Search for Logon Events with Loginsearch.ps1

Contents

Introduction

This document describes how to search for logon events with Loginsearch.ps1, a PowerShell script.

Background Information

Loginsearch.ps1 is a small PowerShell script that collects information useful to Umbrella Support for troubleshooting purposes. It is helpful when troubleshooting why certain users are not showing the correct activity in the reports or activity searching on the OpenDNS Umbrella Dashboard, however can also be used to troubleshoot other types of issues.

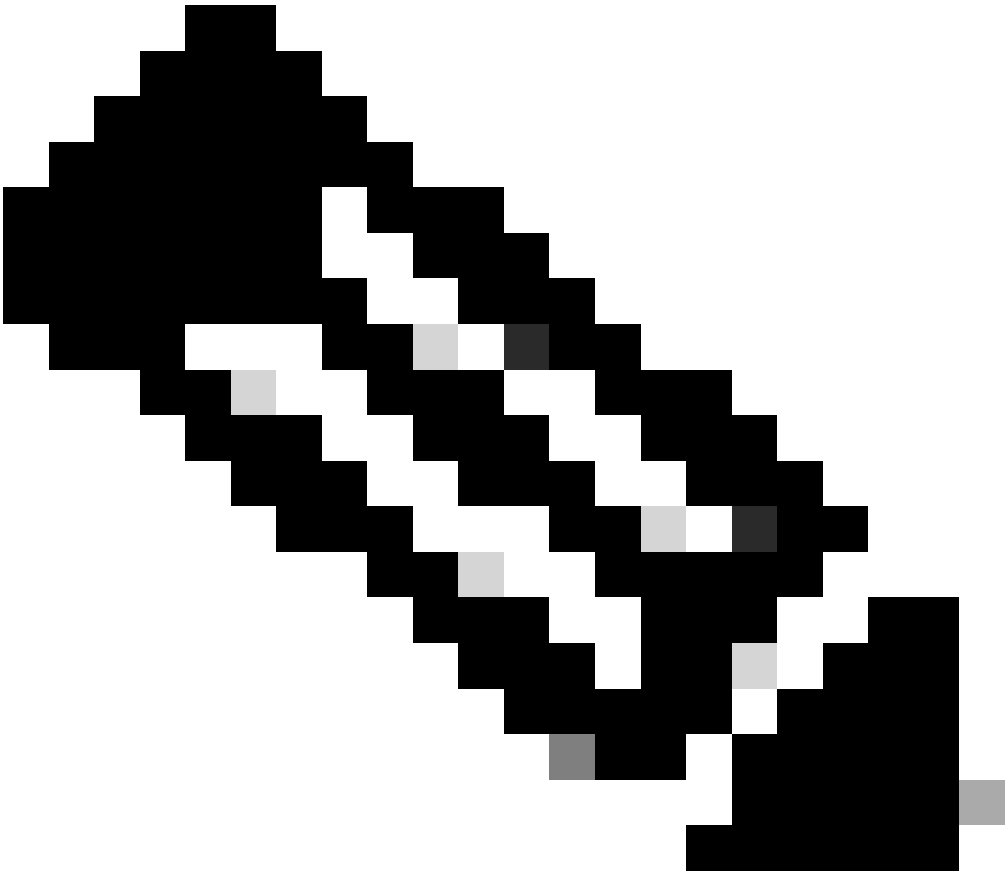
Run this on any standard Domain Controller as login events are replicated between DCs. However, IF when searching you see no events and are expecting to see them from a particular host, there can be an issue replicating event logs between servers. In this instance find out the %LOGONSERVER% used by that host, and then run the script on the Domain Controller specifically indicated. If you STILL see no events, make sure that logon events are being audited.

The script is attached to the bottom of this article. The information gathered can be used for troubleshooting either by yourself or by OpenDNS Support.

Run the Script

Complete these steps:

1. Download the text file attached and rename the extension from '.txt' to '.ps1'.



Note: Be careful of double extensions, and do not accidentally name it ".txt.ps1".

2. Then from a Windows server, open a new PowerShell window that was started by '**Right-Click -->Run as Administrator**'. Navigate to the location you saved the script to **(eg: 'cd C:\Users\admin\Downloads'**) and execute the script by typing **.\loginsearch.ps1.**
3. The script first prompts the username you want to search the Windows security event logs for, and then for a specific IP address if you prefer to search by IP. Use the on-screen prompts. Either one or the other (Username or IP) searches can be used individually, or both can be used at the same time, if you want to limit search results to a specific User AND IP address at the same time.
4. The script is quick to run. When it has finished you see the output both on the screen, which contains time stamps. Additionally complete export of each event log entry represented on the screen located in '**C:\%hostname%.txt**' This can be useful if you want to dig further into a specific event.