認証にUmbrella Active Directoryコネクタを使用する

内容

はじめに

このドキュメントでは、802.1x、RADIUS、またはISE経由の認証にUmbrella Active Directory Connector(AD)を使用する方法について説明します。

概要

Cisco Umbrella Active Directory(AD)コネクタは、ADユーザ/コンピュータを内部IPアドレスにマッピングすることによって機能します。マッピングを正しく行うには、Cisco Umbrella ADコネクタと通信するように設定されているドメインコントローラに対してADユーザを認証する必要があります。

ADユーザが他の手段で認証を行う場合、ドメインコントローラでログインイベントがまったく生成されないか、予期しないマッピングが存在して誤ったポリシーが適用される可能性があります。

802.1x、RADIUS、またはISEによる認証

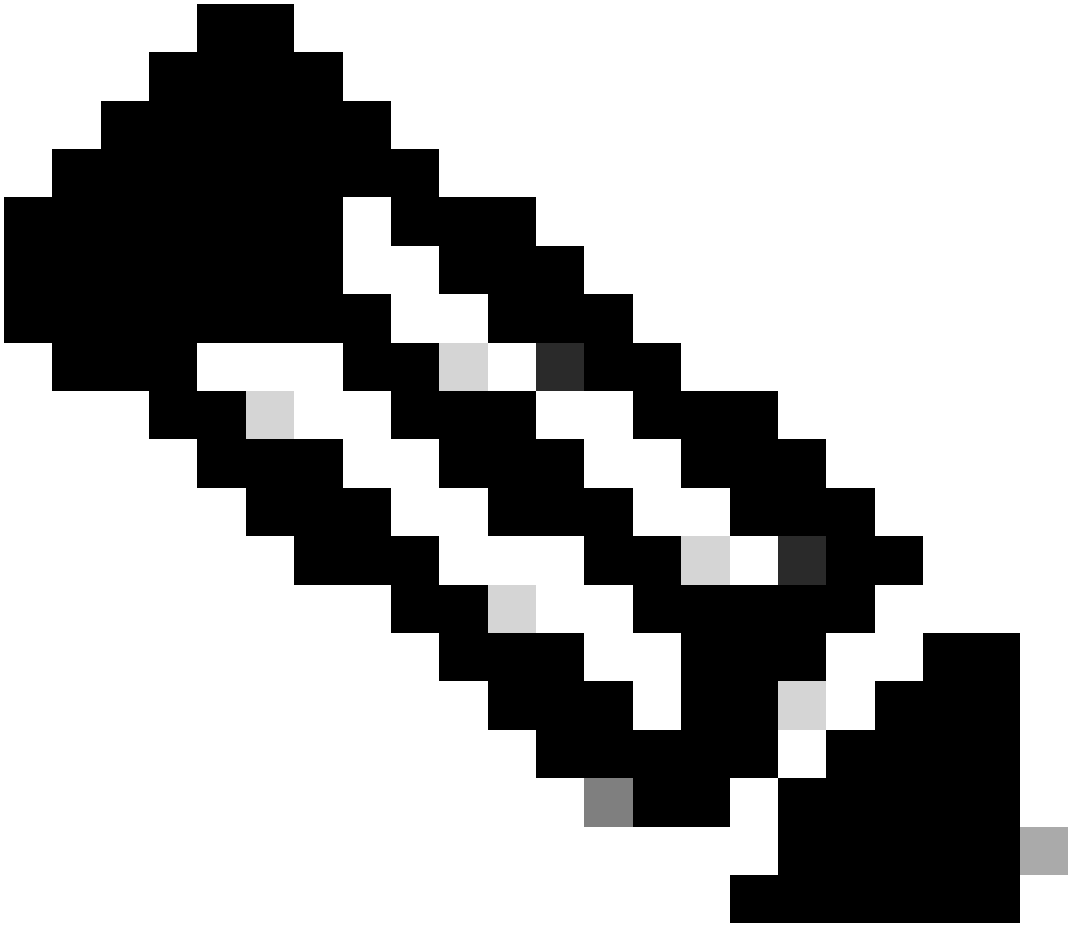
802.1x、RADIUS、またはISEを介した認証は、Active Directoryログインがこれらのソリューションでどのように動作するかについての制限があるため、サポートではありません。ADコネクタが検索するログオンイベントは、多くの場合、生成されません。

ADコネクタが検索するイベントIDの詳細については、こちらを参照してください。コネクタサービスが検索するウィンドウイベント/イベントID

通常、認証サービスのIPアドレスは、ユーザのコンピュータのIPアドレスではなく、ADユーザにマッピングされます。

代替ソリューション

AD統合は、IDサポート機能を有効にしたローミングクライアントを使用して実現することもできます。この機能の詳細については、導入に関するドキュメントを参照してください。



注：このソリューションでは、ローミングするクライアントが無効な「VAの背後」状態に移行するため、仮想アプライアンスがネットワーク上に存在しないことが必要です。

ネットワークで仮想アプライアンスを使用している場合は、識別に内部IPアドレスを使用できます。 たとえば、ワイヤレスネットワークのアドレス範囲の「内部ネットワーク」IDを作成し、このIDにポリシーを適用できます。この方法の唯一の欠点は、このアドレス範囲のすべてのデバイスが同じポリシーを受信することです。

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。