Umbrellaダッシュボードに表示されないActive Directoryユーザのトラブルシューティング

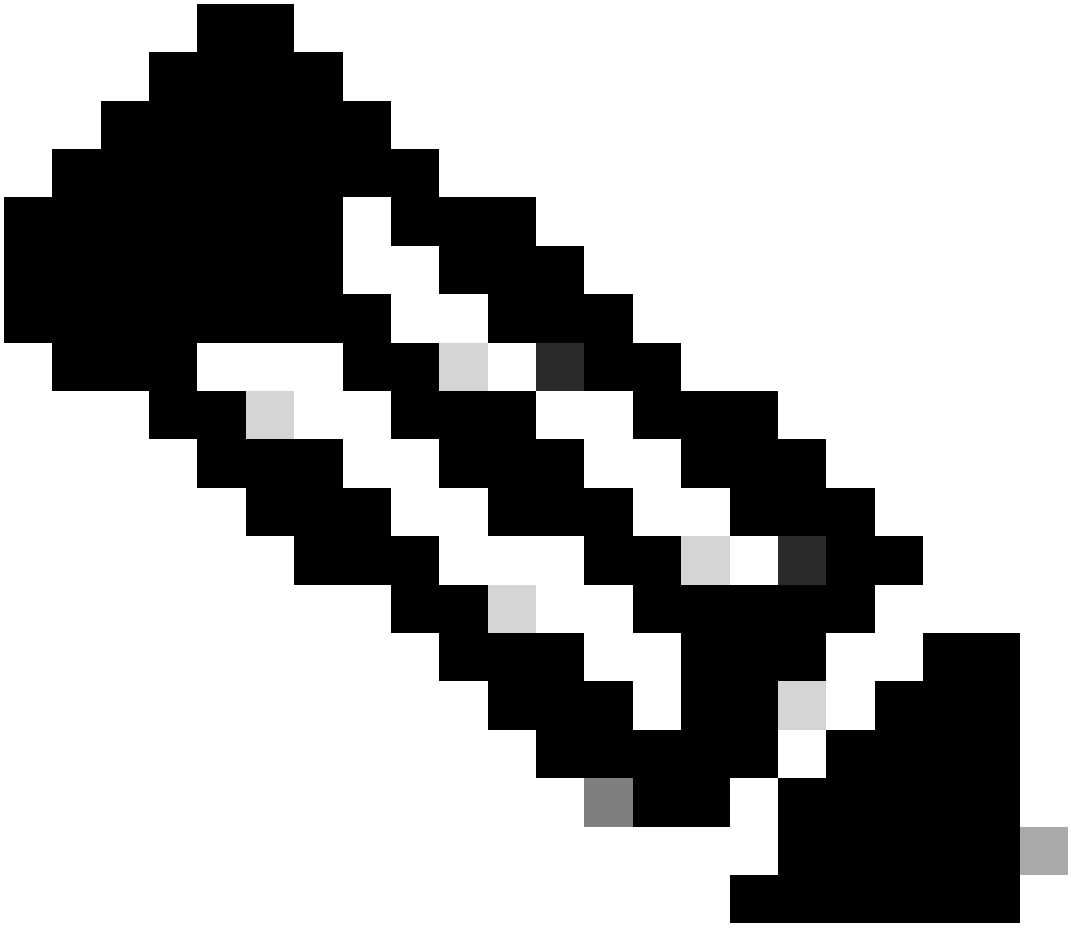
内容

はじめに

このドキュメントでは、Umbrellaダッシュボードに表示されないActive Directory(AD)ユーザ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。

概要

OpenDNSコネクタはActive Directoryに対して同期を実行し、ADユーザ、グループ、およびコンピュータのリストを返します。このリストはUmbrellaダッシュボードに安全に掲載され、ポリシーやレポートに使用できます。

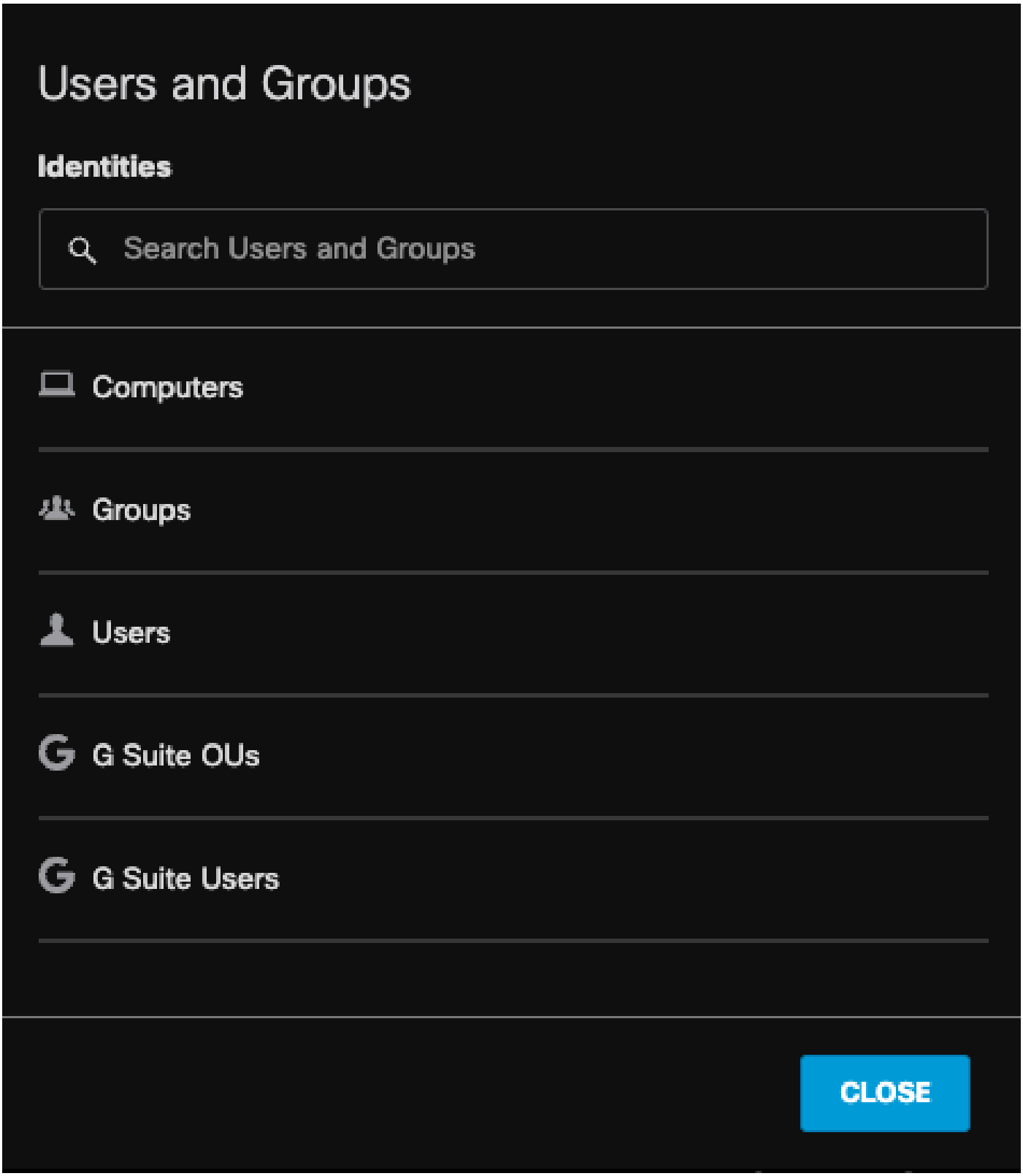


注：コネクタソフトウェアのバージョン1.1.24以降を使用している場合は、Umbrellaに同期するADグループを指定できます。

ダッシュボードに同期されたオブジェクトは、Deployments > Core Identities > Users and Groupsの順に移動して確認できます。

シナリオ1：ダッシュボードに表示されないすべてのユーザとグループ

Identitiesタブにすべてのユーザが表示されない場合は、AD同期が実行されていないことを示します。



26022106541844

考えられる原因には次のものがあります。

- Active Directory統合が構成されていないか、OpenDNSコネクタがインストールされていません。詳細については、『Active Directory Identity Integrations』のドキュメントを参照してください。
- OpenDNSコネクタは、必要なポートでドメインコントローラに接続できません。

- OpenDNS_Connectorユーザがldap経由でディレクトリを読み取れない権限エラーがあります。
- OpenDNS_Connectorユーザーアカウント（同期に使用される）に問題があります。 コネクタのインストール中に入力したパスワードが正しくないか、アカウントがロックされている可能性があります。
- OpenDNSコネクタサービスはインストールされていますが、機能していません。最も一般的な原因は、特にコネクタがドメインコントローラ以外のマシンにインストールされている場合、（LDAP経由のAD同期の実行に使用される）ldifde.exeがインストールされていないことです（通常はAD LDSロールに含まれています）。非DCインストールの前提条件を確認してください。
- C:\CiscoUmbrellaADGroups.datファイルは存在しますが、空であるか、ファイルの形式が正しくありません。

詳細については、コネクタログを使用してCisco Umbrellaサポートに問い合わせてください。

シナリオ2：新しく作成されたユーザ/グループがダッシュボードに表示されない

コネクタはActive Directoryと頻繁に同期して、LDAPを使用しているディレクトリに変更があったかどうかを確認します。最新の変更があった場合は、完全なLDAP同期が実行されます。新しいユーザ/グループがダッシュボードで有効になるまでに数時間かかることがあります。

新しいユーザが表示されない場合は、次の原因が考えられます。

- OpenDNS_Connectorアカウントには、ADの変更を監視するために必要な「ディレクトリ変更のレプリケート」権限がありません。正しいアクセス許可を割り当てるには、OpenDNS_Connectorが'Enterprise Read-Only Domain Controllers'グループのメンバーであることを確認してください。
- コネクタは以前に同期できましたが、現在は同期できません。この問題を解決するには、この記事の手順を参照してください。

シナリオ3：特定のADオブジェクトがダッシュボードにない

Umbrellaポリシーで使用する独自のADグループを作成することをお勧めします。
Domain Adminsおよびその他の複数の「デフォルト」グループは同期から除外されます。バックグラウンドソフトウェア（Exchange、SQL、WSUSなど）に関連する多くの既知のグループも、AD同期から除外されます。

C:\CiscoUmbrellaADGroups.datファイルが存在する場合は、欠落しているADオブジェクトを含むADグループが指定されていることを確認します。

シナリオ4:AD同期は機能しているが、一部のADオブジェクトが同期されていない

OpenDNS_Connectorユーザに、欠落しているオブジェクトからの情報を「読み取り」する権限

があることを確認します。Active Directoryでは、すべてのオブジェクト（ユーザ、グループ、コンピュータを含む）に独自のACLアクセス許可があり、属性を読み取ることができるユーザを決定します。詳細については、「アクセス許可のトラブルシューティング」を参照してください。

C:\CiscoUmbrellaADGroups.datファイルが存在する場合は、非同期のADオブジェクトを含むADグループが指定されていることを確認します。

シナリオ5 – 特定の組み込みADグループとロールがCisco Umbrellaポリシーウィザードに表示されない

Umbrella Active Directory統合コンポーネント、特にADコネクタを展開した後、特定の組み込みADグループがUmbrellaポリシーウィザードで見つからないことがわかりました。

ただし、組み込みではないADグループ、ADユーザ、およびADコンピュータは、想定どおりにUmbrellaポリシーウィザードに引き続き表示されます。ADコネクタは、組み込みのADグループをUmbrella APIにインポートしません。そのため、これらのグループに対してポリシーを定義できないことが予想されます。詳細については、Knowledge Baseで次の文書を参照してください。特定の組み込みActive DirectoryグループがUmbrellaポリシーウィザードに表示されないのはなぜですか。

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。