Buscar eventos de inicio de sesión con Loginsearch.ps1

Contenido

Introducción

Este documento describe cómo buscar eventos de inicio de sesión con Loginsearch.ps1, un script de PowerShell.

Antecedentes

Loginsearch.ps1 es un pequeño script de PowerShell que recopila información útil para Umbrella Support para solucionar problemas. Resulta útil para solucionar problemas por los que determinados usuarios no muestran la actividad correcta en los informes o en la búsqueda de actividades en OpenDNS Umbrella Dashboard. Sin embargo, también se puede utilizar para solucionar otros tipos de problemas.

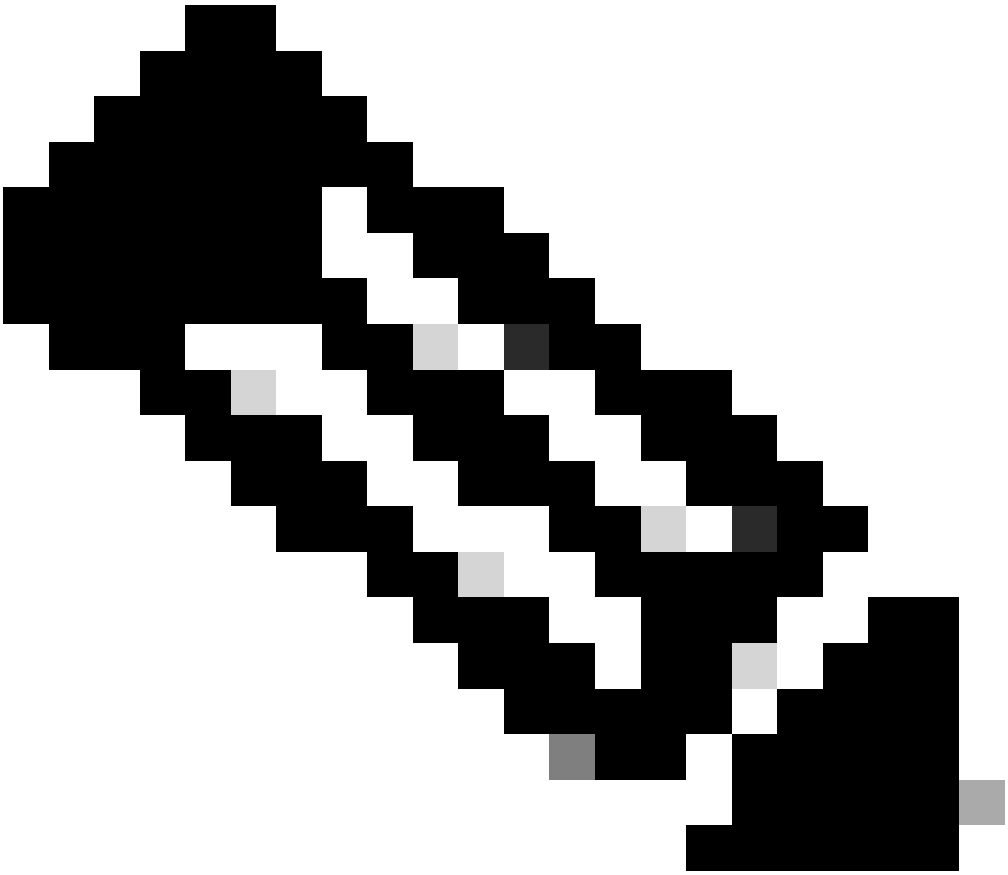
Ejecute esto en cualquier controlador de dominio estándar, ya que los eventos de inicio de sesión se replican entre los DC. Sin embargo, SI al realizar una búsqueda no ve ningún evento y espera verlo desde un host determinado, puede haber un problema al replicar los registros de eventos entre servidores. En este caso, averigüe el %LOGONSERVER% utilizado por ese host y, a continuación, ejecute el script en el controlador de dominio indicado específicamente. Si TODAVÍA no ve ningún evento, asegúrese de que se están auditando los eventos de inicio de sesión.

El guión se adjunta al final de este artículo. La información recopilada puede ser utilizada para la resolución de problemas por usted mismo o por el Soporte de OpenDNS.

Ejecutar el script

Complete estos pasos:

1. Descargue el archivo de texto adjunto y cambie el nombre de la extensión de '.txt' a '.ps1'.



Nota: Tenga cuidado con las extensiones dobles y no le dé por error el nombre ".txt.ps1".

2. A continuación, desde un servidor de Windows, abra una nueva ventana de PowerShell iniciada por **'Right-Click -->Run as Administrator'**. Desplácese hasta la ubicación en la que guardó la secuencia de comandos **(eg: 'cd C:\Users\admin\Downloads'**) y ejecútela escribiendo **.\loginsearch.ps1.**
3. La secuencia de comandos primero solicita el nombre de usuario que desea buscar en los registros de eventos de seguridad de Windows y, a continuación, una dirección IP específica si prefiere buscar por IP. Utilice las indicaciones que aparecen en pantalla. Se puede utilizar una o la otra búsqueda (Nombre de usuario o IP) de forma individual, o ambas al mismo tiempo, si desea limitar los resultados de la búsqueda a una dirección IP Y de usuario específica al mismo tiempo.
4. El script se ejecuta rápidamente. Cuando haya terminado, verá la salida en la pantalla, que contiene marcas de tiempo. Exportación completa adicional de cada entrada del registro de eventos representada en la pantalla ubicada en **'C:\%hostname%.txt'** Puede ser útil si desea profundizar más en un evento específico.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).