收集Windows客戶端和伺服器作業系統上的資料包捕獲

目錄

簡介

本文檔介紹如何在高度安全的客戶環境中使用Windows pktmon實用程式在Windows平台上收集資料包捕獲。例如，銀行、國防、海軍等。

問題

高度安全的政府環境（如銀行、國防、海軍等）會限制安裝第三方工具。尤其是資料包捕獲工具Wireshark，用於排除語音、影片和資料資料包的故障。變更管理核准會消耗時間，並且會在解決問題時造成不必要的延遲。Windows預設提供的公用程式可協助避免延遲。

解決方案

預設情況下，工具名稱PKTMON是隨Microsoft Windows客戶端和伺服器作業系統捆綁提供的預設資料包代碼段實用程式。PKTMON可用於Windows Server 2022、Windows Server 2019、Windows 10、Azure Stack HCI、Azure Stack Hub和Azure。 設定非常容易且耗時較少。該實用程式使用具有管理員許可權的Windows命令提示符(cmd)實用程式運行。

可執行檔目錄： C:\Windows\System32\PktMon.exe

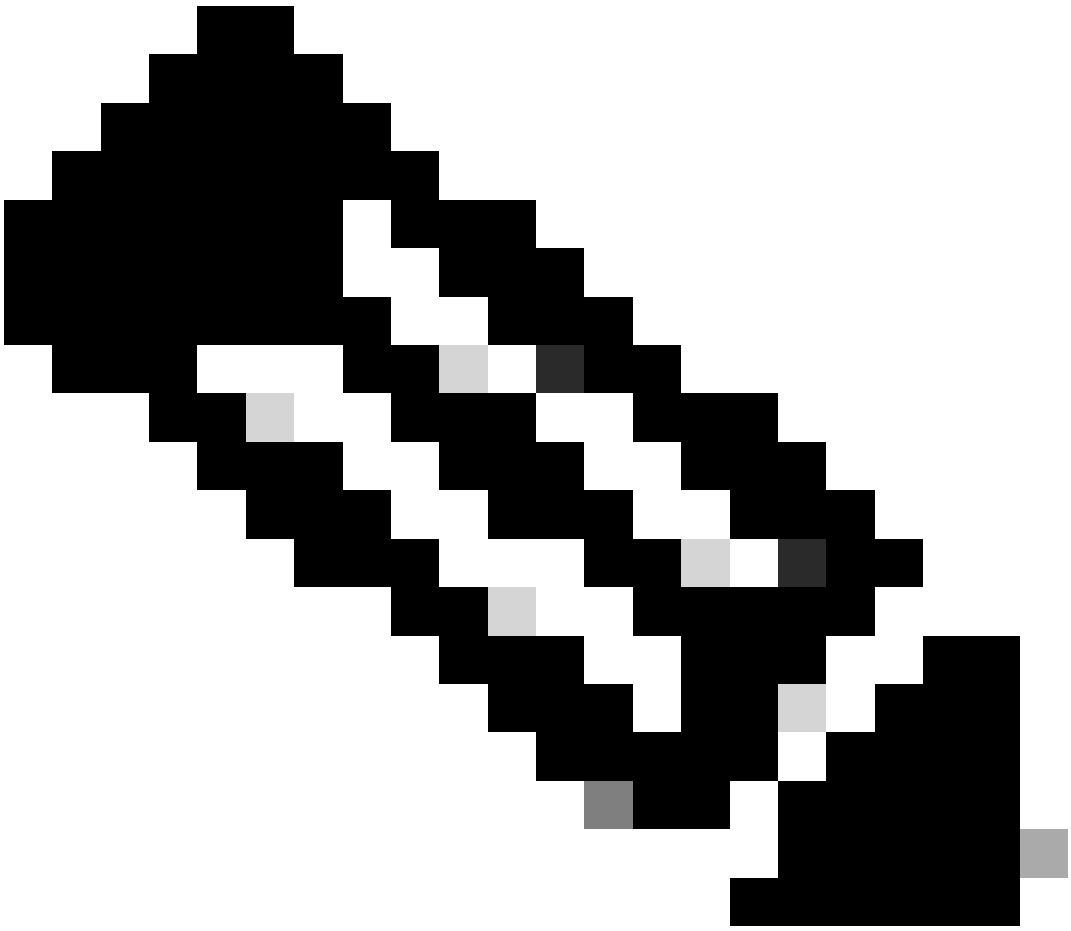
此處假設在System-1 (PG-A)和System-2 (Logger-A)之間跟蹤資料包捕獲。

您必須先辨識系統/虛擬機器器上的介面ID或網路介面控制器或卡(NIC) ID。

pktmon list - 此命令列出系統/虛擬機器上的介面。

輸出：

Network Adapters:
Id MAC Address Name
-- ----------- ----
9 00-50-56-BD-C1-83 vmxnet3 Ethernet Adapter #2
10 00-50-56-BD-82-7B vmxnet3 Ethernet Adapter



注意：如需協助，請使用命令結尾的字尾說明。也就是說，pktmon list 幫助。

表 1. 介面表。

一旦辨識出介面ID，資料包捕獲就會開始。該命令啟用資料包捕獲和資料包計數器。

方法1. pktmon start --capture

此命令開始捕獲預設Windows登入使用者路徑上的資料包。

輸出：

Logger Parameters:
Logger name: PktMon
Logging mode: Circular
Log file: C:\Users\Administrator\PktMon.etl
Max file size: 512 MB
Memory used: 64 MB

Collected Data:
Packet counters, packet capture

Capture Type:
    All packets

Monitored Components:
    All

Packet Filters:
    None

表2. 資料包捕獲開始指示。

方法2. pktmon start --capture --file-name C:\Cisco\Campaigninactive\pga.etl

此命令開始在自定義路徑上捕獲資料包。

輸出：

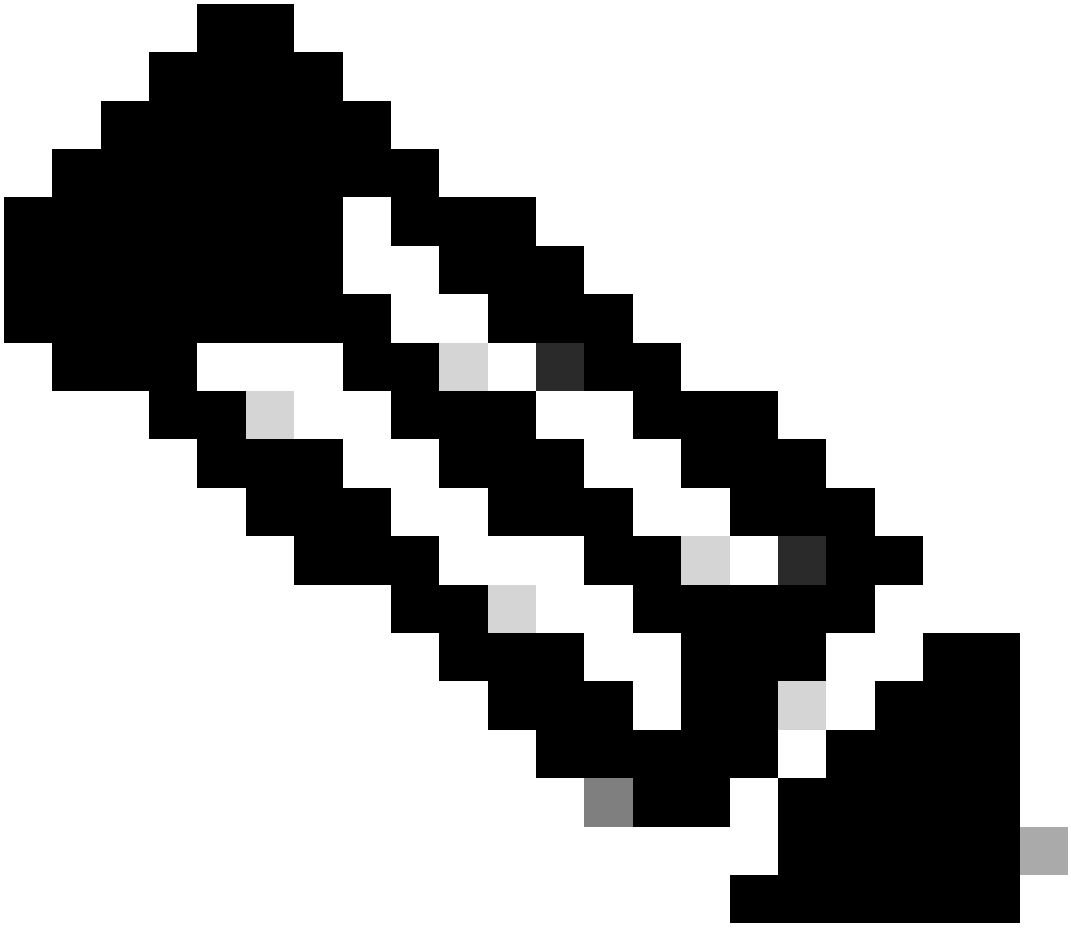
Logger Parameters:
Logger name: PktMon
Logging mode: Circular
Log file: C:\Cisco\Campaigninactive\pga.etl
Max file size: 512 MB
Memory used: 64 MB

Collected Data:
Packet counters, packet capture

Capture Type:
All packets

Monitored Components:
All

Packet Filters:
None



注意：預設情況下，它會捕獲所有介面和所有資料包型別。

表3. 包含路徑位址的封包擷取，以便儲存擷取檔案。

在捕獲過程中，還可以驗證資料包捕獲狀態。

pktmon status- 此命令顯示正在進行的活動**pktmon**執行的資料包捕獲。

輸出：

Collected Data:

Packet counters, packet capture

Capture Type:
All packets

Monitored Components:
All

Packet Filters:
None

Logger Parameters:
Logger name: PktMon
Logging mode: Circular
Log file: C:\Cisco\Campaigninactive\pga_1.etl
Max file size: 512 MB
Memory used: 64 MB
Events lost: 0

Event Providers:

ID	Level	Keywords
Microsoft-Windows-PktMon	4	0x12

C:\Users\Administrator>

表4. 驗證資料包捕獲的狀態。

一旦重現問題，請使用pktmon stop命令停止資料包捕獲。

輸出：

Flushing logs...
Merging metadata...

Log file: C:\Cisco\Campaigninactive\pga.etl (No events lost)

表5. 停止資料包捕獲。

預設情況下，**pktmon**以預設.etl格式儲存，可以透過將其轉換為pcapng以便使用Wireshark進行檢視。

方法1. pktmon etl2pcap PktMon.etl --out C:\Cisco\Campaigninactive\pga.pcapng

此指令會將儲存在PktMon.etl預設目錄檔案中的預設值轉換為**pcapng**格式。

輸出：

C:\Users\Administrator>pktmon etl2pcap PktMon.etl --out C:\Cisco\Campaigninactive\pga_2.pcapng

Processing...

Packets total: 606
Packet drop count: 0
Packets formatted: 606
Formatted file: C:\Cisco\Campaigninactive\pga_2.pcapng

C:\Users\Administrator>

表6.

方法1.將資料包捕獲從本地擴展**.etl**轉換為**.pcapng**的Wireshark可讀格式。

方法2. pktmonetl2pcapC:\Cisco\Campaigninactive\pga_1.etl --out C:\Cisco\Campaigninactive\pga.pcapng

輸出：

C:\Users\Administrator>pktmon etl2pcap C:\Cisco\Campaigninactive\pga_1.etl --out C:\Cisco\Campaigninactive\pga_1.pcapng
Processing...

Packets total: 8964
Packet drop count: 0
Packets formatted: 8964
Formatted file: C:\Cisco\Campaigninactive\pga_1.pcapng

C:\Users\Administrator>

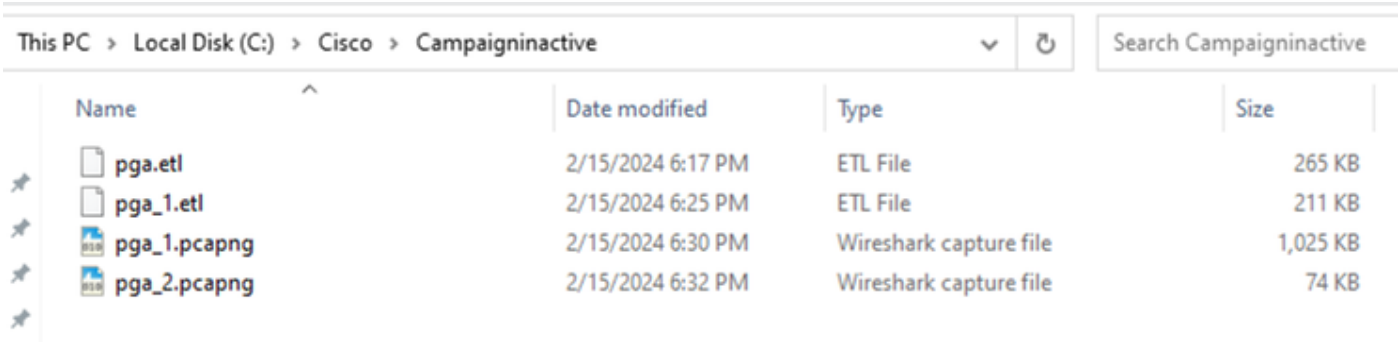


圖1.

方法2.將資料包捕獲從本地擴展**.etl**轉換為Wireshark可讀格式**.pcapng**。

這些基本命令有助於收集檔案，並且有助於對TAC進行故障排除。

相關資訊

- https://learn.microsoft.com/en-us/windows-server/networking/technologies/pktmon/pktmon

- 思科技術支援與下載

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）。