Loginsearch.ps1を使用したログオンイベントの検索

内容

はじめに

このドキュメントでは、Loginsearch.ps1（PowerShellスクリプト）を使用してログオンイベントを検索する方法について説明します。

背景説明

Loginsearch.ps1は、トラブルシューティングの目的でUmbrellaサポートに役立つ情報を収集する小さなPowerShellスクリプトです。特定のユーザがOpenDNS Umbrellaダッシュボードのレポートまたはアクティビティ検索で正しいアクティビティを表示しない原因のトラブルシューティングに役立ちますが、他のタイプの問題のトラブルシューティングにも使用できます。

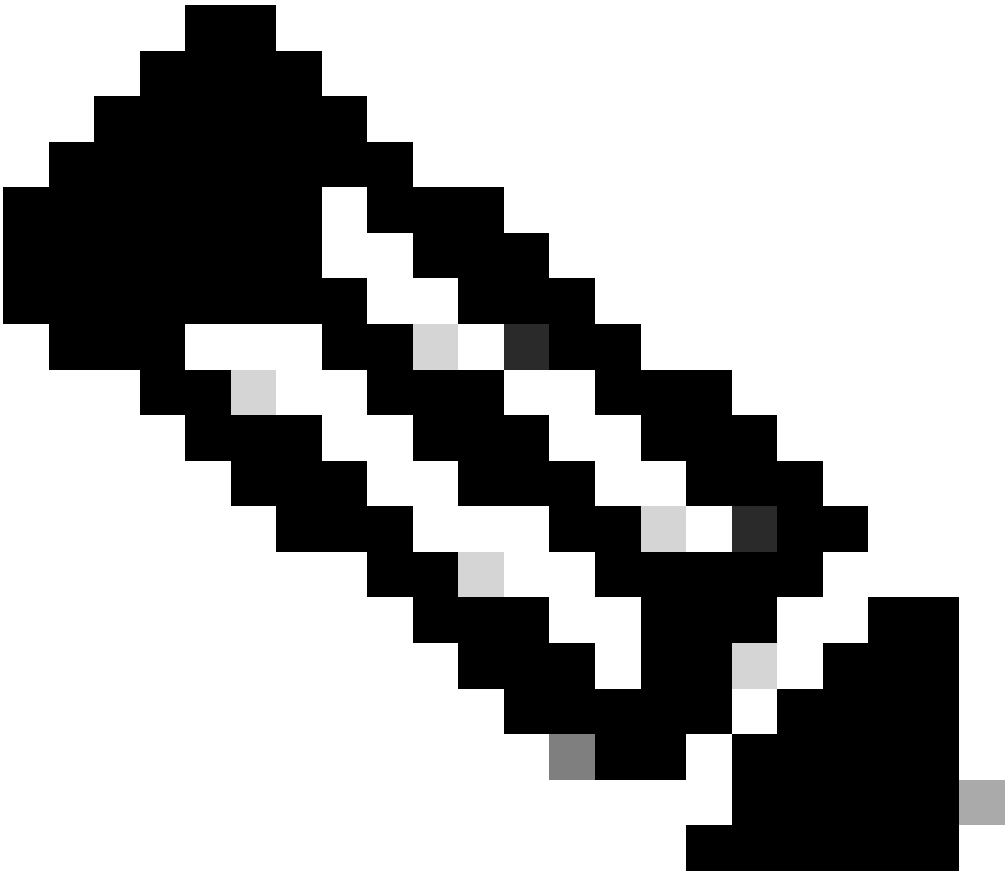
ログインイベントがDC間で複製されるので、任意の標準ドメインコントローラでこれを実行します。ただし、検索の際にイベントが見つからず、特定のホストからイベントが見られることを予期している場合は、サーバ間でイベントログのレプリケーションに問題がある可能性があります。この例では、そのホストで使用される%LOGONSERVER%を検出し、指定されたドメインコントローラでスクリプトを実行します。それでもイベントが表示されない場合は、ログオンイベントが監査されていることを確認します。

スクリプトはこの記事の最後に添付されています。収集した情報は、ご自身またはOpenDNSサポートのいずれかによるトラブルシューティングに使用できます。

スクリプトの実行

次のステップを実行します。

1. 添付されたテキストファイルをダウンロードし、拡張子を「.txt」から「.ps1」に変更します。



注：二重拡張子には注意してください。誤って「.txt.ps1」という名前を付けないでください。

2. 次に、Windowsサーバで、「右クリック－>管理者として実行」で起動した新しいPowerShellウィンドウを開きます。 スクリプトを保存した場所に移動し(例： 'cd C:\Users\admin\Downloads')、.\loginsearch.ps1と入力してスクリプトを実行します。
3. スクリプトでは、まずWindowsセキュリティイベントログを検索するユーザ名を入力し、次にIPで検索する場合は特定のIPアドレスを入力するように求められます。画面上のプロンプトを使用します。検索結果を特定のユーザーとIPアドレスに制限する場合は、どちらか一方（ユーザー名またはIP）の検索を個別に使用することも、両方を同時に使用することもできます。
4. このスクリプトは実行が早い。処理が完了すると、タイムスタンプを含む出力が画面に表示されます。さらに、'C:\%hostname%.txt'にある画面に表示される各イベントログエントリのエクスポートも実行します。これは、特定のイベントをさらに詳しく調べる場合に便利です。

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。