在Cisco Secure Access中使用個人Google帳戶的訪客使用者的ZTNA註冊失敗

目錄

問題

在使用ZTNA（零信任網路訪問）部署專用訪問期間，在Entra ID中成功註冊並在Secure Access中進行設定後，使用個人Google帳戶的訪客使用者註冊失敗。遇到的特定症狀包括：

- 基於客戶端的註冊:註冊過程達到SSO身份驗證，提供憑證，但ZTNA顯示「I/O錯誤」，並且註冊過程停滯
- 無客戶端訪問:返回錯誤消息「Cisco Secure Access Login failure（思科安全訪問登入失敗）」。檢查IDP配置」以及事務ID

這些故障會阻止訪問私有資源，並影響對使用非公司身份的承包商式訪問的ZTNA功能的測試。

環境

- 採用ZTNA部署的Cisco安全訪問
- 作為身份提供程式的Microsoft Entra ID（以前稱為Azure AD）
- 在Entra ID中註冊為訪客使用者的個人Google帳戶(@gmail.com)
- 已設定訪客帳戶並在Secure Access中可見
- 在Entra ID和思科安全訪問之間配置SAML身份驗證

解析

通過修改Microsoft Entra ID中的SAML屬性對映配置解決了註冊失敗。為了解決這一問題，採取了以下步驟：

步驟 1:分析DART捆綁包和客戶端行為

檢視DART捆綁包，確認Cisco Secure Client和ZTA元件正常運行。分析應驗證註冊流是否成功到達思科安全訪問，以及是否在使用身份提供程式進行SAML身份驗證期間發生故障。

步驟 2:檢查Entra ID身份驗證日誌

檢查Entra ID身份驗證日誌，確認從身份提供程式角度成功完成身份驗證過程。日誌應顯示成功的身份驗證，但由於屬性不匹配，安全訪問拒絕登入。

步驟 3:確定SAML屬性對映問題

確定Entra ID正在將UPN（使用者主體名稱）作為SAML宣告發佈，該宣告與Secure Access預期的個人Gmail帳戶標識不匹配。斷言的IdP屬性與預期的使用者識別符號不一致。

步驟 4:修改SAML屬性對映

將Microsoft Entra ID中的SAML屬性對映從UPN更改為Email Address。這可確保電子郵件地址宣告與個人Google帳戶標識相匹配。

步驟 5:驗證註冊成功

實施屬性對映更改後，請重試ZTNA註冊流程。Cisco Secure Access ZTA現在應識別Gmail地址並允許成功完成註冊。

原因

註冊失敗是由於Microsoft Entra ID宣告的SAML屬性與Cisco Secure Access中的預期使用者識別符

號之間的不匹配造成的。Entra ID配置為將UPN（使用者主體名稱）作為SAML宣告傳送，但是對於個人Google帳戶(@gmail.com)，此UPN與實際電子郵件地址身份不一致。Cisco Secure Access將接收作為標識屬性的電子郵件地址，以便與已設定的訪客使用者帳戶匹配，從而導致IdP身份驗證成功後拒絕身份驗證。

相關內容

- 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）。