包括Active Directory統合フローの確認

内容

はじめに

背景説明

Umbrella Active Directory実装との通信フロー

- ADコネクタスクリプトがドメインコントローラ(DC)で実行される場合
- ADコネクタの通信方法
  - クラウドへのコネクタ
  - 仮想アプライアンスへのコネクタ
  - ドメインコントローラへのコネクタ
- クラウドへの仮想アプライアンス(VA)

はじめに

このドキュメントでは、Cisco Umbrella Active Directory(AD)統合の運用コンポーネント間の通信フローについて説明します。

背景説明

Active Directoryの通信フローを理解することは、導入前にトラブルシューティングを行い、正しく設定された環境を確保するのに役立ちます。

Umbrella Active Directory実装との通信フロー

ADコネクタスクリプトがドメインコントローラ(DC)で実行される場合

Windowsスクリプトは、HTTPSを使用してドメインコントローラ(DC)をダッシュボードに登録し、ドメインコントローラ(DC)からポートTCP/443のクラウドへの1回限りの接続を行います。この登録により、コネクタはDCを認識できるようになります。特定のパラメータを指定して、**https://api.opendns.com**にコールが発信されます。スクリプトによってDCが正常に登録されると、ダッシュボードに表示されます。

問題は、Windowsでのルート証明書の更新に関連している場合があります。これを簡単に判別するには、Internet Explorerに移動してブラウザでhttps://api.opendns.com/v2/OnPrem.Assetを指定します。このアクションは、「**1005 Missing API key**」のようなメッセージを出力します。 そのページに証明書の工ラーまたは警告が表示された場合は、Microsoftからの最新のルート証明書の更新がインストールされていることを確認します。

ADコネクタの通信方法

ADコネクタは、次のようにUmbrellaクラウドサービスまたは仮想アプライアンスと通信します。

- クラウドへのコネクタ

  コネクタは、ポート443 TCPのHTTPS接続を使用して、変更が発生すると5分ごとにすべてのActive Directory(AD)データをアップロードします。グループ、ユーザー、およびコンピューターに関する情報のみがアップロードされます。パスワードはアップロードされず、すべてのユーザ情報がローカルでハッシュされ、データが一意になります。

- 仮想アプライアンスへのコネクタ

  コネクタは、ポート443 TCP（暗号化なし）を使用して、ADイベントを仮想アプライアンスに絶えず送信します。 これは一方向の通信であり、アプライアンスはコネクタに戻って通信しません。必須の前提条件は、コネクタと仮想アプライアンス(VA)が信頼できるネットワーク経由で通信することです。

- ドメインコントローラへのコネクタ

  コネクタは、LDAP同期用のポート389 TCPおよび3268 TCP/UDPを使用して、同じサイトにあるすべてのドメインコントローラと通信します。コネクタは、WMI/RPCを使用してドメインコントローラとも通信します。ポート135 TCPは、RPCおよびWMIの標準ポートです。また、WMIは、Windows 2003以前の場合は1024 TCPと65535 TCPの間、Windows 2008以降の場合は49152 TCPと65535 TCPの間でランダムに割り当てられたポートを使用します。バージョン1.1.24では、コネクタはポート636 TCPおよび3269 TCP経由でLDAPS(LDAP over SSL)を使用してドメインコントローラとも通信します。

通信の問題が発生した場合は、データをブロックまたはドロップする可能性のあるレイヤ7アプリケーションプロキシを確認します。よくあるケースとして、DNS、HTTP、HTTPSなどのプロトコルに対して動作するシスコデバイスの検査機能があります。詳細については、アプリケーション層プロトコルインスペクションの適用に関するシスコのドキュメントを参照してください。

クラウドへの仮想アプライアンス(VA)

仮想アプライアンスは、サポートトンネルを確立するために、ポート443 TCPで**api.opendns.com**のほか、DNSクエリまたはプローブの53 TCP/UDP、および22、25、53、80、443、または4766 TCPと頻繁に通信します。仮想アプライアンスは、ポート53 UDP/TCP、443 TCP、123 TCP、80 TCPを使用してクラウドと通信します。これらのポートは、ポート443 TCP（HTTPS接続ではない）でコネクタからデータを受信しますが、コネクタとの通信は不要です。

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。