

01\_外部專案 - 專案資訊 #1075

專案資訊 # 1064 (New-新增): 2025-PenTest

ADCS Web Enrollment Enabled for high-privileged accounts

2025-11-10 13:30 - Joy Liao

|                                                                                                                                                                                                                                                                                                                                                                                                                   |             |        |            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------|------------|
| 狀態:                                                                                                                                                                                                                                                                                                                                                                                                               | Resolved-解決 | 開始日期:  | 2025-08-01 |
| 優先權:                                                                                                                                                                                                                                                                                                                                                                                                              | Normal      | 完成日期:  | 2025-12-31 |
| 被分派者:                                                                                                                                                                                                                                                                                                                                                                                                             | 益利 周        | 完成百分比: | 100%       |
| 分類:                                                                                                                                                                                                                                                                                                                                                                                                               |             | 預估工時:  | 0:00 小時    |
| 版本:                                                                                                                                                                                                                                                                                                                                                                                                               |             | 耗用工時:  | 0:00 小時    |
| 概述                                                                                                                                                                                                                                                                                                                                                                                                                |             |        |            |
| N bookmark20250529113929916258883991 "ADCS Web Enrollment Enabled for high-privileged accounts                                                                                                                                                                                                                                                                                                                    |             |        |            |
| " Enabling ADCS Web Enrollment for high-privileged accounts increases the risk of credential theft, as attackers could exploit web-based vulnerabilities (like MITM or phishing) to intercept or forge certificates. This could lead to privilege escalation and domain compromise if abused for unauthorized authentication. "The following approaches are recommended to mitigate this potential vulnerability. |             |        |            |
| Enable Extended Protection for Authentication (EPA) on the ADCS Server.                                                                                                                                                                                                                                                                                                                                           |             |        |            |
| Disable NTLM on the ADCS Server                                                                                                                                                                                                                                                                                                                                                                                   |             |        |            |
| Enforce SMB and LDAP Signing                                                                                                                                                                                                                                                                                                                                                                                      |             |        |            |
| "                                                                                                                                                                                                                                                                                                                                                                                                                 |             |        |            |

歷史

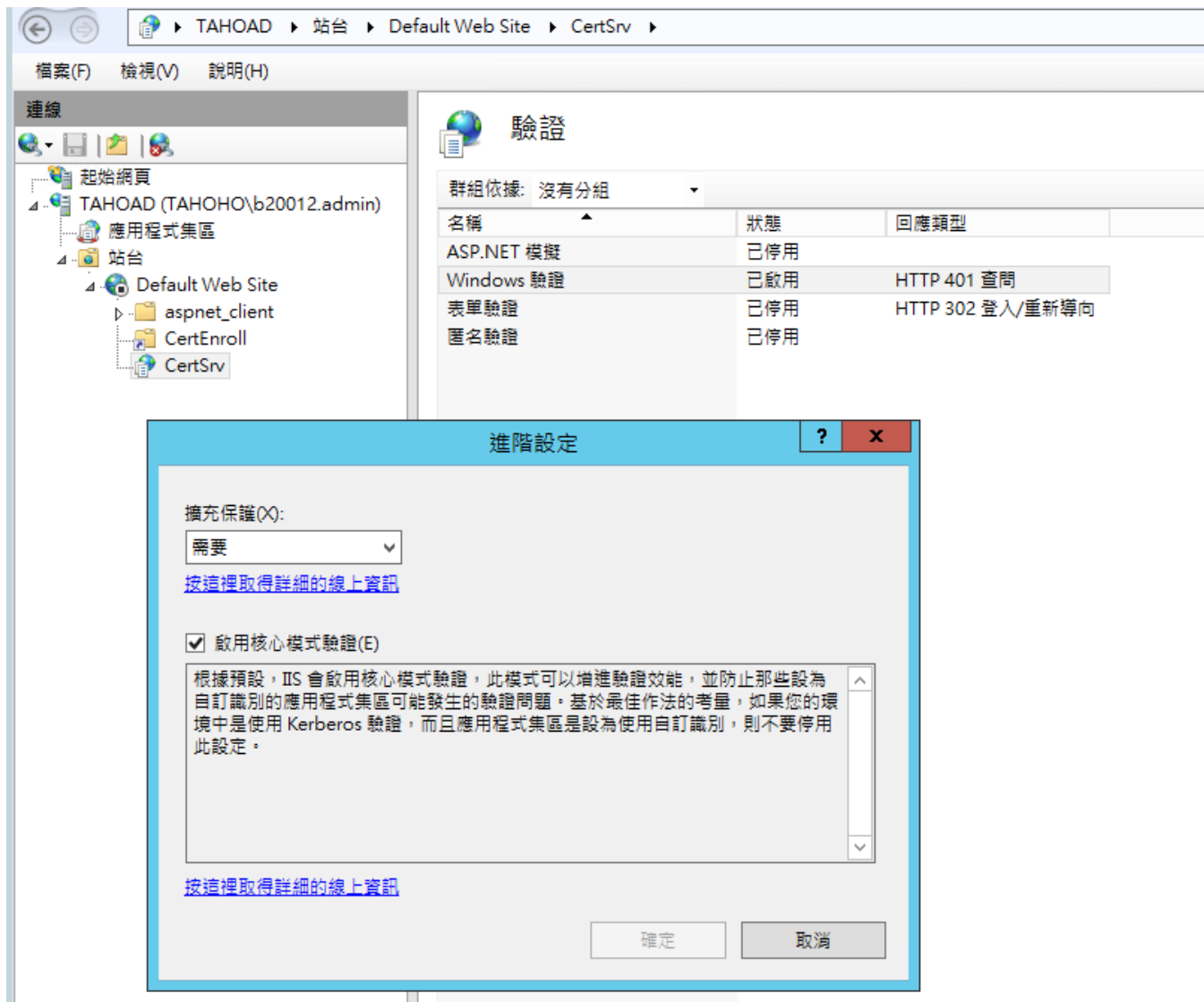
#1 - 2025-11-10 13:34 - Joy Liao

- 完成日期 設定為 2025-12-31
- 被分派者 設定為 益利 周
- 開始日期 從 2025-11-10 變更為 2025-08-01

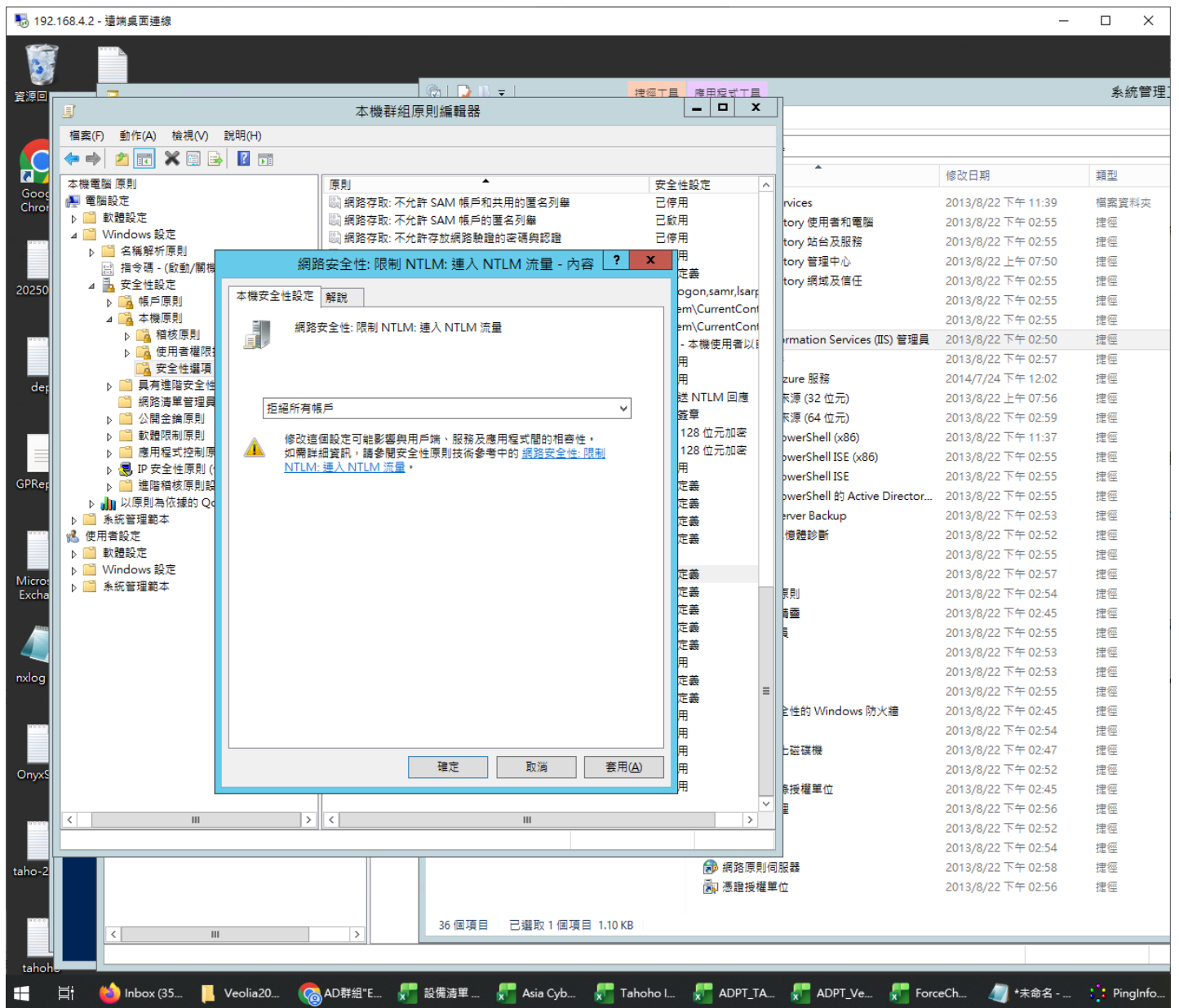
#2 - 2025-11-27 17:45 - 益利 周

- 檔案 clipboard-202511271729-zjpzs.png 已新增
- 檔案 clipboard-202511271734-mjb7z.png 已新增
- 檔案 clipboard-202511271745-7neha.png 已新增
- 狀態 從 New-新增 變更為 Resolved-解決
- 完成百分比 從 0 變更為 100

1.在 AD CS 伺服器上啟用擴充保護以進行驗證 (EPA)



2.在 AD CS 伺服器上停用 NTLM



### 3. 強制執行 SMB 和 LDAP 簽章 (Signing)

NTLM

領域

詳細資料

設定

委派

狀態

NTLM

資料收集: 2025/11/27 下午 05:45:12

電腦設定 (已啟用)

原則

Windows 設定

安全性設定

本機原則/安全性選項

Microsoft Network Server

原則

設定

Microsoft 網路伺服器: 數位簽章伺服器的通訊 (如果用戶端同意)

已啟用

Microsoft 網路伺服器: 數位簽章伺服器的通訊 (自動)

已啟用

網域控制站

原則

設定

網域控制站: LDAP 伺服器簽章要求

要求簽章

其他

原則

設定

網路安全性: 限制 NTLM: 進入 NTLM 流量

拒絕所有帳戶

使用者設定 (已啟用)

沒有設定定義。

檔案

|                                  |         |            |      |
|----------------------------------|---------|------------|------|
| clipboard-202511271729-zjpzs.png | 75.5 KB | 2025-11-27 | 益利 周 |
| clipboard-202511271734-mjb7z.png | 290 KB  | 2025-11-27 | 益利 周 |
| clipboard-202511271745-7neha.png | 34.4 KB | 2025-11-27 | 益利 周 |