Active Directoryからユーザー、グループ、およびコンピューターを構成してOpenDNSコネクタサービスと同期させる

内容

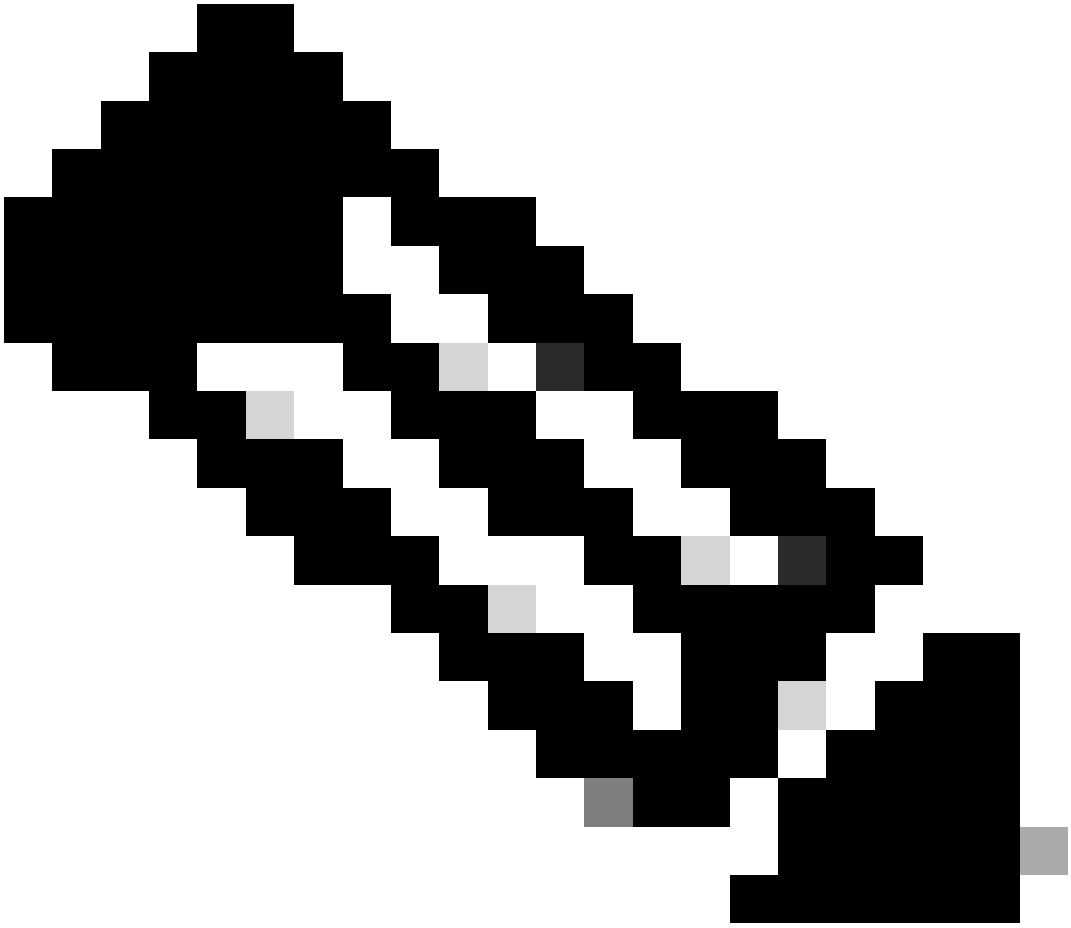
はじめに

このドキュメントでは、Active Directory(AD)からOpenDNSコネクタサービスを使用してユーザ、グループ、およびコンピュータを同期する方法について説明します。

概要

OpenDNS Connectorサービスは、操作の一環として、LDAPプロトコルを使用してActive Directoryからユーザ、グループ、およびコンピュータのリストを同期します。 この記事では、OpenDNS_Connectorアカウントにこれらのオブジェクトを読み取るための正しい権限があることを確認する方法について説明します。

Active Directory内の各オブジェクト（ユーザー、グループ、コンピューター）にはACLセキュリティのアクセス許可が関連付けられており、各オブジェクトはOpenDNS_Connectorユーザーアカウントがその属性を読み取ることを許可する必要があります。



注：この記事では、「OpenDNS_Connector」アカウントの通常の前提条件がすでに確認されていることを前提としています。ADユーザ/グループがダッシュボードにない場合は、まず次の記事を参照してください。
UmbrellaダッシュボードにADユーザ/グループが表示されない

既定のアクセス許可

デフォルトでは、認証されたすべてのユーザがユーザ、グループ、コンピュータのプロパティを読み取ることができるため、OpenDNS_ConnectorユーザはLDAP同期を実行するために追加の権限を必要としません。

通常、デフォルトの権限は次のように設定します。

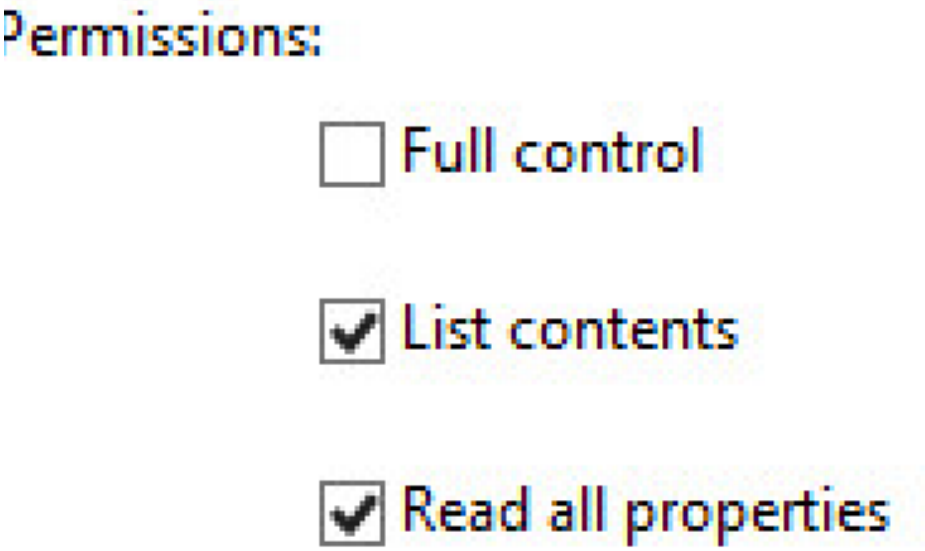
1) 'Pre-Windows 2000 Compatible Access'グループには、'Descendant User Objects'、'Descendant Group Objects'、および'Descendant Computer Objects'に対するドメインの読み取り（すべてのプロパティの読み取り）アクセス許可が割り当てられます。

これは、次のように再確認できます。

- Active Directoryユーザーとコンピューターを開く
- 「View」をクリックして「Advanced Features」オプションにチェックマークを付けます。
- Domainオブジェクトを右クリックし、Properties、Security > Advancedの順に選択します。
- 「Special」権限を持つ「Pre Windows 2000 Compatible Access」エントリを選択します。

115011616667

- これらの権限の詳細を表示するには、'Edit'をクリックします。
- 「Applies to」セクションで「Descendant User objects」を選択します。
- 次の権限を探します。

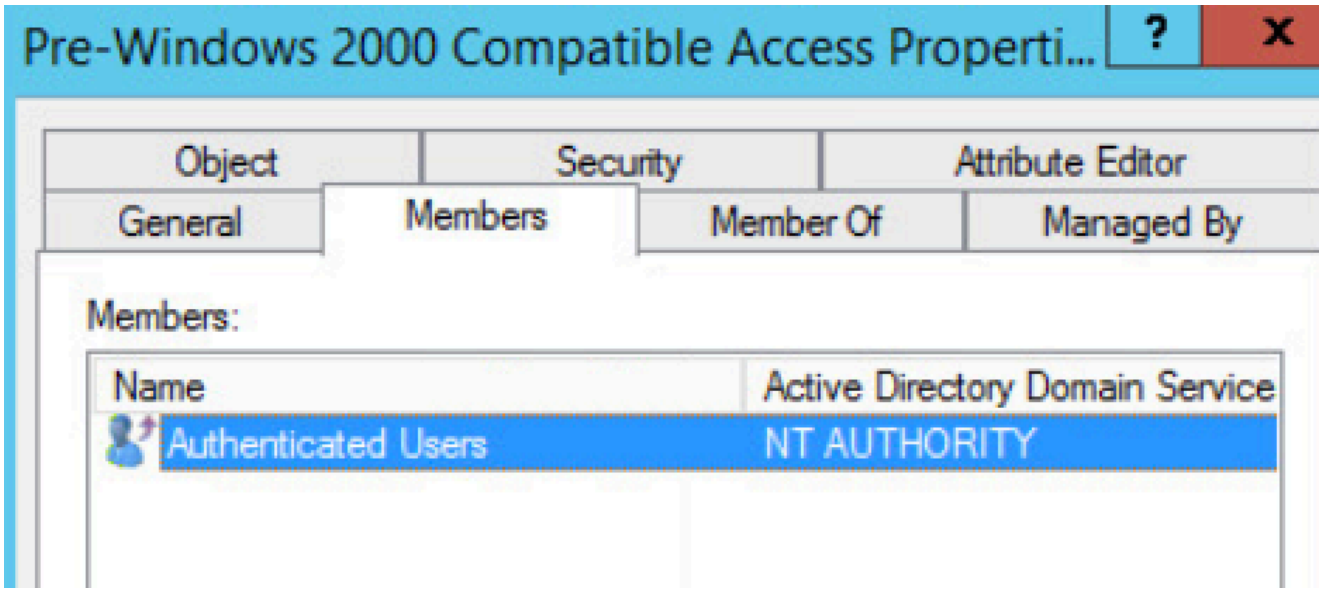


115011616687

- '子孫グループオブジェクト'および'子孫コンピュータオブジェクト'に対してこれらの手順を繰り返します。

2) All 'Authenticated Users'グループは、これらの設定をすべてのユーザーに提供する'Pre-Windows 2000 Compatible Access'グループのメンバーです。

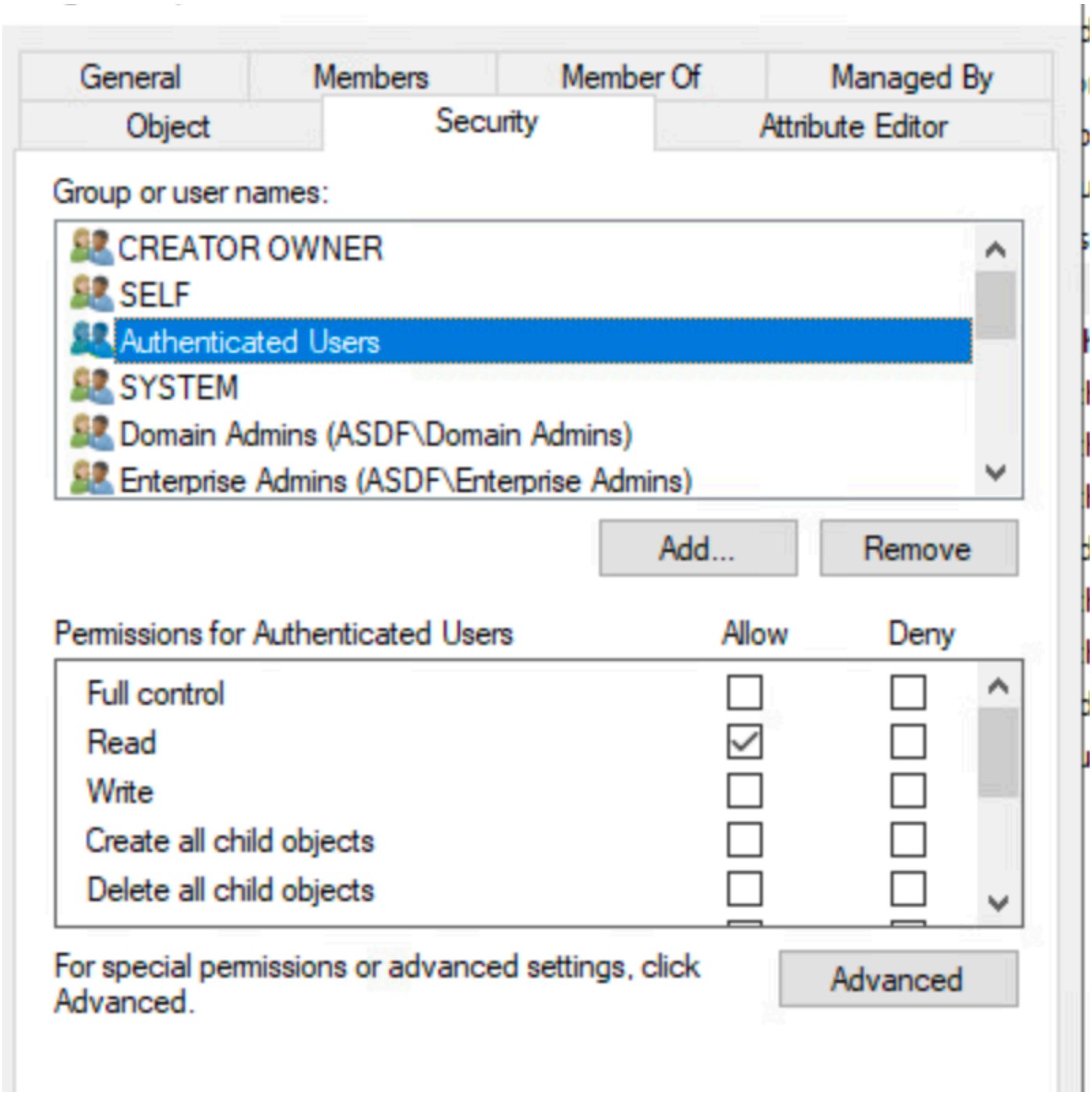
- 通常は組み込みADコンテナにあるPre-Windows 2000 Compatible Accessグループを右クリックします。
- 'Properties'を選択し、'Members'タブに移動します。
- 「認証されたユーザ」がリストされているかどうかを確認します。



115011616707

ただし、一部のAD環境では、この権限モデルが変更され、認証されたユーザが削除される可能性があります。これは、一部のユーザがUmbrellaダッシュボードに表示されないか、グループメンバーシップが正しくないことが判明する可能性があります。その場合は、OpenDNS_Connectorユーザをこのグループに追加し、コネクタサービスを再起動すると、不足している項目がUmbrellaに表示されます。

まれに、この方法では問題に対処できない場合があります。この場合は、Active Directoryのグループセキュリティタブを確認し、認証済みユーザがここに表示され、読み取りアクセス権がチェックされていることを確認します。このチェックボックスがオフになっている場合は、オフにしてコネクタサービスを再起動し、グループメンバーが表示されるかどうかを確認します。さらに、このセキュリティ設定がすべてのグループに存在しない場合、すべてのグループにグローバルに変更を一括して適用する必要があります。



28728163336852

有効なアクセスの表示

Windowsの「Effective Access」ツールを使用して、OpenDNS_Connectorユーザが、存在しない（または不正なグループメンバーシップを持つ）特定のオブジェクトを読み取ることができるかどうかを確認できます。

- Active Directoryユーザーとコンピューターを開く
- 「View」をクリックして「Advanced Features」オプションにチェックマークを付けます。
- ユーザー・オブジェクトを検索し、右クリックして[Properties]を選択します。

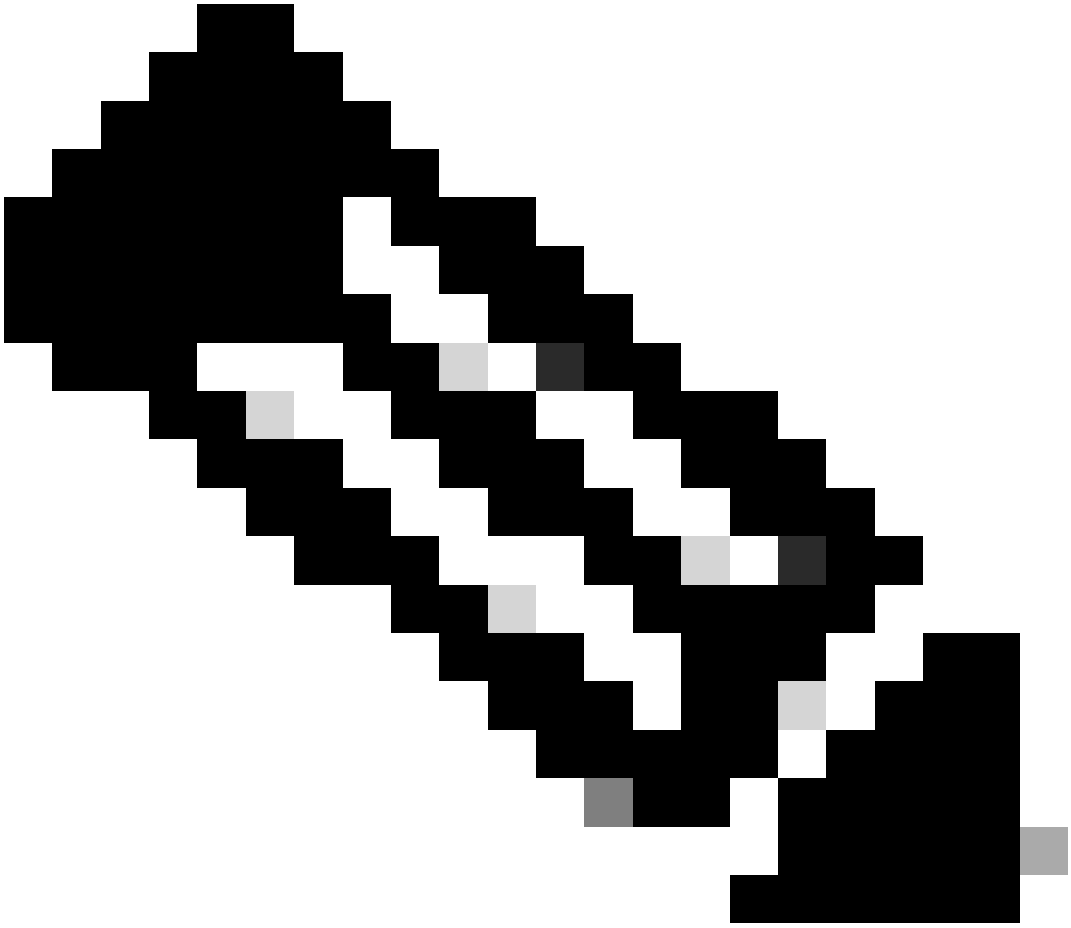
- 「セキュリティ」>「詳細」>「有効なアクセス権」(「有効な権限」と表示できます)に移動します。
- 「Select a user」をクリックし、次に「OpenDNS_Connector」ユーザアカウントを選択します。
- [OK]をクリックし、[有効なアクセスの表示]をクリックします
- コネクタユーザがすべてのプロパティを読み取ることができることを確認します。

115011616727

OpenDNS_Connector LDAPアクセス許可の設定

ADの「デリゲート制御」ウィザードを使用すると、必要な権限を「OpenDNS_Connector」ユーザに簡単に割り当てることができます。

1) [管理ツール]に移動し、[Active Directoryユーザーとコンピューター]スナップインを開きます。
2) OpenDNS_Connectorを含むドメインを右クリックし、「Delegate Control...」を選択してから「Next」をクリックします。
3) OpenDNS_Connectorユーザを追加し、Nextをクリックします。
4) 「Read all user information」を選択し、Nextをクリックします。 [図3を参照]
7) Finishをクリックします。 [図6を参照]



注：一部のオブジェクトで継承が無効になっている場合、これらの手順は失敗する可能性があります。 これらのオブジェクトについては、アクセス許可を手動で設定する必要があります。

userPermsスクリプト

添付のPowerShellスクリプトは、ADで特定のオブジェクト（ユーザーなど）の権限を取得するもう1つの方法です。Umbrellaテクニカルサポートに問い合わせる際は、このスクリプトの出力を含めてください。

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。