使用Azure Entra ID排除SNA管理器SSO身份驗證故障

目錄

問題

在將Azure Entra ID整合為SAML身份驗證的身份提供程式(IdP)後，使用者嘗試登入到SNA管理器時遇到SSO身份驗證失敗。顯示的特定錯誤消息為：

「身份驗證服務無法完成您的請求。如果此問題仍然存在，請與管理員聯絡。」

在設定過程中，匯入SP（服務提供程式）後設資料檔案後，SNA Manager FQDN會自動從原始SNA Manager URL更改為包含「/fedlet」，從而導致身份驗證設定失敗。系統稽核日誌確認身份驗證失敗並出現「未知使用者」錯誤，表明SNA管理器無法識別從Azure傳輸的SAML響應中傳輸的使用者名稱。

環境

- 思科安全網路分析(SNA)管理員版本7.6.0
- 配置為SAML標識提供程式的Microsoft Azure Entra ID

解析

解決方法涉及更正Azure Entra ID和SNA Manager中的SAML NameID屬性配置，以確保正確的使用者名稱格式匹配。

步驟 1:執行SAML跟蹤分析

使用瀏覽器開發者工具執行SAML跟蹤並檢查Azure的IdP響應，以標識正在傳輸的NameID格式。跟蹤顯示，Azure正在傳送NameID屬性中的完整使用者主體名稱(UPN):

<#root>

<Subject><NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" SPNameQualifier="https:/

username@example.com<

/NameID>

步驟 2:檢視SNA管理器稽核日誌

檢查SNA Manager稽核日誌，確認與格式錯誤的NameID相關的身份驗證失敗：

<#root>

Aug 3 06:53:36 device AuditLogger[1480861]: AuditLogger: osaxsd/1480861,4003,2026-08-03T06:53:36TZD+000

步驟 3:修改Azure SAML NameID配置

在Azure Entra ID SAML配置中，將NameID屬性從預設使用者主體名稱更改為使用「本地SAM帳戶名稱」。 這可確保NameID僅包含不帶域字尾的使用者名稱(username@example.com成為使用者名稱)。

步驟 4:更新SNA管理器SAML ID配置

導航到SNA Manager使用者管理頁面，並更新SAML ID值以匹配配置更改後Azure傳輸的已更正的NameID格式。

步驟 5:驗證SSO身份驗證

嘗試通過SAML工作流登入，測試SSO身份驗證。現在，使用者已成功進行身份驗證，並且沒有收

到以前的錯誤消息。

原因

身份驗證失敗是由於Azure Entra ID傳送的NameID格式與SNA管理器預期的使用者名稱格式不匹配。Azure配置為在SAML NameID屬性中以「username@example.com」格式傳送使用者主體名稱(UPN)，而SNA管理器僅期望使用者名稱部分不帶域字尾。這種格式差異導致SNA管理器將傳入的身份驗證請求視為來自無法識別的使用者，導致「未知使用者」身份驗證失敗。

相關內容

- 為Microsoft Azure SAML整合配置SNA管理器
- 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）。