

瞭解Umbrella中的多AD域支援

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[概觀](#)

[多AD域支援的先決條件](#)

[多AD域支援的限制 \(虛擬裝置部署 \)](#)

[多AD域支援的限制 \(漫遊客戶端部署 \)](#)

簡介

本檔案介紹Cisco Umbrella中的多AD網域支援。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Cisco Umbrella。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

Umbrella組織中的多個Active Directory域支援現在預設啟用。

如果您已經在單獨的Umbrella組織中註冊了多個AD域，則這些組織可以整合到具有多AD域支援的單個Umbrella組織。有關更多詳細資訊，請參閱本文。

多AD域支援的先決條件

- 需要在每個域中建立登入名為OpenDNS_Connector的使用者帳戶，該使用者帳戶符合Umbrella文檔[中指定的要求](#)。建議跨AD域為此帳戶保留相同的密碼。
- 對於使用虛擬裝置進行部署，Umbrella站點中的每個AD域都需要一個AD聯結器，如果需要，還需要可選的第二個聯結器用於冗餘。

- 如果部署僅包括漫遊客戶端或AnyConnect，則單個多域AD Connector*可以同步多個域中的AD使用者/組。這要求在每個域中使用相同的密碼建立OpenDNS_Connector帳戶。預設情況下未啟用此功能，您需要提高支援票證才能啟用此功能。
- AD聯結器必須運行版本1.2.3或更高版本。
- Umbrella文檔中指定的[所有其他](#)前提條件也適用於多AD域。

多AD域支援的限制 (虛擬裝置部署)

- AD聯結器當前無法識別跨域身份驗證。如果AD使用者根據屬於某個其他AD域的本地域控制器進行身份驗證，則AD聯結器無法檢索該使用者的AD使用者 — IP對映。虛擬裝置無法將使用者身份與該IP關聯，因此不能為該使用者實施任何基於AD的策略。解決方法是將來自兩個AD域的域控制器包括在同一個Umbrella站點中，只要對Umbrella站點(在Umbrella文檔中[指定](#))的標準不受影響。
- Umbrella策略不適用於具有跨域成員的AD組。要建立應用於多個域中的使用者的策略，必須將每個域中的相關組/使用者新增到策略中。

多AD域支援的限制 (漫遊客戶端部署)

- 漫遊客戶端/AnyConnect部署不受跨域身份驗證限制的影響。
- 啟用多域AD聯結器功能後，Umbrella可以支援具有跨域組成員的AD組。需要通過引發支援票證來明確請求此功能。相同功能還允許單個聯結器從多個AD域同步AD標識。

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）。