AD統合でユーザトラフィックが検出されない場合のUmbrella Insightsのトラブルシューティング

内容

はじめに

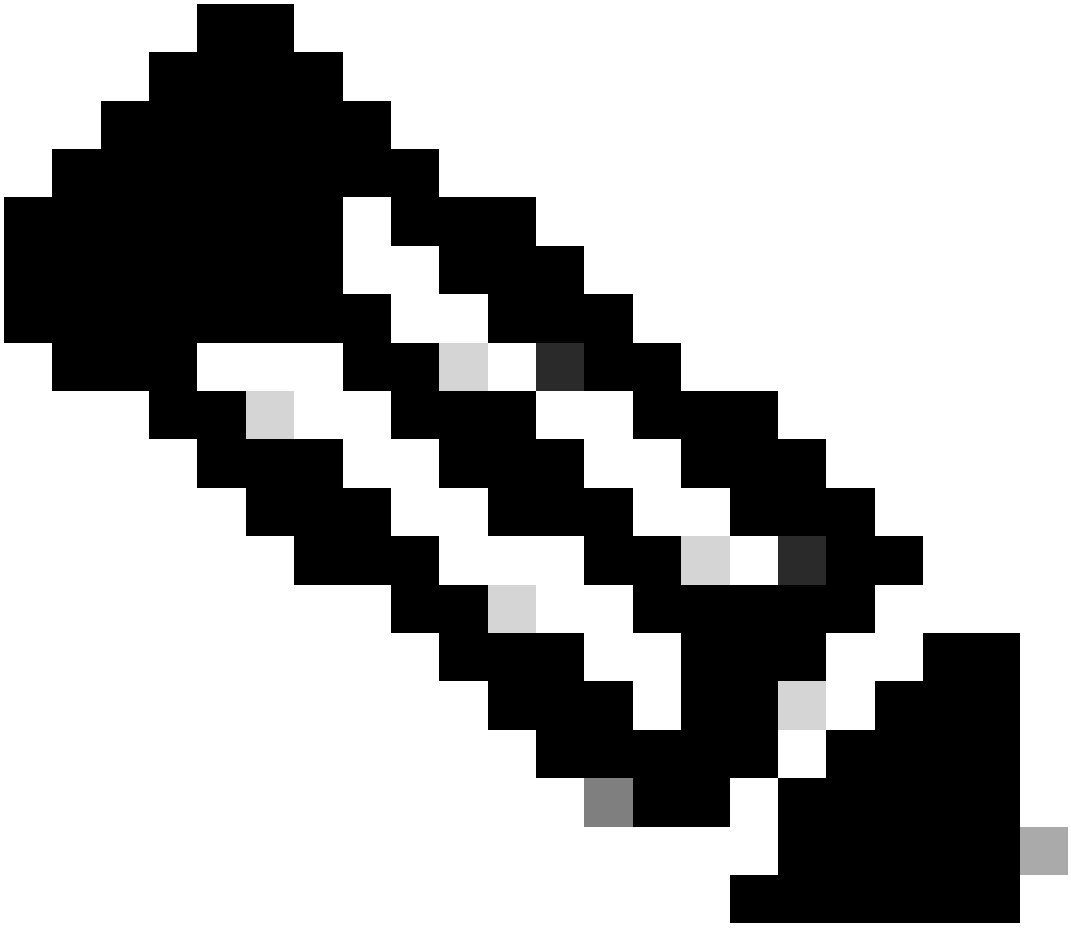
このドキュメントでは、Umbrella Insights AD統合でユーザトラフィックが検出されない場合のトラブルシューティング方法について説明します。

概要

Umbrella Insightsをインストールし、コネクタと仮想アプライアンスをセットアップし、ドメインコントローラを登録しました。 すべてのコンポーネントが緑色で表示され、ダッシュボードの `deployments -> Sites and Active Directory`の下で動作していますが、ADユーザまたはグループオブジェクトを使用するように設定されたポリシーがあっても、ダッシュボードで報告されたユーザアクティビティまたはポリシーが正しく適用されていることがわかります。

また、このエントリはOpenDNSAuditClient.logファイルでも繰り返される場合があります

'最後のイベントは1970-01-01 00:00:00に受信されました'



注：ログファイルは、C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>\にあります
VERSION = v1.1.22など、コネクタサービスに実際にインストールされたバージョン

説明

これが発生する主な理由は、監査ログオンイベントがActive Directoryドメインで構成されていない可能性があるためです。ログメッセージは、コネクタがインストールされてから、1つのユーザイベントがコネクタで発生していないことを示します。 現在、これはダッシュボードでエラーを生成するものではありません。

解決方法

主に、ADグループポリシーの正しい監査ポリシー設定を確認します。

1. ドメインコントローラで、*Administrative Tools*内にあるGroup Policy Managementパネルを開

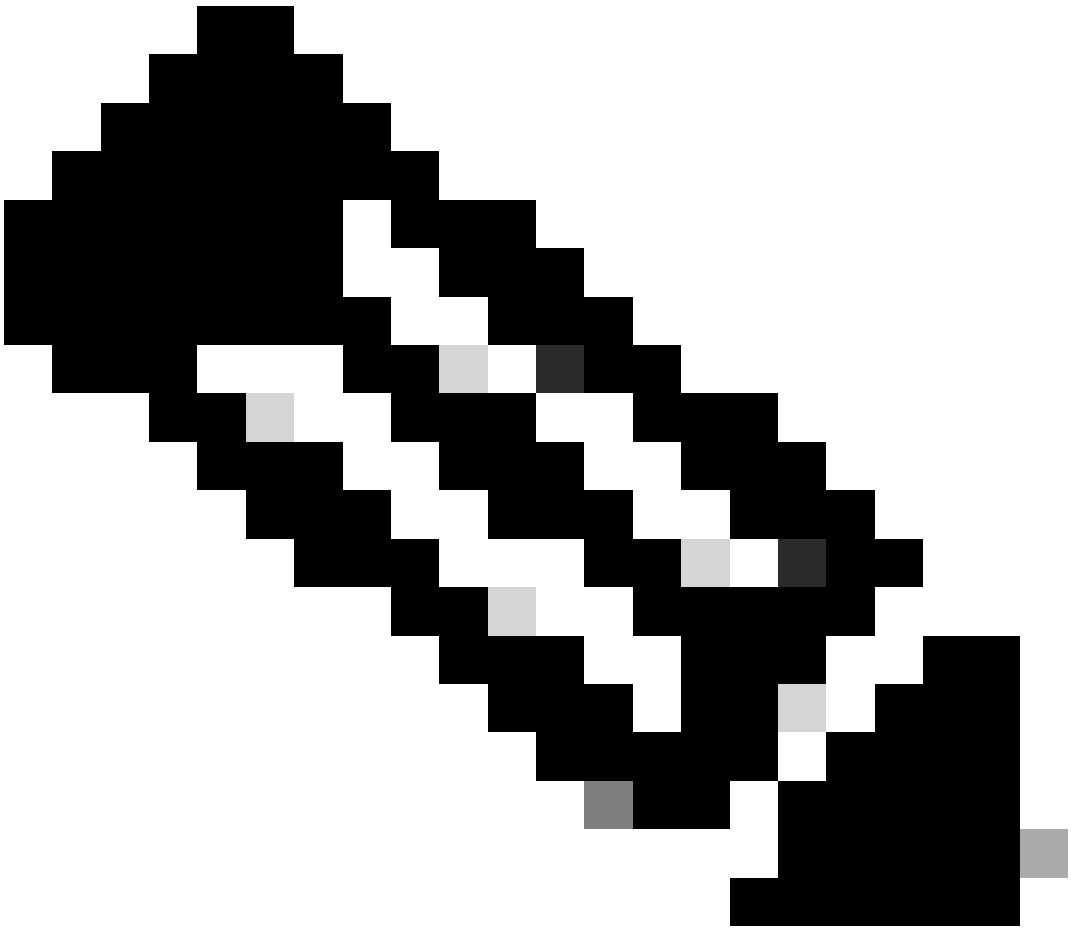
き、ドメインコントローラに適用するポリシー（デフォルトのドメインコントローラポリシーが候補になる可能性があります）を選択します。

2. そのポリシーを右クリックしてEditを選択し、Group Policy Management Editorを起動します。

3. "Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy"フォルダを参照し、Audit logon eventsを選択してプロパティを表示します。

4. このポリシーでは、Successの試行を監査する必要があります。

5. gpupdateコマンドを実行してポリシーを適用します。



注:[既定のドメインコントローラと既定のドメインポリシー]の両方で、その設定を構成する必要がある場合があります。

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。