瞭解從Azure AD和Okta匯入使用者和組標識的Umbrella支援

目錄

簡介

本文檔介紹目前支援根據SCIM標準從Azure Active Directory和Okta設定使用者和組標識的Umbrella。

支援的使用案例

Umbrella SWG:

- 從Azure AD/Okta匯入使用者和組標識，同時針對通過IPsec隧道、PAC檔案或代理連結連線到SWG的終端使用者設定Azure AD/Okta的SAML身份驗證。
- 從Azure AD匯入使用者和組標識，以在針對本地AD或Azure AD進行身份驗證的裝置上啟用AnyConnect SWG模組的使用者標識。
- 從Okta匯入使用者和組標識，以在針對本地AD進行身份驗證的裝置上啟用AnyConnect SWG模組的使用者標識。

Umbrella DNS:

- 從Azure AD匯入使用者和組標識，以在針對本地AD或Azure AD進行身份驗證的裝置上啟用AnyConnect DNS模組/漫遊客戶端的使用者標識。
- 從Okta匯入使用者和組標識，以在針對本地AD進行身份驗證的裝置上啟用AnyConnect DNS模組/漫遊客戶端的使用者標識。

約束

- Azure AD/Okta無法為Umbrella虛擬裝置(VA)提供使用者標識整合。 這是因為Azure AD/Okta沒有私有IP — 使用者對映的可見性，這是VA所必需的。VA部署仍需要部署內部的Umbrella AD聯結器，以促進AD整合。
- 不支援從本地AD和Azure AD/Okta並行部署相同的使用者/組標識。如果您以前部署了本地AD聯結器來調配使用者和組，並且現在希望從Azure AD/Okta調配相同的使用者和組標識，則您必須在開啟Azure AD/Okta調配之前停止AD聯結器。
- 對於可以從Azure AD/Okta調配的使用者數沒有限制。對於組，最多可以將200個組從Azure AD/Okta調配到Umbrella組織。Azure AD支援動態組，因此您可以建立一個「所有使用者」組

，並設定此組以及最多199個其他組，使用者希望在其上定義Umbrella策略。同樣，Okta有一個內建的Everyone組，因此您可以設定該組以及最多199個其他組，這些組希望在其上定義策略。
- AnyConnect SWG不支援對Azure AD進行SAML身份驗證。它依賴於與本地AD相同的被動身份驗證機制。

設定標識

要從這些身份提供方設定身份，您可以使用以下連結中記錄的說明：

- 從Azure AD設定標識：https://docs.umbrella.com/umbrella-user-guide/docs/microsoft-azure-ad-integration
- 從Okta設定標識：https://docs.umbrella.com/umbrella-user-guide/docs/okta-integration

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）。