セキュアアクセスADコネクタのレガシー認証からAPI認証への移行

内容

問題

Cisco Secure Access with Active Directory(AD)コネクタを使用している組織は、Active Directoryと仮想アプライアンスに対してAPI認証が推奨されていることを示す通知を受信します。レガシー認証の有効期限は2026年5月29日に設定されています。ユーザは、有効期限の前にレガシー認証からAPI認証に移行するために設定の支援を必要とし、移行プロセス中のADと仮想アプライアンスの同期に対する潜在的な影響を理解する必要があります。主な懸念事項は、営業時間内にこの変更を実装すると、IDおよびポリシーに依存する操作に影響を与える可能性があるADおよびVAの同期操作で障害が発生するかどうかです。

環境

- Cisco Secure Access（旧称Cisco Umbrella）
- Active Directoryコネクタが展開されました
- 現在使用されている従来の認証方法
- 2026年5月29日までにAPI認証の移行が必要
- ADのみの環境（場合によっては仮想アプライアンスなし）

解決方法

レガシー認証からAPI認証への移行には、セキュアアクセスポータルでのAPIキーの生成と適切な設定が含まれます。このプロセスでは、ADコネクタと仮想アプライアンス用に管理APIキーとクライアントAPIキーの両方を作成する必要があります。

手順1：管理APIキーの生成

セキュアアクセスポータルでAdmin > API Keysに移動し、新しいAdmin API KeyとAdmin Key Secretを生成します。クライアントAPIキーペアの生成に必要に応じて、これらのクレデンシャルを安全に保存します。

ステップ2：クライアントAPIキーペアの生成

Users and Groups > Configuration Management > Advanced Settingsの順に移動し、API Authenticationセクションを見つけます。ステップ1で生成したAdmin API KeyとAdmin Key Secretを入力し、Generate Client API Key Pairをクリックします。これにより、ADコネクタと仮想アプライアンスで使用されるクライアントAPIキーとクライアントシークレットが生成されます。

ステップ3：詳細設定でAPI認証を設定する

生成したクライアントAPIキーとクライアントシークレットをセキュアアクセスポータルのAPI認証の詳細設定セクションにコピーします。すべてのADコネクタと仮想アプライアンスの設定に必要であるため、これらのクレデンシャルを安全に保存します。

手順4:ADコネクタと仮想アプライアンスを更新します。

新しく生成されたクライアントAPIキーとクライアントシークレットを、導入されたすべてのADコネクタと仮想アプライアンスに適用します。これにより、新しいAPI認証方式を使用して、登録とヘルスチェックのために適切に認証できるようになります。

移行の影響とベストプラクティス

Secure AccessポータルでのAPIキーの生成は、通常、中断しません。ただし、新しいクライアントAPIキーとシークレットを使用するようにADコネクタと仮想アプライアンスが更新されるカットオーバー時に、運用への影響が発生します。

カットオーバー時に予想される影響：

- レガシー認証を使用しているコンポーネントでは、一時的な同期とヘルスチェックの失敗が発生する可能性があります。
- 移行ウィンドウ中のAD/VA同期の遅延または障害。
- 同期が失敗した場合、最新のIDおよびグループデータに依存するポリシー決定が影響を受ける可能性があります。

推奨される実装アプローチ：

- 可能な場合は、就業時間外またはメンテナンス時間帯に移行を実行します。
- 稼働時間の実装には、制御されたローリングアップデート方式を使用します。
- 1つのコネクタ/VAを一度に更新し、正常な状態であることを確認してから続行します。
- すべてのノードを同時に更新しないでください。
- ローリングアップデート用の複数のコネクタ/VAを使用して、十分な冗長性を確保します。

互換性と要件：

- API認証はADのみの導入で機能し、仮想アプライアンスを必要としません。
- 移行期間中は、レガシー認証方式とAPI認証方式の両方がアクティブなままになります。
- ADコネクタは、api.opendns.com経由でUmbrellaと同期し、api.umbrella.comに移行できる必要があります。

原因

Cisco Secure Accessは、標準の認証メカニズムとして、従来の認証方式からAPI認証に移行しています。レガシー認証方式では、2026年5月29日に廃止が予定されています。API認証は最終的に唯一のサポートされる認証方式となり、従来の認証方式の期限が切れる前に移行して、サービスの中断や、リカバリのために完全な再インストールが必要になる可能性のあるAD/VA同期の障害を回避する必要があります。

関連コンテンツ

- Cisco Secure Access API認証に関するドキュメント
- Cisco Secure Accessの高度な設定
- Cisco Secure Accessの設定管理
- 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。