Login-Ereignisse mit Loginsearch.ps1 suchen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie mit dem PowerShell-Skript Loginsearch.ps1 nach Anmeldeereignissen suchen.

Hintergrundinformationen

Loginsearch.ps1 ist ein kleines PowerShell-Skript, das Informationen sammelt, die für den Umbrella Support zur Fehlerbehebung nützlich sind. Bei der Fehlerbehebung ist es hilfreich, warum bestimmte Benutzer nicht die richtige Aktivität in den Berichten oder der Aktivitätssuche im OpenDNS Umbrella Dashboard anzeigen. Es kann jedoch auch zur Behebung anderer Probleme verwendet werden.

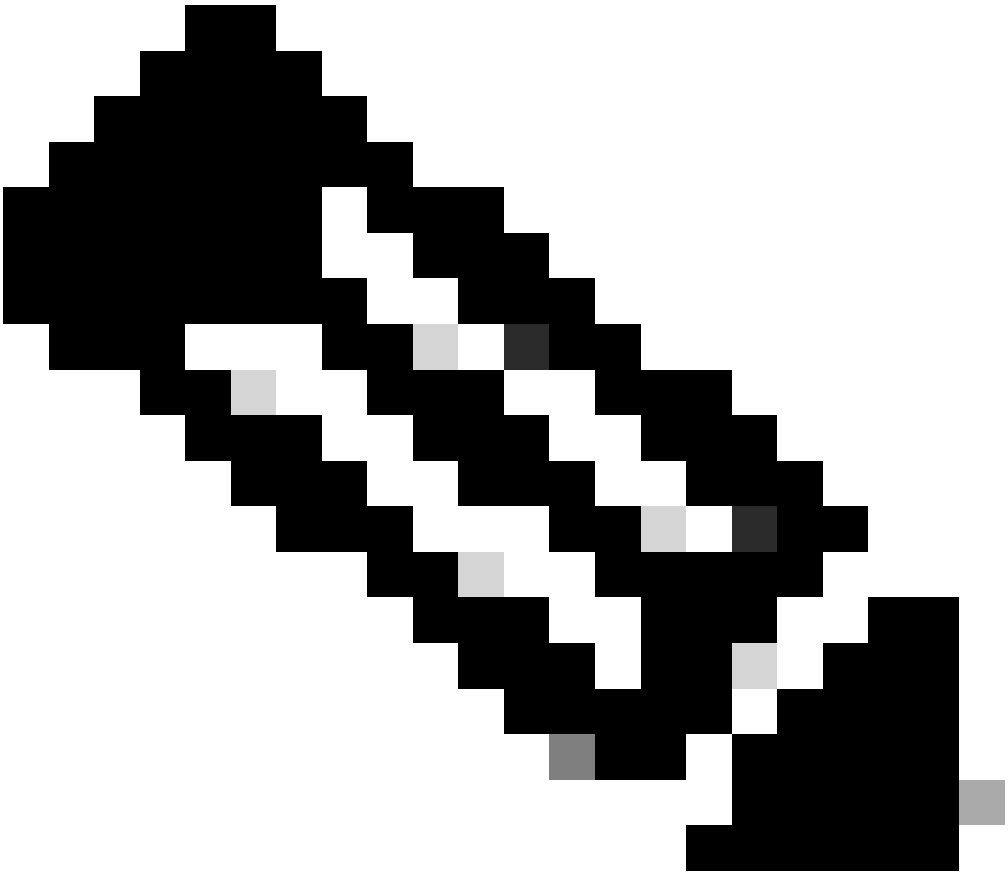
Führen Sie diesen Vorgang auf einem beliebigen Standard-Domänencontroller aus, da Anmeldeereignisse zwischen Rechenzentren repliziert werden. WENN bei der Suche jedoch keine Ereignisse angezeigt werden und diese von einem bestimmten Host erwartet werden, kann es zu einem Problem beim Replizieren von Ereignisprotokollen zwischen Servern kommen. Finden Sie in dieser Instanz heraus, welche %LOGONSERVER% von diesem Host verwendet wird, und führen Sie dann das Skript auf dem speziell angegebenen Domänencontroller aus. Wenn WEITERHIN keine Ereignisse angezeigt werden, stellen Sie sicher, dass die Anmeldeereignisse überwacht werden.

Das Skript ist unten in diesem Artikel angefügt. Die gesammelten Informationen können entweder von Ihnen selbst oder vom OpenDNS-Support zur Fehlerbehebung verwendet werden.

Skript ausführen

Führen Sie diese Schritte aus:

1. Laden Sie die angehängte Textdatei herunter, und benennen Sie die Erweiterung von ".txt" in ".ps1" um.



Anmerkung: Achten Sie auf doppelte Erweiterungen, und nennen Sie es nicht versehentlich ".txt.ps1".

2. Öffnen Sie dann von einem Windows-Server aus ein neues PowerShell-Fenster, das von gestartet wurde **'Right-Click -->Run as Administrator'**. Navigieren Sie zum Speicherort, an dem Sie das Skript gespeichert haben **(eg: 'cd C:\Users\admin\Downloads'**), und führen Sie das Skript durch Eingabe von **.\loginsearch.ps1.**
3. Das Skript fordert zuerst den Benutzernamen auf, nach dem Sie die Windows-Sicherheitsereignisprotokolle durchsuchen möchten, und dann nach einer bestimmten IP-Adresse, wenn Sie die Suche nach IP vorziehen. Verwenden Sie die Eingabeaufforderungen auf dem Bildschirm. Die eine oder die andere Suche (Benutzername oder IP) kann einzeln verwendet werden, oder beide können gleichzeitig verwendet werden, wenn Sie die Suchergebnisse auf eine bestimmte Benutzer- UND IP-Adresse gleichzeitig beschränken möchten.
4. Das Skript lässt sich schnell ausführen. Nach Abschluss der Ausgabe sehen Sie die Ausgabe auf dem Bildschirm, die Zeitstempel enthält. Führen Sie zusätzlich den vollständigen Export aller Ereignisprotokolleinträge aus, die auf dem Bildschirm unter **'C:\%hostname%.txt'** Dies kann nützlich sein, wenn Sie weiter in ein bestimmtes Ereignis einsteigen möchten.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.