Windows Serverでのアカウント不一致によるディレクトリコネクタ認証エラーのトラブルシューティング

内容

問題

Windows ServerにインストールされているCisco Directory Connectorで、サーバへのサインインに使用した管理者アカウントとは異なる管理者アカウントを使用してログインしようとすると、認証に失敗します。認証プロセスで、目的のWebex Control Hub管理者アカウントの代わりにWindowsサーバログインアカウントが誤って使用され、次のエラーメッセージが表示されます。

- Authentication failed
- アカウントが承認されていません。管理者に問い合わせてください。

バックエンドログにSAML2マッピングエラーが表示されます。

```
com.sun.identity.saml2.common.SAML2UserNotFoundException: No local user being mapped.
```

以前、Directory Connectorはログイン時にアカウントの選択を求めるプロンプトを表示していましたが、問題が発生した後、このプロンプトは失敗し、認証は正しくないアカウントで試行されます。アプリケーションの再インストール、サービスの再起動、およびサーバのリブートでは、初期認証の失敗は解決されません。

環境

- Windows Server 2019 StandardにインストールされたCisco Directory Connector
- Googleコンピューティングエンジン VMでホストされるサーバ
- Directory Connector専用のサーバ（その他の主要なサービスなし）

- Active Directoryで個別のユーザアカウント：電子メール権限のないサーバ管理者アカウントとサーバログイン権限のない通常の電子メールアカウント
- 差分同期タイミングで構成されたディレクトリコネクタ同期スケジュール
- セキュアブートがサポートされていないBIOSモードがレガシーに設定される

解決方法

認証の問題は、次の手順で解決されました。

ステップ1：サービスアカウントの設定

適切なActive Directory権限を持つドメインアカウントを使用するように、Directory Connectorサービスアカウントを変更します。

1. Windowsサーバのservices.mscを開きます。
2. Directory Connectorサービスを見つけます。
3. 実行アカウントをローカルシステムから、十分なAD権限を持つドメインアカウントに変更します。
4. Directory Connectorサービスを再起動します。

ステップ2：アカウントマッピングの検証

Directory ConnectorのローカルログインがWebex Control Hubの管理者アカウントと一致していることを確認します。

1. ディレクトリコネクタに使用される電子メールアカウントに、ADユーザーオブジェクトの読み取りアクセス許可があることを確認します。
2. アカウントに、ドメインコントローラに接続してActive Directoryユーザーオブジェクトを読み取る特権があることを確認してください。
3. 必要に応じて、導入ガイドに従って管理者アカウントをActive Directoryの代替電子メールとして追加します。

ステップ3：冗長インスタンスの削除

不要なディレクトリコネクタインスタンスを削除します。

1. Directory Connectorインターフェイスに移動します。
2. 不要なインスタンスの3つのドットメニューをクリックします。
3. Deactivate instanceを選択します。

ステップ4：スケジュール調整の同期

環境の必要に応じて、差分同期のタイミングをデフォルトの24時間インターバルから適切な短いインターバルに調整します。

ステップ5：設定のレビュー

ディレクトリコネクタの設定と同期スケジュールの設定を確認し、正しく動作することを確認します。

原因

主な根本原因は、ローカルサーバログインアカウントとDirectory Connector/Webex管理者アカウントの不一致でした。ディレクトリコネクタは、目的のWebex Control Hub管理者アカウントではなく、Windowsサーバーログインアカウントを使用して認証を試みました。このマッピングの失敗は、Active Directoryでのアカウント分離が原因で発生しました。この場合、Directory Connectorは、異なる管理者アカウントでサーバにログインしたときに、Webex管理者アカウントを正しくマッピングできませんでした。サーバーログインアカウントとWebex Control Hub管理者アカウントの間でローカルユーザーマッピングを確立できなかったため、SAML2認証プロセスが失敗しました。

関連コンテンツ

- Webex Directory Connector導入ガイド
- 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。