對Windows伺服器上的目錄聯結器身份驗證失敗和帳戶不匹配進行故障排除

目錄

問題

Windows Server上安裝的Cisco Directory Connector在嘗試使用與用於登入伺服器的管理員帳戶不同的管理員帳戶登入時身份驗證失敗。身份驗證過程錯誤地嘗試使用Windows伺服器登入帳戶而不是預期的Webex Control Hub管理員帳戶，從而導致以下錯誤消息：

- 身份驗證失敗
- 您的帳戶未獲得授權。請與管理員聯絡。

後端日誌顯示SAML2對映錯誤：

```
com.sun.identity.saml2.common.SAML2UserNotFoundException: No local user being mapped.
```

目錄聯結器先前在登入期間提示選擇帳戶，但在問題出現後，此提示會失敗，並且會嘗試使用不正確的帳戶進行身份驗證。應用程式重新安裝、服務重新啟動和伺服器重新啟動不會解決初始身份驗證失敗。

環境

- Windows Server 2019 Standard上安裝的Cisco Directory Connector
- 託管在Google Compute Engine VM上的伺服器
- 專用於目錄聯結器的伺服器，無其他主要服務
- Active Directory中的單獨使用者帳戶：沒有電子郵件許可權的伺服器管理員帳戶和沒有伺服器登入許可權的常規電子郵件帳戶
- 使用增量同步計時配置的目錄聯結器同步計畫
- BIOS模式設定為傳統，不支援安全引導

解析

通過下列步驟解決了身份驗證問題：

步驟 1:服務帳戶配置

更改Directory Connector服務帳戶，以使用具有適當Active Directory許可權的域帳戶：

1. 在Windows Server上開啟services.msc。
2. 找到目錄聯結器服務。
3. 將運行帳戶從本地系統更改為具有足夠AD許可權的域帳戶。
4. 重新啟動目錄聯結器服務。

步驟 2:帳戶對映驗證

確保目錄聯結器的本地登入與Webex Control Hub中的管理員帳戶匹配：

1. 驗證用於「目錄聯結器」的電子郵件帳戶是否具有AD使用者對象的讀取許可權。
2. 確認帳戶具有連線到域控制器和讀取Active Directory使用者對象的許可權。
3. 如有必要，請按照部署指南在Active Directory中將管理員帳戶新增為備用電子郵件。

步驟 3:刪除冗餘例項

刪除任何不需要的目錄聯結器例項：

1. 導航到Directory Connector介面。
2. 按一下不必要例項的三點選單。

3. 選擇Deactivate instance。

步驟 4:同步計畫調整

根據環境需要，將增量同步計時從預設的24小時時間間隔調整為較短的時間間隔。

步驟 5:配置檢查

檢查並確認目錄聯結器配置和同步計畫設定，以確保正確操作。

原因

主要根本原因是本地伺服器登入帳戶與目錄聯結器/Webex管理員帳戶不匹配。目錄聯結器嘗試使用Windows伺服器登入帳戶（而不是預期的Webex Control Hub管理員帳戶）進行身份驗證。此對映失敗是由於Active Directory中的帳戶分離，其中目錄聯結器在使用其他管理員帳戶登入到伺服器時無法正確對映Webex管理員帳戶。SAML2身份驗證過程失敗，因為無法在伺服器登入帳戶和Webex Control Hub管理員帳戶之間建立本地使用者對映。

相關內容

- Webex目錄聯結器部署指南
- 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）。