解決安全訪問AD聯結器同步問題

目錄

問題

安裝在域控制器上的AD聯結器未與Cisco安全訪問正確同步。聯結器遇到多個同步故障，包括：

- 增量同步失敗並出現「訪問被拒絕」錯誤(COMException 0x80070005)。
- DC事件日誌讀取失敗，出現「UnauthorizedAccessException:已嘗試執行未經授權的操作」。
- 下載清單時顯示「無效URI格式」的雲註冊問題。
- 同步嘗試期間特定AssetID的HTTP 404 "object_not_found"錯誤。

聯結器似乎可以連線到Cisco Secure Access雲服務，但在Active Directory許可權端和雲註冊配置上都失敗。

環境

- 採用AD聯結器的思科安全存取
- AD聯結器版本1.15.2
- 安裝在域控制器上的AD聯結器
- 自定義服務帳戶(svcCiscoUmbrella)而不是預設的Cisco_Connector帳戶
- 測試/試運行環境設定

解析

解決方案涉及通過完整的重新安裝過程解決Active Directory許可權問題和雲註冊問題：

步驟 1:驗證和清除現有的AD聯結器條目

在「安全訪問」控制面板中，驗證主機的AD聯結器條目，並刪除同一伺服器的所有過時或重複條目（如果存在）。

步驟 2:確保完全解除安裝

完全解除安裝現有的AD聯結器服務，以確保沒有殘留可能導致註冊問題的配置。

步驟 3:運行域控制器指令碼

在重新安裝聯結器之前，請運行正確的域控制器配置指令碼以確保設定適當的許可權。需要在每個適用的域控制器上運行指令碼，儘管聯結器本身可以駐留在其他加入域的電腦上的域控制器之外。

步驟 4:配置服務帳戶許可權

將所需的Active Directory許可權授予服務帳戶：

- AD同步許可權（域/根作用域，視情況而定）：
    - 讀取
    - 複製目錄更改
    - 複製全部目錄更改（如果環境需要）
    - 複製篩選集中的目錄更改（如果環境需要）
- 域控制器上的事件日誌訪問:
    - 將服務帳戶新增到「事件日誌讀取器」組。
    - 確保具有同等的、基於策略的許可權才能讀取安全日誌。

步驟 5:重新安裝AD聯結器

重新安裝AD聯結器服務以生成新的清單和有效的AssetID，確保正確註冊雲。

步驟 6:重新啟動和驗證

安裝和許可權配置之後：

1. 重新啟動AD聯結器服務。
2. 監控聯結器日誌，確認訪問被拒絕和未經授權的錯誤停止。
3. 驗證日誌中顯示的同步條目是否成功(例如，「ADSync LDIF RESPONSE:200 Success」)。

原因

同步問題是由兩個主要因素引起的：

1. Active Directory許可權不足：自定義服務帳戶(svcCiscoUmbrella)缺少增量同步和DC事件日誌訪問所需的AD許可權，導致「拒絕訪問」和「UnauthorizedAccessException」錯誤。
2. 雲註冊問題：聯結器例項註冊錯誤或指向無效/舊的AssetID，導致下載清單時出現「Invalid URI format」錯誤，並在同步嘗試期間出現HTTP 404「object_not_found」錯誤。

安裝過程不完整，導致在聯結器安裝之前無法正確執行域控制器配置指令碼，從而加劇了這些問題。

相關內容

- Cisco Secure Access AD聯結器配置
- AD聯結器許可權要求
- AD聯結器安裝指南

- AD聯結器故障排除
- AD聯結器服務帳戶配置
- 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）。