Rechercher les événements de connexion avec Loginsearch.ps1

Table des matières

Introduction

Ce document décrit comment rechercher des événements d'ouverture de session avec Loginsearch.ps1, un script PowerShell.

Informations générales

Loginsearch.ps1 est un petit script PowerShell qui collecte des informations utiles à la prise en charge d'Umbrella à des fins de dépannage. Il est utile lors du dépannage de la raison pour laquelle certains utilisateurs n'affichent pas l'activité correcte dans les rapports ou la recherche d'activité sur le tableau de bord OpenDNS Umbrella, mais peut également être utilisé pour dépanner d'autres types de problèmes.

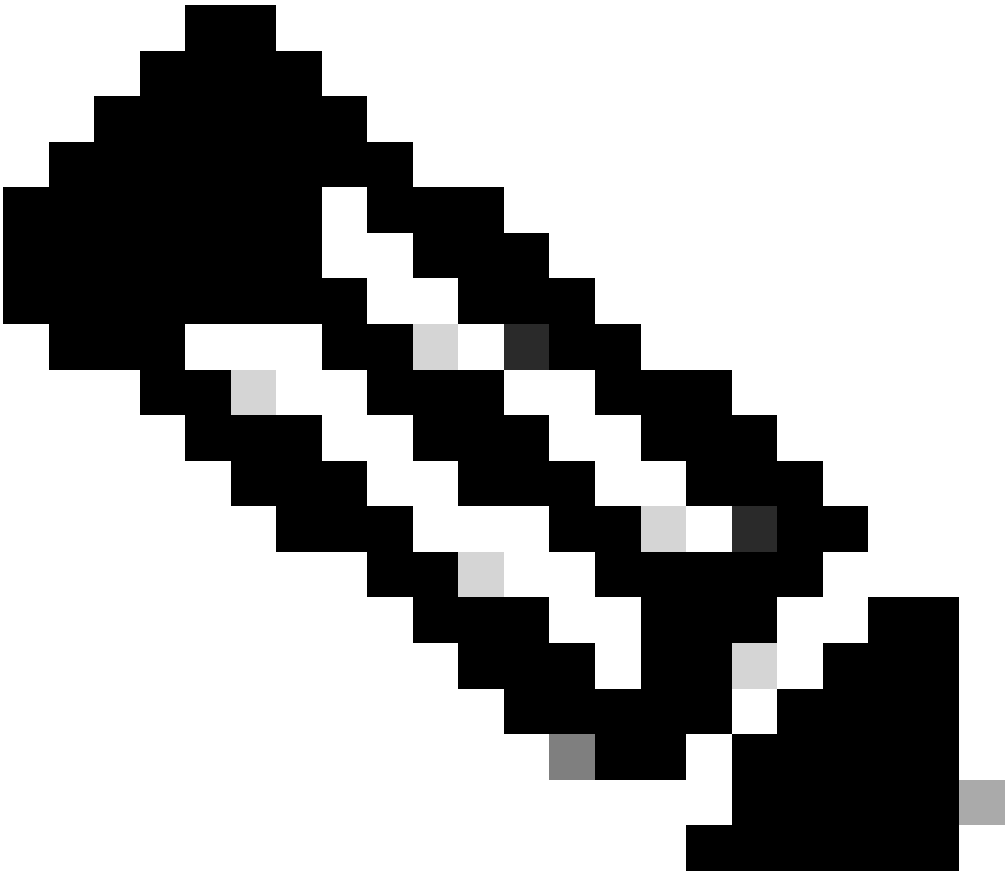
Exécutez cette commande sur n'importe quel contrôleur de domaine standard, car les événements de connexion sont répliqués entre les contrôleurs de domaine. Cependant, SI, lors d'une recherche, vous ne voyez aucun événement et que vous vous attendez à les voir d'un hôte particulier, il peut y avoir un problème de réplication des journaux d'événements entre les serveurs. Dans ce cas, recherchez le %LOGONSERVER% utilisé par cet hôte, puis exécutez le script sur le contrôleur de domaine spécifiquement indiqué. Si vous ne voyez TOUJOURS aucun événement, assurez-vous que les événements d'ouverture de session sont en cours d'audit.

Le script est joint au bas de cet article. Les informations recueillies peuvent être utilisées pour le dépannage par vous-même ou par le support OpenDNS.

Exécuter le script

Procédez comme suit :

1. Téléchargez le fichier texte joint et renommez l'extension de '.txt' en '.ps1'.



Remarque : Méfiez-vous des doubles extensions et ne le nommez pas accidentellement ".txt.ps1".

2. Ensuite, à partir d'un serveur Windows, ouvrez une nouvelle fenêtre PowerShell qui a été démarrée par **'Right-Click -->Run as Administrator'**. Accédez à l'emplacement où vous avez enregistré le script **(eg: 'cd C:\Users\admin\Downloads'**) et exécutez le script en tapant **.\loginsearch.ps1.**
3. Le script demande d'abord le nom d'utilisateur que vous souhaitez rechercher dans les journaux des événements de sécurité Windows, puis une adresse IP spécifique si vous préférez effectuer une recherche par IP. Utilisez les invites affichées à l'écran. L'une ou l'autre recherche (nom d'utilisateur ou adresse IP) peut être utilisée individuellement, ou les deux peuvent être utilisées en même temps, si vous voulez limiter les résultats de la recherche à un utilisateur spécifique ET adresse IP en même temps.
4. Le script est rapide à exécuter. Quand il a terminé, vous voyez le résultat à la fois sur l'écran, qui contient des horodatages. En outre, l'exportation complète de chaque entrée du journal des événements représentée sur l'écran situé dans **'C:\%hostname%.txt'** Ceci peut être utile si vous souhaitez approfondir un événement spécifique.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.