Active Directoryサービスアカウントをブロックするコネクタのトラブルシューティング

内容

はじめに

このドキュメントでは、Active Directory(AD)サービスアカウントがUmbrellaコネクタによってブロックされる原因をトラブルシューティングする方法について説明します。

概要

Umbrellaコネクタサービスは、ログオンイベント情報を読み取るために、同じUmbrellaサイトの一部である登録済みドメインコントローラ(DC)のイベントログへのWMI接続を行います。 これらのログオンイベントは解析され、同じUmbrellaサイトのすべての仮想アプライアンス(VA)にアップロードされます。VAは、そのユーザ名/送信元IPアドレスのユーザとIPの一時的なマッピングを作成します。注目に値する点がいくつかあります。

- Umbrella Insightsは、IPごとに一度に1人のログオンユーザーしかサポートできません
- ソースIPからの最後に処理されたログオンイベントは'wins'です

すべてのログオンイベントが等しいため、コネクタには、イベントが無視される共通のADサービスアカウントのハードコードリストがあります。 コネクタのログファイルで、これらのアカウントのログオンイベントを確認できます。例：

ブラックリストに登録されたユーザーからのイベントは無視されました： OpenDNS_Connector

これは、サービスアカウント（DCセキュリティイベントログにログオンイベントを生成する標準ユーザと同様）が、実際にログオンしたユーザのユーザとIPのマッピングを上書きするのを防ぐためです。

大規模な環境では、サービスアカウントが使用されるプロセスやアプリケーションに応じて、毎分数千のログオンイベントを生成することもできます。これは、コネクタに対する追加の負荷でもあり、ユーザログオンと正しいポリシーが適用される間の遅延、または後で失われる正しいポリシーが適用される間の遅延として現れる可能性があります。

ブロックされたアカウントのリスト

- _vmware_ユーザ_
- Administrator
- 匿名
- 匿名ログオン
- ASPNET
- ローカルサービス
- McAfeeMVSUser
- MC制御
- NETWORK SERVICE
- ネットワーク
- OpenDNS_コネクタ
- peersyncsvc
- s-pcadmin
- SophosUpdateMgr
- SophosUpdMgr
- svc-altiris
- svc.i作成

詳細情報

また、他のADアカウントログオンイベントをコネクタによる処理から除外することもできます。手順については、次の記事を参照してください。

https://support.umbrella.com/hc/en-us/articles/231266088

さらに、コネクタのAD同期から除外できるADグループもあります。これは、ADユーザ、コンピュータ、およびグループのリストをダッシュボードポリシー領域に入力するために実行されます。これは次の場所にあります。

https://support.umbrella.com/hc/en-us/articles/115005206526

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。