Windowsクライアントおよびサーバ OSでのパケットキャプチャの収集

内容

はじめに

このドキュメントでは、高度にセキュリティ保護された顧客環境でWindows pktmonユーティリティを使用して、Windowsプラットフォームでパケットキャプチャを収集する方法について説明します。たとえば、銀行、防衛、海軍などです。

問題

銀行、防衛、海軍など、高度にセキュリティ保護された政府環境では、サードパーティ製ツールのインストールが制限されます。特に、音声、ビデオ、およびデータパケットのトラブルシューティングに使用するパケットキャプチャツールWiresharkは、変更管理の承認には時間がかかり、問題の解決に不必要な遅延が生じます。Windowsでデフォルトで利用可能なユーティリティは、遅延を回避するのに役立ちます。

解決方法

デフォルトでは、ツール名PKTMONは、Microsoft Windowsクライアントおよびサーバオペレーティングシステムにバンドルされている、デフォルトのパケットスニペットユーティリティです。PKTMONは、Windows Server 2022、Windows Server 2019、Windows 10、Azure Stack HCI、Azure Stack Hub、およびAzureで利用できます。 セットアップは非常に簡単で、時間もかかりません。このユーティリティは、管理者権限でWindowsコマンドプロンプト(cmd)ユーティリティを使用して実行します。

実行可能ディレクトリ： C:\Windows\System32\PktMon.exe

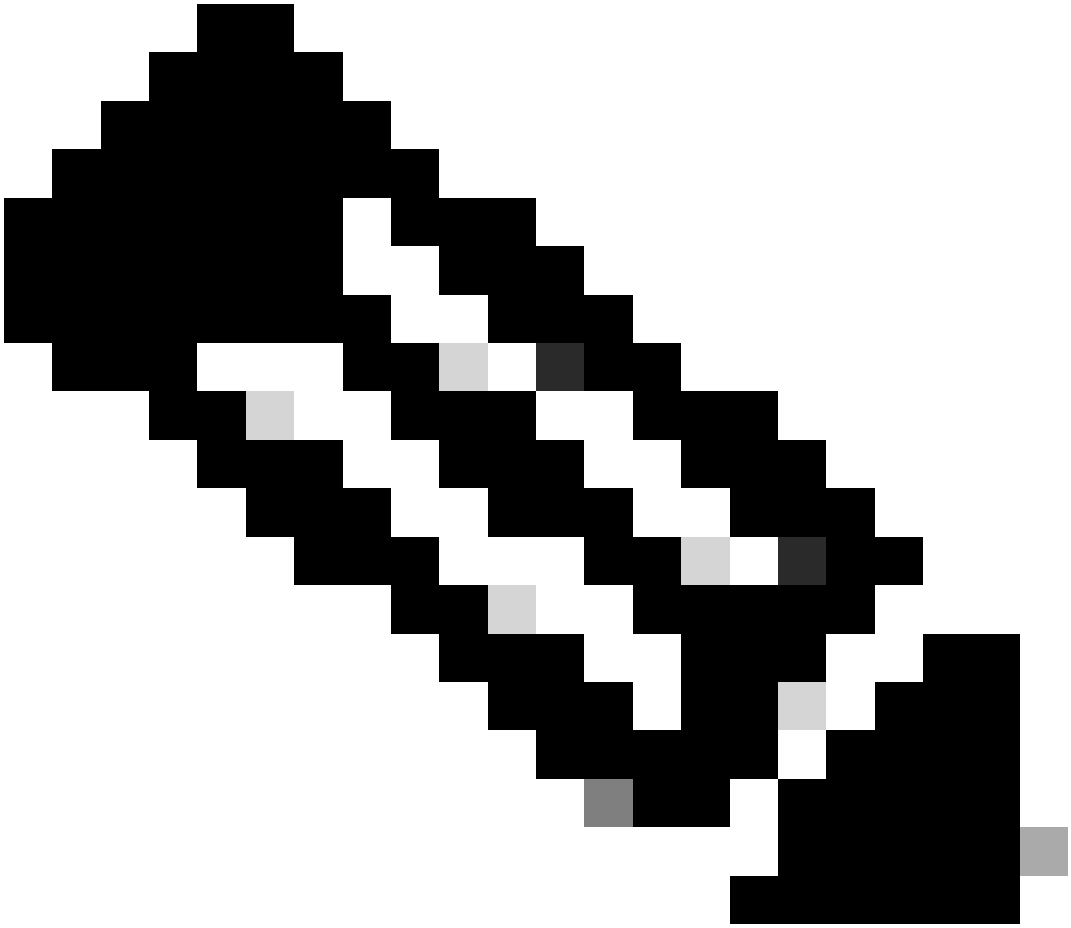
ここでは、System-1(PG-A)とSystem-2(Logger-A)間のパケットキャプチャをトレースすることを想定しています。

最初に、システム/仮想マシンのインターフェイスID、ネットワークインターフェイスコントローラ(NIC)、またはカード(NIC)IDを特定する必要があります。

pktmon list – このコマンドは、システム/仮想マシンのインターフェイスを一覧表示します。

出力：

```
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：ヘルプを表示するには、コマンドの最後に接尾辞helpを使用します。つまり、pktmon list ヘルプです。

表 1. インターフェイステーブル

インターフェイスIDが特定されると、パケットキャプチャが開始されます。このコマンドにより、パケットキャプチャとパケットカウンタがイネーブルになります。

方式 1. pktmon start --capture

このコマンドは、デフォルトのWindowsログインユーザパスでパケットのキャプチャを開始します。

出力：

```
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 パケットキャプチャの開始指示。

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

このコマンドは、カスタム定義パスでパケットのキャプチャを開始します。

出力：

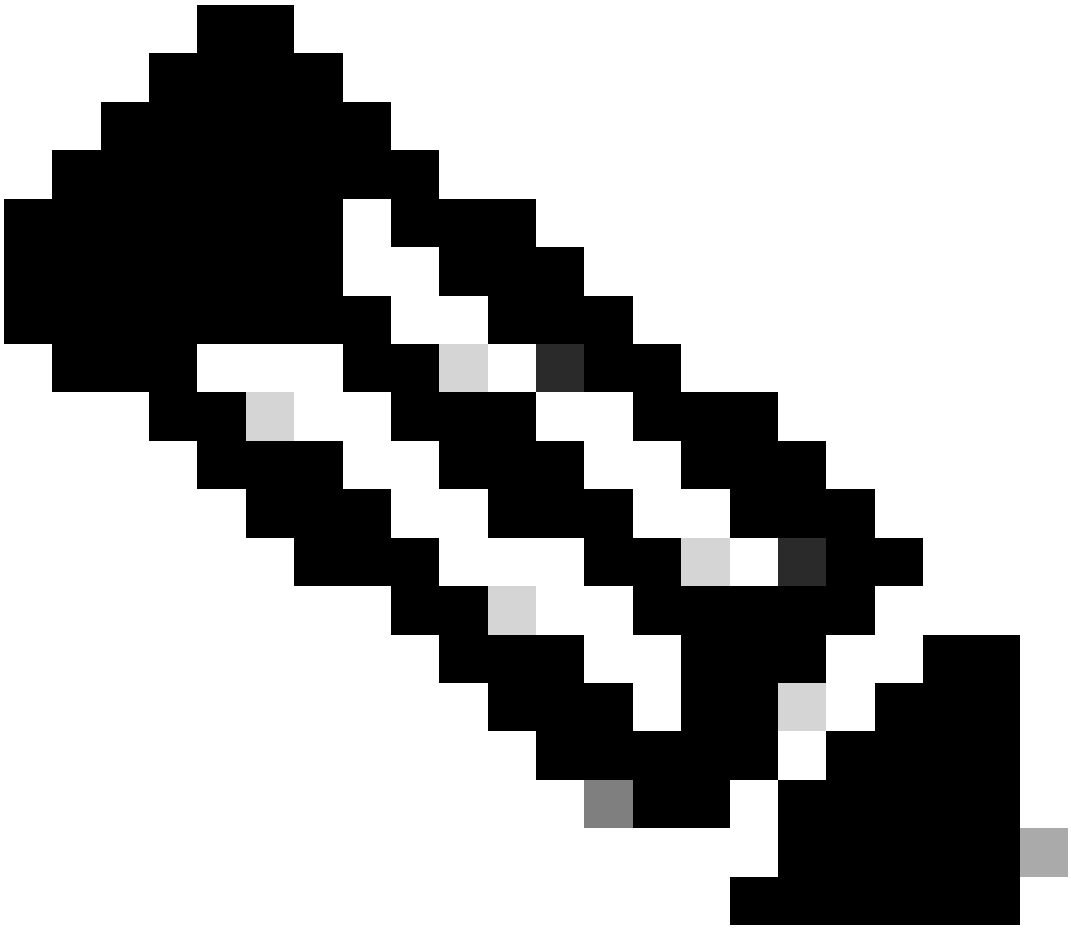
```
Logger Parameters:
Logger name: PktMon
Logging mode: Circular
Log file: C:\Cisco\Campaigninactive\pga.etl
Max file size: 512 MB
Memory used: 64 MB

Collected Data:
Packet counters, packet capture

Capture Type:
All packets

Monitored Components:
All
```

Packet Filters:
None



注：デフォルトでは、すべてのインターフェイスとすべてのパケットタイプをキャプチャします。

表 3 キャプチャファイルを保存するためのパスアドレスを使用したパケットキャプチャ。

キャプチャの途中で、パケットキャプチャのステータスも検証できます。

pktmon status – このコマンドは、実行中のアクティブな**pktmon**によるパケットキャプチャの実行を表示します。

出力：

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 パケットキャプチャのステータスを検証します。

問題が再現したら、pktmon stopコマンドでパケットキャプチャを停止します。

出力：

Flushing logs...
Merging metadata...

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

表 5 パケットキャプチャを停止します。

デフォルトでは、**pktmon**はデフォルトの.etl形式で保存されますが、Wiresharkを使用して確認するために**pcapng**に変換する方法があります。

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

このコマンドは、PktMon.etlファイルのデフォルトディレクトリに保存されているデフォルトを**pcapng**形式に変換します。

出力：

```
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

方式 1.パケットキャプチャをネイティブの拡張子**.etl**からWiresharkで読み取り可能な形式**.pcapng**に変換します。

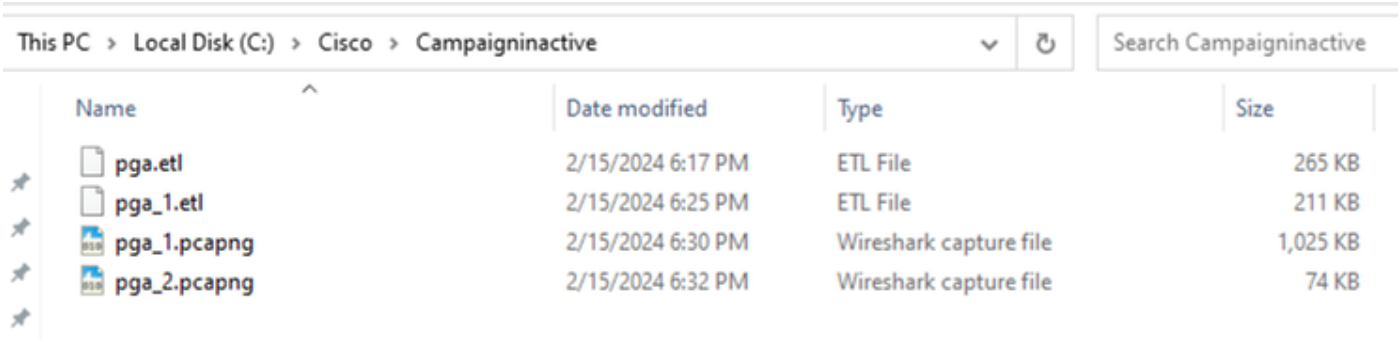
方式 2. pktmonetl2pcapC:\Cisco\Campaigninactive\pga_1.etl --out C:\Cisco\Campaigninactive\pga.pcapng

出力：

```
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>
```



画像 1.

方法2：パケットキャプチャをネイティブの拡張**.etl**からWiresharkで読み取り可能な形式**.pcapng**に変換する

これらの基本的なコマンドは、ファイルの収集に役立ち、TACのトラブルシューティングに役立ちます。

関連情報

- https://learn.microsoft.com/en-us/windows-server/networking/technologies/pktmon/pktmon
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。