

diff IDPを使用したCisco Secure Accessでのユーザ/グループID同期のトラブルシューティング

内容

問題

このドキュメントでは、Okta、Microsoft Entra ID、IBM Cloudなどの異なるアイデンティティプロバイダー(IdP)を使用したCisco Secure Access(ACS)でのユーザおよびグループIDの同期をトラブルシューティングする方法について説明します。

環境

- Cisco Secure Access — SCIMプロビジョニングの統合
- SCIM 2.0 IdPコネクタ(Okta、Azure AD)に適用

解決方法

概要

Cisco Secure Accessは、SCIM 2.0標準を使用して、OktaおよびMicrosoft Entra ID（以前のAzure AD）からユーザーとグループのIDを直接プロビジョニングすることをサポートします。これにより、クラウドのみのIDソースに対してオンプレミスのActive Directory(AD)コネクタを展開する必要がなくなります。この記事では、アーキテクチャの前提条件、一般的な障害モード、およびフィールドエンジニアと管理者が統合を導入または維持する際に最も頻繁に遭遇するトラブルシューティングガイダンスをまとめています。

このドキュメントは、次の4つのセクションで構成されています。

- 設定：正式なセットアップ手順の参照先
- アーキテクチャ上の前提条件に違反すると、サイレント障害や診断が困難な障害が発生する
- プロバイダー固有の問題 (OktaとEntra ID)
- IdPに関係なく適用される汎用SCIMプロトコルの問題

コンフィギュレーション

この記事では、初期設定ではなく、トラブルシューティングに重点を置いています。設定手順については、このドキュメントの公式のCisco TechNotesを使用してください。

- Microsoft Entra ID(Azure AD)を使用してCisco Secure Accessを設定するには、「Entra IDを使用してアクセスを保護するためのユーザーとグループのプロビジョニング」リンクを参照してください
- Cisco Secure Access with Oktaを設定するには、次のリンクを参照してください。OKTA経由でアクセスを保護するためのユーザとグループのプロビジョニング

どちらのドキュメントでも、セキュアアクセスでのSCIMトークンとプロビジョニングURLの生成、IdPでの対応するアプリケーションの設定、および初期プロビジョニング同期の実行について説明しています。

アーキテクチャ入門

トラブルシューティングを行う前に、導入がこれらの主要な前提条件に一致していることを確認します。同期エラーの大部分は、これらの前提条件のいずれかに遡ります。

1つのアイデンティティ・ソースを一度に1つずつ

オンプレミスADコネクタとクラウドIdP (OktaまたはEntra ID) からの同じユーザまたはグループの同時プロビジョニング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。ADコネクタからクラウドIdPに移行する場合：

- オンプレミスのAD Connectorサービスを停止します。

- クラウドIdPプロビジョニングを有効にする前に、残りの同期ジョブが実行されていないことを確認します。

仮想アプライアンスは例外

Entra IDまたはOktaは、仮想アプライアンス(VA)のアイデンティティ統合を提供できません。VAが必要とするプライベートIPとユーザのマッピングに対する可視性がIdPにはないためです。VAの導入では、他のコンポーネントで使用されるものに関係なく、オンプレミスのADコネクタが引き続き必要です。

割り当てとプッシュ

- アクション：アプリケーションへのユーザーまたはグループの割り当て
 - 実際の動作：そのグループのメンバーユーザにセキュアアクセスをプロビジョニングします。
- アクション：グループをプッシュしています(Okta)
 - 実際の機能：グループポリシーオブジェクト自体をプロビジョニングします (ポリシーターゲティング用)。 ユーザは同期されません。



注：ユーザプロビジョニング用にアプリケーションにも割り当てられているグループをプッシュしないでください。これにより、グループの状態が重複または競合する可能性があります。

グループとユーザの制限

どちらのIdPからもプロビジョニングされるユーザ数にハード制限はありません。

グループには上限があります。これまで、OktaまたはEntra IDのいずれかから組織ごとに200のグループがありました。現在のドキュメントの中には、Oktaの上限 (最大1,000) が特に高いものがあります。正確な数は環境に応じて判別し、Cisco Technical Assistance Center(TAC)または最新のシスコドキュメントで確認してください。上限を超えるグループはサイレントプロビジョニングされず、エラーは表示されません。

より広い範囲が必要な場合は、各グループを個別にプッシュするのではなく、動的な「すべてのユーザー」(Entra ID)または「すべてのユーザー」(Okta)グループを使用します。

SCIMトークンのライフサイクル

Cisco Secure Accessでは、Connect > Users, Groups and Endpoint Devices > Configuration Management > Integrate Directoryの順に選択すると、トークンが生成されます。トークンは作成時に1回だけ表示されます。

トークンを再生成すると、Microsoft Entra IDまたはOktaのプロビジョニング設定に新しいトークンが入力されるまで、IdP側でのプロビジョニングがただちに中断されます。猶予期間はなく、IdP側のエラーはトークン期限切れメッセージではなく一般的なメッセージ（認証失敗）であることが多くあります。

トークンを定期的に更新してセキュリティの状態を確認し、ローテーション直後にIdP側で接続をテストします。

Okta固有の問題

- 症状:セキュアアクセスにグループが表示されない
 - 根本原因：グループをプッシュすると、グループオブジェクトのみがプロビジョニングされ、メンバーは同期されません。
 - 解決策：関連するグループ・メンバーが「割当」の下のアプリケーションに個別に割り当てられていることを確認します。
- 症状：ユーザがプロビジョニングされているが、属性が欠落している、または間違っている
 - 根本的な原因：セキュアアクセスはサーフェスの名前とユーザ名のみを表示し、指定された名前とファミリー名は表示されません。
 - 解決策：必要な属性が同期のために明示的に選択されていることを確認します。すべてのOktaプロファイルフィールドが伝播するとは限りません。
- 症状：プロビジョニングは何も実行しません
 - 根本原因：ユーザの作成、ユーザ属性の更新、またはユーザの非アクティブ化の切り替えが有効になっていません。

- 解決策:Okta管理者コンソールのProvisioning > To Appで、3つの項目がすべてチェックされていることを確認します。
- 症状: objectGUIDまたはカスタム属性が同期していません
 - 根本原因：属性がユーザプロフィールマッピングを介して追加およびマッピングされていません。
 - 解決策：この識別子が必要な場合は、objectGUID属性を追加し、対応するプロフィールマッピングを作成します。
- 症状：トークンの回転後に同期が停止する
 - 根本原因：セキュアアクセスで再生成されたがOktaで更新されていないSCIM または APIトークン。
 - 解決策:Provisioning > Configure API Integrationで新しいトークンを入力し、Test API Credentialsを再度実行します。
- 症状:特定のユーザまたはグループで障害が発生した原因を特定できない
 - 根本的な原因：最初にログのチェックが行われませんでした。
 - 解決策：エスカレーションする前に、Oktaで、Cisco User Management Connectorアプリケーションに対してフィルタリングされたReports > System Logにチェックマークを付けます。
- 症状：グループ数が上限を超えています。一部のエントリがエラーなしで見つかりません
 - 根本原因:組織に、セキュアアクセスがサポートしている数よりも多くのスコーピングされたグループがあります。
 - 解決策：範囲をポリシー関連グループのみに限定するか、Cisco TACに上位レベルのグループサポートを依頼します。

Microsoft Entra ID固有の問題

- 症状：ダイナミックグループメンバーシップがセキュアアクセスに反映されない
 - 根本的な原因：動的なグループルールが正しく構成されていないか、グループがプロビジョニングされたスコープにありません。
 - 解決策：セキュアアクセス同期のバグを想定する前に、エントリIDで動的メンバーシップ規則を直接検証します。
- 症状:SAML SSOによるSWG IDの要求

- 根本原因: AnyConnect Secure Web Gateway(SWG)は、Entra IDに対するSecurity Assertion Markup Language(SAML)認証をサポートしていません。オンプレミスADと同じパッシブ認証メカニズムを使用しています。
- 解決策:Entra IDのSAML駆動型SWG IDを中心に設計しないでください。文書化されているように、パッシブ認証を使用してください。
- 症状：ユーザにdeactivatedと誤って表示される
 - 根本的な原因：エントリIDがアクティブに送信されました: false。ユーザが割り当てられたグループスコープから外れたか、アクティブな属性マッピングが正しく設定されていないことが原因です。
 - 解決策：スコーピンググループからユーザが削除されたかどうかを確認し、アクティブなマッピングを確認します(通常はNot([isSoftDeleted])として評価する必要があります)。
- 症状:アプリケーションが隔離され、すべてのプロビジョニングが停止しました
 - 根本的な原因：対象のアプリケーションが、SCIMに準拠していない応答を繰り返しました。
 - 解決策：個々のユーザの障害を想定する前に、隔離フラグに関するエンタープライズアプリケーションプロビジョニングのステータスを確認します。
- 症状：初期プロビジョニングサイクルが完全に失敗する
 - 根本的な原因：最初の実行時に一時的な同期エラーが発生しました。
 - 解決策:「概要」ページで「プロビジョニングの再起動」をクリックして、Enter IDに初期同期を再試行させます。
- 症状：重複したユーザが予期せずマージされる
 - 根本原因:2つの送信元IDが同じ電子メールまたはユーザプリンシパル名(UPN)を共有しています。
 - 解決策：ソースディレクトリで電子メールとUPNの一意性を確認し、メール属性が検証済みドメインからのものであることを確認します。
- 症状：スキーマの変更に属性の更新が停止する
 - 根本的な原因：ターゲット側で属性の型が変更されましたが(たとえば、文字列がブール値に変更されました)、エントリIDマッピングは更新されませんでした。
 - 解決策:属性マッピングの下の詳細設定でタイプを手動で修正します。
- 症状：マネージャのリファレンスが入力されない
 - 根本原因：マネージャがアクティブになる前にユーザがスコープに入っていました。プロビジョニングは自動的にバックフィルしません。

- 解決策：範囲内のすべてのユーザを完全に再評価するために、プロビジョニングを再起動します。

IBMセキュリティ特定の問題の確認

- 症状：ユーザがプロビジョニングしても、グループがセキュアアクセスに表示されない
 - 根本原因：カスタムSCIMコネクタがユーザ操作のみを発行していることを確認します。POST /Groups呼び出しは送信されません (マッピングエラーではなく、アカウントプロビジョニング機能のギャップ)。
 - 解決策：コネクタトレースをキャプチャして、/Groupsコールが発生するかどうかを確認します。発生しない場合は、Cisco ADコネクタ、CSVインポート、またはスケジュールされたスクリプトを使用して、Secure Access SCIMエンドポイントに対してグループをプロビジョニングします。
- 症状：グループメンバーシップの更新が400または404で失敗する
 - 根本原因: members[].value参照ユーザの作成時に返されたSCIM ID Secure Accessの代わりに、内部ユーザIDを確認します。
 - 解決策:Secure Access SCIM IDを使用するようにメンバーのマッピングを修正し、完全同期を再度実行します。
- 症状：グループは表示されるが空である
 - 根本原因：メンバーユーザがSecure Accessに存在する前にグループがプッシュされました。メンバーシップ PATCHが不明なユーザを参照しました。
 - 解決策：ユーザが存在するため、完全同期を再度実行します。同期順序によってグループの前にユーザが作成されることを確認してください。
- 症状:SAMLログインループまたはリダイレクトの繰り返し
 - 根本的な原因:SWGによってIdPエンドポイントがプロキシまたは復号され、認証フローが中断されることを確認します。
 - 解決策:SAMLまたは復号化 (外部ドメインリストまたは選択的な復号化) からVerify IdP URLをバイパスします。
- 症状：ユーザはSAML経由で認証されますが、ユーザベースのポリシーの一致はありません
 - 根本原因: SAML NameIDがプロビジョニングされたユーザauthName(auth-name)と一致しません。
 - 解決策:Verify SAMLアプリケーションのNameID >形式をauthName属性マッピング

(通常は電子メールまたはUPN) に合わせます。もう一度テストしてください。

- 症状：安定性が数週間から数ヵ月続くと、プロビジョニングが機能しなくなる
 - 根本的な原因：セキュアアクセスでSCIMトークンが循環または期限切れになってしましたが、検証コネクタで更新されていません。
 - 解決策:セキュアアクセスでトークンを更新し、カスタムアプリケーションの確認でトークンを更新します。更新シーケンスのカレンダーを設定します。
- 症状:再同期時に重複ユーザが作成される
 - 根本原因：変更可能または一意でない属性にマッピングされたexternalId (例：表示名、変更可能な電子メール) 。
 - 解決策:externalIdを不変のIDにマッピングします (ユーザIDまたはobjectGUIDを確認します) 。重複をクリーンアップして再度同期します。
- 症状：非アクティブ化ユーザがセキュアアクセスでアクティブなままであることを確認します
 - 根本原因：中断アクションがactive:falseにマップされていないか、コネクタで無効になっている操作を非アクティブ化しています。
 - 解決策：非アクティブ化操作を有効にし、中断をactive:falseにマップします。テストユーザに確認してください。
- 症状：検証での属性の変更が伝播しない
 - 根本原因：プロビジョニングポリシースコープのユーザーまたは属性、または更新操作が無効になっています。
 - 解決策：アプリケーションプロビジョニングポリシーまたは権限を確認し、更新を有効にし、手動同期をトリガーします。
- 症状:Secure Accessがスキーマまたは 501スタイルエラーで要求を拒否する
 - 根本的な原因: SCIMに準拠していないペイロード (スキーマ配列が見つからない、URNが正しくない、サポートされていない操作) 。
 - 解決策：ベースラインcurlテストで再現し、ペイロードまたはマッピングを修正し、コネクタが不正な要求を発行する場合はIBMにエスカレーションします。
- 症状:SAMLが機能しているにもかかわらず、ローミングユーザにSWG IDが欠落している
 - 根本的な原因：パッシブまたはエージェントベースのIDを使用する展開モードでは、SAMLがIDをドライブする必要があります。
 - 解決策:Secure Accessのドキュメントに照らして各導入モードのID取得方法を確認します。SAMLを唯一のアイデンティティソースとして設計しないでください。

一般的なSCIMの問題

これらはシスコ固有のものではありませんが、基盤となるトランスポートが標準SCIM 2.0であるため、Secure Accessの導入では一貫して表示されます。

- 隔離状態が個々のエラーをマスクする：同期がユーザ単位で失敗するのではなく完全に停止したように見える場合は、個々の属性の問題を調査する前に、アプリケーションレベルの隔離状態または停止状態を確認します。
- 409 Conflict on deactivation:IdPがユーザを非アクティブ化しようとし、ターゲットが競合をスローする一般的なパターン。これは通常、アクティブな属性マッピングまたはグループスコープの問題であり、実際のシステムエラーではありません。
- 空白またはクリアされたフィールドが常に伝搬されとは限りません。SCIMサーバの実装によっては、最後のNULL以外の値が保持される場合があります。IdPでフィールドをクリアするときに、最初にプレースホルダ値をプッシュする必要がある場合があります。
- URLまたは設定の変更により、認証が自動的に無効になる：通常、SCIMエンドポイントURLを変更するには、ベアラトークンを再度入力する必要があります。実際の問題が古いトークンであっても、エラーが無効なURLとして表示されます。
- ネイティブのwebhookまたはイベントストリームがない：ユーザまたはポリシーの変更に対してリアルタイムのプッシュ通知を期待する自動化では、代わりにReporting APIをポーリングするか、Cisco XDRを介して統合する必要があります。セキュアアクセスでは、アウトバウンドプロビジョニングWebフックは生成されません。

上記の手順で問題が解決しない場合は、IdP側からプロビジョニングログを使用してCisco TACにエスカレーションします。セキュアアクセス側のバックエンドプロビジョニングログを取得するには、通常はTACアクセスが必要です。

原因

期限切れのベアラトークン、属性マッピングの不一致、ターゲットグループの不足、またはプロビジョニングスコープの不足が原因で、SCIMプロビジョニング統合が1つ以上のレコードをプッシュできませんでした。

関連コンテンツ

- シスコ : [ユーザおよびグループをプロビジョニングして、Entra ID経由でアクセスを保護する](#)
- シスコ : [OKTA経由でアクセスを保護するためのユーザとグループのプロビジョニング](#)
- Microsoft Learn:SCIM 2.0プロトコルコンプライアンスに関する既知の問題 – Microsoft Entra ID
- Microsoftラーニング : Microsoft Entra ID SCIM APIエラーのトラブルシューティング
- アイデンティティプロバイダーでSAML SSOを設定する
: <https://www.ibm.com/docs/en/security-verify?topic=sign-configuring-saml-single-in-identity-provider>
- カスタム(SCIM)アプリケーションのプロビジョニング
: <https://www.ibm.com/docs/en/security-verify?topic=endpoints-configuring-provisioning-custom-applications>
- プロビジョニングとガバナンスの概要 (汎用SCIMコネクタ) :<https://docs.verify.ibm.com/verify/docs/use-cases-provisioning-and-governance>
- オンプレミスプロビジョニングブリッジ (AD/LDAPソース) :<https://docs.verify.ibm.com/verify/docs/on-premises-provisioning>

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。