Procurar eventos de logon com Loginsearch.ps1

Contents

Introdução

Este documento descreve como pesquisar eventos de logon com Loginsearch.ps1, um script do PowerShell.

Informações de Apoio

Loginsearch.ps1 é um pequeno script do PowerShell que coleta informações úteis para o Suporte Umbrella para fins de solução de problemas. É útil ao solucionar problemas por que determinados usuários não estão mostrando a atividade correta nos relatórios ou na pesquisa de atividades no painel do OpenDNS Umbrella, no entanto, também pode ser usado para solucionar outros tipos de problemas.

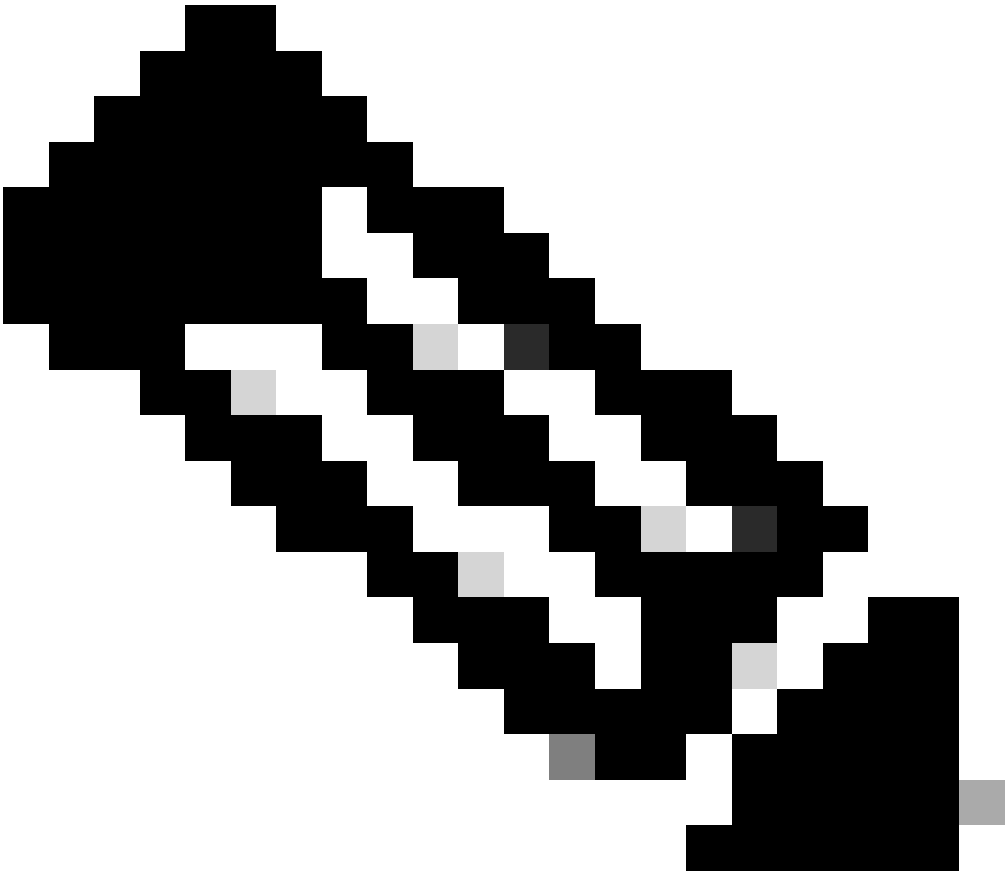
Execute-o em qualquer Controlador de Domínio padrão à medida que os eventos de login forem replicados entre DCs. No entanto, se ao pesquisar você não vir eventos e estiver esperando vê-los de um host específico, pode haver um problema na replicação de logs de eventos entre servidores. Nesta instância, descubra o %LOGONSERVER% usado por esse host e execute o script no Controlador de Domínio especificamente indicado. Se você AINDA NÃO vir nenhum evento, verifique se os eventos de logon estão sendo auditados.

O script está anexado à parte inferior deste artigo. As informações coletadas podem ser usadas para solucionar problemas, seja por você mesmo ou pelo suporte ao OpenDNS.

Executar o script

Conclua estes passos:

1. Baixe o arquivo de texto anexado e renomeie a extensão de '.txt' para '.ps1'.



Note: Tome cuidado com extensões duplas e não o nomeie acidentalmente como ".txt.ps1".

2. Em seguida, em um servidor Windows, abra uma nova janela do PowerShell iniciada por **'Right-Click -->Run as Administrator'**. Navegue até o local em que você salvou o script **(eg: 'cd C:\Users\admin\Downloads'**) e execute o script digitando **.\loginsearch.ps1.**
3. O script solicita primeiro o nome de usuário que você deseja pesquisar nos logs de eventos de segurança do Windows e, em seguida, um endereço IP específico, se preferir pesquisar por IP. Use os prompts na tela. Uma ou outra pesquisa (nome de usuário ou IP) pode ser usada individualmente, ou ambas podem ser usadas ao mesmo tempo, se você quiser limitar os resultados da pesquisa a um usuário específico e endereço IP ao mesmo tempo.
4. O script é rápido de ser executado. Quando terminar, você verá a saída na tela, que contém carimbos de data/hora. Além disso, conclua a exportação de cada entrada do log de eventos representada na tela localizada em **'C:\%hostname%.txt'** . Isso pode ser útil se você quiser detalhar um evento específico.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.