VAまたはCSCを使用したActive Directoryの統合

内容

はじめに

このドキュメントでは、Active Directory(AD)をUmbrellaと統合する2つの方法である、仮想アプライアンス(VA)またはCisco Secure Client(CSC)について説明します。

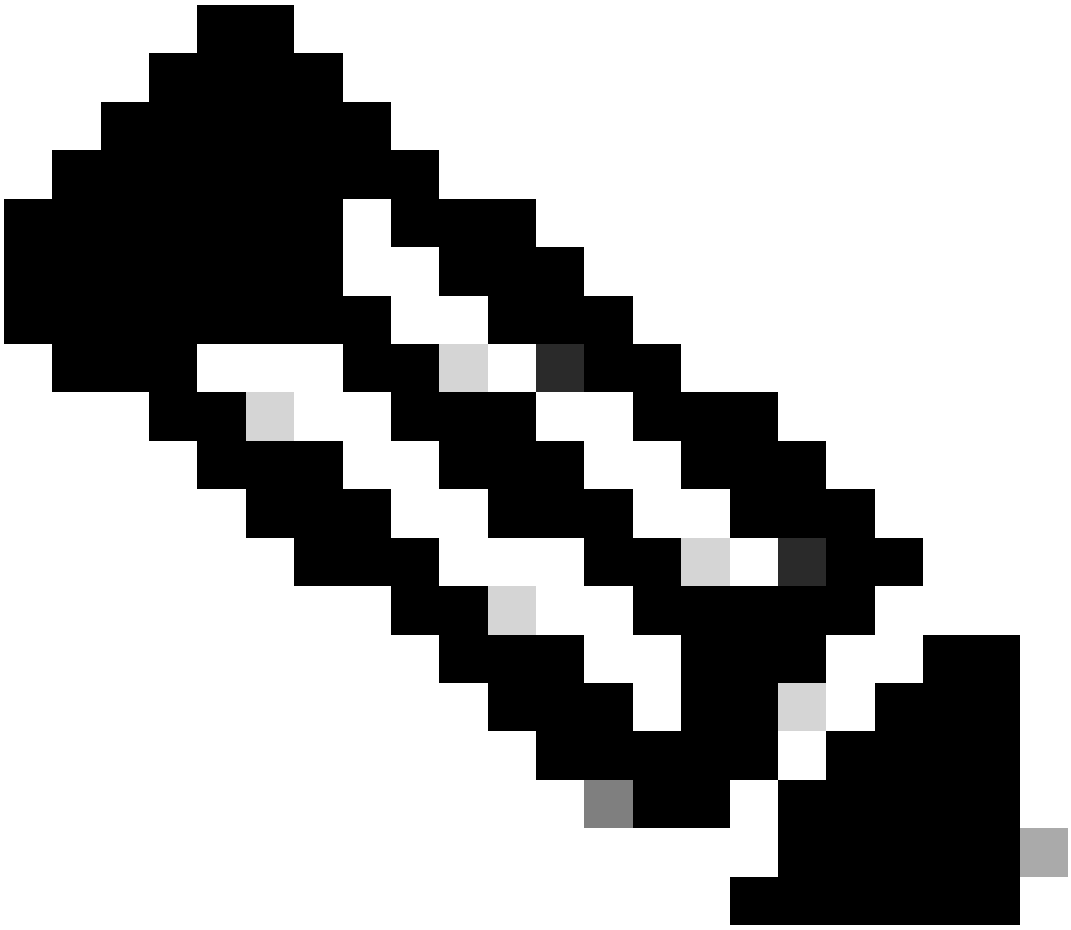
前提条件

要件

次の項目に関する知識があることが推奨されます。

- ADコネクタ：単一のActive DirectoryドメインのADツリーをダッシュボードに同期します。VAの実装では、同じUmbrellaサイトにあるDCからのログインイベントをVAにアクティブに同期します。 組織のADツリーは、ADコネクタによってUmbrellaクラウドに同期され、登録済みDCからこのデータが取得されます。ツリーの更新が検出され、数時間以内にUmbrellaクラウドが更新されます。
- ドメインコントローラ（ADサーバ）:DCは、ダッシュボードからダウンロードした登録設定.wsfスクリプトによってダッシュボードに登録されます。これにより、その名前、ドメイン、および内部IPがダッシュボードに追加され、どのIPと同期を試みるかがコネクタに通知されます。スクリプトを実行できない場合は、手動登録も可能です。詳細とサポートについては、Umbrellaサポートに連絡してください。
- 仮想アプライアンス：包括オンプレミスDNSフォワーダ。（オプション）AD IDをネットワークに適用し、内部IPをレポートに適用します。これにより、その背後にあるすべてのローミングクライアントがトリガーされ、DNS保護が無効になり、「Behind VA protection」モ

ードに保留されます。
- Cisco Secure Client:WindowsおよびmacOSにDNS暗号化とユーザIDを提供する包括的なオンプレミスのソフトウェアサービス。AnyConnectモジュールとしても提供されます。



注：前提条件は、この2つの実装で大きく異なります。前提条件の詳細については、それぞれの実装を参照してください。

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。

概要

この記事では、Active DirectoryとUmbrellaダッシュボードを統合する2つの異なる方法について説明します。現在、ADユーザは、Umbrella仮想アプライアンスまたはCisco Secure Clientを介してポリシーおよびレポートに適用できます。

セキュアクライアントの実装

要件

- 1つのADコネクタ
- ダッシュボード上の1つのDC
- OpenDNS_Connectorユーザーには、読み取り専用ドメインコントローラーのアクセス許可が必要です。
- スタンドアロンクライアント（AnyConnectモジュール）用のセキュアクライアントの最小バージョン：
  - Windows:2.1.0(4.5.01044)
  - OSX: 2.0.39 (4.5.02033)。

仕組み

- 現在ログインしているADユーザは、ローカルレジストリを読み取るローミングクライアントによって、ローカルコンピュータで直接決定されます。
- ワークステーションに同時にログインできるユーザは最大1人までサポートします。
- 2人のユーザが同時に使用すると、ADユーザは適用されません。
- ADユーザGUIDと内部IPは、ローミングクライアントのDNSプロキシ内のEDNS0経由で、Umbrellaリゾルバに送信されるDNSクエリに添付され、ADユーザを一意に識別します。
- すべてのポリシーはリゾルバ側に適用されます。
- アクティブなコネクタは必要ありません。ただし、ADユーザおよびグループポリシーアプリケーションは、最新の正常なADツリー同期を反映できます。

動作する場所

- あらゆるネットワークをグローバルに。
- DNSレイヤがローカルVAに保留するように無効になっているため、Umbrella仮想アプライアンスの背後では機能しません。

制限事項

- ワークステーションでエンドポイントエージェントがアクティブかつ有効になっている必要があります。
- サーバOSをサポートしない
- 内部ネットワークIPに基づいてポリシーを適用できません。
- ADコンピュータにポリシーまたはレポートを適用できません（代わりにローミングホスト名を使用してください）。

コネクタは、登録されている1つのDCからAD口グインイベントを引き出すことができます。この結果、ダッシュボードエラーが発生し、ローミングクライアントベースのAD統合には関係ない可能性があります。実際にイベントをプルせずにログイン・イベントのプルに関連する権限に関するエラーを削除するには、ここから示す監査手順の逆の手順を使用して、ログイン・イベントの監査を無効にします（他の方法で使用しない場合）。

仮想アプライアンスの実装

要件

- Umbrellaサイトあたり2つのVA
- Umbrellaサイトごとに1つのADコネクタ（2つ目は冗長構成、1つはオプション）
- 各DC（読み取り専用DCではない）をダッシュボードに登録する必要があります。
- OpenDNS_Connectorユーザには、前提条件の権限の完全なセットが必要です。
- すべてのDCで4624セキュリティイベントログを記録するには、ログインイベントを有効にする必要があります。詳細なトラブルシューティングのヒントを参照してください。

仕組み

- VAは、Windows DCのセキュリティログインイベントログに基づいてADユーザマッピングを受信します。
- 各ワークステーションのログインは、ADユーザ名またはADコンピュータ名とワークステーションの内部IPを使用して、一意のログインイベントとしてログインサーバDCのセキュリティイベントログに記録されます。
- コネクタは、WMIサブスクリプションを介してこれらのイベントをリアルタイムで解析し、TCP 443を介してこれらのイベントをUmbrellaサイトの各 VAに同期します。
- VAは、ADユーザ/コンピュータの内部IPとADユーザ/コンピュータのユーザ名の間のライブユーザマッピングを構築します。
- VAは、DNSクエリの内部ソースIPに対する可視性のみを持ち、コネクタ同期イベントによって作成された前述のマッピングファイルを利用します。VAは、マシンに現在ログインしているユーザを直接確認することはできません。これにより、EDNS0を介してADユーザGUIDと内部IPが、VAによってUmbrellaリゾルバに送信されるDNSクエリに関連付けられ、ADユーザが一意に識別されます。
- ADコンピュータのハッシュも同様に適用されます。
- すべてのポリシーはリゾルバ側に適用されます。
- ADユーザを受信するには、コネクタが機能し、組織でアクティブである必要があります。また、ログインイベントが最新である必要があります。
- このユーザは、イベントログに示されているように、このマシンに対して認証される最後のADユーザである必要があります。

動作する場所

すべてのDNSが、ユーザが認証したDCと同じUmbrellaサイトに属するUmbrella仮想アプライアンスを指す、ローカルの企業ネットワーク。

制限事項

- コンピュータは、別のADドメインまたはUmbrellaサイトに属するVAを指すことはできません（複数のドメイン上の大規模な展開では、ADアプリケーションをベースネットワークから見ることはできません）。
- 大規模な導入では、個別のVAを持つUmbrellaサイトに分割する必要がある場合があります。
- サービスADユーザに対してADユーザ例外が必要になる場合があります。
- 前述のコネクタには、1秒あたりの最大ログインイベント数が存在するため、ユーザアプリケーションに遅延が発生する可能性があります。これは、ネットワーク遅延とVA数の要因になります。

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。