

使用差異IDP對思科安全訪問中的使用者/組身份同步進行故障排除

目錄

問題

本文描述如何排除思科安全訪問中使用者身份和組身份與不同身份提供程式(IdP) (例如Okta、Microsoft Entra ID和IBM Cloud) 同步的故障。

環境

- Cisco Secure Access - SCIM調配整合
- 適用於SCIM 2.0 IdP聯結器(Okta、Azure AD)

解析

概觀

Cisco Secure Access支援使用SCIM 2.0標準直接從Okta和Microsoft Entra ID (以前稱為Azure AD) 調配使用者和組身份，從而無需為僅雲身份源部署本地Active Directory(AD)聯結器。本文整合了現場工程師和管理員在部署或維護此整合時最常遇到的架構假設、常見故障模式和故障排除指南。

本檔案分為四個部分：

- 配置 — 獲取正式設定說明的位置

- 架構假定，如果違規，會導致靜默或難以診斷的故障
- 提供商特定的問題 (Okta與Entra ID)
- 不考慮IdP而適用的通用SCIM協定問題

組態

本文側重於故障排除，而非初始設定。使用本文檔中的官方Cisco TechNotes進行逐步配置：

- 若要使用Microsoft Entra ID(Azure AD)配置Cisco Secure Access，請參閱以下連結：通過Entra ID將使用者和組設定為安全訪問
- 要使用Okta配置思科安全訪問，請參閱以下連結：調配使用者和組以通過OKTA安全訪問

這兩個文檔都涉及在Secure Access中生成SCIM令牌和調配URL、在IdP中配置相應的應用程式以及運行初始調配同步。

架構初級課程

在排除故障之前，請確認部署符合這些核心假設。大多數同步失敗都追溯到這些假設之一。

一次一個身份源

不支援從本地AD聯結器和雲IdP (Okta或Entra ID) 同時調配相同的使用者或組，從而導致策略實施不一致。如果從AD聯結器遷移到雲IdP:

- 停止本地AD聯結器服務。
- 在啟用雲IdP調配之前，確認沒有剩餘同步作業正在運行。

虛擬裝置是例外

Entra ID或Okta無法為虛擬裝置(VA)提供身份整合，因為IdP無法檢視VA所需的專用IP到使用者對映。無論用於其他元件的裝置如何，VA部署仍需要本地AD聯結器。

分配與推送

- Action:向應用程式分配使用者或組
 - 它實際的作用：將該組的成員使用者設定為安全訪問
- Action:推送組(Okta)
 - 它實際的作用：設定組對象本身（用於策略目標）。它不會同步任何使用者。



附註：請勿推入已分配給應用程式的使用者調配組。這可以建立重複或衝突的組狀態。

組和使用者限制

對從其中一個IdP調配的使用者數量沒有硬性限制。

組被封閉。過去，每個組織有200個組，這些組來自Okta或Entra ID;一些目前的檔案顯示，具體來說，Okta的最高限額（最高可達1,000美元）更高。將確切數字視為與環境相關，並聯絡思科技術支援中心(TAC)或當前思科文檔進行確認。未以靜默方式調配超出上限的組，並且不會出現任何錯誤。

如果您需要更廣泛的覆蓋範圍，請使用動態的「所有使用者」(Entra ID)或「所有人」(Okta)組，而不是嘗試逐個推送每個組。

SCIM令牌生命週期

在Cisco Secure Access中，當您選擇Connect > Users，Groups and Endpoint Devices > Configuration Management > Integrate Directory時會生成令牌。令牌在建立時只顯示一次。

重新生成令牌時，它會立即中斷IdP端的調配，直到在Microsoft Entra ID或Okta的調配配置中輸入新令牌。沒有寬限期，並且IdP端錯誤通常是通用錯誤（身份驗證失敗），而不是令牌過期消息。

定期刷新令牌以確保安全衛生，並在輪換後立即在IdP端測試連線。

特定問題

- 症狀：組不顯示在Secure Access中
 - 根本原因:推送組僅調配組對象；它不會同步成員。
 - 解析度：確保將相關組成員單獨分配給「分配」下的應用程式。
- 症狀：使用者已設定，但屬性缺少或錯誤
 - 根本原因:「僅安全訪問」(Secure Access only)曲面顯示名稱和使用者名稱；給定和姓氏未列出。
 - 解析度：確認已明確選擇所需的屬性以進行同步；不要假定所有Okta配置檔案欄位都會傳播。
- 症狀：無提示設定不會執行任何操作
 - 根本原因:未啟用「建立使用者」、「更新使用者屬性」或「停用使用者」切換。
 - 解析度：驗證是否在Okta管理員控制檯的Provisioning > To App下選中了所有三個選項。
- 症狀：objectGUID或自定義屬性未同步
 - 根本原因:屬性未通過使用者配置檔案對映新增和對映。
 - 解析度：新增objectGUID屬性，並在需要此識別符號時建立相應的配置檔案對映。
- 症狀：令牌旋轉後同步停止
 - 根本原因:SCIM 或API令牌在安全訪問中重新生成，但在Okta中未更新。
 - 解析度：在Provisioning > Configure API Integration下輸入新令牌，然後再次運行Test API Credentials。
- 症狀：無法確定特定使用者或組的失敗原因
 - 根本原因:未首先檢查日誌。
 - 解析度：在升級之前，請檢視Reports > System Log in Okta，過濾至Cisco User Management Connector應用程式。
- 症狀：組計數超過上限，部分缺失且無錯誤
 - 根本原因:組織具有比安全訪問支援的範圍更多的組。

- 解析度：將範圍縮小到僅與策略相關的組，或聯絡Cisco TAC以獲得更高級別的組支援。

Microsoft Entra ID特定問題

- 症狀：動態組成員身份未反映在Secure Access中
 - 根本原因:動態組規則配置錯誤，或組不在已布建的作用域中。
 - 解析度：在假定Secure Access同步錯誤之前，直接在Entra ID中驗證動態成員身份規則。
- 症狀：SAML SSO應驅動SWG標識
 - 根本原因:AnyConnect安全網路閘道(SWG)不支援針對Entra ID的安全斷言標籤語言(SAML)驗證；它使用與本地AD相同的被動身份驗證機制。
 - 解析度：不要針對Entra ID設計SAML驅動的SWG標識；使用被動身份驗證（如所述）。
- 症狀：使用者錯誤地顯示已停用
 - 根本原因:傳送的Entra ID處於活動狀態：false，因為使用者不屬於分配的組範圍，或者活動屬性對映配置錯誤。
 - 解析度：檢查是否已將使用者從作用域組中刪除；驗證活動對映(通常必須計算為Not([isSoftDeleted]))。
- 症狀：已隔離應用程式，所有設定都已停止
 - 根本原因:目標應用程序返回了重複的不符合SCIM的響應。
 - 解析度：在假定各個用戶失敗之前，檢查隔離標誌的企業應用程式調配狀態。
- 症狀：初始調配週期完全失敗
 - 根本原因:第一次運行時出現臨時同步失敗。
 - 解析度：在「概述」頁中按一下重新啟動調配，以強制輸入ID再次嘗試初始同步。
- 症狀：重複使用者意外合併
 - 根本原因:兩個源身份共用相同的電子郵件或使用者主體名稱(UPN)。
 - 解析度：確保電子郵件和UPN在源目錄中的唯一性；驗證郵件屬性是否來自已驗證的域。

- 症狀：在架構更改後，屬性停止更新
 - 根本原因:目標端的屬性型別已更改（例如，字串更改為布林型），但未更新Entra ID對映。
 - 解析度：手動更正屬性對映下的高級設定中的型別。
- 症狀：從不填寫經理引用
 - 根本原因:使用者在其經理之前處於作用域中；調配不會自動回填。
 - 解析度：重新啟動調配，以強制對範圍內的所有使用者進行完全重新評估。

IBM安全驗證特定問題

- 症狀：使用者設定，但組從不顯示在Secure Access中
 - 根本原因:驗證自定義SCIM聯結器是否僅發出使用者操作；從未傳送過任何POST/Groups呼叫（帳戶調配功能差距，不是對映錯誤）。
 - 解析度：捕獲聯結器跟蹤並確認是否發生任何/組呼叫；如果沒有，則通過Cisco AD Connector、CSV匯入或針對Secure Access SCIM端點的計畫腳本來調配組。
- 症狀：組成員身份更新失敗，400或404
 - 根本原因:members[].value引用驗證內部使用者ID，而不是使用者建立時返回的SCIM ID安全訪問。
 - 解析度：更正成員對映以使用安全訪問SCIM ID並再次運行完全同步。
- 症狀：組顯示但為空
 - 根本原因:在Secure Access中存在其成員使用者之前推入的組;membership PATCH引用未知使用者。
 - 解析度：既然使用者存在，請再次運行完全同步；確保同步排序在組前建立使用者。
- 症狀：SAML登入循環或重複的重新定向
 - 根本原因:驗證IdP端點是否由SWG代理或解密，這將中斷身份驗證流程。
 - 解析度：繞過來自SAML或解密(外部域列表或選擇性解密)的驗證IdP URL。
- 症狀：使用者通過SAML進行身份驗證，但沒有基於使用者的策略匹配
 - 根本原因:SAML NameID與已布建的使用者authName不匹配。
 - 解析度：將驗證SAML應用程序中的NameID >格式與authName屬性對映（通常為

email或UPN) 對齊；再次測試。

- 症狀：配置在幾週或幾個月的穩定後停止工作
 - 根本原因:SCIM令牌在Secure Access中旋轉或過期，但在Verify聯結器中未更新。
 - 解析度：在Secure Access中刷新令牌，並在驗證自定義應用程式中更新;為刷新節奏設定日曆。
- 症狀：重新同步時建立的重複使用者
 - 根本原因:externalId映射到可變或非唯一屬性(例如，顯示名稱、可更改的電子郵件)。
 - 解析度：將externalId對映到不可變識別符號(驗證使用者ID或objectGUID);清除重複項並重新同步。
- 症狀：已停用驗證使用者在Secure Access中保持活動狀態
 - 根本原因:掛起未對映到active:false的操作，或者停用聯結器中的操作。
 - 解析度：啟用停用操作並將掛起對映到active:false;使用測試使用者進行驗證。
- 症狀：驗證中的屬性更改不傳播
 - 根本原因:使用者或屬性超出設定策略範圍，或者更新操作已禁用。
 - 解析度：審查應用程式調配策略或權利；啟用更新；觸發手動同步。
- 症狀：Secure Access拒絕包含架構或501樣式錯誤的請求
 - 根本原因:不符合SCIM的負載 (缺少架構陣列、錯誤的URN、不支援的操作) 。
 - 解析度：用基線捲曲試驗復制；更正負載或對映；如果聯結器發出格式錯誤的請求，則升級至IBM。
- 症狀：漫遊使用者缺少SWG標識，儘管SAML正在工作
 - 根本原因:希望使用SAML來驅動使用被動身份或基於代理身份的部署模式的身份。
 - 解析度：根據Secure Access文檔確認每種部署模式的身份獲取方法；請勿將SAML設計為唯一的身份源。

通用SCIM問題

這些不是思科專用的，但始終出現在安全訪問部署中，因為底層傳輸是標準SCIM 2.0:

- 隔離狀態遮蓋各個錯誤:如果同步似乎已完全停止而不是每個使用者失敗，請在調查單個屬性問題之前檢查應用程式級別的隔離或暫停狀態。
- 409停用衝突:一種常見模式，其中IdP嘗試停用使用者而目標引發衝突。這通常是活動屬性對映或組範圍問題，而不是真正的系統錯誤。
- 空白或清除的欄位不會一律傳播:某些SCIM伺服器實現保留最後一個非Null值；清除IdP中的欄位時，可能需要先將佔位符值推入。
- URL或配置更改以靜默方式使身份驗證失效:對SCIM端點URL的任何更改通常要求您再次提供持有者令牌。即使真正的問題是過時令牌，錯誤也會顯示為無效URL。
- 沒有本機webhook或事件流:期望對使用者或策略更改進行即時推送通知的自動化必須輪詢Reporting API或通過Cisco XDR整合。安全訪問不會發出出站設定網路掛接。

如果上述步驟不能解決問題，請從IdP端使用調配日誌升級至Cisco TAC。安全訪問端上的後端調配日誌通常需要TAC訪問才能提取。

原因

由於承載令牌過期、屬性對映不匹配、缺少目標組或設定範圍不足，SCIM設定整合無法推送一個或多個記錄。

相關內容

- Cisco:[通過Entra ID將使用者和組設定為安全訪問](#)
- Cisco:[調配使用者和組以通過OKTA安全訪問](#)
- Microsoft瞭解：SCIM 2.0協定合規性的已知問題 — Microsoft Entra ID
- Microsoft瞭解：疑難排解Microsoft Entra ID SCIM API錯誤
- 在身份提供程式中配置SAML SSO:<https://www.ibm.com/docs/en/security-verify?topic=sign-configuring-saml-single-in-identity-provider>
- 自定義(SCIM)應用的調配：<https://www.ibm.com/docs/en/security-verify?topic=endpoints-configuring-provisioning-custom-applications>
- 調配和監管概述（通用SCIM聯結器）：<https://docs.verify.ibm.com/verify/docs/use-cases-provisioning-and-governance>

- 本地調配網橋 (AD/LDAP源) : <https://docs.verify.ibm.com/verify/docs/on-premises-provisioning>

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）。