Umbrella ADコネクタの"；アクセス拒否"；アラート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、Cisco Umbrella Active Directory(AD)コネクタがアラート状態またはエラー状態の場合の「アクセス拒否」のトラブルシューティングについて説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Umbrellaに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

問題

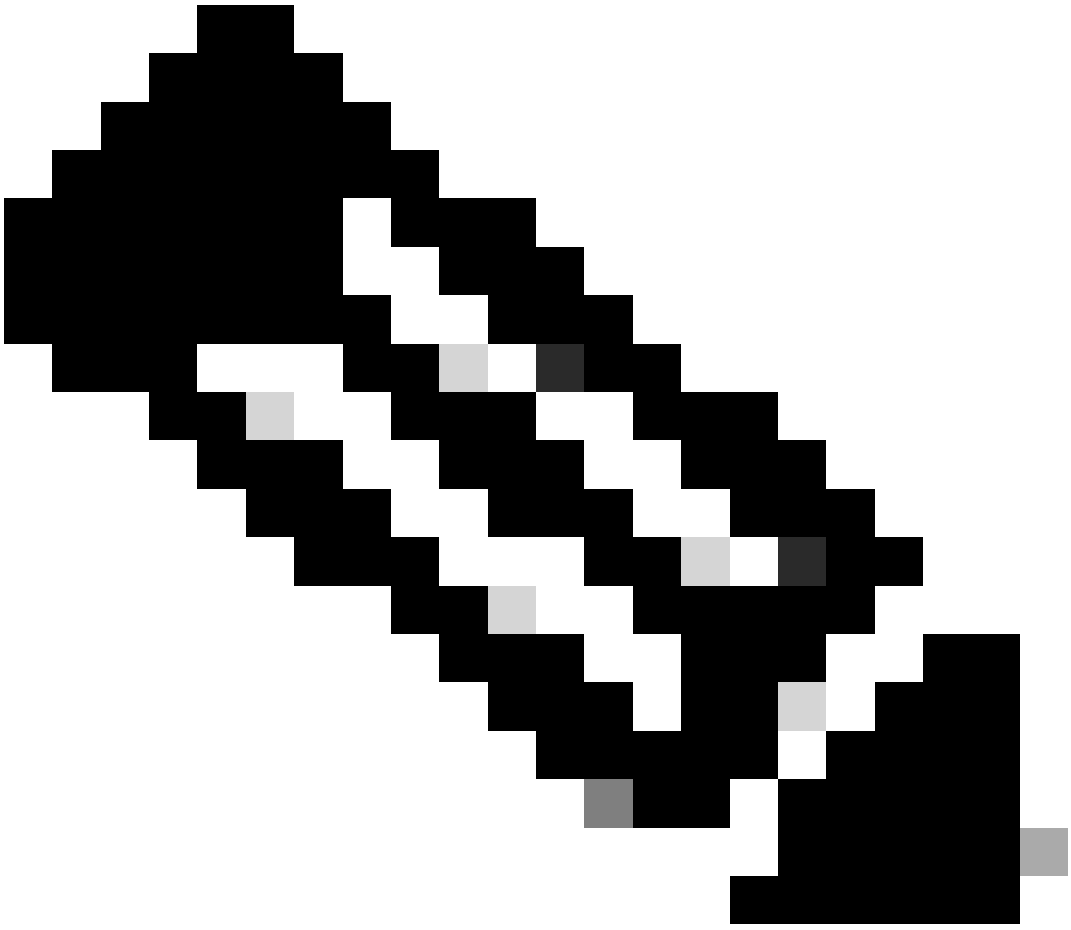
ADコネクタにアラートまたはエラー状態が表示され、アラートの上にカーソルを合わせると表示されるメッセージに、登録済みADサーバの1つに「アクセス拒否」が含まれることがわかります。

解決方法

OpenDNS_Connectorユーザが次のADグループのメンバーであることを確認してください。

- イベントログリーダー
- 分散COMユーザー
- エンタープライズ読み取り専用ドメインコントローラー

この問題の解決策は、DCOM、WMI、および監査とセキュリティログの管理が問題のADサーバで正しく設定されていることです。



注：複数のドメインまたは複数のフォレストは、デフォルトではサポートされていません。UmbrellaでのマルチADドメインサポートの発表を参照してください。また、これらの問題が発生した場合は、設定に関してUmbrellaサポートに連絡してサポートを受けることもできます。

WMI権限を確認するには、次の手順を実行します。

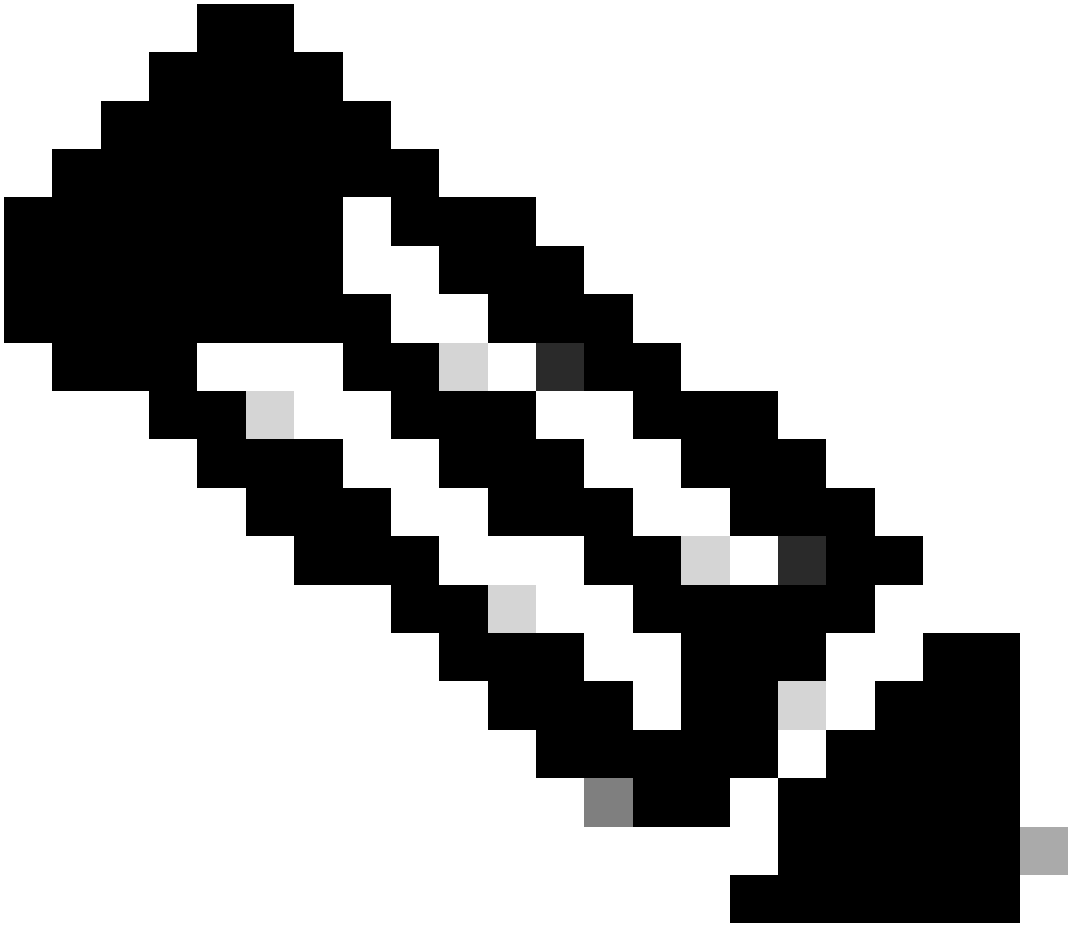
1. Start > Run > wmimgmt.mscの順に選択して、Windows Management Infrastructure Controlコン

ソールにアクセスします。
2. WMIコントロール>プロパティ>セキュリティタブを右クリックします。
3. Root > CIMV2 namespaceの順に選択し、Securityボタンを選択します。
4. OpenDNS_Connectorユーザを追加して、次の権限を許可します。

- アカウントの有効化
- リモートの有効化
- 読み取りセキュリティ

DCOM権限を確認するには、次の手順に従います。

1. コマンドラインから、dcomcnfgを実行します。
2. Console Root > Component Services > Computersの順に移動します。
3. My Computerを右クリックして、Propertiesを選択します。
4. [マイコンピュータのプロパティ]で、[COMセキュリティ]タブを選択します。
5. 「起動およびアクティブ化の権限」セクションで、「制限の編集」を選択します。
6. OpenDNS_Connectorユーザを追加し、リモート起動およびリモートアクティベーション権限を許可します。
7. OKを選択して確認し、マイコンピュータのプロパティを閉じます。



注：ほとんどの場合、DCOMの変更を有効にするには、そのDCのリブートが必要になります。

Windows 2003サーバで「監査およびセキュリティログの管理」を確認するには、次の手順を実行します。

1. ドメインコントローラでコマンドプロンプトを開き、次のコマンドを入力します（Windows 2003を実行している場合は、/rを/vに置き換えます）。

```
gpresult /scope computer /r
```

2. Applied Group Policy Objects行を探します。その下には、そのドメインコントローラに適用されるポリシーのリストがあります。すべてのドメインコントローラに適用できる項目を書き留めます。
（「Default Domain Controllers Policy」など）。 存在しない場合は、作成して適用する必要があ

ります。

適切なポリシーを編集するには：

3.（Start/Administrative Tools経由で）Group Policy Managementパネルを開きます。 目的のポリシーを選択します。「Domain Controllers」フォルダに何かが入っている可能性があります。

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

5. Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignmentフォルダを参照し、Manage audit and security logを選択してそのプロパティを表示します。

6. Define these policy settings >Add user or groupの順に選択します。OpenDNS_Connectorユーザを参照して選択します。

7. ドメインコントローラで「gpupdate /force」コマンドを実行して、ポリシーが適用されていることを確認します。

原因

このエラーは通常、OpenDNS_Connectorユーザが操作するのに十分な権限を持っていないことを示します。

通常、WindowsコネクタスクリプトはOpenDNS_Connectorユーザに必要な権限を設定します。 ただし、厳密なAD環境では、一部の管理者はドメインコントローラでVBスクリプトを実行することが許可されていないため、Windows構成スクリプトのアクションを手動でレプリケートする必要があります。

追加情報

この問題の解決方法の詳細については、「アクセス拒否の解決に関する完全なトピック」を参照してください。

上記の設定を確認または変更した後も、ダッシュボードに「アクセス拒否」メッセージが表示される場合は、この記事の「ADコネクタログでサポートを提供する」に記載されているように、コネクタログをサポートしてください。

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。