使用Loginsearch.ps1搜尋登入事件

目錄

簡介

本文檔介紹如何使用PowerShell指令碼Loginsearch.ps1搜尋登入事件。

背景資訊

Loginsearch.ps1是一個小型PowerShell指令碼，用於收集對Umbrella支援有用的資訊以進行故障排除。在排除某些使用者未在OpenDNS Umbrella控制板上的報告或活動搜尋中顯示正確活動的原因時，此命令非常有用，但也可用於排除其他型別的問題。

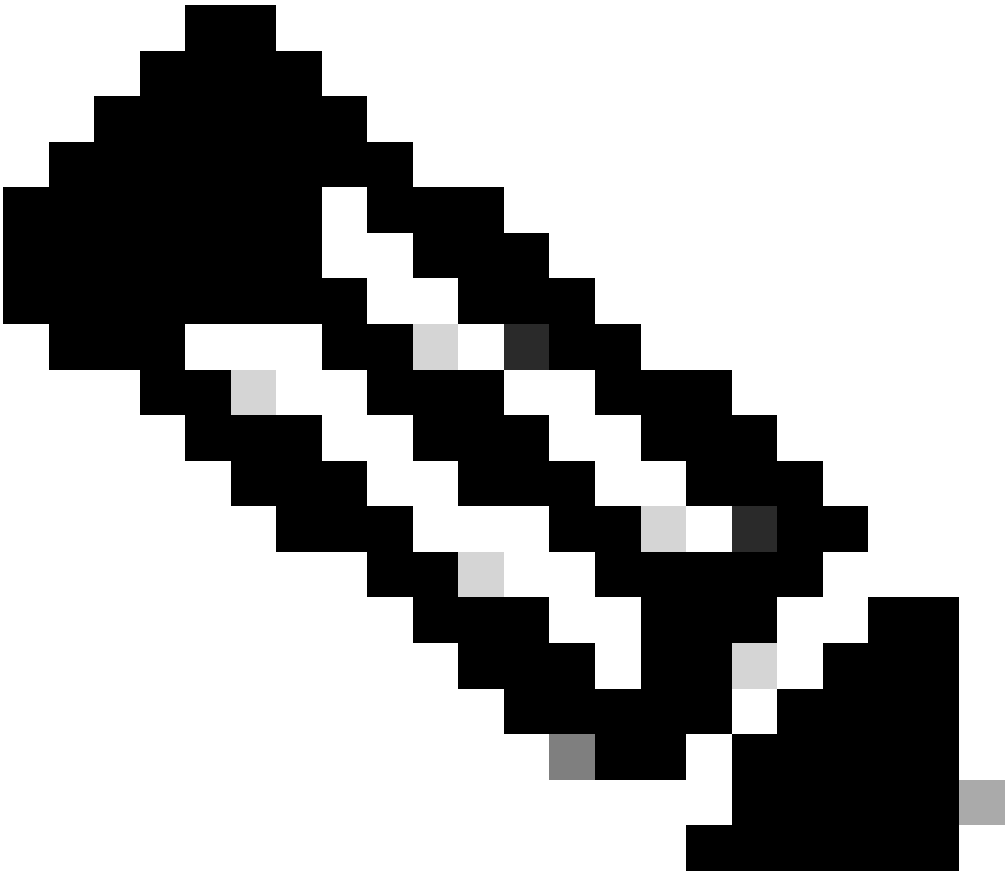
在DC之間複製登入事件時，在任何標準域控制器上運行此命令。但是，如果在搜尋時沒有看到任何事件並且希望從特定主機看到它們，則復制伺服器之間的事件日誌可能會出現問題。在此例項中，找出該主機使用的%LOGONSERVER%，然後在指定的域控制器上運行該指令碼。如果仍然看不到任何事件，請確保正在稽核登入事件。

指令碼附在本文的底部。所收集的資訊可用於自行進行故障排除，也可由OpenDNS支援進行故障排除。

運行指令碼

請完成以下步驟：

1. 下載附加的文本檔案，並將副檔名從「.txt」重新命名為「.ps1」。



附註：請注意雙分機，不要不小心將其命名為「.txt.ps1」。

2. 然後，從Windows伺服器開啟由啟動的新PowerShell窗**'Right-Click -->Run as Administrator'**口。導航到將指令碼儲存到的位置)**(eg: 'cd C:\Users\admin\Downloads'**並通過鍵入執行指令碼 **.\loginsearch.ps1.**
3. 指令碼首先提示您在Windows安全事件日誌中搜尋的使用者名稱，然後提示您輸入特定IP地址（如果您希望按IP搜尋）。使用螢幕提示。如果要將搜尋結果限製為同時具有特定的使用者和IP地址，可以單獨使用其中一種搜尋或其它（使用者名稱或IP）搜尋，也可以同時使用這兩種搜尋。
4. 指令碼可以快速運行。完成後，您將在螢幕上看到兩個輸出，其中包含時間戳。另外完成匯出螢幕上顯示的每個事件日誌條目。如果您想進一步深入挖掘特定事件**'C:\%hostname%.txt'**，這樣做很有用。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。