Zoeken naar evenementen met Loginsearch.ps1

Inhoud

Inleiding

In dit document wordt beschreven hoe u kunt zoeken naar aanmeldingsgebeurtenissen met Loginsearch.ps1, een PowerShell-script.

Achtergrondinformatie

Loginsearch.ps1 is een klein PowerShell-script dat informatie verzamelt die nuttig is voor Umbrella Support voor het oplossen van problemen. Het is handig bij het oplossen van problemen waarom bepaalde gebruikers niet de juiste activiteit tonen in de rapporten of het zoeken naar activiteiten op het OpenDNS Umbrella Dashboard, maar kan ook worden gebruikt om andere soorten problemen op te lossen.

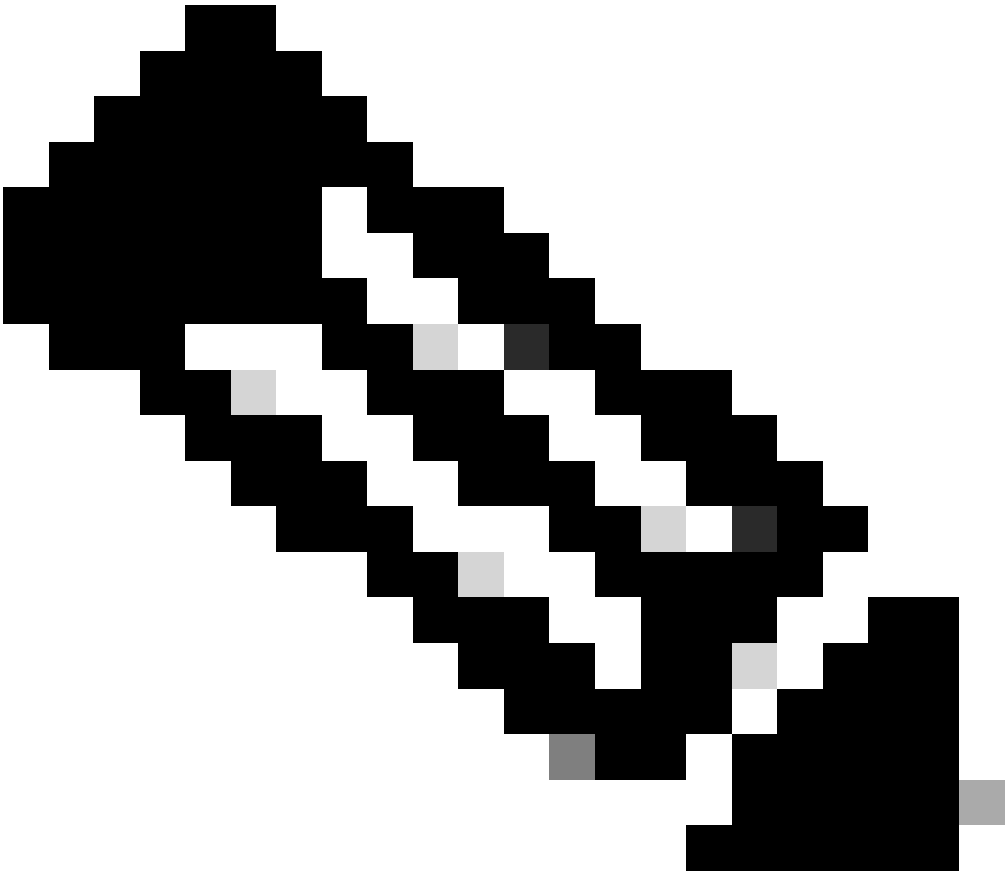
Voer dit uit op elke standaard domeincontroller, omdat aanmeldingsgebeurtenissen worden gerepliceerd tussen DC's. Als u tijdens het zoeken echter geen gebeurtenissen ziet en verwacht deze van een bepaalde host te zien, kan er een probleem zijn met het repliceren van gebeurtenislogboeken tussen servers. Zoek in dit geval de %LOGONSERVER% die door die host wordt gebruikt en voer het script uit op de domeincontroller die specifiek is aangegeven. Als u NOG STEEDS geen gebeurtenissen ziet, moet u ervoor zorgen dat aanmeldingsgebeurtenissen worden gecontroleerd.

Het script staat onderaan dit artikel. De verzamelde informatie kan worden gebruikt voor het oplossen van problemen, hetzij door uzelf of door OpenDNS Support.

Voer het script uit

Voer de volgende stappen uit:

1. Download het bijgevoegde tekstbestand en hernoem de extensie van '.txt' naar '.ps1'.



Opmerking: Wees voorzichtig met dubbele extensies en noem het niet per ongeluk ".txt.ps1".

2. Open vervolgens vanaf een Windows-server een nieuw PowerShell-venster dat is gestart door **'Right-Click -->Run as Administrator'**Microsoft. Navigeer naar de locatie waar u het script hebt opgeslagen **(eg: 'cd C:\Users\admin\Downloads'**) en voer het script uit door te typen **.\loginsearch.ps1.**
3. Het script vraagt eerst de gebruikersnaam waarnaar u wilt zoeken in de Windows-beveiligingsevenementlogboeken en vervolgens naar een specifiek IP-adres als u liever op IP zoekt. Gebruik de aanwijzingen op het scherm. Beide (gebruikersnaam of IP) zoekopdrachten kunnen afzonderlijk worden gebruikt, of beide kunnen tegelijkertijd worden gebruikt, als u de zoekresultaten tegelijkertijd wilt beperken tot een specifieke gebruiker EN IP-adres.
4. Het script is snel uit te voeren. Als het klaar is, zie je de uitvoer beide op het scherm, die tijdstempels bevat. Bovendien volledige export van elk item in het gebeurtenissenlogboek dat wordt weergegeven op het scherm in Dit kan handig zijn als u verder wilt graven in een specifieke **'C:\%hostname%.txt'** gebeurtenis.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.