セキュアアクセスADコネクタの同期問題のトラブルシューティング

内容

問題

ドメインコントローラにインストールされているADコネクタがCisco Secure Accessと正しく同期していません。コネクタで、次のような複数の同期エラーが発生します。

- 「Access is denied」エラーによるデルタ同期エラー(COMException 0x80070005)
- 「UnauthorizedAccessException: Attempted to perform an unauthorized operation」というエラーメッセージが表示され、DCイベントログの読み取りに失敗します。
- マニフェストのダウンロード時に「Invalid URI format」と表示されるクラウド登録の問題。
- 同期試行中の特定のAssetIDに対するHTTP 404「object_not_found」エラー。

コネクタはCisco Secure Accessクラウドサービスに接続しているように見えますが、Active Directoryの権限側とクラウド登録の両方の設定で失敗します。

環境

- ADコネクタを使用したCisco Secure Access
- AD Connectorバージョン1.15.2
- ドメインコントローラにインストールされたADコネクタ
- デフォルトのCisco_Connectorアカウントではなく、カスタムサービスアカウント(svcCiscoUmbrella)
- テスト/パイロット環境のセットアップ

解決方法

この問題を解決するには、完全な再インストールプロセスを通じて、Active Directoryの権限の問題とクラウド登録の問題の両方に対処する必要がありました。

手順1：既存のADコネクタのエントリの確認とクリーニング

セキュアアクセスダッシュボードで、ホストのADコネクタエントリを確認し、同じサーバの古いエントリまたは重複したエントリがあれば削除します。

ステップ2：完全なアンインストールの確認

既存のAD Connectorサービスを完全にアンインストールし、登録問題の原因となる残りの設定がないことを確認します。

ステップ3：ドメインコントローラースクリプトの実行

コネクタを再インストールする前に、適切なドメインコントローラの構成スクリプトを実行して、適切なアクセス許可が設定されていることを確認してください。このスクリプトは、該当する各ドメインコントローラで実行する必要があります。ただし、コネクタ自体は、ドメインに参加している別のコンピュータのドメインコントローラの外部に配置できます。

ステップ4：サービスアカウント権限の設定

必要なActive Directory権限をサービスアカウントに付与します。

- AD同期権限（必要に応じてドメイン/ルートスコープ）：
  - read
  - ディレクトリ変更の複製
  - ディレクトリ変更をすべてレプリケートする（環境で必要な場合）
  - フィルタ・セット内のディレクトリ変更のレプリケート（環境で必要な場合）

- ドメインコントローラのイベントログアクセス:
  - サービスアカウントをイベントログリーダーグループに追加します。
  - セキュリティログを読み取るための同等のポリシーベースのアクセス許可を確認します。

手順5: AD Connectorを再インストールする

AD Connectorサービスを再インストールして、新しいマニフェストと有効なAssetIDを生成し、適切なクラウド登録を行います。

ステップ6：再起動と検証

インストールと権限の設定後：

1. AD Connectorサービスを再起動します。
2. コネクタログを監視して、アクセス拒否および不正なエラーの停止を確認します。
3. 正常な同期エントリがログに表示されることを確認します（例：「ADSync LDIF RESPONSE: 200 Success」）。

原因

同期の問題は、主に次の2つの要因によって発生しました。

1. Active Directoryのアクセス許可が不十分：カスタムサービスアカウント(svcCiscoUmbrella)で、デルタ同期とDCイベントログへのアクセスに必要なADアクセス許可が不足しており、「アクセスが拒否されました」と「UnauthorizedAccessException」エラーが発生しました。
2. クラウド登録の問題：コネクタインスタンスが誤って登録されたか、無効または古いAssetIDを指しているため、マニフェストのダウンロード時に「無効なURI形式」エラーが発生し、同期試行中にHTTP 404の「object_not_found」エラーが発生します。

これらの問題は、コネクタのインストール前にドメインコントローラの設定スクリプトが正しく実行されなかった不完全なインストール手順によって複雑化しました。

関連コンテンツ

- Cisco Secure Access AD Connectorの設定
- ADコネクタのアクセス許可の要件
- ADコネクタのインストールガイド
- ADコネクタのトラブルシューティング
- ADコネクタサービスアカウントの構成
- 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。