與Active Directory和Microsoft EntraID的Cisco安全訪問身份同步

目錄

問題

使用者嘗試在Cisco Secure Access中調配來自兩個具有相同域名的身份源的使用者和組時遇到了挑戰。特定方案涉及同步本地Active Directory和Microsoft EntraID（以前稱為Azure AD）的標識，其中兩個源使用相同的域名(例如，domain.com)。

主要關注事項有：

- 瞭解當身份源和身份源中存在相同使用者和組時，身份所有權和組成員對映的行為方式
- 確保為訪問本地和雲資源的混合使用者實施一致的安全訪問策略
- 在此混合身份配置中為使用者保持內部IP可視性
- 確定來自兩個源的併發同步是否會導致生產環境中的問題

文檔顯示「不支援從Cisco AD Connector和Cisco User Management for Secure Access應用並行同步相同使用者和組，從而導致不一致的訪問規則實施。」

環境

- 採用AD聯結器和EntraID整合的Cisco安全訪問
- 域名與EntraID域匹配的本地Active Directory
- Microsoft EntraID(Azure AD)與本地AD具有相同域名
- 用於聯合身份驗證的SAML SSO配置
- 用於策略實施的安全網路網關(SWG)模組

- 需要同時訪問本地和雲資源的混合環境

解析

已確認來自Active Directory和EntraID源的併發同步以下行為：

組同步行為

當同步來自兩個源的具有相同名稱的組時：

- 在Cisco Secure Access中建立兩個單獨的組對象 — 每個源各一個
- 組可以根據其訪問策略中的源字首進行區分
- 本地AD組顯示為：AD域/組名
- EntraID組顯示為：組名

實驗室驗證顯示同步成功，並顯示「成功」消息。**<<<<** Synced"表示來自多個EntraID域的組。

使用者同步行為

同步來自兩個源的具有相同使用者ID的使用者時：

- 在同步期間覆蓋使用者標識
- 在Secure Access中，只有一個唯一使用者ID保持可見
- 最終同步源確定使用者的屬性和組成員身份
- 當同時配置了本地AD時，EntraID同步通常優先於本地AD

訪問策略配置

兩種組型別均可用於訪問策略：

- 使用完整路徑引用本地AD組：AD域/組名
- 使用簡單名稱引用EntraID組：組名
- 策略可以根據使用者的組成員身份源來區分使用者

後續設定對許多客戶都非常有效。

```
1    Only provision identities from on-prem AD - for VA DNS protection
2    Use Azure entra for SSO/user authentication (no identities to be provisioned from Azure) - for SWG
```

原因

在我們的測試中，我們確認，無論何時從本地AD聯結器同步使用者，它都會在Umbrella控制面板中有效「宣告」該身份。如果通過Azure AD同步已存在同一使用者，本地同步將覆蓋現有的EntraID使用者資料。

此行為是有案可稽的限制。根據思科官方技術文檔：https://securitydocs.cisco.com/docs/csa/china/olh/129444.dita

不支援從Umbrella AD聯結器和Cisco Umbrella Azure AD應用並行同步相同的使用者和組標識，從而導致策略實施不一致。

結論:所需的設定（Azure和On-Prem中現有使用者的VA可見性）被確認為不受支援的配置。路徑轉發需要使用漫遊客戶端以確保一致的標識實施。

相關內容

- 從Azure AD設定標識 — Cisco Umbrella文檔
- 思科技術支援與下載

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）。