Cerca eventi di accesso con Loginsearch.ps1

Sommario

Introduzione

In questo documento viene descritto come cercare gli eventi di accesso con Loginsearch.ps1, uno script di PowerShell.

Premesse

Loginsearch.ps1 è un piccolo script di PowerShell che raccoglie informazioni utili per il supporto Umbrella per la risoluzione dei problemi. È utile per la risoluzione dei problemi relativi al motivo per cui alcuni utenti non visualizzano l'attività corretta nei report o nella ricerca di attività in OpenDNS Umbrella Dashboard, tuttavia può essere utilizzato anche per la risoluzione di altri tipi di problemi.

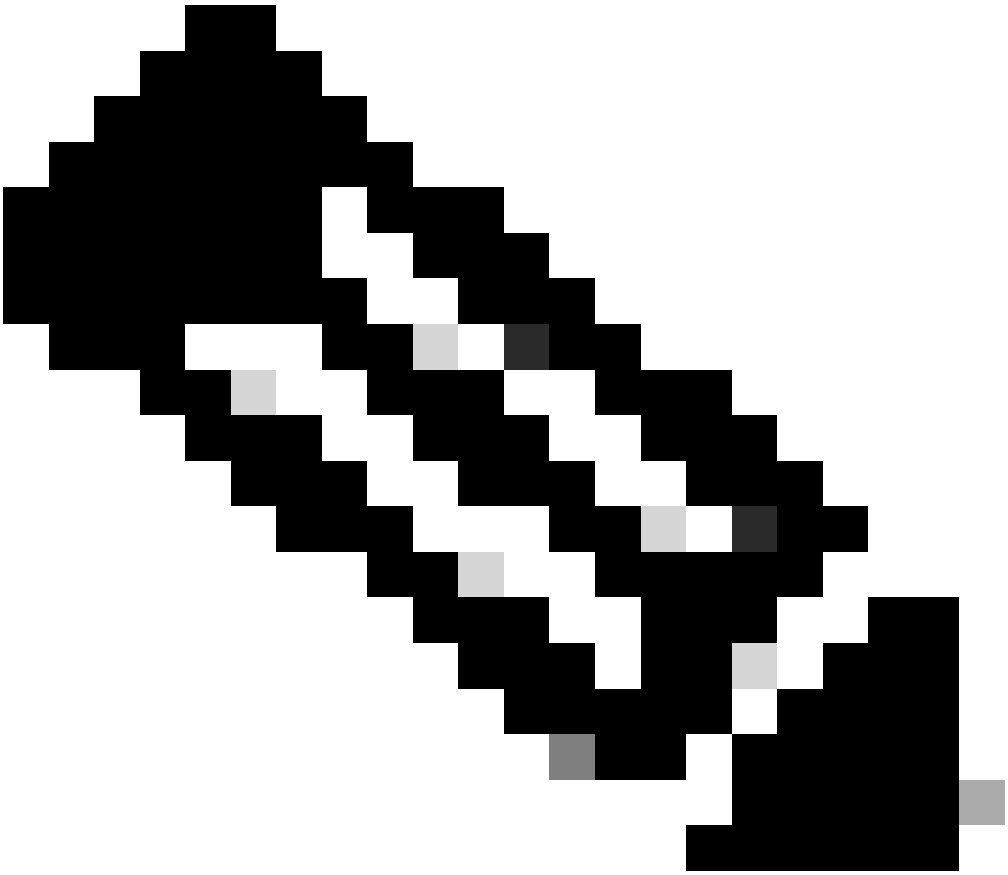
Eseguire questa operazione in qualsiasi controller di dominio standard, poiché gli eventi di accesso vengono replicati tra controller di dominio. Tuttavia, SE durante la ricerca non vengono visualizzati eventi e si prevede che vengano visualizzati da un determinato host, potrebbe verificarsi un problema durante la replica dei registri eventi tra i server. In questa istanza individuare il %LOGONSERVER% utilizzato da tale host, quindi eseguire lo script nel controller di dominio indicato in modo specifico. Se non viene ancora visualizzato alcun evento, verificare che gli eventi di accesso siano controllati.

Lo script è allegato in fondo a questo articolo. Le informazioni raccolte possono essere utilizzate per la risoluzione dei problemi da soli o dal supporto OpenDNS.

Esegui lo script

Attenersi alla seguente procedura:

1. Scaricare il file di testo allegato e rinominare l'estensione da 'txt' a 'ps1'.



Nota: Prestare attenzione alle estensioni doppie e non denominarle accidentalmente ".txt.ps1".

2. Quindi, da un server Windows, aprire una nuova finestra di PowerShell avviata da **'Right-Click ->Run as Administrator'**. Passare alla posizione in cui è stato salvato lo script **(eg: 'cd C:\Users\admin\Downloads')** ed eseguire lo script digitando **.\loginsearch.ps1.**
3. Lo script richiede innanzitutto il nome utente che si desidera cercare nei registri eventi di protezione di Windows e quindi un indirizzo IP specifico se si preferisce eseguire la ricerca in base all'indirizzo IP. Utilizzare le istruzioni visualizzate sullo schermo. È possibile utilizzare una o l'altra ricerca (Nome utente o IP) singolarmente oppure entrambe contemporaneamente, se si desidera limitare i risultati della ricerca a un utente e a un indirizzo IP specifici contemporaneamente.
4. L'esecuzione dello script è rapida. Al termine dell'operazione, l'output viene visualizzato su entrambi gli schermi, che contengono i timestamp. Esportazione completa di ogni voce del registro eventi rappresentata sullo schermo in **'C:\%hostname%.txt'** Può essere utile se si desidera approfondire l'analisi di un evento specifico.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).