FottiOS 5.2 SSL VPN 配合 Windows AD 帳號 LDAP 認證設定說明

臺中市政府教育局資訊教育暨網路中心 沈俊達

壹、目的

解決在 FG-200D 上手動新增帳號及維護密碼的困境，採用與校內 AD 帳號或 LDAP 帳號結合方式來管理認證。

另一種採用 RADIUS 認證的方法，請參閱 2013 年這篇：**FG110C SSL VPN 配合 Windows AD 帳號認證設定說明.pdf**，因 LDAP 設定方式較簡單，如果可以不建議再用 RADIUS 認證方式。

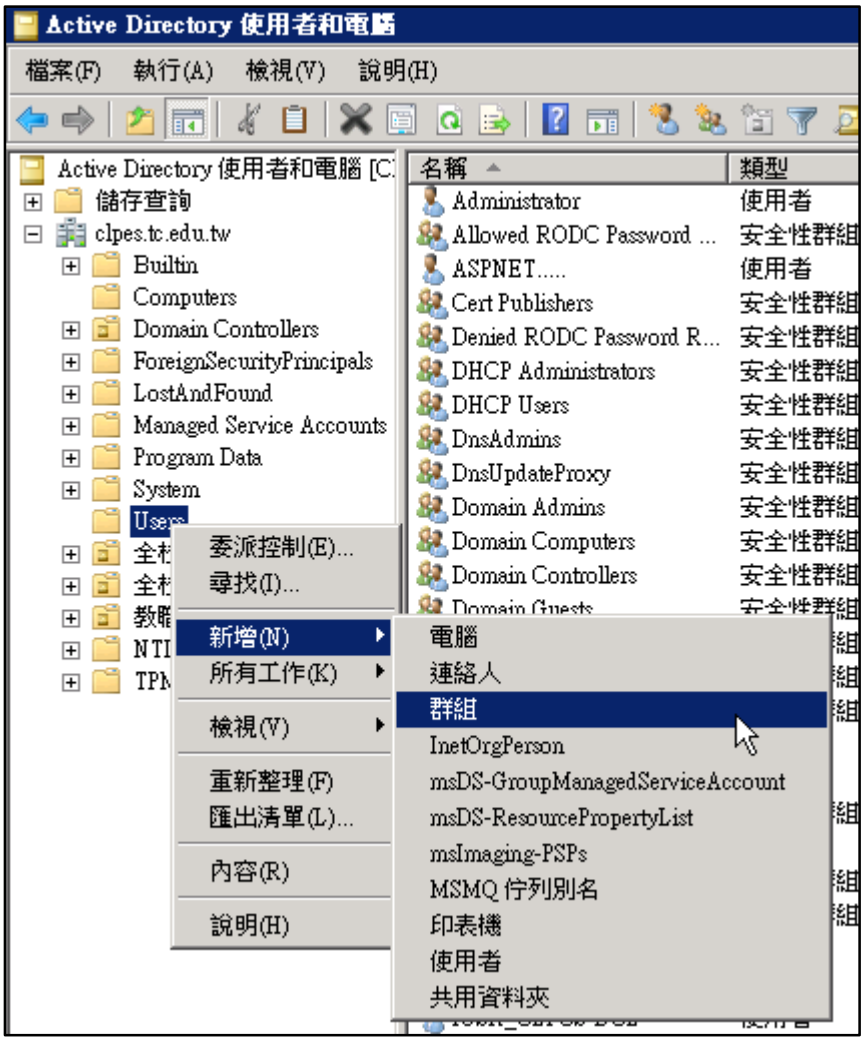
貳、本技術文件假定貴校已依據下面兩篇文件，完成相關設定，並已成功讓 vpndemo1 用戶可以正常登入 SSLVPN，並存取相關服務。

本文件重點再直接將 AD 帳號或 LDAP 帳號，加入一個新的群組，並讓此群組可以登入 SSLVPN，並存取相關服務。

參、DC 或 LDAP Server 上的預備動作：

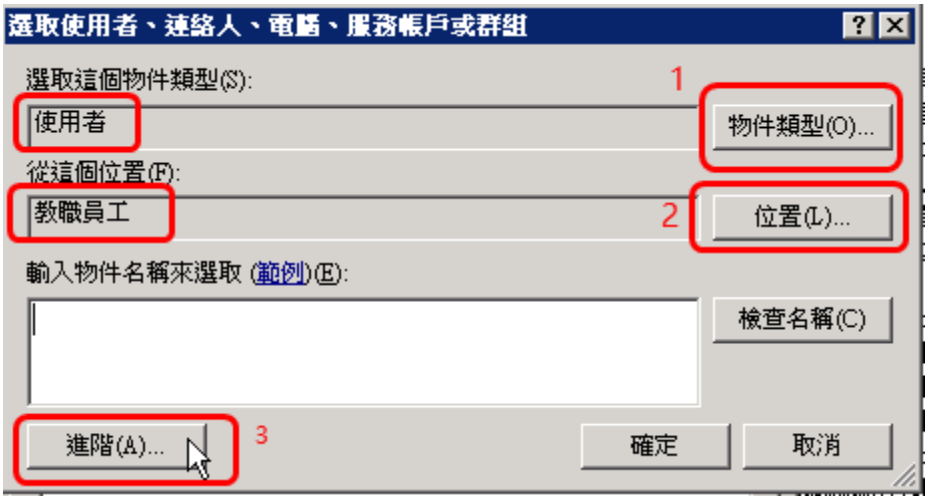
建立一個新的群組，例如：SSLVPNUSERs，將要允許 SSLVPN 登入的**帳號**，一一加入此群組，注意是帳號，**不能用群組加入群組方式**。

一、 新增 SSLVPNUSERs 群組



二、將允許 SSLVPN 登入的**帳號**，一一加入此群組

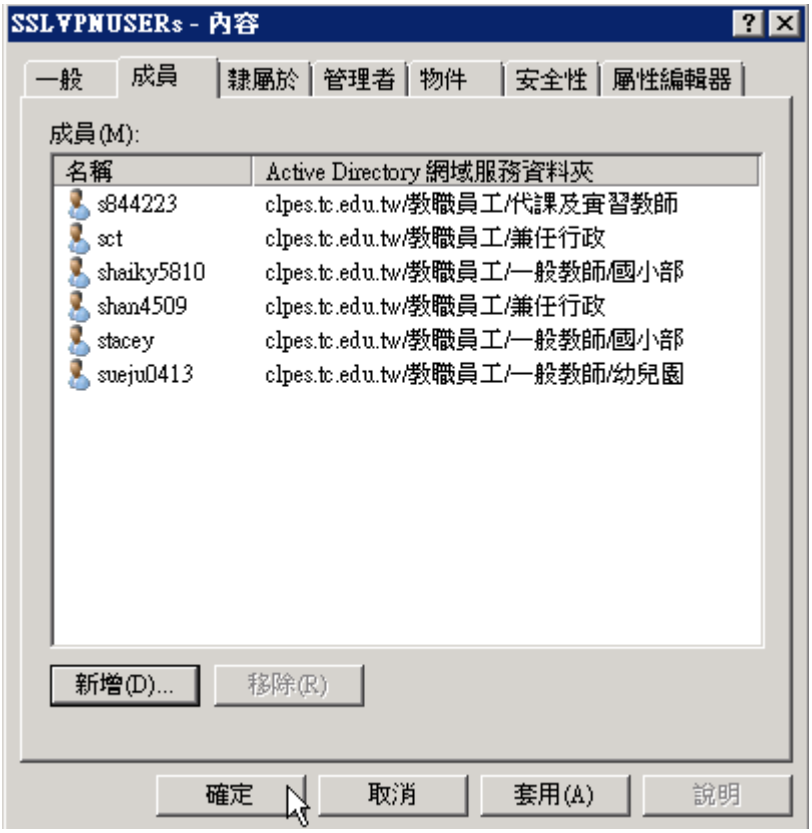
物件類型只選：使用者，位置：一次先選一個 OU，按下進階



按下立即尋找

將要加入的帳號複選起來，按確定

繼續新增帳號，或按確定離開



肆、FG-200D 的設定

用戶與設備→認證→LDAP→Create New

設定一個用戶名稱，例如 Windows DC LDAP，並輸入 DC 的 ip 位址

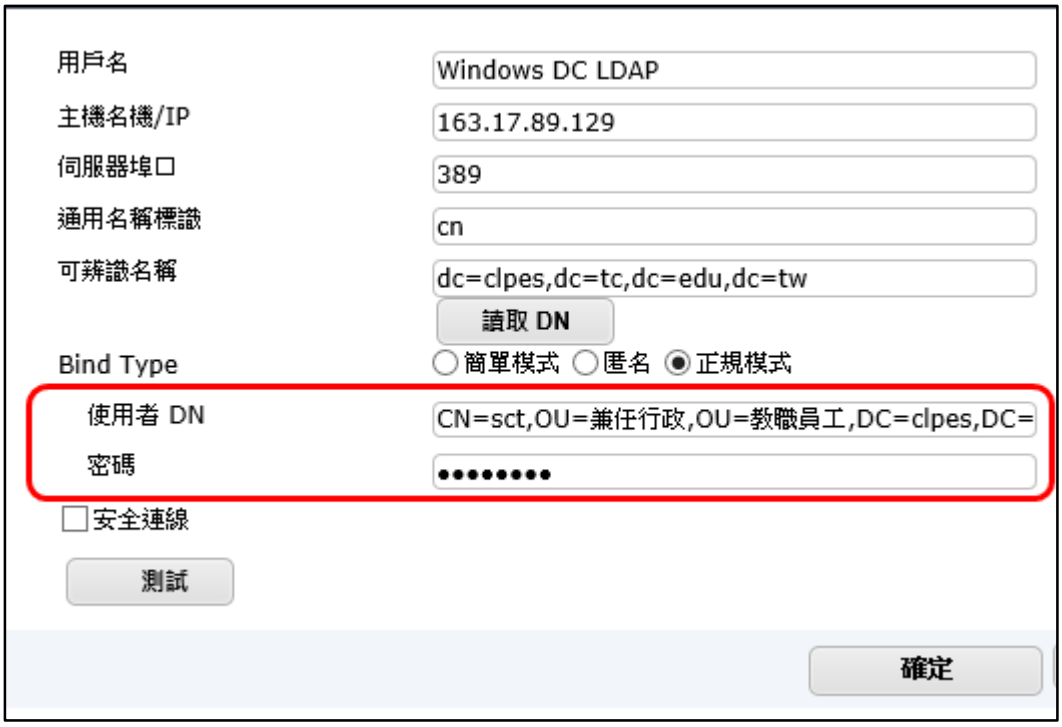
可識別名稱填入 AD 網域的 LDAP 路徑

Bind Type 選擇：正規模式

使用者 DN 及密碼：請填一個擁有讀取 AD 帳號內容權限的帳號及密碼，如果要用 Administrator 的話，標準路徑是：CN=Administrator,CN=Users,DC=clpes,DC=tc,DC=edu,DC=tw

完成後請按「讀取 DN」及「測試」都會出現成功訊息。

最後請按確定，完成。

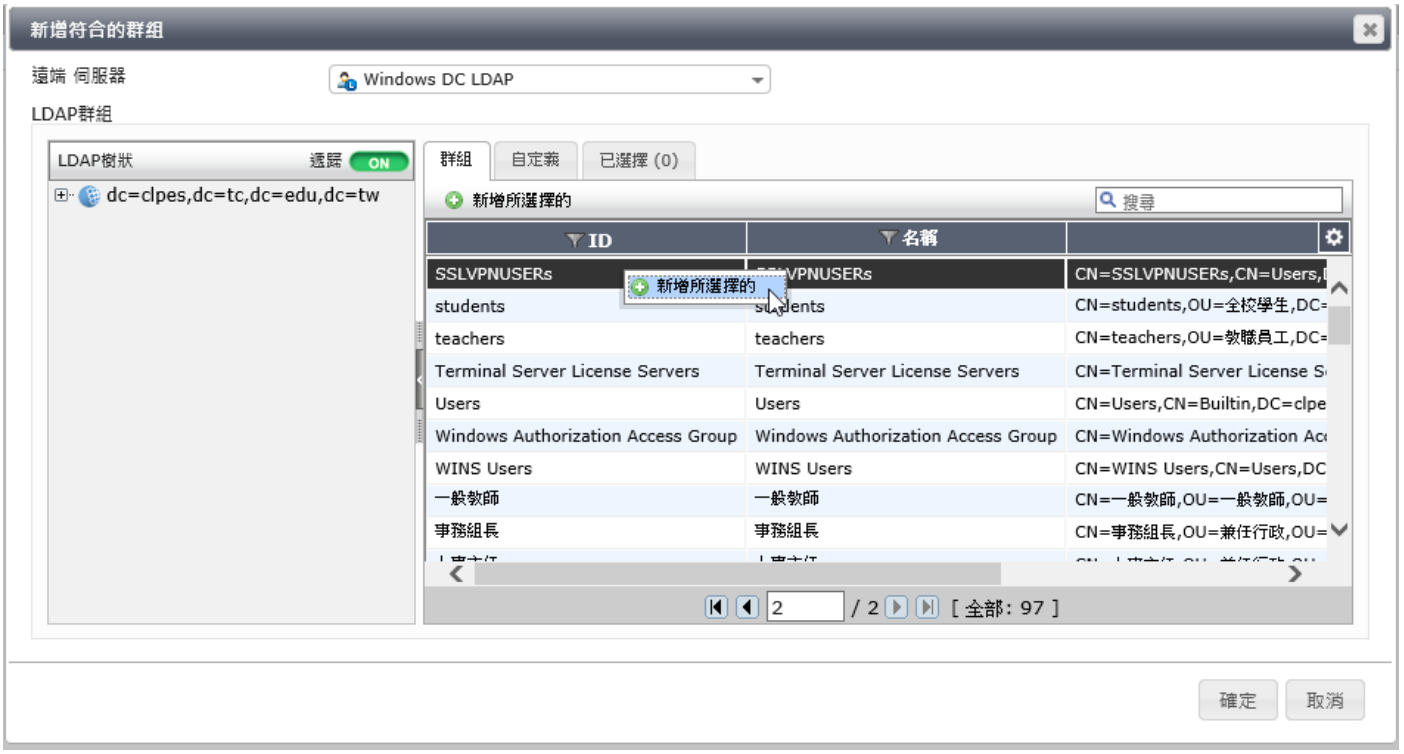


伍、把 AD 帳號加入 vpndemo_users 群組

操作步驟：編輯之前建立的 vpndemo_users 群組，按 Create New

遠端伺服器下拉選單點選剛剛建立的 Windows DC LDAP

分頁尋找到剛剛在 DC 上建立的 SSLVPNUSERs 群組，按滑鼠左鍵一下選「新增所選擇的」，然後按下確定



完成遠端群組加入 FG-200D 的 vpndemo_users 群組，按確定離開

陸、現在只要是 AD 帳號隸屬於 SSLVPNUSERs 群組的，都可以使用 SSLVPN 連線了！您可以開放所有老師，國中為了十二年國教也可以開放學生使用。

但建議學生部分建一個獨立的 Web-only 門戶網站，只提供一個書籤連到學務系統即可。

教師部分另建一個或多個門戶網站，是各校需求設定 Web-only 或 Tunnel Mode。

此部分細節，爾後辦理研習時，再實作給大家練習。

2016-1-3