使用Duo SAML整合時安全訪問RAVPN身份驗證失敗

目錄

問題

在嘗試使用Duo作為身份提供者(IDP)並在後台整合Active Directory連線到思科安全訪問遠端訪問VPN(RAVPN)時，儘管在Duo門戶級別身份驗證成功，但使用者仍會遇到身份驗證失敗。

具體症狀包括：

- Duo portal顯示身份驗證成功消息。
- Duo成功後，Cisco SecureClient立即顯示「身份驗證失敗」錯誤消息。
- Duo日誌顯示「已授予訪問許可權」狀態。
- 思科安全訪問門戶日誌顯示「AAA故障」狀態。

這將建立一個斷開連線，外部身份提供方確認身份驗證成功，但VPN客戶端由於安全訪問基礎設施中的身份驗證驗證失敗而無法建立連線。

環境

- Cisco Secure Access RAVPN部署
- 作為SAML身份提供商的Duo Security
- Active Directory與Duo整合
- Cisco SecureClient for VPN連線
- 基於SAML的身份驗證流程

解析

通過更正Duo和Cisco Secure Access之間的使用者屬性對映解決了身份驗證故障。為查明和解決該問題，採取了以下各節中概述的步驟。

步驟 1:檢查活動搜尋

1. — 登入思科安全訪問控制面板。按一下Monitor > Remote Access Logs。

2. — 檢查授權檢查失敗消息下的使用者名稱欄位。

3. — 將其與Connect > User and Groups下的UPN值相匹配。

思科安全訪問檢視用於授權檢查的使用者主體名稱值。

從Duo傳遞的使用者主體名稱與該使用者在使用者和組下的使用者主體名稱值不匹配。

調查顯示：

- 使用者電子郵件地址：user@gmail.com
- 使用者主體名稱(UPN使用者名)

步驟 2:Duo配置調整

解決方案涉及修改Duo SAML配置以確保正確的使用者屬性對映：

- 訪問Duo Admin Panel。
- 導航到Cisco Secure Access的SAML應用程式配置。
- 修改使用者屬性對映以傳送電子郵件地址，該電子郵件地址必須與該使用者的「使用者」和「組」下的「使用者主體名稱」值相匹配。
- 儲存配置更改。

步驟 4:驗證

調整Duo配置後，驗證流程已經過測試，並且驗證成功。使用者能夠使用遠端訪問VPN進行連線，而無需身份驗證失敗。

原因

身份驗證失敗的根本原因是Duo SAML斷言和Cisco Secure Access期望之間的使用者屬性對映不匹配。Duo配置為在SAML斷言中以使用者主體名稱(UPN)傳送使用者名稱，而Cisco Secure Access配置為預期使用者電子郵件地址。這種不匹配導致身份驗證在安全訪問級別失敗，儘管身份驗證在Duo IDP級別成功，導致「AAA故障」登入安全訪問，而Duo日誌顯示「已授予訪問許可權」。

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）。