安全訪問證書檢查狀態檢查身份驗證失敗

目錄

問題

嘗試使用證書檢查功能使用終端安全狀態配置檔案部署安全訪問時，所有登入嘗試都會失敗，儘管在DART捆綁日誌中無法識別失敗的具體原因。使用者嘗試使用SAML IDP身份驗證，同時還希望通過安全狀態檢查機制實施證書驗證，但此配置會導致一致的身份驗證失敗，即使後端證書匹配成功。

環境

- 思科安全訪問 — 安全客戶端遠端訪問（VPN、安全狀態、專用資源）
- SAML IDP身份驗證整合
- 已啟用證書檢查功能的終端狀態配置檔案
- SAN中具有UPN欄位的使用者證書與電子郵件地址匹配
- 使用使用者、組和終端裝置的安全訪問租戶配置

解析

僅當使用要求使用者證書和機器證書驗證的多證書身份驗證時，才會實施證書終端狀態檢查。由於部署方案涉及僅擁有使用者證書且需要使用單個VPN配置檔案的使用者，因此解決方案涉及實施SAML +單一證書身份驗證，而不是依賴狀態證書檢查。

身份驗證配置步驟

步驟 1:配置SAML +單證書身份驗證

將身份驗證方法配置為將SAML身份驗證與單個證書身份驗證結合使用，而不是嘗試通過狀態檢查強制進行證書驗證。

步驟 2:配置證書UPN匹配

確保證書的使用者備用名稱(SAN)中的UPN欄位包含與在「使用者」、「組」和「終端裝置」下的「安全訪問」中為使用者配置的auth屬性相匹配的使用者電子郵件地址。

步驟 3:設定主要身份驗證欄位

配置主欄位以使用證書中的UPN進行身份驗證，確保它與Secure Access使用者資料庫中的使用者電子郵件地址相對應。

證書結構要求

必須配置證書結構，以便證書中的UPN或輔助值與安全訪問中使用者的auth屬性相匹配。如果使用者提供的證書的UPN或輔助值與安全訪問中為該使用者配置的auth屬性不匹配，則身份驗證將被拒絕。

重要配置說明

如果需要執行狀態證書檢查，則需要多證書身份驗證(IDP SAML + Multi-Cert Auth)，但這需要使用者和電腦證書。對於使用者僅擁有使用者證書且需要使用單個VPN配置檔案的部署，SAML +單一證書身份驗證提供了合適的解決方案，同時仍保持基於證書的安全控制。

原因

僅當配置了多證書身份驗證時，才會實施證書終端狀態檢查。將SAML身份驗證與狀態證書檢查配合使用時，系統希望存在使用者和電腦證書以進行驗證。由於部署僅使用具有SAML身份驗證的使用者證書，因此儘管後端證書匹配成功，但安全狀態證書檢查功能始終無法進行身份驗證嘗試，因為安全狀態機制未設計用於單個證書身份驗證方案。

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）。