Umbrella Active Directoryでのローカルアカウントへのポリシーの適用

内容

はじめに

このドキュメントでは、Umbrellaのオンプレミス製品をActive Directory(AD)およびローカルユーザアカウントと同期する際に予想されるポリシー動作について説明します。

包括的な仮想アプライアンスとローカルアカウントの特定

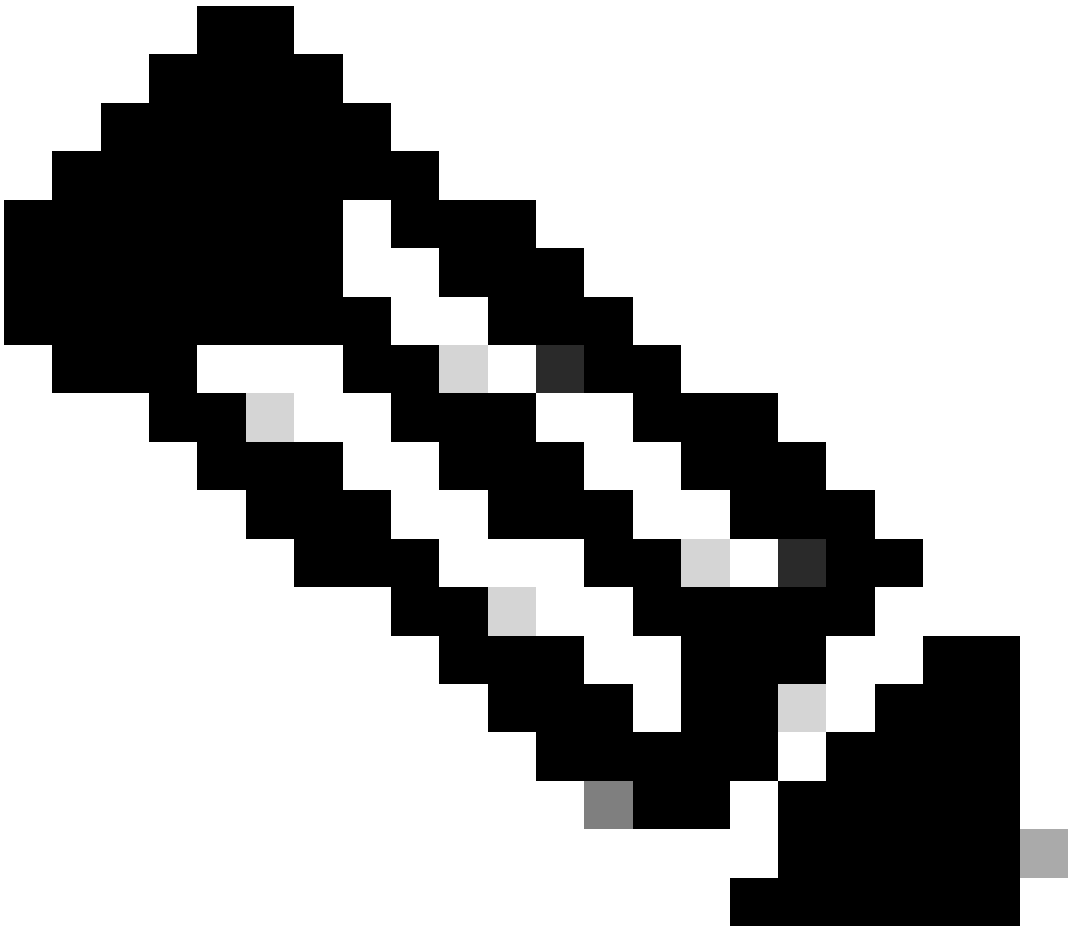
Umbrella仮想アプライアンスは、WindowsドメインコントローラからActive Directoryログオン情報を受信します。Active Directoryユーザをキャッシュに格納し、その送信元IPアドレスに基づいてユーザを識別します。

- ドメインコントローラはローカルユーザログオンを追跡しないため、これらのユーザを仮想アプライアンスで直接識別することはできません。
- Active Directoryユーザが最近IPアドレスからログインした場合でも、キャッシュされたIDはキャッシュに基づいて引き続き使用できます。 仮想アプライアンスでは、ADユーザがローカルアカウントで置き換えられていることを認識する方法はありません。
- キャッシュユーザが存在しない場合、仮想アプライアンスはデフォルト（非AD）IDを使用します。 トリガーされるIDは次のいずれかです。
  - 包括サイト名（例：デフォルトサイト）
  - 内部ネットワーク（内部IPアドレス）
  - ネットワーク（外部IPアドレス）

Umbrella仮想アプライアンスの推奨事項

- ローカルアカウントとパスワードへのアクセスを制限します。
- Umbrellaサイト名に対して別のポリシーを作成します（たとえば、Default Site）。 このポリシーには、標準のActive Directoryユーザポリシーよりも低い優先順位を割り当てます。この制限ポリシーは、ADユーザが検出されない場合に適用されます。
- ローカルユーザアカウントに異なるポリシーが必要な場合は、Umbrella Roamingクライアントの導入を検討してください。

Umbrellaローミングクライアントとローカルアカウントポリシー



注: Roaming ClientとActive Directoryの統合を使用するには、Identities > Roaming Computersに移動し、Enable Active Directory user and group policy enforcementの設定を有効にします。

Roaming Clientは、Windowsレジストリからログオンユーザーを検出し、一意のAD GUIDによってActive Directoryユーザーを識別できるようにします。

- Roaming Clientはポリシーの目的でローカルユーザ名を識別できません。
- ADユーザが検出されると、ADユーザIDがポリシーの適用に適用されます。これには、オフネットワークでキャッシュされたクレデンシャルを使用してログインしたADユーザも含まれます。
- ADユーザーが検出されない場合（ローカルユーザーがログオンしている場合など）、ポリシーの適用にローミングコンピューターIDが使用されます。

Umbrellaローミングクライアントの推奨事項

- ローカルアカウントとパスワードへのアクセスを制限します。
- 標準のADユーザポリシーよりも低い優先順位で、Roaming コンピュータ用の個別のポリシーを作成します。このポリシーは、ドメインに参加していない、またはローカルユーザーによって使用されていないローミングコンピューターに適用されます。

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。