

ISE 3.5 EntraID外部組查詢效能問題和Microsoft Graph API許可權解析

目錄

問題

查詢EntraID.ExternalGroups時，帶有EntraID REST ID Store配置的Cisco ISE 3.5 patch2在EAP-TLS身份驗證期間遇到嚴重的身份驗證延遲。Queried PIP - EntraID.ExternalGroups階段需要超過30秒才能完成，導致EAP客戶端超時並重新啟動身份驗證，從而阻止會話成功完成。

此外，嘗試在EntraID REST ID儲存配置中儲存組屬性時，會出現以下錯誤消息：

```
java.rmi.RemoteException: null; nested exception is: java.lang.NullPointerException
```

身份驗證日誌顯示外部組查詢過程中出現非同步PIP錯誤和策略引擎掛起。該問題顯示為身份驗證失敗的工作流，客戶端由於查詢時間延長而無法完成EAP會話。

環境

- 思科身份服務引擎(ISE)版本3.5.0.527，帶補丁2
- 通過REST ID儲存的Microsoft EntraID(Azure Active Directory)整合
- 已配置EAP-TLS身份驗證
- 為具有組屬性檢索的EntraID配置的REST源
- 在ISE 3.4 patch4/patch5和ISE 3.5 patch2/patch3上觀察到問題

解析

解決方案涉及向ISE EntraID REST ID儲存整合使用的Azure應用程式授予正確的Microsoft Graph API許可權。

步驟 1:授予所需的Microsoft Graph API許可權

導航到Azure門戶並找到用於ISE整合的應用程式註冊。授予此應用程式型別API許可權：

Directory.Read.All

確保授予對此許可權的管理員同意。

步驟 2:重新啟動ISE服務

授予Directory.Read.All許可權後，在所有ISE節點上執行服務重新啟動，以確保新許可權生效。

步驟 3:驗證解析度

測試身份驗證過程，以確認已查詢的PIP - EntraID.ExternalGroups階段在可接受的時限內完成，並且Group屬性可以儲存而不會出現錯誤。

解析日誌必須顯示成功完成，而不顯示AsynchronousPIPEError:

```
2026-05-26 14:21:47,981 DEBUG [I/O dispatcher 1][[]] cisco.ise.ropc.utilities.HttpClientWrapper -:::--
```

原因

此問題是由思科錯誤ID CSCwu13703引起的，它影響ISE 3.5補丁3和相關版本。此錯誤與EntraID整合的Microsoft Graph API許可權不足有關。如果沒有適當的Directory.Read.All許可權

，ISE無法從EntraID有效查詢外部組，導致超時條件和通過AsynchronousPIPErro異常的策略引擎掛起。

身份驗證過程失敗，因為每次失敗的評估都會導致策略引擎拋出AsynchronousPIPErro並掛起身份驗證工作流，從而導致延長的查詢時間並最終導致客戶端超時。

相關內容

- [思科錯誤ID CSCwu13703](#)
- [Cisco ISE with Microsoft Active Directory Entra ID和Intune配置指南](#)

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）。