使用Loginsearch.ps1搜索登录事件

目录

简介

本文档介绍如何使用Loginsearch.ps1（PowerShell脚本）搜索登录事件。

背景信息

Loginsearch.ps1是一个小型PowerShell脚本，用于收集对Umbrella支持有用的信息以进行故障排除。在排除某些用户在报告中未显示正确活动或OpenDNS Umbrella控制面板上搜索活动的原因时，该功能非常有用，但也可用于排除其他类型的问题。

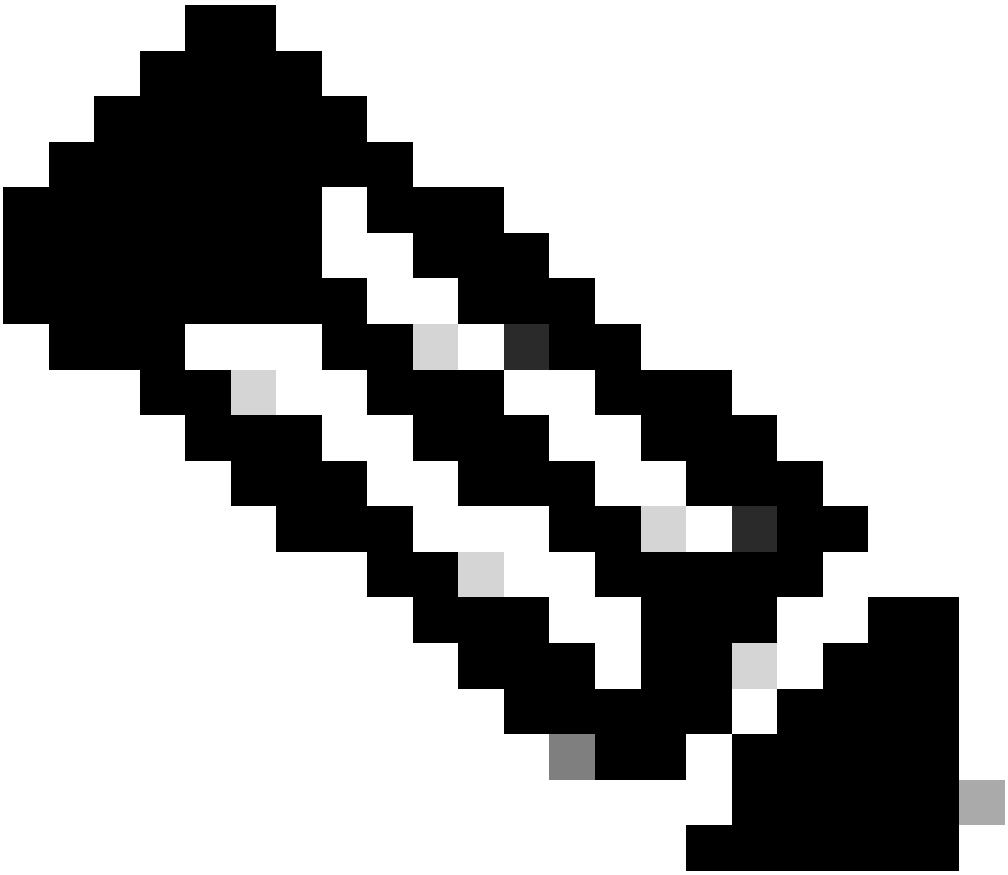
在DC之间复制登录事件时，请在任何标准域控制器上运行此命令。但是，如果在搜索时没有看到任何事件并且希望从特定主机看到这些事件，则复制服务器之间的事件日志可能会有问题。在此实例中，找出该主机使用的%LOGONSERVER%，然后在指定的域控制器上运行该脚本。如果仍然看不到任何事件，请确保正在审核登录事件。

脚本附加到本文的底部。收集到的信息既可用于自行排除故障，也可用于OpenDNS支持部门进行故障排除。

运行脚本

完成这些步骤：

1. 下载附加的文本文件并将扩展名从“.txt”重命名为“.ps1”。



注意：请注意双分机，不要不小心将其命名为“.txt.ps1”。

2. 然后，从Windows服务器打开由启动的新PowerShell窗**'Right-Click -->Run as Administrator'**口。导航到保存脚本的位置)**(eg: 'cd C:\Users\admin\Downloads'**并通过键入执行脚本 **.\loginsearch.ps1.**
3. 脚本首先提示您要在Windows安全事件日志中搜索的用户名，然后提示您特定IP地址（如果您希望按IP搜索）。使用屏幕提示。如果要将搜索结果同时限制到特定的用户和IP地址，可以单独使用其中一种搜索或其它（用户名或IP）搜索，也可以同时使用这两种搜索。
4. 脚本可以快速运行。完成后，您将在屏幕上看到两个输出，其中包含时间戳。另外完成导出屏幕上显示的每个事件日志项**'C:\%hostname%.txt'**。如果您想进一步深入挖掘特定事件，这会非常有用。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。