延伸功能，並且 Windows 色彩系統將使用其基準線模組處理，而不會使用廠商想要的處理。這可能會導致色彩呈現方式不正確	\\Windows 設定\ 安全性設定\系統 服務\Windows Color System		CCE-3667 8-1
111	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 694	系統 服務	Windows Driver Foundation-U ser-mode Driver Framework	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	CCE-ID : CCE-3668 0-7
112	Windows Server	TWG CB-01	系統 服務	Windows Error	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，	電腦設定 \\Windows 設定\ 	手動	CCE-ID : CCE-3673

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 Web Server	-006-0 695		Reporting Service	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	安全性設定\系統 服務\Windows Error Reporting Service		7-5
113	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 696	系統 服務	Windows Event Collector	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 Vista 事件記錄檔、硬體與啟用 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	CCE-ID： CCE-3677 7-1
114	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 697	系統 服務	Windows Event Log	這個服務管理事件與事件記錄檔。它支援記錄事件、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。它可以使用 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	電腦設定 \Windows 設定\ 安全性設定\系統 服務\Windows Event Log	自動	CCE-ID： CCE-3683 2-4
115	Windows	TWG	系統	Windows	Windows 防火牆經由阻止未授權使用者透過	電腦設定	自動	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
	Server 2012 R2 Web Server	CB-01 -006-0 698	服務	Firewall	網際網路或網路取得對電腦的存取來保護電腦	\\Windows 設定\ 安全性設定\\系統 服務\\Windows Firewall		CCE-3673 8-3
116	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 699	系統 服務	Windows Font Cache Service	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	CCE-ID： CCE-3673 9-1
117	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 700	系統 服務	Windows Installer	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	CCE-ID： CCE-3708 4-1
118	Windows Server	TWG CB-01	系統 服務	Windows Management	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。	電腦設定 \\Windows 設定\ 	自動	CCE-ID： CCE-3700

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 Web Server	-006-0 701		Instrumentation	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	安全性設定\系統 服務\Windows Management Instrumentation		6-4
119	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 702	系統 服務	Windows Modules Installer	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	CCE-ID： CCE-3674 2-5
120	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 703	系統 服務	Windows Process Activation Service	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 Process Activation Service	手動	CCE-ID： CCE-3674 4-1
121	Windows	TWG	系統	Windows	Windows 遠端管理(WinRM)服務為遠端管理	電腦設定	自動	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
	Server 2012 R2 Web Server	CB-01 -006-0 704	服務	Remote Management (WS-Management)	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 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	\\Windows 設定\ 安全性設定\系統 服務\Windows Remote Management (WS-Management)		CCE-3674 5-8
122	Windows Server	TWG CB-01	系統 服務	Windows Store Service	提供「Windows 市集」的基礎結構支援。此服務會視需要啟動，而且若停用此服務，使	電腦設定 \\Windows 設定\ 	手動	CCE-ID： CCE-3678

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值	備註
	2012 R2 Web Server	-006-0 705		(WSService)	用「Windows 市集」購買的應用程式將無法正常運作	安全性設定\系統 服務\Windows Store Service (WSService)		5-4
123	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 706	系統 服務	Windows Time	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	CCE-ID： CCE-3704 7-8
124	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 707	系統 服務	Windows Update	啟用偵測、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	CCE-ID： CCE-3703 3-8
125	Windows Server 2012 R2	TWG CB-01 -006-0	系統 服務	WinHTTP Web Proxy Auto-Discover	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	電腦設定 \Windows 設定\ 安全性設定\系統	手動	CCE-ID： CCE-3651 6-3

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
	Web Server	708		ry Service	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	服務\WinHTTP Web Proxy Auto-Discovery Service		
126	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 709	系統 服務	Wired AutoConfig	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	CCE-ID： CCE-3690 4-1
127	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 710	系統 服務	WMI Performance Adapter	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	CCE-ID： CCE-3677 9-7

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
128	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 711	系統 服務	Workstation	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	CCE-ID： CCE-3690 5-8
129	Windows Server 2012 R2 Web Server	TWG CB-01 -006-0 712	系統 服務	World Wide Web Publishing Service	經由 Internet Information Services 管理員可提供網頁的連接及管理能力	電腦設定 \\Windows 設定\ 安全性設定\\系統 服務\\World Wide Web Publishing Service	自動	CCE-ID： CCE-3678 0-5

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.html

[2]CIS Security Benchmarks.

<https://benchmarks.cisecurity.org>

[3]Microsoft Security Compliance Toolkit 1.0

<https://www.microsoft.com/en-us/download/details.aspx?id=55319>

[4]Windows Server 2012/2012 R2 Domain Controller Security Technical Implementation Guide, Version 2, Release 21.

<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	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值
1	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 713	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	<ul style="list-style-type: none"> ▪ 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，可用的安全性方法如下： <ul style="list-style-type: none"> ➤ 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 	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(TLS 1.0)

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
					<ul style="list-style-type: none"> ➤ 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(TLS 1.0)：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 		
2	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 714	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	<ul style="list-style-type: none"> ▪ 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 	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	已啟用

本文件之智慧財產權屬行政院資通安全處擁有。

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值
					<p>「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」</p> <ul style="list-style-type: none"> ▪ 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處理程序後期執行 	<p>使用者驗證</p>	
3	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 715	系統 管理 範本 /檔 案總 管框 架窗	開啟或關閉詳細資料窗格	<ul style="list-style-type: none"> ▪ 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 	<p>使用者設定\系統管理範本</p> <p>\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</p>	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
			格		<p>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</p> <ul style="list-style-type: none"> ▪ 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 		
4	Windows Server 2012 R2 Computer Settings	TWG CB-01 -006-0 716	系統 管理 範本 /檔 案總 管框 架窗 格	關閉預覽 窗格	<ul style="list-style-type: none"> ▪ 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

●刪除列表

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
1	Windows Server 2012 R2 Computer Settings	TWG CB-01-006-0094	安全性選項\網路安全性	網路安全性：強制限制登入時數	<ul style="list-style-type: none"> 此安全性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 啟用此原則時，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 若停用此原則，當用戶端登錄時數到期之後，可以允許保留已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\網路安全性：強制限制登入時數	已停用
2	Windows Server 2012 R2 DC Server	TWG CB-01-006-0245	使用者權限指派	讓電腦及使用者帳戶受信賴，以進行委派	<ul style="list-style-type: none"> 此安全性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 	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，以進行委派	No One

項次	GPO	TWG CB-ID	類別	原則設定 名稱	說明	GPO 設定路徑	GCB 設定值
					<ul style="list-style-type: none"> 此使用者權限會定義在「預設網域控制站群組原則」物件(GPO)及工作站、伺服器的本機安全性原則中 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 		

資料來源：本中心整理

●修改列表

項次	修改 對照	GPO	TWGC B-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 2012 R2 Account Settings	TWGC B-01-0 06-000 2	密碼 原則	密碼最長 使用期限	<ul style="list-style-type: none"> 這項<u>安全性</u>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)。您可以設定密碼在 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 	電腦設定 \Windows 設定 \安全性設定\ 帳戶原則\密碼 原則\密碼最長	90 天以下

本文件之智慧財產權屬行政院資通安全處擁有。

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						<p>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</p> <ul style="list-style-type: none"> 注意：根據您的環境而定，安全性的最佳作法是讓密碼每 30 至 90 天到期。如此一來，攻擊者破解使用者密碼及存取您的網路資源的時間便很有限 	使用期限	
	修改後	Windows Server 2012 R2 Account Settings	TWGC B-01-006-0002	密碼原則	密碼最長使用期限	<ul style="list-style-type: none"> 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 注意：根據使用者的環境而定，安全性的最佳作法是讓密碼每 30 至 90 天到期。如此一 	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	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						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		
2	修改前	Windows Server 2012 R2 Account Settings	TWGC B-01-006-0003	密碼原則	最小密碼長度	此安全性設定決定使用者帳戶的密碼可包含的最少字元數。您可以設定介於 1 到 14 個字元之間的值，或是 <u>可以</u> 將字元數設為 0，如此便不需要密碼	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 2012 R2 Account Settings	TWGC B-01-006-0003	密碼原則	最小密碼長度	<ul style="list-style-type: none"> ▪ 這項原則<u>設定</u>決定使用者帳戶的密碼可包含的最少字元數 ▪ <u>使用者</u>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 	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 <u>以上</u>
3	修改前	Windows Server 2012 R2 Account	TWGC B-01-006-000	密碼原則	密碼必須符合複雜性需求	<ul style="list-style-type: none"> ▪ 這項<u>安全性</u>設定決定密碼是否必須符合複雜性需求 ▪ 如果啟用了此原則，則密碼必須符合下列最 	電腦設定\Windows 設定\安全性設定\	啟用

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings	4			<p>小需求：</p> <ul style="list-style-type: none"> ▶ 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： <ol style="list-style-type: none"> (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：!、\$、#、%) <p>▪ 建立或變更密碼時會強制執行複雜性需求</p>	帳戶原則\密碼原則\密碼必須符合複雜性需求	
	修改後	Windows Server 2012 R2 Account Settings	TWGC B-01-006-0004	密碼原則	密碼必須符合複雜性需求	<ul style="list-style-type: none"> ▪ 這項原則設定決定密碼是否必須符合複雜性需求 ▪ 如果啟用了此原則，則密碼必須符合下列最小需求： <ul style="list-style-type: none"> ▶ 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 	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則\密碼必須符合複雜性需求	已啟用

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						<ul style="list-style-type: none"> ▶長度至少為 6 個字元 ▶包含下列四種字元中的三種： <ol style="list-style-type: none"> (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 	求	
4	修改前	Windows Server 2012 R2 Account Settings	TWGC B-01-006-0006	密碼原則	使用可還原的加密來存放密碼	<ul style="list-style-type: none"> ▪這項<u>安全性</u>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，基本上和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，否則絕不應該啟用這個<u>原則</u> ▪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 	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	停用

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						時，便需要這項原則。在網際網路資訊服務 (IIS) 中使用摘要式驗證時，也需要這個原則		
	修改後	Windows Server 2012 R2 Account Settings	TWGC B-01-006-0006	密碼原則	使用可還原的加密來存放密碼	<ul style="list-style-type: none"> ▪ 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，否則絕不應該啟用這項原則 ▪ 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 	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
5	修改前	Windows Server 2012 R2 Account	TWGC B-01-006-000	帳戶鎖定原則	帳戶鎖定閾值	<ul style="list-style-type: none"> ▪ 此安全性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 	電腦設定 \\Windows 設定 \\安全性設定\\	5次不正確的登入嘗試

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings	7			<p>該鎖定帳戶。<u>您可以將失敗的登入嘗試值設定為介於 0 到 999 之間。如果將值設定為 0，將永遠不會鎖定該帳戶</u></p> <ul style="list-style-type: none"> 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 	帳戶原則\帳戶鎖定原則\帳戶鎖定閾值	
	修改後	Windows Server 2012 R2 Account Settings	TWGC B-01-006-0007	帳戶鎖定原則	帳戶鎖定閾值	<ul style="list-style-type: none"> <u>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。可以將失敗的登入嘗試值設定為介於 0 到 999 之間。如果將值設定為 0，將永遠不會鎖定該帳戶</u> 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 	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
6	修改前	Windows Server 2012	TWGC B-01-0	帳戶鎖定	重設帳戶鎖定計數	<ul style="list-style-type: none"> <u>此安全性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</u> 	電腦設定\Windows 設定	15 分鐘

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		R2 Account Settings	06-0008	原則	器的時間間隔	<p>重設為 0 次失敗。可用的範圍是從 1 分鐘到 99,999 分鐘</p> <ul style="list-style-type: none"> ▪ 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 	<p>\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</p>	
	修改後	Windows Server 2012 R2 Account Settings	TWGC B-01-006-0008	帳戶鎖定原則	重設帳戶鎖定計數器的時間間隔	<ul style="list-style-type: none"> ▪ <u>這項原則</u>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<u>時間</u> 	<p>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</p>	15 分鐘 <u>以上</u>
7	修改前	Windows Server 2012 R2 Account Settings	TWGC B-01-006-0009	帳戶鎖定原則	帳戶鎖定時間	<ul style="list-style-type: none"> ▪ <u>此安全性</u>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 	<p>電腦設定 \Windows 設定 \安全性設定\ 帳戶原則\帳戶鎖定原則\帳戶</p>	15 分鐘

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						<ul style="list-style-type: none"> ▪ 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 	鎖定時間	
	修改後	Windows Server 2012 R2 Account Settings	TWGC B-01-006-0009	帳戶鎖定原則	帳戶鎖定時間	<ul style="list-style-type: none"> ▪ 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
8	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0016	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	<ul style="list-style-type: none"> ▪ 此安全性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 ▪ 對於此原則設定，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 	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，	15 分鐘

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						99,999， <u>即 208 天</u> ；實際上，此值會停用此原則	要求的閒置時間	
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-001	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	<ul style="list-style-type: none"> ▪ 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 ▪ 對於此原則設定，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，此值會停用此原則 	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
9	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-008-001	安全性選項 MS S	MSS：(NoDefaultExempt) Configure IPsec exemption	<ul style="list-style-type: none"> ▪ 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)設定為 0：代表「多點傳送廣播，RSVP、Kerberos 及 ISAKMP 流量不受限於 IPsec 	電腦設定 \\Windows 設定 \\安全性設定 \\本機原則\\安全性選項\\MSS：(NoDefaultExe	Multicast, broadcast, and ISAKMP are exempt (Best for Windows

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					s for various types of network traffic.	<p>篩選功能」</p> <p>(2)<u>設定為 1</u>：代表「Kerberos 及 RSVP 流量並不受 IPsec 篩選，但多點傳播、廣播及 ISAKMP 流量都是豁免」</p> <p>(3)<u>設定為 2</u>：代表「多點傳播和廣播流量並不受 IPsec 篩選，但 RSVP、Kerberos 及 ISAKMP 流量被豁免」</p> <p>(4)<u>設定為 3</u>：代表「只有 ISAKMP 流量是免除 IPsec 篩選功能」</p>	mpt) Configure IPsec exemptions for various types of network traffic	XP)
修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0018	安全性選項	MS S	MSS : (NoDefaultExempt) Configure IPsec exemptions for various types of	<ul style="list-style-type: none"> 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： <ul style="list-style-type: none"> (1)<u>Allow all exemptions (least secure)</u>：代表「多點傳送廣播，RSVP、Kerberos 及 ISAKMP 流量不受限於 IPsec 篩選功能」 (2)<u>Multicast, broadcast, & ISAKMP exempt (best for Windows XP)</u>：代表「Kerberos 及 	電腦設定 \Windows 設定 \安全性設定\本機原則\安全性選項\MSS : (NoDefaultExempt) Configure IPsec exemptions for	Multicast, broadcast, & ISAKMP exempt (best for Windows XP)

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					network traffic.	<p>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」</p> <p>(3)RSVP, Kerberos, and ISAKMP are <u>exempt</u>：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」</p> <p>(4)Only ISAKMP is exempt (recommended for <u>Windows Server 2003</u>):代表「只有 ISAKMP 流量是免除 IPsec 篩選功能」</p>	various types of network traffic	
10	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0020	安全性選項 \MS S	MSS : (TcpMaxDataRetransmissions) How many times unacknowledged	<ul style="list-style-type: none"> 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	3

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					data is retransmitted (3 recommended, 5 is default)		unacknowledged data is retransmitted (3 recommended, 5 is default)	
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0020	安全性選項 MS S	MSS : (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3	<ul style="list-style-type: none"> ▪ 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	3 以下，但須大於 0

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					recommended, 5 is default)		recommended, 5 is default)	
11	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0026	安全性選項 MS S	MSS : (TcpMax DataRetransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended, 5 is	<ul style="list-style-type: none"> 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 recommended , 5 is default)	3

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					default)			
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0026	安全性選項 MS S	MSS : (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	<ul style="list-style-type: none"> 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 recommended , 5 is default)	3 以下,但須大於 0

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
12	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0034	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	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。有了這個事先警告，使用者便有時間建構一個強式密碼	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 2012 R2 Computer Settings	TWGC B-01-006-0034	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	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。有了這個事先警告，使用者便有時間建構一個強式密碼	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 <u>以上</u>
13	修改	Windows	TWGC	安全	互動式登	▪ 每個唯一使用者的登入資訊會存放於本機快	電腦設定	4 次

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	前	Server 2012 R2 Computer Settings	B-01-006-003	性選項\互動式登入	<p>入：網域控制站無法使用時，要快取的先前登入次數</p>	<p>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，則會以下列訊息提示使用者：</p> <ul style="list-style-type: none"> ▪ <u>目前無可用的登入伺服器來服務登入請求</u> ▪ 在此原則設定中，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取資訊 	<p>\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</p>	
	修改後	Windows Server 2012 R2	TWGC B-01-006-003	安全性選項\	<p>互動式登入：網域控制站無</p>	<ul style="list-style-type: none"> ▪ 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 	<p>電腦設定\ \Windows 設定\ \安全性設定\ \</p>	4 次以下

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Computer Settings	6	互動式登入	法使用時，要快取的先前登入次數	<p>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「<u>目前無可用的登入伺服器來服務登入請求</u>」訊息提示使用者</p> <ul style="list-style-type: none"> 在此原則設定中，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取資訊 	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	
14	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0041	安全性選項\互動式登入	互動式登入：電腦未使用時間限制	<u>Windows</u> 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	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\互動式	900 秒

本文件之智慧財產權屬行政院資通安全處擁有。

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
				入			登入：電腦未使用時間限制	
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-004 1	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	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
15	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-004 3	安全性選項\ 系統加密編譯	系統加密編譯： <u>使用 FIPS 140 相容密碼編譯演算法</u> ， <u>包括加密、雜湊與簽署演</u>	<ul style="list-style-type: none"> 對於 Schannel Security Service Provider (SSP)，<u>此安全性</u>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 	電腦設定\ Windows 設定\ 安全性設定\ 本機原則\ 安全性選項\ 系統加密編譯： <u>使用 FIPS 140 相容密碼編譯演算法</u> ， <u>包括加</u>	已啟用

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					<u>算法</u>	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 與 SHA512) 用於 TLS 雜湊需求 <ul style="list-style-type: none"> 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 DES 加密演算法來加密遠端桌面服務網路通訊 	<u>密、雜湊與簽署演算法</u>	
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0043	安全性選項\系統加密編譯	系統加密編譯： <u>使用 FIPS 相容演算法於加密，雜湊，以及簽章</u>	<ul style="list-style-type: none"> 對於 Schannel Security Service Provider (SSP)，<u>這項原則</u>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 	電腦設定 \Windows 設定 \安全性設定 \本機原則\安全性選項\系統加密編譯： <u>使用 FIPS 相容演算法於加密，雜</u>	已啟用

本文件之智慧財產權屬行政院資通安全處擁有。

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						<p>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 與 SHA512)用於 TLS 雜湊需求</p> <ul style="list-style-type: none"> 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 DES 加密演算法來加密遠端桌面服務網路通訊 	湊，以及簽章	
16	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0049	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	<ul style="list-style-type: none"> 此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。如果您未停用「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 	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	已停用

本文件之智慧財產權屬行政院資通安全處擁有。

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						<p>上，而非安全桌面</p> <ul style="list-style-type: none"> 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 	安全桌面來提升權限	
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0049	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	<ul style="list-style-type: none"> 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 	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示提升權限	已停用

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						設定才能停用安全桌面		
17	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-005 1	安全性選項\使用者帳戶控制	使用者帳戶控制：僅針對已簽署與驗證過的 <u>可執行檔</u> ， <u>提升</u> 其權限	<ul style="list-style-type: none"> ▪ <u>此</u>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。企業的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： <ul style="list-style-type: none"> ➤ 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 	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：僅針對已簽署與驗證過的 <u>可執行檔</u> ， <u>提升</u> 其權限	已停用
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-005 1	安全性選項\使用者帳戶控	使用者帳戶控制：僅針對已簽章與驗證過的 <u>可執行檔</u> ，	<ul style="list-style-type: none"> ▪ <u>這項</u>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。企業的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： 	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	已停用

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
				制	提高其權限	<ul style="list-style-type: none"> ➤ 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 	針對已簽章與驗證過的可執行檔，提高其權限	
18	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-005 5	安全性選項\使用者帳戶控制	使用者帳戶控制：標準使用者之提升權限提示的行為	<ul style="list-style-type: none"> ▪ 此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： <ul style="list-style-type: none"> ➤ 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 ➤ 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 	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：標準使用者之提升權限提示的行為	提示輸入認證

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						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		
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0055	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	<ul style="list-style-type: none"> ▪ <u>這項原則設定</u>會控制標準使用者之提高權限提示的行為 ▪ 選項如下： <ul style="list-style-type: none"> ➤ 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 ➤ 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 	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行為	提示輸入認證

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						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		
19	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0058	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料夾	<ul style="list-style-type: none"> ▪ 啟用此安全性選項便可以使用修復主控台 SET 命令，此命令可讓您設定下列修復主控台環境變數： <ul style="list-style-type: none"> ➢ AllowWildCards：對某些命令啟用萬用字元支援(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 	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取所有磁碟和所有資料夾	已停用
	修改後	Windows Server 2012	TWGC B-01-0	安全性選	修復主控台：允許	<ul style="list-style-type: none"> ▪ <u>這項原則設定決定是否允許使用修復主控台 SET 命令</u> 	電腦設定\ Windows 設定	已停用

本文件之智慧財產權屬行政院資通安全處擁有。

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		R2 Computer Settings	06-005 8	項\ 修復 主控 台	軟碟複製 以及存取 所有磁碟 和所有資 料夾	<ul style="list-style-type: none"> ▪ 啟用此安全性選項便可以使用修復主控台 SET 命令，此命令可讓使用者設定下列修復主控台環境變數： <ul style="list-style-type: none"> ➢ AllowWildCards：對某些命令啟用萬用字元支援(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 	\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取所有磁碟和所有資料夾	
20	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-0 06-006 9	安全 性選 項\ 網域 成員	網域成員：最長電腦帳戶密碼有效期	此安全性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	30 天

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
							帳戶密碼有效期	
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0069	安全性選項\ 網域成員	網域成員：最長電腦帳戶密碼有效期	<u>這項原則</u> 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 天以下， <u>但須大於 0 天</u>
21	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0075	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	<ul style="list-style-type: none"> ▪ <u>此安全性</u>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，您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 	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	傳統-本機使用者以自身身份驗證

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						<p>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」</p> <p>▪ <u>重要：</u></p> <p>▪ 使用「僅適用於來賓」模式，可經由網路存取<u>您</u>電腦的所有使用者(包括匿名網際網路使用者)都能存取<u>您的</u>共用資源。<u>您</u>必須使用 Windows 防火牆或其他類似裝置來保護<u>您的</u>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</p>	本機帳戶	
	修改後	Windows Server 2012 R2 Computer	TWGC B-01-006-0075	安全性選項\網路	網路存取：共用和安全性模式用於	<p>▪ <u>這項原則</u>設定決定如何驗證使用本機帳戶的網路登入</p> <p>▪ 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</p>	電腦設定\Windows 設定\安全性設定\本機原則\安全	傳統-本機使用者以自身身分驗證

本文件之智慧財產權屬行政院資通安全處擁有。

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings		存取	本機帳戶	<p>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</p> <ul style="list-style-type: none"> ▪ 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」 ▪ <u>注意</u>：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 	性選項\網路存取：共用和安全性模式用於本機帳戶	
22	修改	Windows	TWGC	安全	網路存	<ul style="list-style-type: none"> ▪ 啟用時，<u>此安全性</u>設定會將共用和管道的匿 	電腦設定	已啟用

本文件之智慧財產權屬行政院資通安全處擁有。

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	前	Server 2012 R2 Computer Settings	B-01-006-0077	性選項\ 網路存取	取：限制匿名存取具名管道和共用	名存取限制為以下設定： <ul style="list-style-type: none"> ➤ 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 	\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	
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0077	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	<ul style="list-style-type: none"> ▪ <u>這項原則設定決定是否限制匿名存取具名管道和共用</u> ▪ 啟用時，<u>這項原則設定</u>會將共用和管道的匿名存取限制為以下設定： <ul style="list-style-type: none"> ➤ 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
23	修改前	Windows Server 2012 R2	TWGC B-01-006-008	安全性選項\ Local	網路安全性：允許 Local	<ul style="list-style-type: none"> ▪ <u>這個原則設定</u>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 	電腦設定\ Windows 設定\ 安全性設定\ 	已啟用

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Computer Settings	6	網路安全性	System 對 NTLM 使用電腦身分識別	<p>分識別</p> <ul style="list-style-type: none"> ▪ 如果啟用這個原則設定，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 ▪ 如果未設定這個原則設定，則以 Local System 執行且使用交涉的服務在還原為 NTLM 驗證時將會匿名驗證。<u>這是舊版 Windows 中的行為</u> ▪ <u>必須至少是 Windows 7 或 Windows Server 2008 R2 才支援此原則</u> 	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	
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-008 6	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	<ul style="list-style-type: none"> ▪ 這項原則設定允許使用交涉的 Local System 服務在還原使用 NTLM 驗證時，使用電腦身分識別 ▪ 如果啟用這項原則設定，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 	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	已啟用

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					分識別	驗證要求失敗並記錄錯誤 ▪ 如果 <u>停用</u> 這項原則設定，則以 Local System 執行且使用交涉的服務在還原為 NTLM 驗證時將會匿名驗證	對 NTLM 使用電腦身分識別	
24	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0088	安全性選項\ 網路安全性	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	在已加入網域的電腦上預設會關閉此原則。這樣便不會允許使用線上身分識別來向已加入網域的電腦驗證	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：允許對此電腦的 PKU2U 驗證要求使用線上身分識別	已停用
	修改後	Windows Server 2012 R2	TWGC B-01-006-008	安全性選項\ 網路安全性	網路安全性：允許對此電腦	▪ <u>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</u> ▪ 在已加入網域的電腦上預設會 <u>停用</u> 此原則，	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：允許對此電腦的 PKU2U 驗證要求使用線上身分識別	已停用

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Computer Settings	8	網路安全性	的 PKU2U 驗證要求使用線上身分識別	這樣便不會允許使用線上身分識別來向已加入網域的電腦驗證	本機原則\安全性選項\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	
25	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-009 2	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	<ul style="list-style-type: none"> ▪ 這個原則 <u>允許您設定允許 Kerberos 使用的加密類型</u> ▪ 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。允許多個選取項目 <u>必須至少是 Windows 7 或 Windows Server 2008 R2 才支援此原則</u> 	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 2012 R2	TWGC B-01-006-009	安全性選項\網路安全性	網路安全性：設定 Kerberos	<ul style="list-style-type: none"> ▪ 這項原則 <u>提供使用者設定允許 Kerberos 使用的加密類型</u> 	電腦設定\Windows 設定\安全性設定\	AES128_HMAC_SHA1, AES256_HMAC_SHA1

本文件之智慧財產權屬行政院資通安全處擁有。

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Computer Settings	2	網路安全性	允許的加密類型	<ul style="list-style-type: none"> 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。允許多個選取項目 	本機原則\安全性選項\網路安全性：設定 Kerberos 允許的加密類型	AC_SHA1, 未來的加密類型
26	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0098	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) 可以覆寫稽核原則類別設定	<ul style="list-style-type: none"> 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」系統管理工具 	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	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						<ul style="list-style-type: none"> ▪ 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 2012 R2 Computer Settings	TWGC B-01-006-0098	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	<ul style="list-style-type: none"> ▪ 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 	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	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						登錄機碼		
27	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-012 2	使用者權限指派	存取認證管理員作為信任的呼叫者	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 <u>作</u> 信任的呼叫者	No One
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-012 2	使用者權限指派	存取認證管理員 <u>做</u> 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 <u>做</u> 為信任的呼叫者	No One

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
28	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0146	事件記錄服務/安全性	指定記錄檔大小上限(KB)	<ul style="list-style-type: none"> ▪ 這個原則設定可指定記錄檔的大小上限(以 KB 為單位) ▪ 如果您啟用這個原則設定，即可將記錄檔大小上限設定為介於 1 MB(1024 KB)至 2 TB(2147483647 KB)之間(以 KB 為遞增單位) ▪ 如果您停用或未設定這個原則設定，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
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0146	事件記錄服務/安全性	指定記錄檔大小上限(KB)	<ul style="list-style-type: none"> ▪ 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(1024 KB)至 2 TB(2147483647 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 	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

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						這個值，此值預設為 20 MB		
29	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0148	事件記錄服務/系統	指定記錄檔大小上限(KB)	<ul style="list-style-type: none"> ▪ 這個原則設定可指定記錄檔的大小上限(以 KB 為單位) ▪ 如果您啟用這個原則設定，即可將記錄檔大小上限設定為介於 1 MB(1024 KB)至 2 TB(2147483647 KB)之間(以 KB 為遞增單位) ▪ 如果您停用或未設定這個原則設定，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： 32768KB
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0148	事件記錄服務/系統	指定記錄檔大小上限(KB)	<ul style="list-style-type: none"> ▪ 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(1024 KB)至 2 TB(2147483647 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 	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 <u>以上</u>

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						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		
30	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0150	事件記錄服務/應用程式	指定記錄檔大小上限(KB)	<ul style="list-style-type: none"> ▪ 這個原則設定可指定記錄檔的大小上限(以 KB 為單位) ▪ 如果您啟用這個原則設定，即可將記錄檔大小上限設定為介於 1 MB(1024 KB)至 2 TB(2147483647 KB)之間(以 KB 為遞增單位) ▪ 如果您停用或未設定這個原則設定，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\應用程式\指定記錄檔大小上限(KB)	已啟用： 32768KB
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0150	事件記錄服務/應用程式	指定記錄檔大小上限(KB)	<ul style="list-style-type: none"> ▪ 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(1024 KB)至 2 TB(2147483647 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 	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	已啟用： 32,768KB <u>以上</u>

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						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	上限(KB)	
31	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0165	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	<ul style="list-style-type: none"> ▪ 這個原則設定指定「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 ▪ 如果您啟用這項原則設定，將會從「Windows」資料夾的檔案和資料夾工作中移除這些工作 ▪ 如果您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
	修改後	Windows Server 2012 R2 Computer	TWGC B-01-006-0165	系統管理範本/網	關閉檔案及資料夾的「發佈到網站」	<ul style="list-style-type: none"> ▪ 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 	電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路	已啟用

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings		際網路通訊管理	工作	<ul style="list-style-type: none"> ▪ 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 	通訊設定\關閉檔案及資料夾的「發佈到網站」工作	
32	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0173	進階稽核原則\系統	稽核其他系統事件	<ul style="list-style-type: none"> ▪ <u>這個原則設定可讓您稽核下列任一事件：</u> <ul style="list-style-type: none"> ➢ 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	<u>沒有稽核</u>
	修改後	Windows Server 2012 R2 Computer	TWGC B-01-006-0173	進階稽核原則\系	稽核其他系統事件	<ul style="list-style-type: none"> ▪ <u>這項原則設定決定是否稽核下列任一事件：</u> <ul style="list-style-type: none"> ➢ 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 	電腦設定\Windows 設定\安全性設定\進階稽核原則	<u>成功與失敗</u>

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings		統		<ul style="list-style-type: none"> ➤ 加密編譯金鑰檔案及移轉操作 ▪ 預設值：成功，失敗 	設定\稽核原則\系統\稽核其他系統事件	
33	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0175	進階稽核原則\物件存取	稽核其他物件存取事件	<ul style="list-style-type: none"> ▪ <u>這個原則設定可讓您稽核因管理工作排程器物件或 COM+物件而產生的事件</u> ▪ 如果是排程器工作，則會稽核下列項目： <ul style="list-style-type: none"> ➤ 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： <ul style="list-style-type: none"> ➤ 新增類別目錄物件 ➤ 更新類別目錄物件 ➤ 刪除類別目錄物件 	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	<u>沒有稽核</u>
	修改	Windows	TWGC	進階	稽核其他	<ul style="list-style-type: none"> ▪ <u>這項原則設定決定是否稽核因管理工作排程</u> 	電腦設定	<u>成功與失敗</u>

本文件之智慧財產權屬行政院資通安全處擁有。

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	後	Server 2012 R2 Computer Settings	B-01-006-0175	稽核原則 物件存取	物件存取事件	<p>器物件或 COM+物件而產生的事件</p> <ul style="list-style-type: none"> ▪ 如果是排程器工作，則會稽核下列項目： <ul style="list-style-type: none"> ➢ 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： <ul style="list-style-type: none"> ➢ 新增類別目錄物件 ➢ 更新類別目錄物件 ➢ 刪除類別目錄物件 	\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	
34	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0177	進階稽核原則 物件存	稽核檔案 共用	<ul style="list-style-type: none"> ▪ <u>這個原則設定可讓您稽核存取共用資料夾的嘗試</u> ▪ 如果您設定<u>這個原則設定</u>，則會在嘗試存取共用資料夾時產生稽核事件。如果定義<u>這個原則設定</u>，則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	<u>沒有稽核</u>

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
				取		<p>功、只稽核失敗，或同時稽核兩者</p> <ul style="list-style-type: none"> 注意：共用資料夾沒有系統存取控制清單 (SACL)。如果啟用這個原則設定，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	
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0177	進階稽核原則 \物件存取	稽核檔案共用	<ul style="list-style-type: none"> 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	<u>成功與失敗</u>
35	修改前	Windows Server 2012 R2 Computer	TWGC B-01-006-0185	進階稽核原則 \物	稽核詳細的檔案共用	<ul style="list-style-type: none"> 這個原則設定可讓您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 	電腦設定 \Windows 設定 \安全性設定\ 進階稽核原則	<u>沒有稽核</u>

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings		物件存取		<p>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</p> <ul style="list-style-type: none"> ▪ 如果您設定此原則設定，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)。如果啟用此原則設定，則會稽核系統上所有共用檔案與資料夾的存取 	設定\稽核原則\物件存取\稽核詳細的檔案共用	
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0185	進階稽核原則\物件存取	稽核詳細的檔案共用	<ul style="list-style-type: none"> ▪ <u>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</u>。「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 	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	<u>失敗</u>

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						<p>的詳細資訊</p> <ul style="list-style-type: none"> ▪ 如果設定此原則設定，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)。如果啟用此原則設定，則會稽核系統上所有共用檔案與資料夾的存取 	共用	
36	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0189	進階稽核原則\原則變更	稽核授權原則變更	<ul style="list-style-type: none"> ▪ <u>這個原則設定可讓您稽核因授權原則變更而產生的事件</u>，例如： <ul style="list-style-type: none"> ➢ 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 	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	<u>沒有稽核</u>

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						<ul style="list-style-type: none"> ▪ 如果您設定這個原則設定，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 ▪ 如果您未設定這個原則設定，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 2012 R2 Computer Settings	TWGC B-01-006-0189	進階稽核原則\原則變更	稽核授權原則變更	<ul style="list-style-type: none"> ▪ <u>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：</u> <ul style="list-style-type: none"> ➢ 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，則會在嘗試變更授權原則時產生稽核事件。成功稽核會記錄成 	電腦設定\Windows 設定\安全性設定\進階稽核原則設定\稽核原則\原則變更\稽核授權原則變更	<u>成功</u>

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						<p>功嘗試，而失敗稽核則會記錄失敗嘗試</p> <ul style="list-style-type: none"> ▪ 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 		
37	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0191	進階稽核原則 \原則變更	稽核 MPSSVC 規則層級原則變更	<ul style="list-style-type: none"> ▪ <u>這個原則設定可讓您稽核因 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：</u> <ul style="list-style-type: none"> ➢ 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 ▪ 如果您設定這個原則設定，則會在嘗試變更 	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 MPSSVC 規 則層級原則變 更	<u>沒有稽核</u>

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						<p>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</p> <ul style="list-style-type: none"> ▪ 如果您未設定這個原則設定，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 		
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-019 1	進階稽核原則\原則變更	稽核 MPSSVC 規則層級原則變更	<ul style="list-style-type: none"> ▪ <u>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：</u> <ul style="list-style-type: none"> ➢ 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 	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 規則層級原則變更	<u>成功與失敗</u>

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						<ul style="list-style-type: none"> ➢ 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 		
38	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0192	進階稽核原則\原則變更	稽核其他原則變更事件	<ul style="list-style-type: none"> ▪ 這個原則設定可讓您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： <ul style="list-style-type: none"> ➢ 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 	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	<u>沒有稽核</u>

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						<ul style="list-style-type: none"> 預設值：沒有稽核 		
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-019 2	進階稽核原則 \原則變更	稽核其他原則變更事件	<ul style="list-style-type: none"> 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： <ul style="list-style-type: none"> 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 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	<u>失敗</u>
39	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-019 6	進階稽核原則 \帳戶登入	稽核 Kerberos 驗證服務	<ul style="list-style-type: none"> 這個原則設定可讓您稽核因 Kerberos 驗證票證授權票證(TGT)要求而產生的事件 如果您設定這個原則設定，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 	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	<u>沒有稽核</u>

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						<ul style="list-style-type: none"> ▪ 如果您未設定這個原則設定，則不會在 Kerberos 驗證 TGT 要求之後產生稽核事件 ▪ 用戶端版本的預設值：沒有稽核 ▪ 伺服器版本的預設值：成功 	證服務	
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0196	進階稽核原則 帳戶登入	稽核 Kerberos 驗證服務	<ul style="list-style-type: none"> ▪ 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
40	修改前	Windows Server 2012 R2 Computer	TWGC B-01-006-0198	進階稽核原則 帳戶	稽核 Kerberos 服務票證操作	<ul style="list-style-type: none"> ▪ 這個原則設定可讓您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 ▪ 如果您設定這個原則設定，則會在針對使用 	電腦設定 \\Windows 設定 \\安全性設定 \\進階稽核原則	沒有稽核

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings		戶登入		<p>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</p> <ul style="list-style-type: none"> ▪ 如果您未設定這個原則設定，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 	設定\稽核原則\帳戶登入\稽核 Kerberos 服務票證操作	
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0198	進階稽核原則\帳戶登入	稽核 Kerberos 服務票證操作	<ul style="list-style-type: none"> ▪ 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 ▪ 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 	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 服務票證操作	成功與失敗

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
						核事件 ▪ 伺服器版本的預設值：成功		
41	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0204	進階稽核原則 帳戶管理	稽核發佈群組管理	<ul style="list-style-type: none"> ▪ <u>這個原則設定可稽核因發佈群組變更而產生的事件</u>，例如： <ul style="list-style-type: none"> ➤ 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<u>這個原則設定</u>，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<u>這個原則設定</u>，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	<u>沒有稽核</u>
	修改	Windows	TWGC	進階	稽核發佈	<ul style="list-style-type: none"> ▪ <u>這項原則設定決定是否稽核因發佈群組變更</u> 	電腦設定	<u>成功</u>

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	後	Server 2012 R2 Computer Settings	B-01-006-0204	稽核原則 帳戶管理	群組管理	<p>而產生的事件，例如：</p> <ul style="list-style-type: none"> ➤ 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 <ul style="list-style-type: none"> ▪ 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 	\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	
42	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0206	進階稽核原則 登入/	稽核帳戶鎖定	<ul style="list-style-type: none"> ▪ 此原則設定可以讓您稽核因嘗試登入的帳戶被鎖定而失敗所產生的事件 ▪ 若您設定此原則設定，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 	電腦設定 \Windows 設定 \安全性設定\ 進階稽核原則 設定\稽核原則	<u>沒有稽核</u>

本文件之智慧財產權屬行政院資通安全處擁有。

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
				登出		<p>功的嘗試</p> <ul style="list-style-type: none"> 預設值：成功 	\登入\登出\稽核帳戶鎖定	
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0206	進階稽核原則 登入/登出	稽核帳戶鎖定	<ul style="list-style-type: none"> 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 若設定此原則設定，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
43	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0222	Windows 防火牆/網域設定檔	Windows 防火牆：網域設定檔：允許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	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
							牆\內容\網域設定檔\允許套用本機防火牆規則	
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0222	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\套用本機防火牆規則	是(預設)
44	修改	Windows Server 2012	TWGC B-01-0	Windows	Windows 防火牆：	這項原則設定決定當程式因為接收輸入連線	電腦設定\Windows 設定	是

本文件之智慧財產權屬行政院資通安全處擁有。

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	前	R2 Computer Settings	06-022 3	防火 牆/ 網域 設定 檔	網域設定 檔：顯示 通知	而被封鎖時，是否為使用者顯示通知	\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\顯示通 知	
	修改 後	Windows Server 2012 R2 Computer Settings	TWGC B-01-0 06-022 3	Wind ows 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	是

項次	修改對照	GPO	TWGC B-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\ 顯示通知	
45	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0224	Windows 防火牆/網域設定檔	Windows 防火牆：網域設定檔：允許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\允許套用本機連線安全性規則	是(預設)
	修改後	Windows Server 2012 R2 Computer	TWGC B-01-006-022	Windows 防火牆/	Windows 防火牆：網域設定檔：套用	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	是(預設)

本文件之智慧財產權屬行政院資通安全處擁有。

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings	4	網域設定檔	本機連線安全性規則		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	
46	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0225	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\允許單	否

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
							點傳播回應	
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0225	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
47	修改前	Windows Server 2012 R2 Computer	TWGC B-01-006-0228	Windows 防火牆/私人	Windows 防火牆：私人設定檔：允許套用本機	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)

本文件之智慧財產權屬行政院資通安全處擁有。

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings		設定檔	防火牆規則		防火牆\具有進階安全性的 Windows 防火牆\內容\私人設定檔\允許套用本機防火牆規則	
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0228	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\套用本機防火	是(預設)

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
							牆規則	
48	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0229	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
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0229	Windows 防火牆/私人設定	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	是

本文件之智慧財產權屬行政院資通安全處擁有。

項次	修改對照	GPO	TWGC B-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\顯示通知	
49	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0230	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\允許單點傳播回應	否
	修改	Windows Server 2012	TWGC B-01-0	Windows	Windows 防火牆：	這項原則設定決定此電腦是否接收其傳出之	電腦設定\Windows 設定	否

本文件之智慧財產權屬行政院資通安全處擁有。

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	後	R2 Computer Settings	06-023 0	防火 牆/ 私人 設定 檔	私人設定 檔：允許 單點傳播 回應	多點傳送或廣播訊息的單點傳送回應	\\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	
50	修改 前	Windows Server 2012 R2 Computer Settings	TWGC B-01-0 06-023 1	Wind ows 防火 牆/ 私人 設定 檔	Windows 防火牆： 私人設定 檔：允許 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	TWGC B-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\允許套用本機連線安全性規則	
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0231	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)
51	修改	Windows Server 2012	TWGC B-01-0	Windows	Windows 防火牆：	這項原則設定決定此電腦是否接收其傳出之	電腦設定\Windows 設定	否

本文件之智慧財產權屬行政院資通安全處擁有。

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	前	R2 Computer Settings	06-023 3	防火 牆/ 公用 設定 檔	公用設定 檔：允許 單點傳播 回應	多點傳送或廣播訊息的單點傳送回應	\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	
	修改 後	Windows Server 2012 R2 Computer Settings	TWGC B-01-0 06-023 3	Wind ows 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	否

項次	修改對照	GPO	TWGC B-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\ 允許單點傳播 回應	
52	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0234	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\ 顯示通知	是
	修改後	Windows Server 2012 R2 Computer	TWGC B-01-006-023	Windows 防火牆/	Windows 防火牆：公用設定檔：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	是

本文件之智慧財產權屬行政院資通安全處擁有。

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings	4	公用設定檔	通知		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	
53	修改前	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-023 5	Windows 防火牆/公用設定檔	Windows 防火牆：公用設定檔： <u>允許</u> 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\ <u>允許</u> 套用本機連線安	是(預設)

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
							全性規則	
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0235	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\ 套用本機連線安全性規則	是(預設)
54	修改前	Windows Server 2012 R2 Computer	TWGC B-01-006-0237	Windows 防火牆/公用	Windows 防火牆：公用設定檔： <u>允許</u> 套用本機	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)

本文件之智慧財產權屬行政院資通安全處擁有。

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		Settings		設定檔	防火牆規則		防火牆\具有進階安全性的 Windows 防火牆\內容\公用設定檔\允許套用本機防火牆規則	
	修改後	Windows Server 2012 R2 Computer Settings	TWGC B-01-006-0237	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\套用本機防火	是(預設)

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
							牆規則	
55	修改前	Windows Server 2012 R2 DNS Server	TWGC B-01-006-0359	系統服務	Human Interface Device <u>Access</u>	啟用並維護鍵盤、遙控器與其他多媒體裝置上之常用按鈕的使用。建議您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 <u>Access</u>	手動
	修改後	Windows Server 2012 R2 DNS Server	TWGC B-01-006-0359	系統服務	Human Interface Device <u>Service</u>	啟用並維護鍵盤、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 <u>Service</u>	手動
56	修改前	Windows Server 2012	TWGC B-01-0	系統服務	Human Interface	啟用並維護鍵盤、遙控器與其他多媒體裝置上之常用按鈕的使用。建議您讓這個服務繼續執	電腦設定 \\Windows 設定	手動

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
		R2 File Server	06-0490		Device <u>Access</u>	行	\安全性設定\ 系統服務\ Human Interface Device <u>Access</u>	
	修改後	Windows Server 2012 R2 File Server	TWGC B-01-006-0490	系統服務	Human Interface Device <u>Service</u>	啟用並維護鍵盤、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 <u>Service</u>	手動
57	修改前	Windows Server 2012 R2 Web Server	TWGC B-01-006-0618	系統服務	Human Interface Device <u>Access</u>	啟用並維護鍵盤、遙控器與其他多媒體裝置上之常用按鈕的使用。建議 <u>您</u> 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	手動

本文件之智慧財產權屬行政院資通安全處擁有。

項次	修改對照	GPO	TWGC B-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
							Device <u>Access</u>	
	修改後	Windows Server 2012 R2 Web Server	TWGC B-01-006-0618	系統服務	Human Interface Device <u>Service</u>	啟用並維護鍵盤、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 <u>Service</u>	手動

資料來源：本中心整理