AD同期の包括の暗号化について

内容

[はじめに](#)
[背景説明](#)
[ADデータアップロードの暗号化](#)
[ADデータ取得のための暗号化](#)

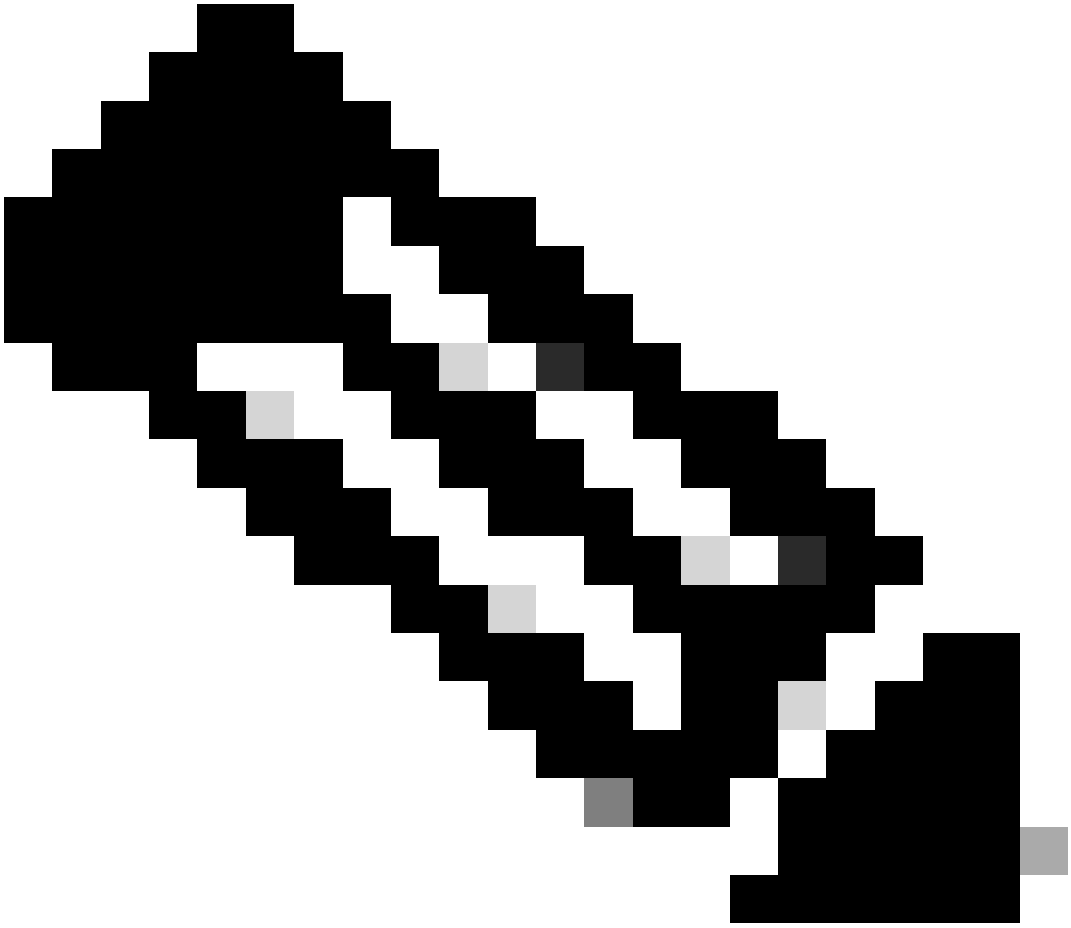
はじめに

このドキュメントでは、このデータ転送の暗号化方法など、AD同期のUmbrella暗号化について説明します。

背景説明

Umbrella AD Connectorソフトウェアは、LDAPを使用してADドメインコントローラからユーザ、コンピュータ、およびグループの詳細情報を取得します。必要な属性だけが各オブジェクトから保存されます。これには、sAMAccountName、dn、userPrincipalName、memberOf、objectGUID、primaryGroupId（ユーザおよびコンピュータ用）、およびprimaryGroupToken（グループ用）が含まれます。

このデータは、ポリシーの設定とレポートで使用するためにUmbrellaにアップロードされます。このデータは、ユーザ単位またはコンピュータ単位のフィルタリングにも必要です。



注:objectGUIDはハッシュ形式で送信されます。

同期されている内容を正確に把握するには、次のディレクトリに含まれる.ldifファイルを確認します。

```
C:\Program Files\OpenDNS\OpenDNS Connector\ADSync\*.ldif
```

この記事では、このデータ転送を暗号化する方法について説明します。

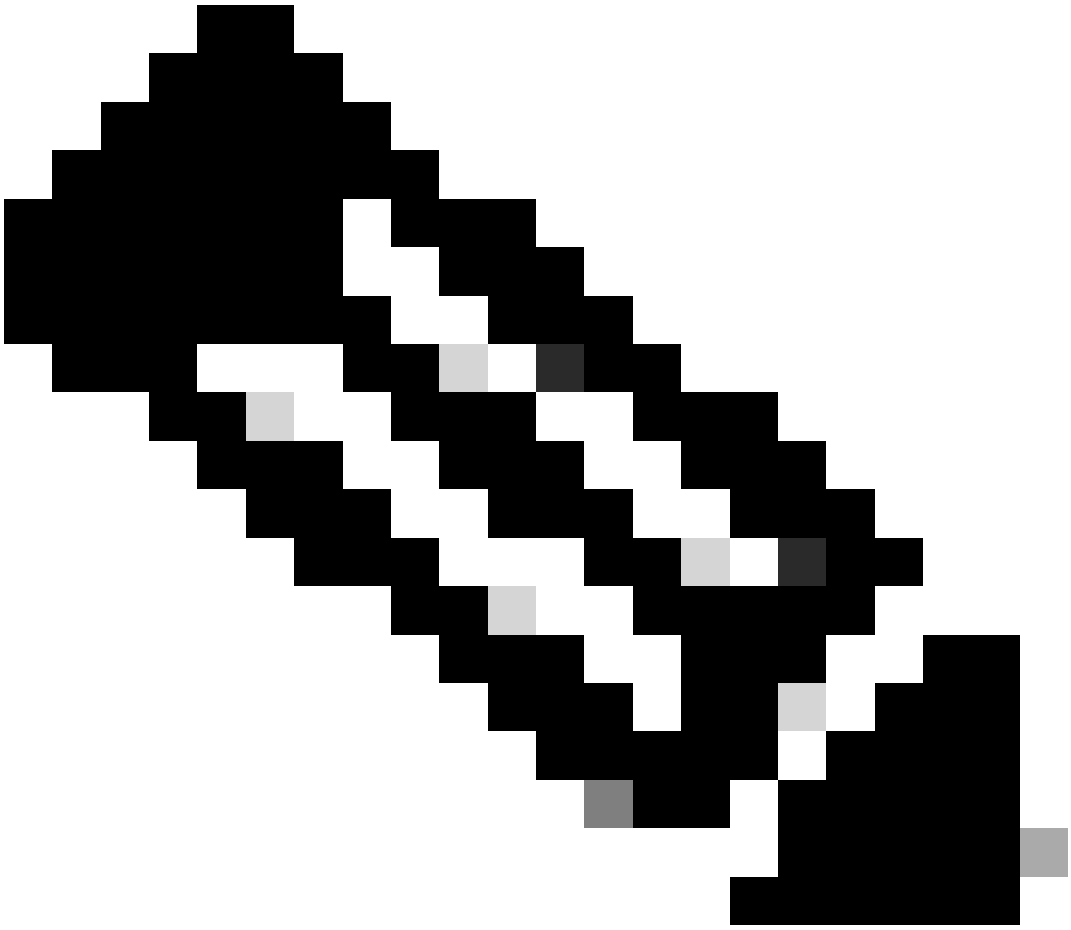
ADデータアップロードの暗号化

Umbrella ADコネクタは、セキュアHTTPS接続を使用してAD情報をUmbrellaにアップロードします。Connector <> Umbrellaクラウド間のアップロードは常に暗号化されます。

ADデータ取得のための暗号化

v1.1.22以降、コネクタはドメインコントローラ<>コネクタ間で暗号化を使用してユーザの詳細の取得を試みるようになりました。次の2つの方法が試みられます。

- LDAPS.データは安全なトンネル経由で送信されます。
- Kerberos認証を使用するLDAPパケットレベルの暗号化を提供します。



> 注：コネクタソフトウェアがADsyncに使用されるドメインコントローラと同じサーバで実行されている場合、LDAPSは使用されません。

この試行が何らかの理由で失敗した場合は、次のメカニズムに戻ります。

- NTLM認証を使用するLDAPこれによりセキュアな認証が提供されますが、DC >コネクタ間のデータ転送は暗号化なしで行われます。

暗号化を確実に実行するために、次のことを推奨します。

- ドメインコントローラでLDAPSを有効にします。 これはUmbrellaサポートの範囲外ですが、Microsoftのドキュメントで有効にできます。
- ドメインコントローラのホスト名が正しく設定されていることを、[展開] > [サイトとAD]で確認します。両方の暗号化方式で正しいホスト名が必要です。何らかの理由でホスト名が正しくない場合は、コンフィギュレーションスクリプトを使用してドメインコントローラを再登録するか、Umbrellaサポートに問い合わせることをお勧めします。

暗号化が行われていることを確認します。ログファイルは次の場所で確認できます。

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>\OpenDNSAuditClient.log
```

ADの同期中に、次のようなログエントリが表示されます。

LDAPS接続に成功しました：
DNを取得するために<SERVER>通信用にSSLを使用しています。

Kerberos認証が成功しました：
DNを取得するための<SERVER>通信にKerberosを使用する。

使用中のNTLMフェールバックメカニズム：
DC Host <SERVER>に対するKerberosが失敗しました。ホスト名は無効である可能性があります。NTLMクエリーにフォールバックします。

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。