VPNaaS SAML身份驗證失敗，並顯示"；解密中繼狀態失敗"使用Duo IdP時出錯

目錄

問題

嘗試使用具有SAML身份驗證的安全客戶端遠端訪問和Duo作為身份提供程式(IdP)建立VPNaaS連線時，觀察到以下錯誤：

- 處理SSO身份驗證請求時失敗。請與系統管理員聯絡
- 解密中繼狀態失敗

具有相同IdP和Duo配置的身份驗證成功用於ZTNA（零信任網路訪問），但對於VPN連線失敗。Duo中為ZTNA和VPN配置了兩個不同的應用程式，它們都使用相同的IdP。

環境

- 技術：解決方案支援（SSPT — 需要合約）
- 子技術：安全訪問 — 安全客戶端遠端訪問（VPN、安全狀態、專用資源）
- 身份驗證方法：含Duo IdP的SAML
- 配置了兩個Duo應用程式：一個用於ZTNA，一個用於VPN
- 身份驗證適用於ZTNA，VPN失敗
- 軟體版本:ALL
- 未指定最近的硬體/軟體版本更改

解析

通過更正VPN的Duo應用程式上的實體ID和宣告使用者服務(ACS)URL的配置，解決了此問題。從Secure Access下載了正確的後設資料並將其上傳到VPN Duo應用程式，從而解決了SAML中繼狀態解密錯誤。

1. 登入到CSA儀表板。轉到連線>終端使用者連線 — >虛擬專用網路。查詢您連線的配置檔案。
2. 按一下該Profile和Edit。轉到Authentication頁籤。
3. 下載用於安全訪問的SAML後設資料。
4. Check entityID="https://X.vpn.sse.cisco.com/saml/sp/metadata/saml"和 <AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://X.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=Profilename"></AssertionCo
5. 確保entityID和AssertionConsumerService與為VPN SSO身份驗證配置的Duo應用程式匹配。

原因

Duo VPN應用程式上的實體ID和ACS URL配置錯誤導致SAML中繼狀態解密失敗。Duo for VPN中不存在正確的配置，即使ZTNA身份驗證使用相同的IdP也是如此。使用來自Secure Access的準確後設資料更新Duo VPN應用程式解決了問題。

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）。