ターミナルサービス、Citrix、およびUmbrellaのActive Directoryとの統合について

内容

はじめに

このドキュメントでは、ターミナルサービス、Citrix、およびUmbrellaとActive Directoryの統合について説明します。

概要

適用対象プログラム：Windows Terminal ServicesおよびRemote Desktop Services、Windows 10 Enterprise multi-session、Citrix XenAppおよびXenDesktop

ターミナルサービスとCitrixサーバは、複数の同時クライアントセッションを1台のサーバでホストする機能を提供します。 2つの異なる設定があります。

- リモートデスクトップサービス(RDS)。複数のユーザーが、同じサーバー上の1つの仮想マシンでセッションを実行します。 これらのセッションはすべて同じOSとIPアドレスを共有します。 これは一般に、ターミナルサービスと呼ばれます。
- 仮想デスクトップインフラストラクチャ(VDI)。サーバは仮想マシンのプールを実行し、各ユーザは独自のオペレーティングシステムとIPアドレスを使用して一意のVMに接続します

Webポリシー：RDSおよびVDIに適用

PACファイル、CDFWトンネル、およびプロキシチェーンを介したSAML Cookieベースの認証によるセキュアなWebゲートウェイは、単一のIPアドレスへの複数のユーザをサポートします。これは、ユーザのWebポリシー適用ごとに仮想デスクトップ(Citrix/TS)がサポートされることを意味します。

DNSポリシー：AD統合を使用したRDS

RDS/リモートデスクトップセッションホスト/ターミナルサーバーでは、ユーザーごとの識別はサポートされていません。これには、AzureのみのWindows 10 Enterpriseマルチセッション OSが

含まれます。

これらのサーバでホストされるクライアントセッションは、1つのIPアドレス（ホストマシンに属するもの）を共有します。 Umbrella Active Directory(AD)と仮想アプライアンス(VA)の統合は、ユーザとIPアドレスの一意のマッピングを使用して正しく動作します。 つまり、ユーザが同じ送信元IPアドレスを共有する状況では、ユーザ単位の識別は不可能です。

複数のログインユーザが同じIPを共有している場合、ポリシーの適用とレポートに悪影響が及びます。すべてのユーザが同じポリシーを受信し、特定されたユーザは最後にログオンしたユーザに基づいて継続的に変更できます。

DNSポリシー：解決策 – AD統合を使用したRDS

この問題に対処する最善の方法は、ターミナルサーバまたはCitrixサーバのIPアドレスに一意のポリシーを設定することです。 これは、ターミナルサーバのすべてのユーザが同じ一貫したポリシーを受信することを意味します。

1. 「Deployments」>「Internal networks」で、内部ネットワークを作成します。 これで、ターミナルサーバの/32のIPアドレスがカバーされます。 該当する仮想アプライアンスと同じUmbrellaサイトにネットワークを割り当てます。
2. ポリシーウィザードに移動し、新しいポリシーを作成します。
3. Select Identitiesセクションで、「Sites」をクリックして関連するUmbrellaサイトを開きます。
4. 前に作成したInternal Network IDを選択します
5. 通常どおりにポリシーを設定します
6. ターミナルサーバーのポリシーを作成した後、このポリシーを必ずポリシーの一覧の一番上に並べ替えて、ユーザーベースのポリシーよりも優先されるようにします。

または、ADコンピュータIDに基づいてターミナルサーバのポリシーを作成することもできます。 この方法は同じように動作します。サーバのすべてのユーザは、ターミナルサーバのコンピュータ名として識別されます。 ただし、これが一貫して機能するためには、ホストとIPのマッピングを最適化するようにVAを設定する必要があります。 詳細については、ADホストGUIDタイムアウトの手順を参照してください。または、Umbrellaサポートに問い合わせてください。

DNSポリシー：AD統合でのVDIの使用

VDIタイプの導入では、各ユーザに対して一意の仮想マシンが実行されますが、ユーザごとのIDを受信できます。 要件は次のとおりです。

- 仮想アプライアンス：各ユーザは、仮想アプライアンスから認識できる一意のソースIPを持っている必要があります。 送信元IPは、アプライアンスに到達する前に「ソースNAT」の対象となってはいけません。
- ローミングクライアント：ローミングクライアントが各仮想マシンにインストールされている場合、ローミングクライアントのAD統合が可能です。 この方法による導入は、各ユーザが永続的な（個人用の）仮想マシンを持っている場合に、より実行可能です。

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。