

01_外部專案 - 專案資訊 #1087

專案資訊 # 1064 (New-新增): 2025-PenTest

Dangerous Permission over Domain Controllers Group

2025-11-10 13:33 - Joy Liao

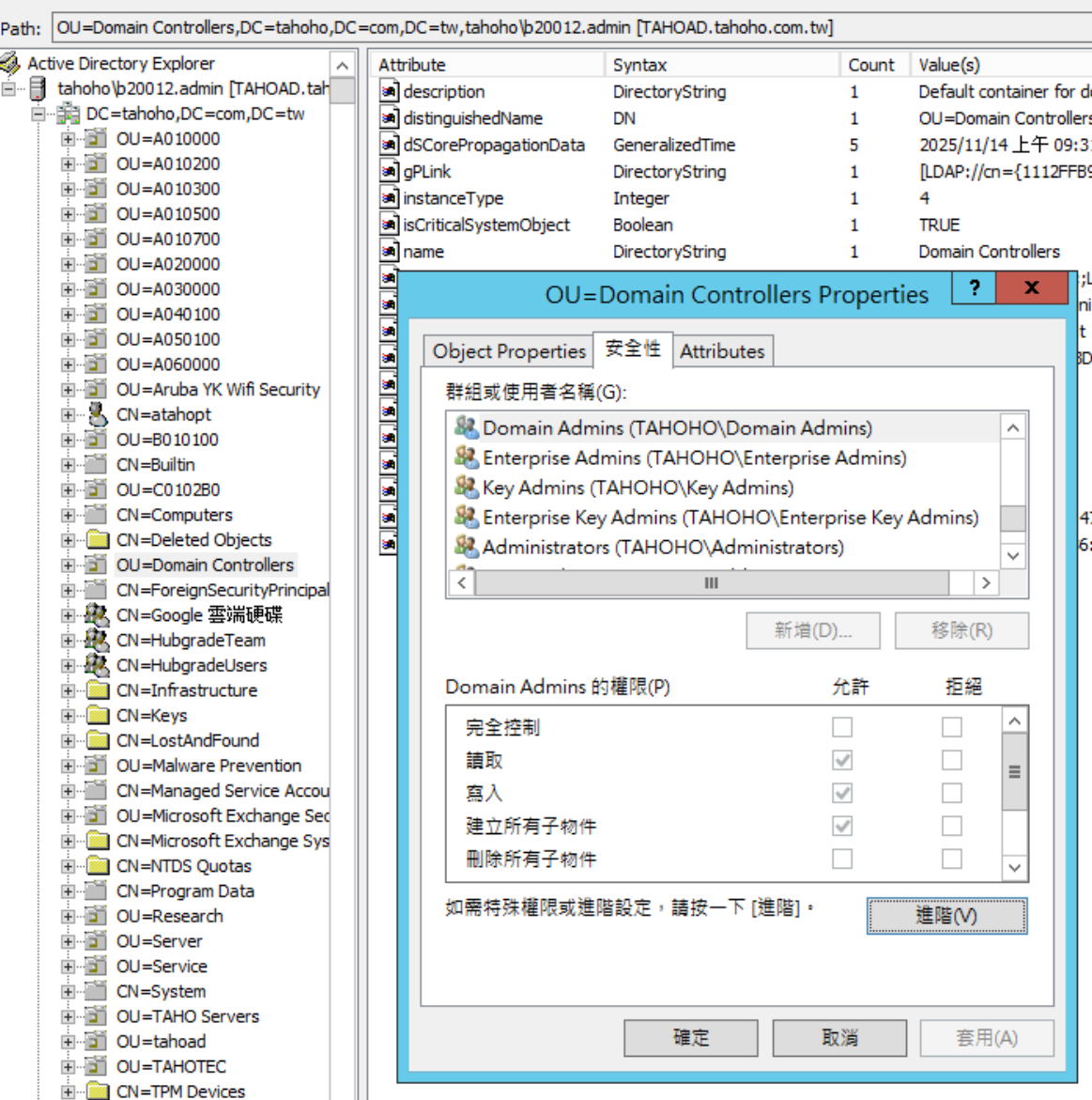
狀態:	Resolved-解決	開始日期:	2025-08-01
優先權:	Normal	完成日期:	2025-12-31
被分派者:	益利 周	完成百分比:	100%
分類:		預估工時:	0:00 小時
版本:		耗用工時:	0:00 小時
概述			
bookmark20250527172903274457208324 "Dangerous Permission over Domain Controllers Group			
" Unrestricted Domain Controllers group access lets attackers seize control of AD authentication, enabling silent domain takeover. "It is essential to meticulously review the permissions assigned to the DomainControllers group for non-administrative domain objects, ensuring that permissions are granted only for the minimum necessary.			
"			

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 - 2025-11-28 10:08 - 益利 周
- 檔案 clipboard-202511281009-zzw1a.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. 識別與稽核「Domain Controllers」群組權限
確認哪些帳戶或群組目前擁有修改「Domain Controllers」群組的權限。
2. 移除不必要帳戶的修改權限
實施嚴格的最小權限原則：
在「Domain Controllers」群組的「安全性」標籤頁中，明確地從「Domain Users」、「Authenticated Users」或任何其他標準使用者群組的權限列表中，移除所有允許修改成員資格的 ACE。
確保只有 Domain Admins、Enterprise Admins 和內建的 Administrators 群組具有修改此群組的權限。



檔案

clipboard-202511281009-zzw1a.png

98.8 KB

2025-11-28

益利 周