Active DirectoryおよびMicrosoft EntraIDを使用したCisco Secure Access IDの同期

内容

お問い合わせ内容

Cisco Secure Accessで、同じドメイン名を持つ2つのIDソースからユーザとグループをプロビジョニングしようとすると、課題が発生します。具体的なシナリオでは、オンプレミスのActive Directory(AD)とMicrosoft EntraID（以前のAzure AD）の両方のソースが同じドメイン名(domain.comなど)を使用する場合に、両方のIDを同期する必要がありました。

主な懸念事項は次のとおりです。

- 両方のアイデンティティソースに同じユーザーとグループが存在する場合の、ID所有権とグループメンバーシップマッピングの動作について
- オンプレミスとクラウドの両方のリソースにアクセスするハイブリッドユーザに対して、一貫した安全なアクセスポリシーを確実に適用
- このハイブリッドID構成のユーザーに対する内部IP可視性の維持
- 両方のソースからの同時同期が本番環境で問題を引き起こすかどうかを判断する

ドキュメントには、「Cisco AD ConnectorとCisco User Management for Secure Accessアプリケーションからの同じユーザおよびグループの同時同期はサポートされておらず、一貫性のないアクセスルールの適用につながります」と記載されています。

環境

- Cisco Secure AccessとAD ConnectorおよびEntraIDの統合
- ドメイン名がEntraIDドメインと一致するオンプレミスのActive Directory
- オンプレミスADと同じドメイン名のMicrosoft EntraID (Azure AD)

- IDフェデレーション用のSAML SSO設定
- ポリシー適用のためのセキュアWebゲートウェイ(SWG)モジュール
- オンプレミスとクラウドの両方のリソースへのアクセスを必要とするハイブリッド環境

解決策

Active DirectoryとEntraIDの両方のソースから同時同期に対して次の動作が確認されました。

グループ同期動作

両方のソースから同じ名前のグループを同期する場合：

- Cisco Secure Accessでは、2つの個別のグループオブジェクト（各ソースから1つずつ）が作成されます
- アクセスポリシーでは、グループを送信元プレフィクスで区別できます
- オンプレミスADグループはAD-Domain/GroupNameのように表示されます。
- EntraIDグループはGroupNameと表示されます。

ラボ検証では、「Success.複数のEntraIDドメインのグループの<<<<同期済み」です。

ユーザ同期動作

両方のソースから同じユーザIDを持つユーザを同期する場合：

- ユーザーIDは同期中に上書きされます
- セキュアアクセスでは、一意のユーザIDが1つだけ表示されます
- 最終的な同期ソースによって、ユーザの属性とグループメンバーシップが決まります
- EntraID同期は通常、オンプレミスADが設定されている場合に優先されます

アクセスポリシーの設定

アクセスポリシーでは、両方のグループタイプを使用できます。

- 完全パスAD-Domain/GroupNameを使用してオンプレミスADグループを参照します。
- 単純な名前GroupNameを使用してEntraIDグループを参照します。
- ポリシーは、グループメンバーシップソースに基づいてユーザを区別できます

次の設定は、多くのお客様に適しています。

```
1    Only provision identities from on-prem AD - for VA DNS protection
2    Use Azure entra for SSO/user authentication (no identities to be provisioned from Azure) - for SWG
```

原因

テスト中、ユーザがオンプレミスADコネクタから同期されるたびに、Umbrellaダッシュボードでそのidが事実上「要求」されることを確認しました。同じユーザーがAzure AD同期を介して既に存在する場合、オンプレミスの同期は既存のEntraIDユーザーデータを上書きします。

この動作はドキュメント化された制限です。シスコの公式技術文書：https://securitydocs.cisco.com/docs/csa/china/olh/129444.dita

「Umbrella AD ConnectorとCisco Umbrella Azure ADアプリからの同じユーザIDとグループIDの同時同期はサポートされておらず、一貫性のないポリシー適用につながります。」

結論：目的のセットアップ（Azureとオンプレミスの両方に存在するユーザーのVA可視性）が、サポートされていない構成であることが確認されました。パス転送では、IDの一貫した適用を保証するためにローミングクライアントを使用する必要があります。

関連コンテンツ

- Azure ADからのIDのプロビジョニング – Cisco Umbrellaドキュメント
- シスコのテクニカルサポートとダウンロード

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。