政府組態基準
Microsoft SQL Server 2016
TWGCB-04-008
(V1.0)

行政院國家資通安全會報技術服務中心
中華民國110年9月

修訂歷史紀錄表

項次	版次	修訂日期	說明
1	1.0	110/9/1	新編
2			
3			
4			
5			

目　次

表 目 次

1. 前言

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

1.1 適用環境

本文件適用於微軟公司所發行之 Microsoft SQL Server 2016 應用程式。

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。Microsoft SQL Server 2016 組態基準共 31 項設定項目，項目統計詳見表 1。

表1　Microsoft SQL Server 2016 組態基準項目統計

項次	類別	項數	合計
1	密碼原則	2	31
2	帳戶管理	8	
3	存取授權	15	
4	稽核紀錄	3	
5	資料加密	3	

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. Microsoft SQL Server 2016 政府組態基準列表

表2　Microsoft SQL Server 2016 政府組態基準列表

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
1	TWGCB-04-008-0001	密碼原則	系統管理者帳戶強制執行密碼逾期	▪這項原則設定決定系統管理者帳戶是否啟用「強制執行密碼逾期」功能 ▪SQL 驗證登入帳戶啟用「強制執行密碼逾期」功能時，將套用 Windows 密碼原則，強制密碼到期時須進行密碼變更，以降低因長期使用同一組密碼而遭破解之情形發生，同時，可讓 SQL 驗證登入帳戶與	▪執行以下任一操作，以強制 SQL 驗證登入帳戶執行密碼逾期功能： ➢ 使用 SQL Server Management Studio(以下簡稱 SSMS)工具 (1)開啟 SSMS 工具，連線至資料庫執行個體後 (2)於「物件總管」視窗展開「安全性→登入」 (3)針對每個系統管理者帳戶按右鍵點選「屬性」，並於「一般」頁面中勾選「強制執行密碼逾期」選項後，按下「確定」 ➢ 執行 T-SQL 指令 SQL 伺服器管理者執行以下操作：	啟用，並設為 90 天以下

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				Windows 驗證登入帳戶遵循相同密碼逾期原則 ▪ Windows 密碼原則由主機管理者依照該作業系統平台 GCB 所提供之設定方法，透過群組原則設定「密碼最長使用期限」為 90 天以下	(1)執行下列指令，尋找具有 sysadmin 或相同權限但未啟用強制密碼逾期變更之 SQL 驗證登入帳戶： SELECT l.[name], 'sysadmin membership' AS 'Access_Method' FROM sys.sql_logins AS l WHERE IS_SRVROLEMEMBER('sysadmin',name) = 1 AND l.is_expiration_checked <> 1 UNION ALL SELECT l.[name], 'CONTROL SERVER' AS 'Access_Method' FROM sys.sql_logins AS l JOIN sys.server_permissions AS p ON l.principal_id = p.grantee_principal_id	

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
					WHERE p.type = 'CL' AND p.state IN ('G', 'W') AND l.is_expiration_checked <> 1; GO (2)針對步驟 1 發現之帳戶，執行下列指令： ALTER LOGIN [<login_name>] WITH CHECK_EXPIRATION = ON; GO <login_name>：帳戶名稱 ▪主機管理者接續將「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」群組原則設為 90 天以下	
2	TWG CB-04-	密碼原則	強制執行密碼原則	▪這項原則設定決定是否啟用「強制執行密碼原則」功能	▪執行以下任一操作，以強制執行密碼原則： ➢使用 SSMS 工具 (1)開啟 SSMS 工具，連線至資料庫執行個體 (2)於「物件總管」視窗展開「安全性→登入」	啟用

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
	008-0002			▪ SQL 驗證登入帳戶啟用「強制執行密碼原則」功能時，將套用 Windows 密碼原則，強制密碼必須符合複雜性需求與最小密碼長度，以降低攻擊者利用暴力破解或字典檔攻擊等方式成功取得密碼之機會，同時，可讓 SQL 驗證登入帳戶與 Windows 驗證登入帳戶遵循相同密碼原則 ▪ Windows 密碼原則由主機管理者依照該作業系統平台 GCB 所提供之設定方法，透過	(3)針對每個帳戶按右鍵點選「屬性」，並於「一般」頁面中勾選「強制執行密碼原則」選項後，按下「確定」 ➢ 執行 T-SQL 指令 SQL 伺服器管理者執行以下操作： (1)執行下列指令，尋找未啟用強制執行密碼原則之 SQL 驗證登入帳戶： SELECT name, is_disabled FROM sys.sql_logins WHERE is_policy_checked = 0; (2)針對步驟 1 發現之帳戶，執行下列指令以啟用「強制執行密碼原則」功能： ALTER LOGIN [<login_name>] WITH CHECK_POLICY = ON; GO <login_name>：帳戶名稱 ▪ 主機管理者接續將「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	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
				群組原則啟用「密碼必須符合複雜性需求」，並設定「最小密碼長度」為 12 個字元以上	性需求」設為啟用，並將「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」設為 12 個字元以上	
3	TWGCB-04-008-0003	帳戶管理	sa 帳戶	▪ 這項原則設定決定啟用或停用 sa 帳戶 ▪ sa 為安裝過程中所建立之 SQL Server 預設系統管理者帳戶，容易成為攻擊者嘗試進行密碼暴力破解之目標，建議建立一個新的系統管理者帳戶，並停用 sa 帳戶，以降低此類風險	▪ 執行下列指令，確認 sa 帳戶是否為啟用狀態： SELECT name, is_disabled FROM sys.server_principals WHERE sid = 0x01 AND is_disabled = 0; GO ▪ 若 sa 帳戶仍為啟用，執行下列指令，以停用 sa 帳戶： USE [master] GO DECLARE @tsql nvarchar(max)	停用

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				▪ sa 帳戶之主體識別碼為 1(principal_id=1)，安全性識別碼為 0x01(sid=0x01) ▪ 請務必確認已有其他帳戶可取代 sa 帳戶之角色，以避免停用 sa 帳戶後，無法正常使用系統管理功能	SET @tsql = 'ALTER LOGIN ' + SUSER_NAME(0x01) + ' DISABLE' EXEC (@tsql) GO	
4	TWG CB-04-008-0004	帳戶管理	重新命名 sa 帳戶名稱	▪ 這項原則設定決定是否變更 sa 帳戶名稱 ▪ sa 為安裝過程中所建立之 SQL Server 預設系統管理者帳戶，容易成為攻擊者嘗試進行密碼暴力破解之目標，建議重新命名 sa	▪ 執行下列指令，確認 sa 帳戶名稱是否已重新命名： SELECT name FROM sys.server_principals WHERE sid = 0x01; GO ▪ 若帳戶名稱仍為 sa，執行下列指令進行變更：	非 sa 帳戶名稱

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				帳戶名稱，以提高密碼暴力破解之困難度	ALTER LOGIN sa WITH NAME = [<Renamed_sa>]; GO <Renamed_sa>：變更後之帳戶名稱，機關可自行取為非 sa 之名稱	
5	TWG CB-04-008-0005	帳戶管理	MSSQL Server 服務帳戶所屬群組	▪ 這項原則設定決定 MSSQL Server 服務帳戶是否為管理者帳戶 ▪ SQL Server 組態管理員是 SQL Server 管理工具，可設定 SQL Server 所使用之網路通訊協定，以及管理 SQL Server 用戶端電腦之網路連接組態 ▪ 為避免運行此服務之帳戶權限過大，建議	針對每個執行個體執行下列步驟： ▪ 取得 MSSQL Server 服務所使用之帳戶名稱： (1)開啟「SQL Server 2016 組態管理員」 (2)左側視窗點選「SQL Server 服務」後，在右側視窗之「SQL Server(執行個體名稱)」上點選右鍵，接著再點選「內容」 (3)點選「登入」索引標籤，於「帳戶名稱」欄位可取得 MSSQL Server 服務所使用之帳戶名稱 ▪ 接續執行下列步驟，以確認該帳戶是否隸屬於 Administrators 群組： (1)開啟「電腦管理」	不隸屬於 Windows Administrators 群組

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				該帳戶不在 Windows Administrators 群組中，以遵循最小權限原則，降低攻擊者取得 MSSQL Server 服務權限後，因擁有較高權限而危害到系統	(2)點選「本機使用者和群組」，接著再點選「群組」 (3)確認「Administrators」群組中不包含 MSSQL Server 服務所使用之帳戶，如有，請變更至其他較低權限之群組	
6	TWG CB-04-008-0006	帳戶管理	全文檢索服務帳戶所屬群組	▪ 這項原則設定決定全文檢索(Full-Text)服務帳戶是否為管理者帳戶 ▪ 全文檢索可以快速地在結構化與半結構化資料內容與屬性上建立索引，讓 SQL Server 可進行文件篩選與斷詞	針對每個執行個體執行下列步驟： ▪ 取得全文檢索(Full-Text)服務所使用之帳戶名稱： (1)開啟「SQL Server 2016 組態管理員」 (2)左側視窗點選「SQL Server 服務」後，在右側視窗之「SQL Full-text Filter Daemon Launcher(執行個體名稱)」上點選右鍵，接著再點選「內容」 (3)點選「登入」索引標籤，於「帳戶名稱」欄位可取得全文檢索服務所使用之帳戶名稱	不隸屬於 Windows Administrators 群組

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				▪ 為避免運行此服務之帳戶權限過大，建議該帳戶不在 Windows Administrators 群組中，以遵循最小權限原則，降低攻擊者取得全文檢索服務權限後，因擁有較高權限而危害到系統	▪ 接續執行下列步驟，以確認該帳戶是否隸屬於 Administrators 群組： (1)開啟「電腦管理」 (2)點選「本機使用者和群組」，接著再點選「群組」 (3)確認「Administrators」群組中不包含全文檢索(Full-Text)服務所使用之帳戶，如有，請變更至其他較低權限之群組	
7	TWG CB-04-008-0007	帳戶管理	Guest 帳戶之連線權限	▪ 這項原則設定決定在 master、msdb 及 tempdb 以外的任何資料庫中，是否藉由移除連線權限，以停用 Guest 帳戶 ▪ 當使用者登入 SQL 伺服器，且其他資料庫允許 Guest 帳戶進行	除 master、msdb、tempdb 系統資料庫外，請針對其他任何資料庫執行下列指令，以移除 Guest 連線權限： USE [<database_name>]; GO REVOKE CONNECT FROM guest; GO <database_name>：資料庫名稱	在 master、msdb 及 tempdb 以外的任何資料庫中，移除 Guest

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				連線時，則使用者可利用 Guest 身分存取其他資料庫之資料，將可能發生非授權之存取行為而導致資料外洩，因此，除了 master、msdb 及 tempdb 系統資料庫為了維持 SQL 伺服器正常運作外，其餘資料庫應移除 Guest 帳戶之連線權限		帳戶之連線權限
8	TWG CB-04-008-0008	帳戶管理	孤兒帳戶	▪ 這項原則設定決定是否刪除孤兒(Orphaned)帳戶 ▪ 下列情況可能產生孤兒帳戶：	▪ 針對每個資料庫執行下列指令，以確認是否存在孤兒帳戶： USE [<database_name>]; GO EXEC sp_change_users_login @Action='Report';	刪除

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				➢ 帳戶對應的安全性識別碼(SID)未出現在 master 系統資料庫中 ➢ 資料庫還原或附加到其他 SQL 伺服器時，未建立登入的執行個體 ▪ 資料庫中若存在孤兒帳戶，將可能遭不當利用，應定期清查並予以刪除，以降低資安風險	GO ▪ 若發現孤兒帳戶，請接續執行下列指令予以刪除： USE [<database_name>]; GO DROP USER [<user_name>]; GO <database_name>：資料庫名稱 <user_name>：孤兒帳戶名稱	
9	TWG CB-04-	帳戶管理	使用者身分驗證模式	▪ 這項原則設定決定當使用者登入執行個體時使用何種驗證模式	▪ 執行以下任一操作，以採用 Windows 驗證模式： ➢ 使用 SSMS 工具 (1)開啟 SSMS 工具，連線至資料庫執行個體	Windows 驗證模式

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
	008-0009			▪ SQL Server 提供下列 2 種驗證模式： ➢ Windows 驗證模式：SQL Server 只允許合法的 Windows 本機/網域使用者登入 ➢ 混合模式(SQL Server 驗證與 Windows 驗證)：除了允許合法的 Windows 本機/網域使用者登入外，也允許其他使用 SQL Server 所建立與管理之使用者帳戶登入	(2)於「物件總管」視窗之執行個體名稱上按右鍵點選「屬性」 (3)在「伺服器屬性」視窗中選取「安全性」頁面，將伺服器驗證設為「Windows 驗證模式」後，按下「確定」 ➢ 執行 T-SQL 指令 SQL 伺服器管理者執行下列指令： USE [master] GO EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'LoginMode', REG_DWORD, 1 GO ▪ 完成後，請重新啟動伺服器以使設定生效	

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				▪ 僅系統管理者可變更此項設定，此外，無論選擇何種模式，Windows 驗證模式一定啟用且無法停用 ▪ 因 Windows 驗證模式採用較安全之驗證機制，以及支援較周全之密碼強化設定與帳戶鎖定功能，建議選擇「Windows 驗證模式」		
10	TWG CB-04-008-0010	帳戶管理	自主資料庫使用者類型	▪ 這項原則設定將確認自主資料庫(Contained Database)內不包含採用 SQL 驗證之使用者	▪ 執行下列指令，尋找系統中是否有自主資料庫： SELECT name FROM sys.databases WHERE containment=1; GO	僅允許 Windows 驗證使用者

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				▪ 自主資料庫與裝載資料庫之 SQL Server 執行個體之間彼此是獨立隔離的，當需將自主資料庫搬移到另一個執行個體時，無須額外的管理組態作業 ▪ 自主資料庫不使用原有的 SQL 登入方式，改提供下列兩種使用者類型進行登入： ➢ 具有密碼之 SQL 驗證使用者：使用者帳戶與密碼直接存在該自主資料庫 ➢ Windows 驗證使用者：已授權之 Windows 使用者或	▪ 如有自主資料庫，請針對每個自主資料庫執行下列指令，以確認是否存在 SQL 驗證使用者： USE [<database_name>] GO SELECT name AS DBUser FROM sys.database_principals WHERE name NOT IN ('dbo','Information_Schema','sys','guest') AND type IN ('U','S','G') AND authentication_type = 2; GO ▪ 若自主資料庫中存在 SQL 驗證使用者，請刪除使用者： USE [<database_name>] GO DROP User [<login_name>]	

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				Windows 群組的成員可直接連接至自主資料庫 ▪ 由於具有密碼之 SQL 驗證使用者帳戶不會強制套用密碼複雜度規則，可能因使用弱密碼而遭攻擊者成功破解密碼，進而存取或變更資料庫內容，故建議僅允許 Windows 驗證使用者可登入自主資料庫	GO <database_name>：自主資料庫名稱 <login_name>：帳戶名稱	
11	TWG CB-04-	存取授權	預設服務埠	▪ 這項原則設定決定是否修改資料庫預設服務埠	▪ 執行以下操作，以修改預設服務埠： (1)開啟「SQL Server 2016 組態管理員」	非 1433 埠

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
	008-0011			▪ SQL Server 預設服務埠為 1433，改用其他埠可防止遭攻擊者針對預設服務埠進行攻擊	(2)左側視窗展開「SQL Server 網路組態→<執行個體名稱>的通訊協定」後，在右側視窗之「TCP/IP」名稱上按右鍵點選「內容」 (3)在「TCP/IP 內容」視窗中點選「IP 位址」索引標籤，將 IPAll 段落之 TCP Port 改為非 1433 埠 ▪ 完成後，請重新啟動伺服器以使設定生效	
12	TWGCB-04-008-0012	存取授權	msdb 資料庫共用角色之 SQL Server Agent Proxy 存取權限	▪ 這項原則設定決定 msdb 資料庫共用(public)角色是否可具有 SQL Server Agent Proxy 存取權限 ▪ 共用(public)角色包含 msdb 資料庫內所有使用者帳戶 ▪ SQL Server Agent 是 Windows 服務，透過	▪ 執行下列指令，檢查 msdb 資料庫之共用角色已擁有哪些 SQL Server Agent Proxy 的存取權限： USE [msdb] GO SELECT sp.name AS proxyname FROM dbo.sysproxylogin spl JOIN sys.database_principals dp ON dp.sid = spl.sid JOIN sysproxies sp	msdb 資料庫共用角色不具有 SQL Server Agent Proxy 存取權限

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				該服務可建立排程與設計批次作業(如定期備份資料庫)，運用 SQL Server Agent Proxy，可進一步定義作業步驟的安全性內容，包含執行該步驟之使用者身分，以及該使用者可存取之子系統 ▪ SQL Server Agent Proxy 存取權限可授予下列 3 種身分，符合身分之使用者就可以使用作業步驟中的 Proxy： (1)SQL Server 登入使用者	ON sp.proxy_id = spl.proxy_id WHERE principal_id = USER_ID('public'); GO ▪ 若共用角色擁有 Proxy 存取權限，請將每個可存取之 Proxy 的名稱(<proxy_name>)帶入下列指令，以進行權限移除： USE [msdb] GO EXEC dbo.sp_revoke_login_from_proxy @name = N'public', @proxy_name =N'<proxy_name>'; GO	

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				(2)伺服器角色 (3)msdb 資料庫中的角色 ▪若 msdb 資料庫中的共用角色具有 SQL Server Agent Proxy 存取權限，將可能導致 msdb 資料庫內所有使用者帳戶透過該 Proxy 所賦予權限，執行原權限以外之動作，進而造成系統危害，應遵循最小權限原則，禁止該角色擁有 SQL Server Agent Proxy 存取權限 ▪注意：從 SQL Server Agent Proxy 移除共用		

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
				角色前，請確認已新增同等權限之登入帳戶或資料庫角色，否則與該 Proxy 有關之存取將會失敗		
13	TWGCB-04-008-0013	存取授權	特定分散式查詢方式	▪ 這項原則設定決定是否啟用特定分散式查詢(Ad Hoc Distributed Queries)功能，以存取多個不同來源之資料 ▪ 特定分散式查詢透過在 OPENROWSET 與 OPENDATASOURCE 函數中定義使用 OLE DB(Object Linking and Embedding Database)存取遠端資料所需之連線資訊(如提供者名	執行以下任一操作，以停用特定分散式查詢方式： ➢ 使用 SSMS 工具 (1)開啟 SSMS 工具，連線至資料庫執行個體 (2)於「物件總管」視窗之執行個體名稱上按右鍵點選「Facet」 (3)在「檢視 Facet」視窗中選取「一般」頁面，並於「Facet」選項選擇「介面區組態」後，將「AdHocRemoteQueriesEnabled」屬性設為 False	停用

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				稱、帳號及密碼等)，以成功取得資料 ▪ 啟用特定分散式查詢時，將可能遭攻擊者濫用，對遠端 SQL Server 進行遠端存取與漏洞利用，或執行惡意語法，停用此功能以降低資安風險 ▪ 此功能預設為停用，如欲變更這項設定需具備系統管理者(sysadmin)或伺服器管理員(serveradmin)固定伺服器角色之權限	(4)接續於「Facet」選項選擇「伺服器組態」，將「AdHocRemoteQueriesEnabled」屬性設為 False，並按下「確定」 ➢ 執行 T-SQL 指令 SQL 伺服器管理者執行下列指令： EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure 'Ad Hoc Distributed Queries', 0; RECONFIGURE; GO EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE; GO	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
14	TWGCB-04-008-0014	存取授權	跨資料庫擁有權鏈結	▪ 這項原則設定決定是否啟用跨資料庫擁有權鏈結功能 ▪ 啟用此功能時，將允許資料庫中具有db_owner 角色之使用者可存取另一個資料庫中由其他使用者所擁有的物件，將可能導致資料外洩 ▪ 此功能預設為停用，如欲變更這項設定需具備系統管理者(sysadmin)或伺服器管理員(serveradmin)固定伺服器角色之權限	執行下列指令，以停用跨資料庫擁有權鏈結功能： EXECUTE sp_configure 'cross db ownership chaining', 0; RECONFIGURE; GO	停用

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				▪ 使用者可以透過使用者介面(UI)之「執行個體→屬性→安全性」，選取「跨資料庫擁有權鏈結」進行設定 ▪ 在 master、model 及 tempdb 系統資料庫中，無法變更此項設定		
15	TWG CB-04-008-0015	存取授權	Database mail XPs	▪ 這項原則設定決定是否啟用 Database Mail XPs，以透過 SQL Server 發送電子郵件 ▪ 啟用 Database Mail XPs 後，可透過 Database Mail 服務直	執行以下任一操作，以停用 Database Mail XPs： ➢ 使用 SSMS 工具 (1)開啟 SSMS 工具，連線至資料庫執行個體 (2)於「物件總管」視窗之執行個體名稱上按右鍵點選「Facet」 (3)在「檢視 Facet」視窗中選取「一般」頁面，並於「Facet」選項選擇「介面區組	停用

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				接將資料庫查詢結果以電子郵件方式發送給使用者 ▪ Database Mail 相關組態設定與帳戶資訊(如帳戶名稱、電子郵件地址)皆儲存在 msdb 資料庫中 ▪ 啟用 Database Mail XPs 後，將可能遭受阻斷服務攻擊或導致資料外洩，建議停用此功能，以降低此類資安風險 ▪ 此功能預設為停用，如欲變更這項設定需具備系統管理者(sysadmin)或伺服器管	態」後，將「DatabaseMailEnabled」屬性設為 False (4)接續於「Facet」選項選擇「伺服器組態」，將「DatabaseMailEnabled」屬性設為 False，並按下「確定」 ➢ 執行 T-SQL 指令 SQL 伺服器管理者執行下列指令： EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure 'Database Mail XPs', 0; RECONFIGURE; GO EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE;	

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				理員(serveradmin)固定伺服器角色之權限	GO	
16	TWG CB-04-008-0016	存取授權	專用管理者連線	▪ 這項原則設定決定是否啟用專用管理者連線(Dedicated Administrative Connection, 簡稱 DAC) ▪ DAC 預設使用 1434 埠進行連線，當 SQL Server 運作異常、遭鎖定或沒有回應時，系統管理者可透過 DAC 針對 SQL Server 進行診斷作業、執行查詢語法或排除障	▪ 執行以下任一操作，以停用專用管理者連線： ➢ 使用 SSMS 工具 (1)開啟 SSMS 工具，連線至資料庫執行個體 (2)於「物件總管」視窗之執行個體名稱上按右鍵點選「Facet」 (3)在「檢視 Facet」視窗中選取「一般」頁面，並於「Facet」選項選擇「介面區組態」後，將「RemoteDacEnabled」屬性設為 False (4)接續於「Facet」選項選擇「伺服器組態」，將「RemoteDacEnabled」屬性設為 False，並按下「確定」 ➢ 執行 T-SQL 指令 SQL 伺服器管理者執行下列指令：	停用

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				礙，停用 DAC 可減少系統被攻擊面 ▪ 此功能預設為停用，如欲變更這項設定需具備系統管理者(sysadmin)權限	EXECUTE sp_configure 'remote admin connections', 0; RECONFIGURE; GO	
17	TWG CB-04-008-0017	存取授權	隱藏執行個體	▪ 這項原則設定決定是否隱藏資料庫引擎執行個體(Hide Instance) ▪ SQL Server 使用 SQL Server Browser 服務列舉電腦上安裝的資料庫引擎執行個體，讓用戶端應用程式瀏覽伺服器時，可區別同一部電腦上之多個執行個體	執行以下任一操作，以隱藏執行個體： ➢ 使用 SQL Server 2016 組態管理員工具 (1)開啟「SQL Server 2016 組態管理員」 (2)左側視窗展開「SQL Server 網路組態→<執行個體名稱>的通訊協定」後，在「<執行個體名稱>的通訊協定」名稱上按右鍵點選「內容」 (3)點選「旗標」索引標籤，將「Hide Instance」設為「是」，並按下「確定」 ➢ 執行 T-SQL 指令	啟用

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				▪單一伺服器資料庫建議停用此功能，可防止因不當列舉而導致執行個體資料外洩之情況，以提高資料庫安全性	SQL 伺服器管理者執行下列指令： EXEC master.sys.xp_instance_regwrite @rootkey = N'HKEY_LOCAL_MACHINE', @key = N'SOFTWARE\Microsoft\Microsoft SQL Server\MSSQLServer\SuperSocketNetLib', @value_name = N'HideInstance', @type = N'REG_DWORD', @value = 1; GO	
18	TWG CB-04-008-0018	存取授權	自主資料庫自動關閉	▪這項原則設定決定自主資料庫是否啟用自動關閉功能 ▪由於自主資料庫直接在資料庫中驗證使用者身分，並非在伺服器層級或執行個體層	執行以下操作，以停用自主資料庫自動關閉功能： ➢ 執行下列指令，尋找系統中是否有自主資料庫啟用自動關閉功能： (1) SELECT name, containment, containment_desc, is_auto_close_on FROM sys.databases	停用

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				級執行，若啟用自動關閉功能，當使用者連線結束時將自動關閉資料庫，頻繁的開啟或關閉資料庫將造成效能降低，使得攻擊者可利用此特性進行阻斷服務攻擊，停用此功能以降低資安風險	WHERE containment <> 0 and is_auto_close_on = 1; GO (2) 如有自主資料庫啟用自動關閉功能，請執行下列指令，以停用該資料庫之自動關閉功能： ALTER DATABASE [<database_name>] SET AUTO_CLOSE OFF; GO <database_name>：自主資料庫名稱	
19	TWG CB-04-008-0019	存取授權	共通語言執行環境	▪ 這項原則設定決定是否啟用共通語言執行環境(Common Language Runtime, 簡稱 CLR) ▪ SQL 伺服器支援.NET 共通語言執行環境，	▪ 執行下列指令，以停用共通語言執行環境： EXECUTE sp_configure 'clr enabled', 0; RECONFIGURE; GO ▪ 或執行下列指令，啟用共通語言執行環境，並將共通語言執行環境程序集設為 SAFE：	停用，或啟用並將共通語言執行環境程序

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				可以透過.NET 組件定義包含預存程序、觸發程序、使用者自訂函數、使用者自訂型態及使用者自訂彙總函數等 5 種 SQL 物件 ▪ 停用此項設定，可避免因執行.NET 惡意程式碼而危害系統安全 ▪ 如需啟用此項設定，應進一步設定共通語言執行環境程序集，選項如下： ➢ SAFE：預設為此等級，僅能存取 SQL Server 內部資源	EXECUTE sp_configure 'clr enabled', 1; RECONFIGURE; ALTER ASSEMBLY <assembly_name> WITH PERMISSION_SET = SAFE; EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE; GO <assembly_name>：CLR 程序集名稱	集設為 SAFE

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				➢ EXTERNAL_ACCESS：除可存取 SAFE 等級之資源外，亦可存取外部系統的資源，例如檔案、網路及系統環境變數等 ➢ UNSAFE：除可存取 EXTERNAL_ACCESS 等級之資源外，亦可存取作業系統所有資源		
20	TWG CB-04-	存取授權	Ole 自動化程序	▪ 這項原則設定決定是否啟用 Object Linking and Embedding (Ole)自動化程序	▪ 執行以下任一操作，以停用 Ole 自動化程序： ➢ 使用 SSMS 工具 (1)開啟 SSMS 工具，連線至資料庫執行個體	停用

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
	008-0020			▪ 啟用 Ole 自動化程序時，Ole 自動化物件可在 Transact-SQL 批次內部啟動，將可能因惡意物件而危害資料庫安全，建議停用以降低此類風險 ▪ 這項設定預設為停用，如欲變更需具備系統管理者(sysadmin)或伺服器管理員(serveradmin)固定伺服器角色之權限	(2)於「物件總管」視窗之執行個體名稱上按右鍵點選「Facet」 (3)在「檢視 Facet」視窗中選取「一般」頁面，並於「Facet」選項選擇「介面區組態」後，將「OleAutomationEnabled」屬性設為 False (4)接續於「Facet」選項選擇「伺服器組態」，將「OleAutomationEnabled」屬性設為 False，並按下「確定」 ➢ 執行 T-SQL 指令 SQL 伺服器管理者執行下列指令： EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure 'Ole Automation Procedures', 0; RECONFIGURE;	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
					GO EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE; GO	
21	TWGCB-04-008-0021	存取授權	遠端存取	▪ 這項原則設定決定是否啟用遠端存取(remote access)功能 ▪ 遠端存取功能會控制本機或遠端伺服器(SQL Server 執行個體的執行所在)上執行的預存程序 ▪ 若設為啟用，可從遠端伺服器執行本機預存程序，或從本機伺服器執行遠端預存程	▪ 執行下列指令，以停用遠端存取功能： EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure 'remote access', 0; RECONFIGURE; GO EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE; GO ▪ 完成後，請重新啟動伺服器以使設定生效	停用

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				序，將可能因誤用而導致遠端伺服器對其他主機執行阻斷服務攻擊 ▪若設為停用，則無法在遠端伺服器上執行本機預存程序，亦無法在本機伺服器上執行遠端預存程序 ▪這項設定預設為啟用，如欲變更需具備系統管理者(sysadmin)或伺服器管理員(serveradmin)固定伺服器角色之權限		
22	TWG CB-	存取授權	掃描啟動程序	▪這項原則設定決定在 SQL Server 啟動期間	▪執行下列指令，以停用掃描啟動程序：	停用

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
	04-008-0022			是否掃描並執行所有自動執行預存程序 ▪啟用這項設定時，可於啟動 SQL Server 時自動執行所有預存程序，但可能因自動執行惡意程序而危害系統安全，建議停用以降低此類風險 ▪這項設定預設為停用，如欲變更需具備系統管理者(sysadmin)權限	EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure 'scan for startup procs', 0; RECONFIGURE; GO EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE; GO ▪完成後，請重新啟動伺服器以使設定生效	
23	TWGCB-04-	存取授權	Trustworthy	▪這項原則設定決定是否啟用 Trustworthy 資料庫屬性	針對除 msdb 外之其他資料庫執行下列指令，以將 Trustworthy 屬性設為停用： ALTER DATABASE [<database_name>] SET TRUSTWORTHY OFF;	停用

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
	008-0023			▪ Trustworthy 資料庫屬性是用來指定 SQL Server 執行個體是否信任資料庫及其中的內容 ▪ 啟用 Trustworthy 資料庫屬性時，將允許該資料庫物件存取其他資料庫物件，可能因執行.NET 惡意程式碼而危害系統安全，建議停用以降低此類風險 ▪ 這項設定在 msdb 系統資料庫預設為啟用，以確保 SQL Server 正常運作，在其他資料庫則預設為停用，如	GO <database_name>：資料庫名稱	

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				欲變更需具備系統管理者(sysadmin)權限		
24	TWG CB-04-008-0024	存取授權	xp_cmdshell	▪ 這項原則設定決定是否啟用 xp_cmdshell ▪ 啟用 xp_cmdshell 時，攻擊者可嘗試利用此功能向底層作業系統執行讀取檔案、寫入資料或提升權限等動作，建議停用以降低資安風險 ▪ 這項設定預設為停用，如欲變更需具備系統管理者(sysadmin)或伺服器管理員(serveradmin)固定伺服器角色之權限	▪ 執行以下任一操作，以停用 xp_cmdshell： ➢ 使用 SSMS 工具 (1)開啟 SSMS 工具，連線至資料庫執行個體 (2)於「物件總管」視窗之執行個體名稱上按右鍵點選「Facet」 (3)在「檢視 Facet」視窗中選取「一般」頁面，並於「Facet」選項選擇「介面區組態」後，將「XPCmdShellEnabled」屬性設為 False (4)接續於「Facet」選項選擇「伺服器組態」，將「XPCmdShellEnabled」屬性設為 False，並按下「確定」 ➢ 執行 T-SQL 指令 SQL 伺服器管理者執行下列指令：	停用

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
					EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure 'xp_cmdshell', 0; RECONFIGURE; GO EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE; GO	
25	TWG CB-04-008-0025	存取授權	範例資料庫	▪ 這項原則設定決定是否刪除範例資料庫 ▪ 範例資料庫可供使用者快速學習 SQL 語法與熟悉資料庫操作方式	▪ 執行以下操作，以刪除範例資料庫： (1)執行下列指令，列舉所有資料庫名稱： SELECT name, database_id, create_date FROM sys.databases ; GO	刪除

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				▪為避免範例資料庫因設定不當，遭攻擊者利用進行攻擊，應刪除所有範例資料庫 ▪下列為常見之範例資料庫名稱： ➢pubs ➢Northwind ➢AdventureWorks ➢WorldwideImporters	(2)若發現範例資料庫，執行下列指令予以刪除： DROP database [<database_name>] GO <database_name>：範例資料庫名稱	
26	TWG CB-04-008-0026	稽核紀錄	錯誤記錄檔的最大數目	▪這項原則設定決定錯誤記錄檔之最大數目 ▪錯誤記錄檔內容包含使用者嘗試登入資訊，以及 SQL 伺服器事件內容，可用以協	執行下列指令，將錯誤記錄檔的最大數目設為 12 以上： EXEC master.sys.xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'NumErrorLogs',	12 以上

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				助排除障礙與查找資安事件發生原因 ▪ SQL Server 預設會保留前 6 個錯誤記錄檔，每次啟動 SQL Server 執行個體時會建立新的錯誤記錄檔，系統預存程序 sp_cycle_errorlog 可用以循環錯誤記錄檔，當錯誤記錄檔達到最大數目時，將刪除時間最早之錯誤記錄檔，應設定錯誤記錄檔的最大數目，以減少發生錯誤記錄檔遭刪除而遺失重要資訊之情形	REG_DWORD, <NumberAbove12>; RECONFIGURE; GO <NumberAbove12>：12 以上之數字	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
27	TWGCB-04-008-0027	稽核紀錄	預設追蹤	▪ 這項原則設定決定是否啟用預設追蹤 ▪ 預設追蹤功能可記錄包含建立帳戶、權限提升及執行DBCC(Database Consistenecy Checker)指令等資料庫動作，這些資訊可協助系統管理者排除障礙與查找資安事件發生原因 ▪ 這項設定預設為啟用，如欲變更需具備系統管理者(sysadmin)或伺服器管理員(serveradmin)固定伺服器角色之權限	▪ 執行以下任一操作，以啟用預設追蹤： ➢ 使用 SSMS 工具 (1)開啟 SSMS 工具，連線至資料庫執行個體 (2)於「物件總管」視窗之執行個體名稱上按右鍵點選「Facet」 (3)在「檢視 Facet」視窗中選取「一般」頁面，並於「Facet」選項選擇「伺服器組態」後，將「DefaultTraceEnabled」屬性設為 True，並按下「確定」 ➢ 執行 T-SQL 指令 SQL 伺服器管理者執行下列指令： EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure 'default trace enabled', 1; RECONFIGURE;	啟用

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
					GO EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE; GO	
28	TWGCB-04-008-0028	稽核紀錄	登入稽核紀錄	▪ 這項原則設定決定是否啟用登入稽核紀錄，以及早發現異常登入行為 ▪ 登入稽核分為 4 種設定選項： ➢ 無 ➢ 僅限失敗的登入 ➢ 僅限成功的登入 ➢ 失敗和成功的登入	▪ 執行下列指令，將登入稽核選項設為「失敗和成功的登入」： EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD,3 GO ▪ 完成後，請重新啟動伺服器以使設定生效	失敗和成功的登入

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
29	TWGCB-04-008-0029	資料加密	備份服務主金鑰	▪ 這項原則設定決定是否備份服務主密鑰(Service Master Key)，並設定密碼加以保護 ▪ 服務主金鑰會在 SQL Server 執行個體第一次啟動時自動產生，用以加密各資料庫之連結伺服器密碼、憑證及資料庫主金鑰 ▪ 服務主金鑰之備份與復原，對於資料庫完整還原非常重要，應妥善保存	執行下列指令，以備份服務主金鑰並予以加密： BACKUP SERVICE MASTER KEY TO FILE = '<path_to_file>' ENCRYPTION BY PASSWORD = '<password>'; GO <path_to_file>：服務主金鑰備份檔案欲存放路徑 <password>：欲設定之密碼	建立服務主金鑰備份
30	TWGCB-04-	資料加密	備份資料庫主金鑰	▪ 這項原則設定決定是否備份資料庫主金鑰(Database Master	執行下列指令，以備份資料庫主金鑰並加密： BACKUP MASTER KEY TO FILE = '<path_to_file>' ENCRYPTION BY PASSWORD = '<password>';	建立資料庫主

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
	008-0030			Key)，並設定密碼加以保護 ▪ 資料庫主金鑰可用來加密資料庫內部的其他非對稱金鑰、對稱金鑰及憑證 ▪ 若資料庫主金鑰遭刪除或損毀，將導致 SQL Server 無法執行解密動作，為避免此類風險發生，建議應備份資料庫主金鑰，並加密後妥善保存	GO <path_to_file>：資料庫主金鑰備份檔案欲存放路徑 <password>：欲設定之密碼	金鑰備份
31	TWG CB-04-	資料加密	TLS 加密協定	▪ 這項原則設定決定允許資料庫使用哪些 TLS 加密協定版本	執行「regedit」指令啟動登錄編輯程式，並於「HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\」路徑下設定下	啟用 TLS 1.2，停用 TLS

項次	TWG CB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
	008-0031			▪ 因安全通訊協定(SSL)與舊版本傳輸層安全協定(TLS)存在已知漏洞，可能因未經授權存取導致資料外洩，故僅使用 TLS 1.2 加密協定，並停用舊版 TLS 加密協定	列機碼值，以啟用 TLS 1.2，並停用 TLS1.2 以下版本： (1)「TLS 1.0\Client\DisabledByDefault」設為 1 (2)「TLS 1.0\Client\Enabled」設為 0 (3)「TLS 1.0\Server\DisabledByDefault」設為 1 (4)「TLS 1.0\Server\Enabled」設為 0 (5)「TLS 1.1\Client\DisabledByDefault」設為 1 (6)「TLS 1.1\Client\Enabled」設為 0 (7)「TLS 1.1\Server\DisabledByDefault」設為 1 (8)「TLS 1.1\Server\Enabled」設為 0 (9)「TLS 1.2\Client\DisabledByDefault」設為 0 (10)「TLS 1.2\Client\Enabled」設為 1 (11)「TLS 1.2\Server\DisabledByDefault」設為 0 (12)「TLS 1.2\Server\Enabled」設為 1	1.2 以下版本

資料來源：本中心整理

3. 參考文獻

[1]Center for Internet Security, CIS Microsoft SQL Server 2016 Benchmark v1.2.0.

https://www.cisecurity.org/cis-benchmarks/

[2]Defense Information Systems Agency (DISA), MS SQL Server 2016 Database STIG Version: 1 Release: 5.

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

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

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