

教育部 111 年度補助國立圖書館發展館藏特色  
及強化營運服務計畫

資通訊系統與資料安全升級計畫(一)

執行成果報告

執行單位：國家圖書館

112 年 2 月 3 日

# 壹、計畫目標

## 一、計畫背景

本館持續維運的資訊系統與服務平臺逾 60 個、典藏數位資料逾 1 億 1,000 萬筆、保存數位檔案逾 250TB，每年資訊服務次數高達 4 億，確保「資通訊系統及資料安全」尤為重要。本館已盤點、評估各資訊系統的資安風險，並持續地就具有資安問題的系統與設備進行安全漏洞的修補、作業系統及資料庫版本的升級等作業，110 年在補助經費的支持下完成「全國新書資訊網」、「國際標準錄音錄影資料碼系統」、「電子書刊送存閱覽服務系統」及「臺灣書目整合查詢系統」升級工作。111 年將持續推動資安升級工作，在有限的經費額度下，依系統使用率、重要性及資安風險評鑑結果，擇選二個系統進行系統安全升級；同時為確保資料的安全，將就已購置經年、效能已不敷使用的伺服器主機及存儲設備進行汰換。

有鑑於網路技術與通訊科技不斷的推陳出新，資訊安全持續受到高度重視的環境下，唯有建構安全的資通訊環境與完整的資料安全防護，才能提供讀者便利安全的資訊服務，也才能面對未來資安議題的各種挑戰與衝擊。

## 二、預期目標

本案計畫目標有二：

### (一) 資訊系統版本升級，確保系統安全

為符應無障礙網頁規範、資訊系統向上集中、資訊安全等政策規定，進行官網及活動報名系統主機架構優化、測試環境建置及取得新版無障礙標章等，以建置安全穩定的網站環境。

### (二) 資訊設備汰換，確保資料安全

辦理 102-103 年老舊伺服器主機及儲存設備汰換，以提升資訊安全及效能。

## 三、內容要項

### (一) 系統架構優化暨官網無障礙網頁重新取得標章認證

1. 為符合教育部向上集中、行政院主機組態基準值(GCB)等要求，重新調整系統架構，關閉非必要的服務埠，導入政府組態基準作業、建置測試環境，符合資安政策。
2. 辦理升級主機包括 2 部官網前臺網站，以及活動報名前臺網站、資料庫、FILE SERVER、網站內容管理及測試環境等，因應軟體升級並重新設定主機 WEBCONFIG 環境、備份及校時等工作排程功能的統整、程式修正、資料搬

移及效能調校。

3. 官網中英文網站重新取得政府無障礙網頁開發規範最新版 A 級標章。

## (二) 伺服器及儲存設備汰換

本館目前使用於虛擬環境之實體伺服器有 18 臺、共用儲存設備有 17 臺，其中 104 年以前(不含 104 年)購置之實體伺服器 4 臺、儲存設備 10 臺，老舊伺服器及儲存設備其安全與效能已難以負荷現今運算及存儲所需，且故障率偏高，故本項計畫擬汰換老舊設備，包括汰換伺服器 2 臺(102 年購置 DELL R720 1 臺、103 年購置 DELL R820 1 臺)及新購儲存設備 1 臺(可使用空間 70TB)，汰換 99 年~102 年儲存設備 2 臺(IBM DS4700、infotrend enstor 總計可用空間 33TB)，以提高服務效能。

設備	預訂規格	台數	預估單價	金額
伺服器	2U 伺服器 Intel Xeon Gold 系列 16 核心 2.9GHz 以上二顆 RAM 512GB	2	540,000 元	1,080,000 元
儲存設備	2U 機架式提供 2 組以上控制器，記憶體合計總容量 64GB。提供 FC to SAS 硬碟轉數 10000RPM(含)以上，可用空間達 66TB 以上。	1	1,520,000 元	1,520,000 元
				2,600,000 元

表 1: 預計採購設備明細

## 貳、成果內容

### 一、執行方式

#### (一) 系統架構優化暨官網無障礙網頁重新取得標章認證

1. 擬訂軟體規格與需求，撰寫專案需求招標文件，招標案於 1/3 簽奉核准，1/21 日決標。
2. 依經濟部工業局共同供應契約購置微軟作業系統 Windows 2022 Server 及資料庫 Microsoft SQL Server 2019 軟體以升級原有的系統，並於 5/16 日完成驗收。
3. 6/17 日辦理專案會議，確認系統架構優化相關軟硬體資源配置，廠商依規

定提交系統架構優化相關軟硬體資源配置規劃及系統主機升級安裝計畫書，7/6 日完成專案第 1 期驗收。

4. 8/17 日完成虛擬主機作業系統等軟體安裝及網站服務軟體部署。另官網中英文網站分別於 9/7 日及 9/25 日通過全網站無障礙 A 級新版 Freego2.0 軟體機器檢測報告，10/5 日完成專案第 2 期驗收。
5. 官網英文網站於 10 月 4 日通過人工檢測取得新版無障礙網頁標章，官網中文網站於 10 月 31 日通過人工檢測取得新版無障礙網頁標章。
6. 官網及活動報名等網站完成導入 HTTPS 傳輸協定服務，並於 12/19 日完成新主機升級移轉作業，廠商提交系統架構優化功能測試之書面確認文件及資安檢測報告，112/1/3 日完成專案第 3 期驗收(全案驗收)。

## (二) 伺服器主機及儲存設備汰換

1. 辦理採購作業：擬訂規格與需求，撰寫專案需求招標文件，並辦理招標事宜。
2. 安裝及設定作業：由廠商進行設備軟硬體安裝及設定，將新設備加入本館虛擬主機及儲存池，舊設備移作測試環境使用，並進行測試。
3. 驗收與付款作業。

## 二、執行進度

計畫項目 \ 月份	1	2	3	4	5	6	7	8	9	10	11	12
<b>全球資訊網無障礙網頁 A 級標章重新認證及主機升級調整</b>												
1.細部需求建構	◆	◆	◆									
2.擬訂規格與需求，撰寫專案需求招標文件，並辦理招標事宜。			◆	◆	◆	◆						
3.優化網站及調整網頁、主機升級移轉作業、測試							◆	◆	◆	◆	◆	
4.驗收與付款											◆	◆
<b>伺服器主機及儲存設備汰換</b>												
1.擬訂規格與需求，撰寫專案需求招標文件，並辦理招標事宜。	◆	◆										
2.廠商履約安裝及設定、測試			◆	◆	◆	◆						
3.驗收與付款						◆						

### 三、績效成果

(一) 系統架構優化建構安全穩定的網站環境，有效提升網站服務品質。官網無障礙網頁重新取得標章認證並確保所有網頁正常持續運作，將提供身心障礙者無障礙使用網頁服務，保障他們獲取公共資訊之權益。

#### 1. 完成 8 臺虛擬主機作業系統等軟體安裝及網站服務軟體部署

項次	設備名稱及數量	配置說明
1	官網前端 WEB 虛擬主機 2 臺	作業系統 Windows 2022 Server 標準版 Microsoft® .NET Framework 4.8 IIS 10.0
2	活動報名前端 WEB 虛擬主機 1 臺	作業系統 Windows 2022 Server 標準版 Microsoft® .NET Framework 4.8 IIS 10.0
3	官網及活動報名後臺管理系統虛擬主機 1 臺	作業系統 Windows 2022 Server 標準版 Microsoft® .NET Framework 4.8 IIS 10.0
4	官網及活動報名系統資料庫 虛擬主機 1 臺	作業系統 Windows 2022 Server 標準版 Microsoft SQL Server 2019 標準版
5	官網及活動報名系統 File Server 虛擬主機 1 臺	作業系統 Windows 2022 Server 標準版 Microsoft® .NET Framework 4.8 IIS 10.0
6	官網及活動報名系統測試環境 虛擬主機 1 臺	作業系統 Windows 2022 Server 標準版 Microsoft® .NET Framework 4.8 IIS 10.0
7	官網及活動報名系統跳板 虛擬主機 1 臺	作業系統 Windows 2022 Server 標準版

2. 主機完成設定行政院要求的組態基準值(GCB)，並建立例外清單。

部署資源

項目	部署資源
作業系統	TWGCB-01-009_Microsoft Windows Server 2019 (V1.0)
瀏覽器	TWGCB-02-006_Microsoft Edge (V1.0)
應用程式	TWGCB-04-002_Microsoft IIS 8.5 (V1.2)
	TWGCB-04-008_Microsoft SQL Server 2016 (V1.0)

#### 組態基準項目

項目	項數	小計	合計
Windows Server 2019 Account Settings	9	313	554
Windows Server 2019 Common Settings	304		
Windows Server 2019 File Server	122	122	
Windows Server 2019 Web Server	119	119	
Microsoft Edge	61	61	61
Microsoft IIS 8.5	54	54	54
Microsoft SQL Server 2016	31	31	31

3.設定備份排程，保存資料庫備份及最近 6 個月之日誌紀錄於外部備份主機。

4.建置測試主機環境，達成正式環境與測試環境實體隔離的目標。

5.調整架構，分享檔案的方式以 FTP 23 PORT 取代原本不安全的網芳 445 139 PORT。

(二) 新購 2 臺 DELL EMC R750 伺服器(總記憶體 1TB)、1 臺 DELL EMC Unity XT380 儲存設備(儲存空間 70TB 以上)及 2 臺 10G 網路交換器，汰換老舊伺服器及儲存設備，有效提升系統運算及存取效能。

(三) 購置 Netwrix 軟體，建立廠商遠端連線之側錄機制，符合系統防護基準要求。

## 參、成效檢討

一、系統架構優化暨官網無障礙網頁重新取得標章認證

1.因修補資安弱掃問題，升級官網前臺主機 jQuery 套件(1.12.9→3.6.1)，導致部份網

頁版面因升級後無法正常呈現，必須尋找替換套件，而系統則不斷因應資安漏洞修補辦理軟體升級而持續調整修正程式，影響網站的正常運作，目前已建置測試主機環境，可先行於測試主機修正後再於正式環境上線，以降低風險。

2. 目前主機已依行政院要求的現行組態基準值(GCB)設定，惟該 GCB 設定作業系統 WINDOWS 2019、IIS8.5 及資料庫 SQL2016 的版本較舊，俟後續行政院組態基準值(GCB)發布與現行網站主機符合版本(WINDOWS 2022、IIS10 及資料庫 SQL2019 的版本)的設定如有不同處將進行調整，而系統將因應 GCB 調整影響網站的正常運作，今已建置測試主機環境，可先行於測試主機修正後再於正式環境上線，以降低風險。

3. 為保障身心障礙者權益，「各級政府及其附屬機關(構)、學校所建置之網站，應通過無障礙檢測，並取得認證標章」，惟標章自核發起 3 年有效，3 年後仍須重新辦理檢測，配合新規範持續修正網站版型程式，並調校升級相關軟體功能，以維持所有網頁及功能之正常持續運作，目前已建置測試主機環境，可先行於測試主機修正後再於正式環境上線，以降低風險。

## 二、伺服器及儲存設備汰換

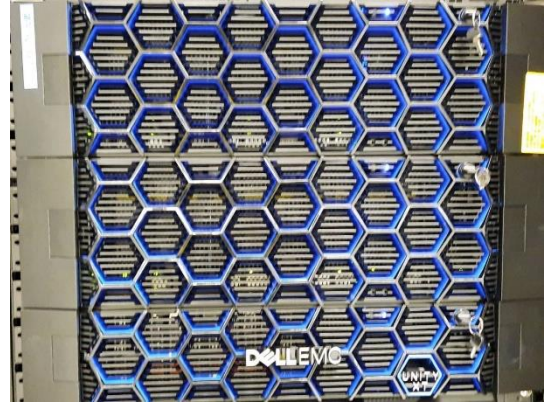
1. 新購主機及儲存設備可提升系統運算及存取效能，確保系統及資料安全。
2. 虛擬主機記憶體整體增加 512GB，緩解記憶體不足問題。
3. 汰換老舊伺服器及儲存設備，作為測試區使用，達成正式境與測試環境實體隔離的目標。

三、建立廠商遠端連線之側錄機制，強化遠端連線維護之安全監控，並符合系統防護基準之資安要求。

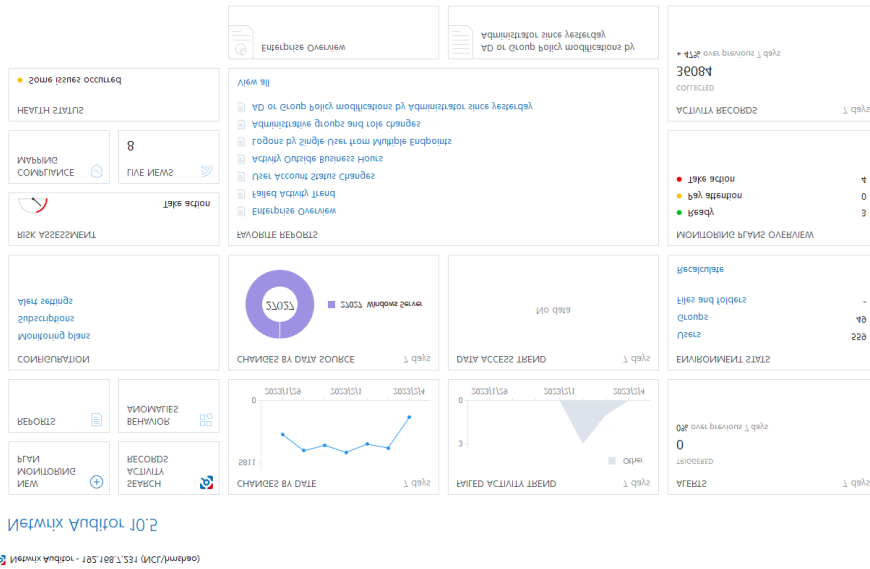
## 伍、附件(成果照片)



伺服器主機 2 臺



DELL EMC Unity XT380 儲存設備 1 臺



遠端連線側錄軟體



## 無障礙網路空間服務網

[最新消息](#) [標章申請](#) [標章查詢](#) [App檢測專區](#) [常見問題](#) [關於無障礙](#) [活動資訊](#) [下載專區](#)

現在位置：首頁 > 標章查詢 > 標章明細

### ■ 標章資訊

標章狀態	啟用
機關代碼	A09050000E
機關名稱	國家圖書館
網站名稱	國家圖書館全球資訊網中文版
網址	<a href="https://www.ncl.edu.tw/">https://www.ncl.edu.tw/</a>
標章等級	A
登錄日期	111-09-27
標章啟用日期	111-10-31
標章到期日期	114-10-31
FreeGo 檢測紀錄	通過
備註	

官網中文網站重新取得政府無障礙網頁開發規範最新版 A 級標章

## 無障礙網路空間服務網

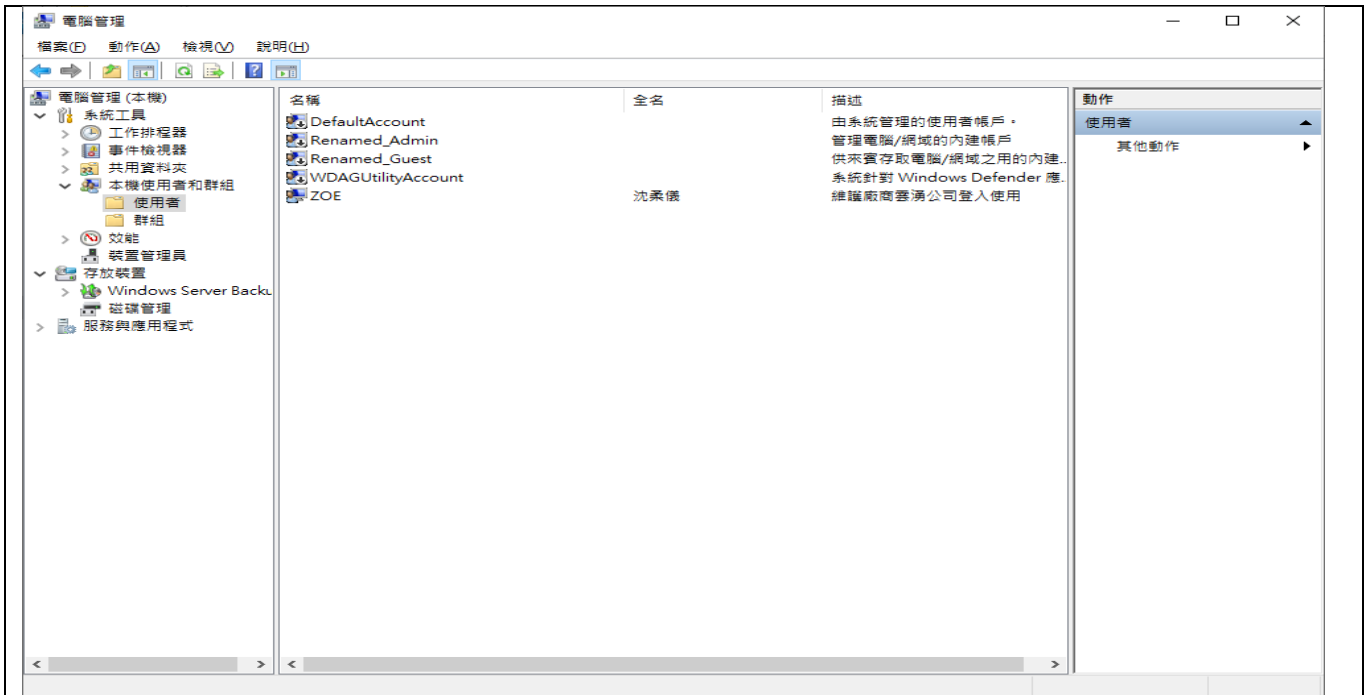
[最新消息](#) [標章申請](#) [標章查詢](#) [App檢測專區](#) [常見問題](#) [關於無障礙](#) [活動資訊](#) [下載專區](#)

現在位置：首頁 > 標章查詢 > 標章明細

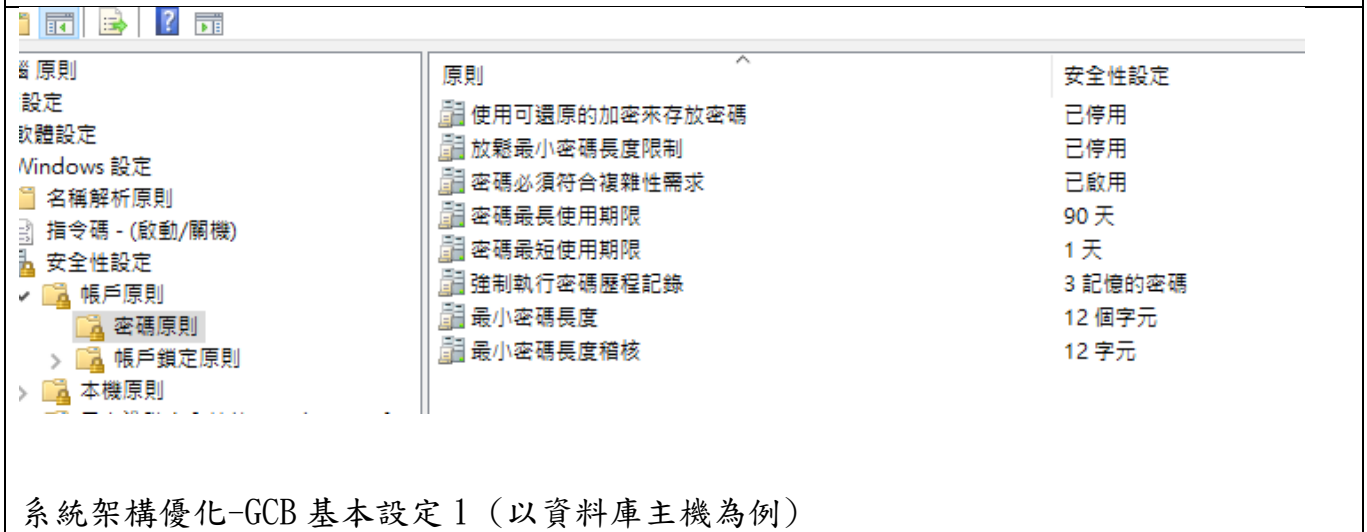
### ■ 標章資訊

標章狀態	啟用
機關代碼	A09050000E
機關名稱	國家圖書館
網站名稱	國家圖書館全球資訊網英文版
網址	<a href="https://enwww.ncl.edu.tw/">https://enwww.ncl.edu.tw/</a>
標章等級	A
登錄日期	111-09-05
標章啟用日期	111-10-04
標章到期日期	114-10-04
FreeGo 檢測紀錄	通過
備註	

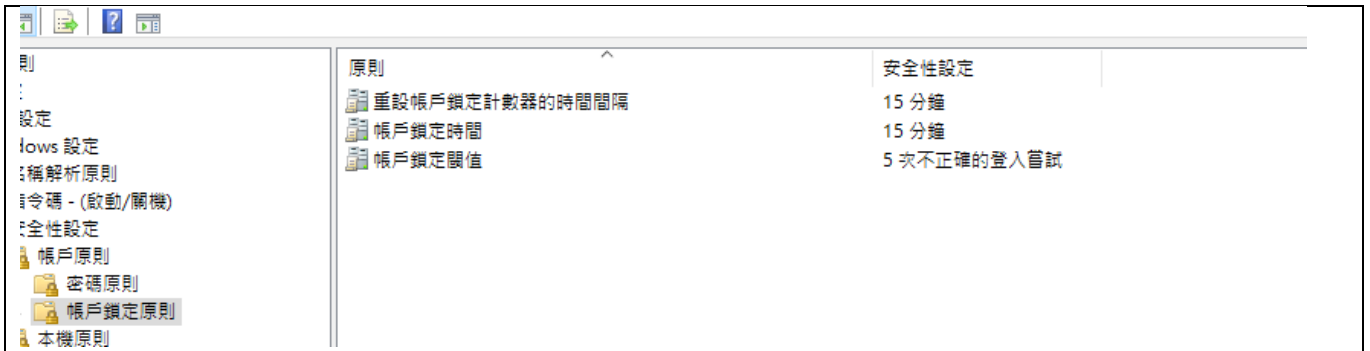
官網英文網站重新取得政府無障礙網頁開發規範最新版 A 級標章



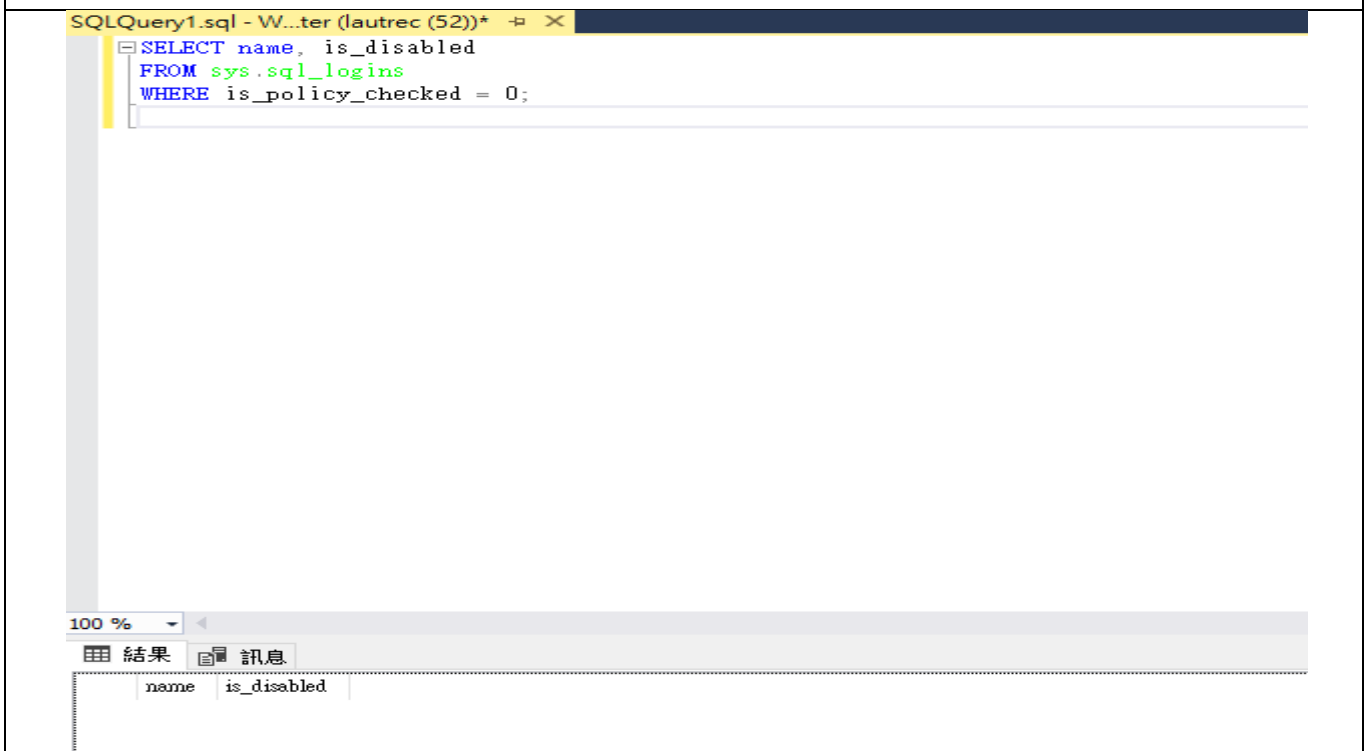
系統架構優化-帳號設定 (以資料庫主機為例)



系統架構優化-GCB 基本設定 1 (以資料庫主機為例)



### 系統架構優化-GCB 基本設定 2 (以資料庫主機為例)



### 系統架構優化-GCB 基本設定 3 強制執行密碼原則 (以資料庫主機為例)

IIS Crypto 3.3

**NARTAC SOFTWARE**

**Schannel**

These settings enable or disable various options system wide. When the checkbox is grey it means no setting has been specified and the default for the operating system will be used. Click the Apply button to save changes.

**Server Protocols**

- Multi-Protocol Unified Hello
- PCT 1.0
- SSL 2.0
- SSL 3.0
- TLS 1.0
- TLS 1.1
- TLS 1.2
- TLS 1.3

**Ciphers**

- NULL
- DES 56/56
- RC2 40/128
- RC2 56/128
- RC2 128/128
- RC4 40/128
- RC4 56/128
- RC4 64/128
- RC4 128/128
- Triple DES 168
- AES 128/128
- AES 256/256

**Hashes**

- MD5
- SHA
- SHA 256
- SHA 384
- SHA 512

**Key Exchanges**

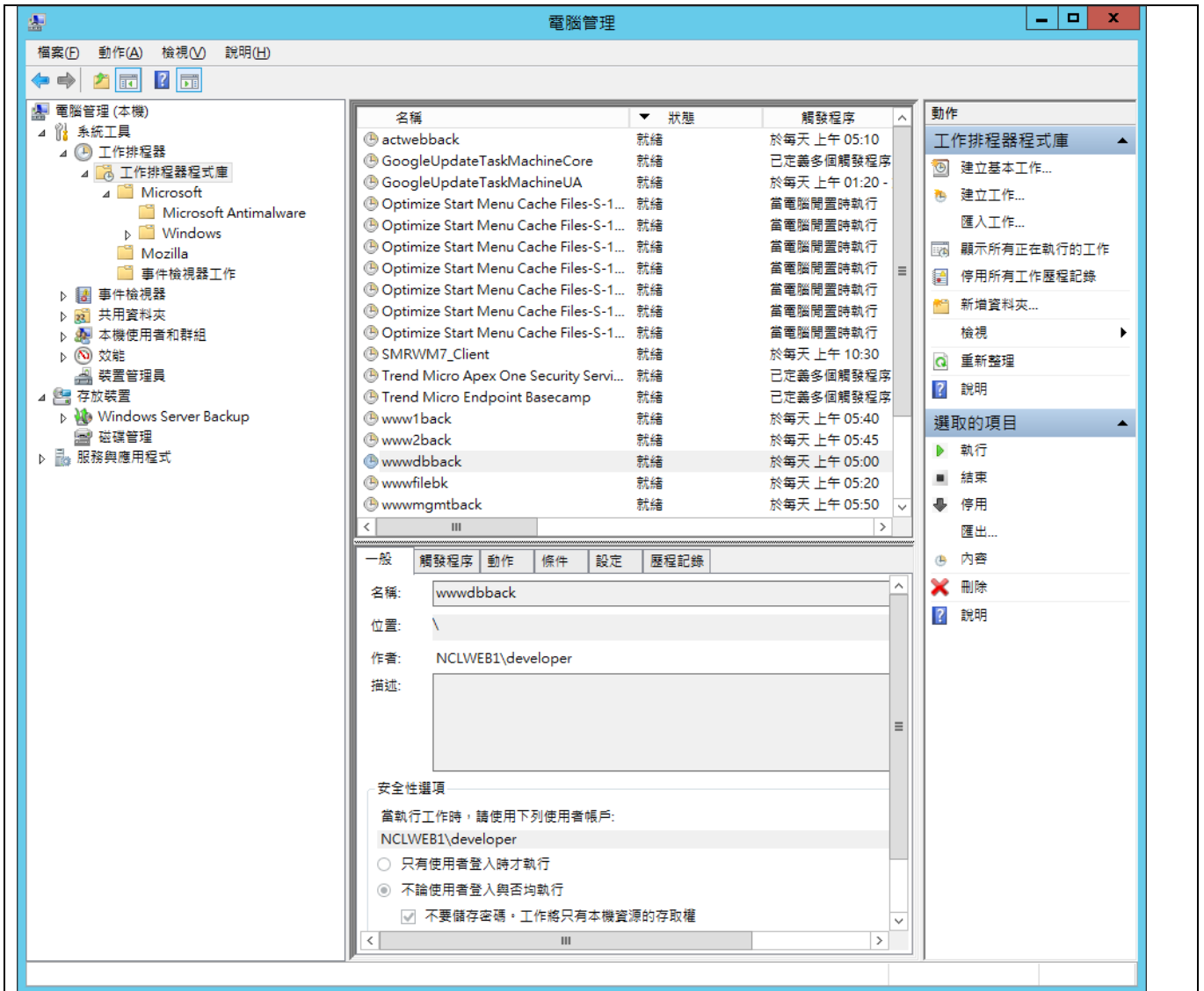
- Diffie-Hellman
- PKCS
- ECDH

**Client Protocols**

- Multi-Protocol Unified Hello
- PCT 1.0
- SSL 2.0
- SSL 3.0
- TLS 1.0
- TLS 1.1
- TLS 1.2
- TLS 1.3

Best Practices Reboot:  Apply

系統架構優化-GCB 基本設定 4 啟用 TLS 1.3 TLS 1.2 加密協定 (以檔案管理主機為例)



系統架構優化-備份排程