

ISE 3.5 EntraID外部グループクエリパフォーマンスの問題とMicrosoft Graph API権限の解決

内容

問題

EntraID REST IDストア設定を含むCisco ISE 3.5 patch2で、EntraID.ExternalGroupsのクエリを実行する際にEAP-TLS認証中に著しい認証遅延が発生します。Queried PIP - EntraID.ExternalGroupsフェーズが完了するまでに30秒以上かかり、EAPクライアントがタイムアウトして認証を再開する原因となるため、セッションが正常に完了しません。

また、EntraID REST IDストア設定でグループ属性を保存しようとする、次のエラーメッセージが表示されます。

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

認証ログには、外部グループのルックアッププロセス中の非同期PIPエラーおよびポリシーエンジンの一時停止が表示されます。この問題は、クエリー時間が長いためにクライアントがEAPセッションを完了できない失敗した認証ワークフローとして現れます。

環境

- Cisco Identity Services Engine(ISE)バージョン3.5.0.527 (パッチ2)
- REST IDストアによるMicrosoft EntraID (Azure Active Directory)の統合
- EAP-TLS認証が設定されました
- グループ属性を取得するEntraID用に設定されたRESTソース
- ISE 3.4 patch4/patch5およびISE 3.5 patch2/patch3で発生する問題

解決方法

この問題を解決するには、ISE EntraID REST IDストア統合で使用されるAzureアプリケーションに適切なMicrosoft Graph API権限を付与する必要があります。

ステップ1：必要なMicrosoft Graph API権限の付与

Azureポータルに移動し、ISE統合に使用するアプリケーション登録を見つけます。次のアプリケーションタイプAPI権限を付与：

Directory.Read.All

このアクセス許可に対して管理者の同意が与えられていることを確認してください。

ステップ2:ISEサービスを再起動します。

Directory.Read.All権限を付与した後、すべてのISEノードでサービスの再起動を実行して、新しい権限が有効になるようにします。

ステップ3：解決策の確認

認証プロセスをテストして、Queried PIP - EntraID.ExternalGroupsフェーズが許容時間内に完了し、グループ属性がエラーなしで保存できることを確認します。

解決ログには、AsynchronousPIPErrorを使用せずに正常に完了したことが示されている必要があります。

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

原因

この問題は、ISE 3.5パッチ3および関連バージョンに影響を与えるCisco Bug ID CSCwu13703が原因で発生します。このバグは、EntraID統合に対するMicrosoft Graph APIの権限が不十分なことに関連しています。適切なDirectory.Read.All権限がない場合、ISEはEntraIDから外部グループに対して効率的にクエリを実行できません。その結果、タイムアウト状態が発生し、AsynchronousPIPError例外を通じてポリシーエンジンが一時的に停止します。

評価が失敗するたびにポリシーエンジンがAsynchronousPIPErrorをスローして認証ワークフローを中断し、クエリ時間が長くなり、クライアントタイムアウトが発生するため、認証プロセスは失敗します。

関連コンテンツ

- [Cisco Bug ID CSCwu13703](#)
- [Microsoft Active Directory Entra IDおよびIntuneを使用したCisco ISEの構成ガイド](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。