為什麼在訪問策略中執行目錄搜尋時無法找到受信任域的AD組？

目錄

問題：

為什麼在訪問策略中執行目錄搜尋時無法找到受信任域的AD組？

環境：思科網路安全裝置(WSA)、NTLM身份驗證、受信任域

症狀：

- 使用者正試圖查詢「Active Directory組」以用作其某個訪問策略中的策略成員定義，並且該組未顯示在目錄搜尋中。
- 該組屬於受信任的AD域，而不是WSA已加入的域。

此行為是設計好的。在訪問策略中配置組時，來自受信任域的組不會顯示在Directory Search中。

在所有AsyncOS版本中，如果另一個域與WSA加入的域具有雙向信任，則WSA能夠驗證來自其他域的使用者並匹配其各自的AD組。

在這種情況下，我們可以透過以下步驟在訪問策略中增加受信任域中的組：

1. 瀏覽到GUI —> Web Security Manager —> Access Policies —> <Policy Name> —> Selected Groups and Users —> Groups
2. 在「目錄搜尋」欄位中手動鍵入整個組名和域名
3. 按一下「增加」按鈕
4. 按一下「完成」，然後按一下「提交並認可變更」

請注意，如果另一個域與WSA加入的域沒有雙向信任關係，則WSA將與手動配置的組不匹配

附註： 在AsyncOS版本7.7及更高版本中，WSA支援多個NTLM領域，對於兩個域之間沒有信任關係的方案，我們可以為第二個域建立新的NTLM領域。使用多個NTLM領域，WSA可以在訪問策略內查詢來自不同域的組。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。