從Active Directory配置使用者、組和電腦以與OpenDNS聯結器服務同步

目錄

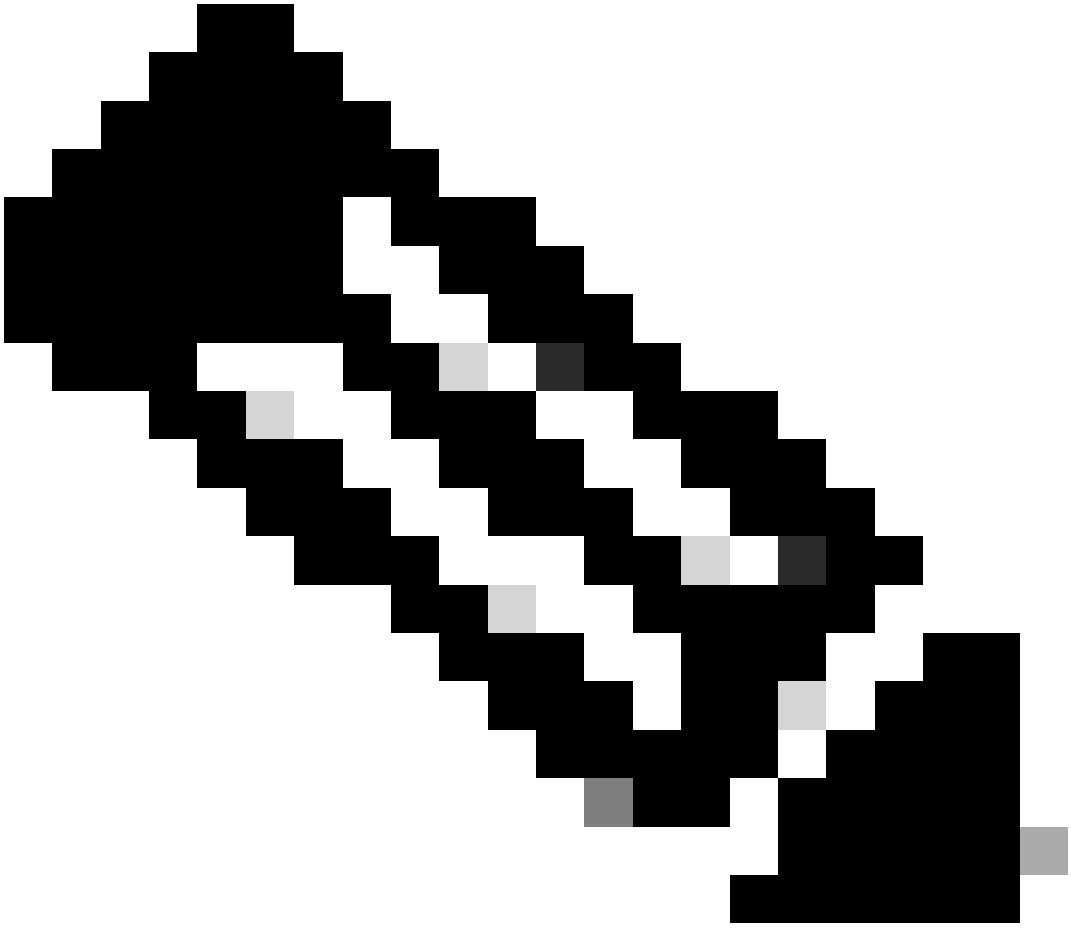
簡介

本文檔介紹如何使用OpenDNS Connector服務從Active Directory同步使用者、組和電腦。

概觀

作為其操作的一部分，OpenDNS聯結器服務使用LDAP協定從Active Directory同步使用者、組和電腦的清單。 本文介紹如何檢查OpenDNS_Connector帳戶是否具有讀取這些對象的正確許可權。

Active Directory中的每個對象（使用者/組/電腦）都具有與其關聯的ACL安全許可權，並且每個對象必須允許OpenDNS_Connector使用者帳戶讀取其屬性。



附註：本文假定已選中「OpenDNS_Connector」帳戶的正常先決條件。如果儀表板中缺少AD使用者/組，請先參閱以下文章：
Umbrella Dashboard中缺少AD使用者/組。

預設許可權

預設情況下，所有經過身份驗證的使用者都可以讀取使用者/組/電腦的屬性，因此OpenDNS_Connector使用者不需要任何額外許可權即可執行LDAP同步。

default permissions通常按如下方式設定：

1)在域上為「Pre-Windows 2000 Compatible Access」組分配了「Descendant User Objects」、「Descendant Group Objects」和「Descendant Computer Objects」的讀取（讀取所有屬性）許可權。

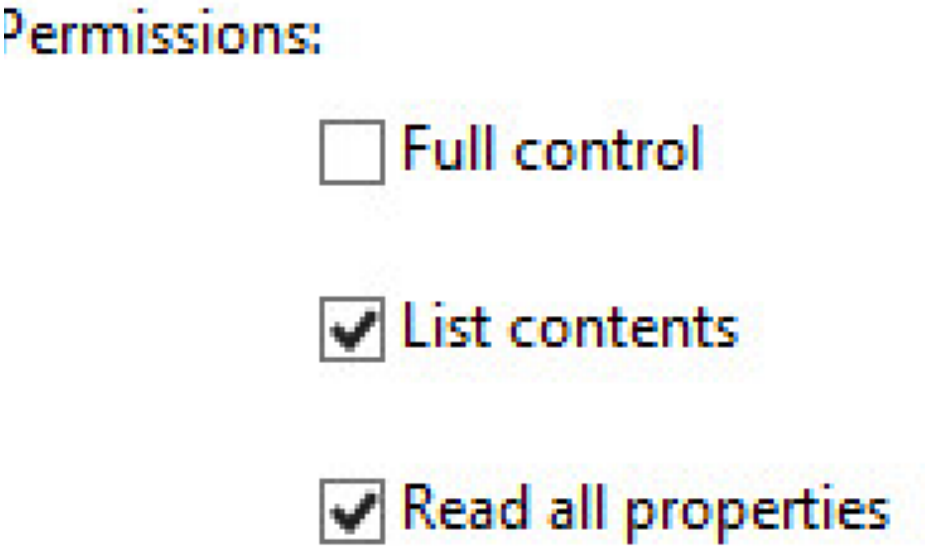
您可以按如下方式仔細檢查此項：

- 開啟Active Directory使用者和電腦

- 按一下「檢視」並選中「高級功能」選項。
- 按一下右鍵域對象，然後選擇「屬性」，然後選擇「安全」>「高級」
- 選擇具有「特殊」許可權的「Windows 2000前相容訪問」項：

115011616667

- 按一下「編輯」可詳細檢視這些許可權。
- 在「應用」部分中選擇「後代使用者對象」
- 查詢以下許可權：

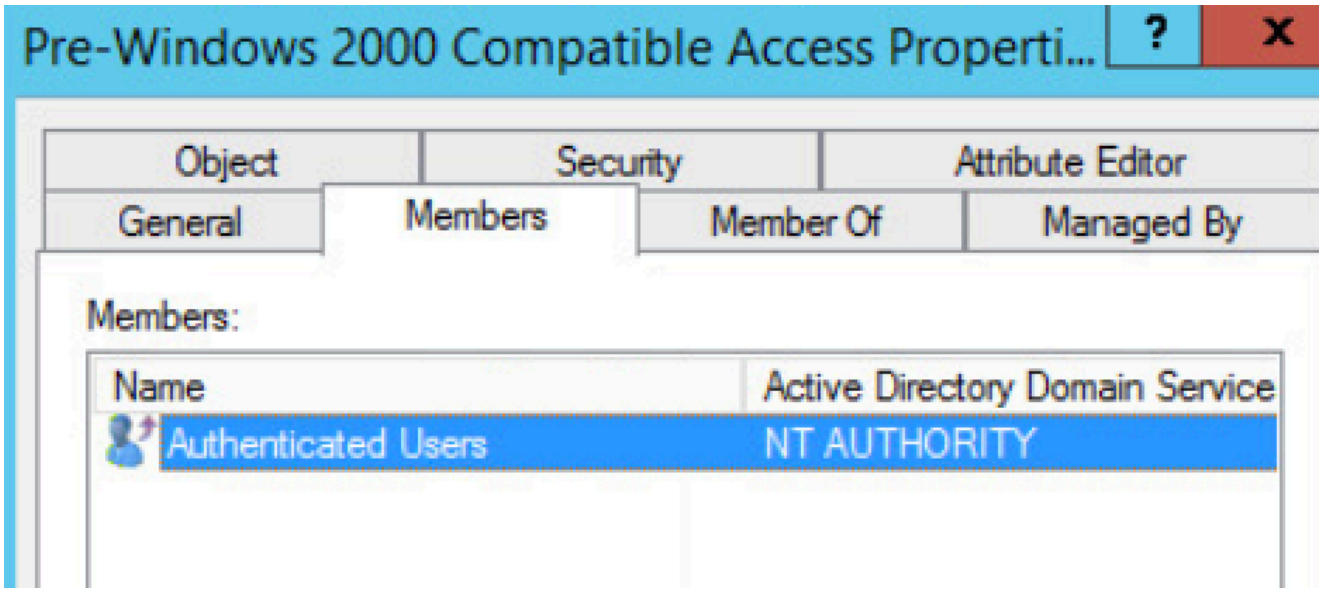


115011616687

- 對「後代組對象」和「後代電腦對象」重複這些步驟

2)所有「經過身份驗證的使用者」組是「Pre-Windows 2000 Compatible Access」組的成員，該組向所有使用者提供這些設定。

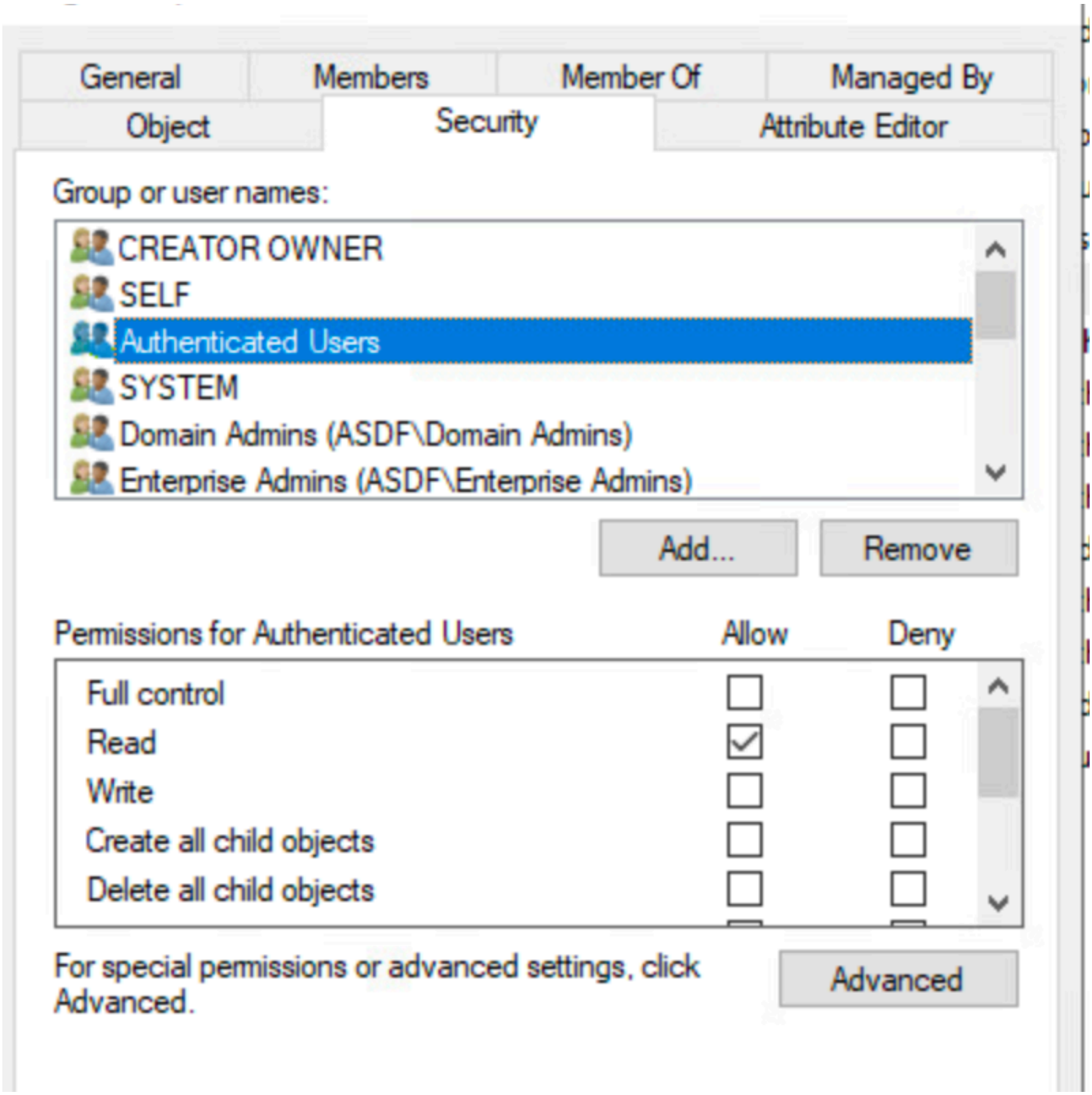
- 按一下右鍵Pre-Windows 2000 Compatible Access組，該組通常位於內建AD容器中。
- 選擇「屬性」，然後轉到「成員」選項卡。
- 檢查「Authenticated Users」是否列出。



115011616707

但是，在某些AD環境中，此許可權模型可能已更改，並且已刪除通過身份驗證的使用者。這可能會表現為某些使用者在Umbrella Dashboard中丟失，或者組成員身份不正確。如果是這種情況，請將OpenDNS_Connector使用者新增到此組，重新啟動聯結器服務，丟失的專案將顯示在Umbrella中。

在某些極少數情況下，這仍無法解決此問題。如果您發現這種情況，請檢查active directory中的groups security頁籤，確保您看到此處列出了具有檢入讀取許可權的已驗證使用者。如果未選中此覈取方塊，請將其選中，然後重新啟動聯結器服務以檢視組成員是否顯示。此外，如果他們發現所有組都缺少此安全設定，他們需要批次將更改應用到全域性的所有組。



28728163336852

檢視有效訪問

您可以使用Windows「有效訪問」工具來檢視OpenDNS_Connector使用者是否能夠讀取缺少的特定對象（或該對象具有不正確的組成員身份）。

- 開啟Active Directory使用者和電腦
- 按一下「檢視」並選中「高級功能」選項。
- 查詢使用者對象，然後按一下右鍵以選擇「屬性」
- 轉到「Security > Advanced > Effective Access」(這可以是「Effective Permissions」)

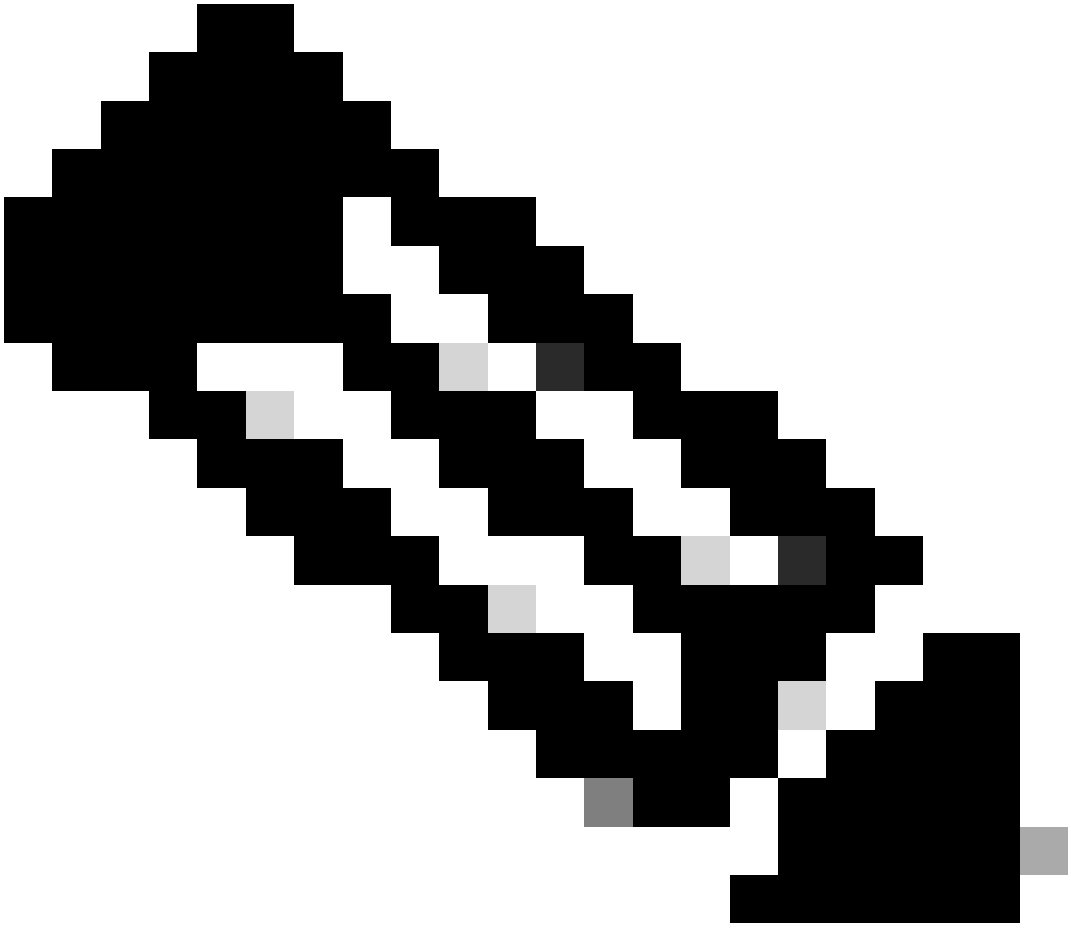
- 按一下「選擇使用者」，然後選擇「OpenDNS_Connector」用戶帳戶。
- 按一下「確定」，然後「檢視有效訪問」
- 確保聯結器使用者能夠讀取所有屬性:

115011616727

設定OpenDNS_Connector LDAP許可權

AD中的「委託控制」嚮導是向「OpenDNS_Connector」使用者分配必要許可權的快速方法：

1)轉到「管理工具」，開啟「Active Directory使用者和電腦」管理單元。
2)按一下右鍵包含OpenDNS_Connector的域，然後選擇「Delegate Control...」，然後按一下「Next」。
3)新增OpenDNS_Connector使用者，然後按一下「下一步」。
4)選擇「Read all user information(讀取所有使用者資訊)」，然後單擊「Next（下一步）」。 [見圖3。]
7)按一下Finish。 [見圖6。]



附註：如果在某些對象上禁用繼承，這些步驟可能會失敗。 對於這些對象，您需要手動設定許可權。

userPerms指令碼

附加的powershell指令碼是獲取特定對象(例如，使用者)。 請在聯絡Umbrella技術支援時包括此指令碼的輸出。

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）。