DNS要求をUmbrellaに転送するための Windowsサーバの設定

内容

はじめに

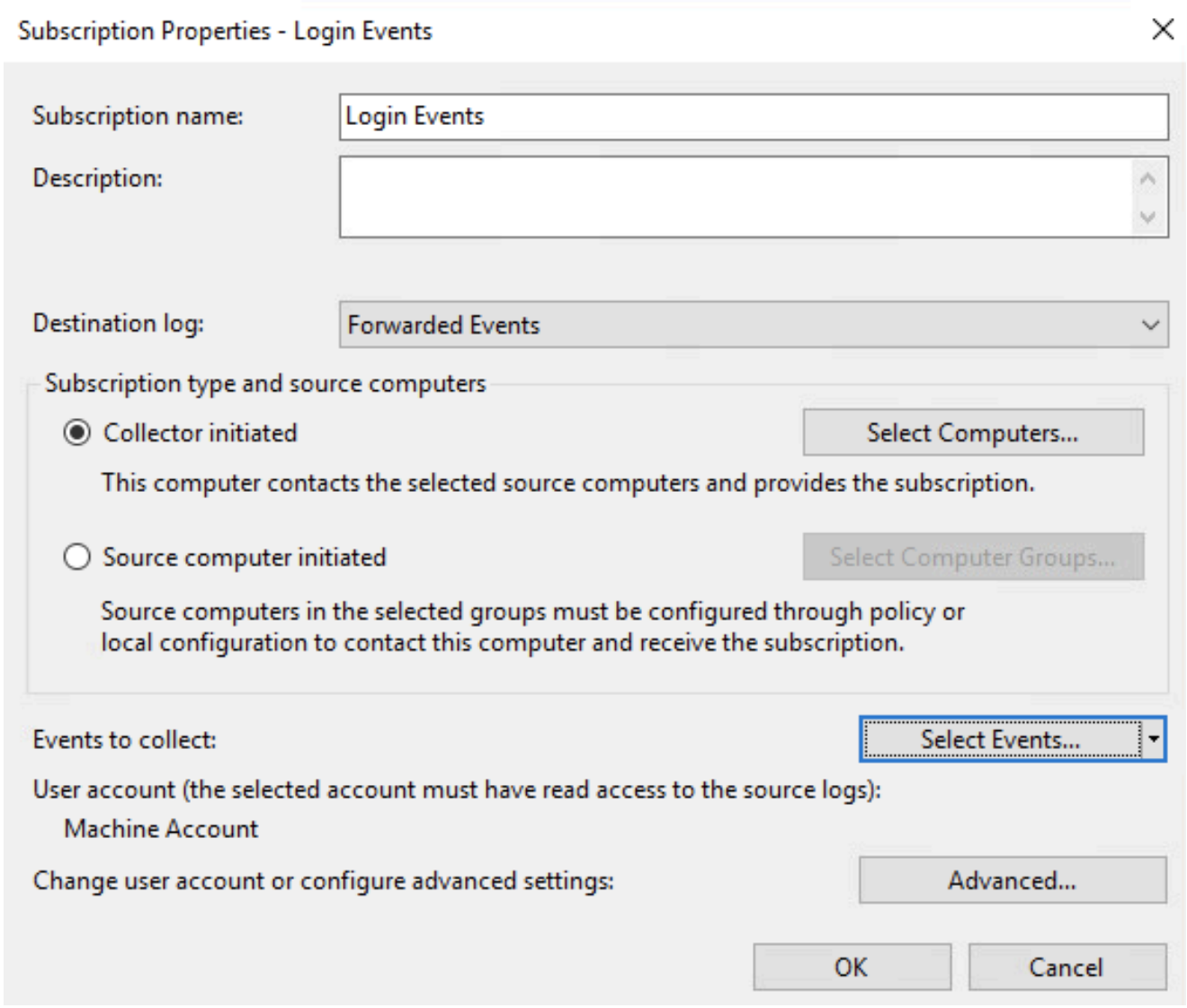
このドキュメントでは、クライアント保護と口ギングを強化するためにDNS要求をUmbrellaに転送するようにWindows Serverを設定する方法について説明します。

概要

Windows Serverは、DNSフォワーダとして機能することにより、ネットワークIDを使用してクライアントを保護できます。ドメインコントローラまたはDNSロールを持つ他のサーバは、登録済みネットワークからUmbrellaにDNSを送信できます。

設定手順

1. DNS Manager(dnsmgmt.msc)を開きます。
2. ツリーでサーバ名を右クリックし、Propertiesを選択します。
3. Forwardersタブを選択します。
4. Edit...をクリックし、Umbrella DNSサーバのIPアドレスを入力します。
5. Edit Forwardersウィンドウで OKをクリックします。エントリがフォワーダのリストに表示されます。
6. Use root hints if no forwarders are availableというラベルのボックスのチェックマークを外します。



mceclip0.png

ベストプラクティスのメモ

- Use root hints if no no forwarder are availableがオフになっていることを確認します。オンにすると、Umbrella保護とロギングが一致しなくなります。たとえば、ドメインがDNSSEC検証に失敗した場合、またはDDoS軽減イベントの対象である場合、Windows DNSサーバーはUmbrellaが応答しないと見なし、ルートヒントを使用してUmbrellaをバイパスして直接再帰を試みることができます。

- フォワーダとしてUmbrellaのみを使用します。サードパーティ製のリゾルバを設定しないでください。Umbrellaは、受信したDNSクエリのみをログに記録して保護できます。

- 冗長性を確保するため、前のスクリーンショットに示すように、4つすべてのUmbrellaエニーキャストIPアドレスをフォワーダとして設定します。

- Umbrellaサイトと仮想アプライアンスを使用している場合は、Umbrellaエニーキャストアド

レスではなく、フォワーダとしてローカル仮想アプライアンスを指定します。

    - 要求ループの回避：仮想アプライアンスがサーバをローカルDNSサーバの1つとしてリストする場合は、その仮想アプライアンスをフォワーダとして追加しないでください。
    - 仮想アプライアンスは、DNSサーバのIPアドレスだけを認識し、サービスを提供する個々のクライアントのアドレスは認識しません。
    - Active Directory統合と仮想アプライアンスを使用している場合は、例外としてWindows DNSサーバIPを追加します。Umbrellaダッシュボードで**Deployments > Sites and Active Directory > Service Account Exceptions**の順に移動し、DNSサーバのIPを追加します。これにより、サーバトラフィックに対するユーザIDの不正な帰属が防止されます。

- 「ルートヒント」タブにはUmbrellaサーバを追加しないでください。包括DNSサーバは再帰リゾルバであり、反復ルックアップのルートとしては機能しません。ルートヒントとしてこれらを追加すると、望ましくない動作が発生し、Umbrella保護と口ギングがバイパスされます。

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。