

Sammeln von Paketerfassungen auf Windows-Client- und Server-Betriebssystemen

Inhalt

[Einleitung](#)

[Problem](#)

[Lösung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie die Paketerfassung auf der Windows-Plattform mit dem Windows-Dienstprogramm pktmon in einer hochgradig sicheren Kundenumgebung gesammelt wird. Bank-, Verteidigungs-, Marine- und andere Bereiche.

Problem

Hochgradig sichere Umgebungen für Behörden (Banken, Verteidigung, Marine usw.) verhindern die Installation von Drittanbieter-Tools. Insbesondere das Paketerfassungs-Tool Wireshark zur Fehlerbehebung bei Sprach-, Video- und Datenpaketen. Genehmigungen für das Änderungsmanagement erfordern einen hohen Zeitaufwand und unnötige Verzögerungen bei der Problemlösung. Das standardmäßig in Windows verfügbare Dienstprogramm kann helfen, die Verzögerung zu vermeiden.

Lösung

Standardmäßig ist der Toolname PKTMON ein standardmäßiges Paket-Snippet-Dienstprogramm, das mit Microsoft Windows-Client- und Server-Betriebssystemen gebündelt ist. PKTMON ist unter Windows Server 2022, Windows Server 2019, Windows 10, Azure Stack HCI, Azure Stack Hub und Azure verfügbar. Die Einrichtung ist sehr einfach und zeitsparend. Das Dienstprogramm wird mit dem Windows-Befehlszeilendienstprogramm (cmd) mit Administratorberechtigungen ausgeführt.

Ausführbares Verzeichnis: `C:\Windows\System32\PktMon.exe`

Hier wird davon ausgegangen, dass die Paketerfassung zwischen System-1 (PG-A) und System-2 (Logger-A) nachverfolgt wird.

Sie müssen zuerst die Schnittstellen-ID oder die Netzwerkschnittstellen-Controller- oder Karten-ID (NIC) auf dem System/virtuellen System identifizieren.

pktmon list - Dieser Befehl listet die Schnittstellen auf dem System/der virtuellen Maschine auf.

Ausgabe:

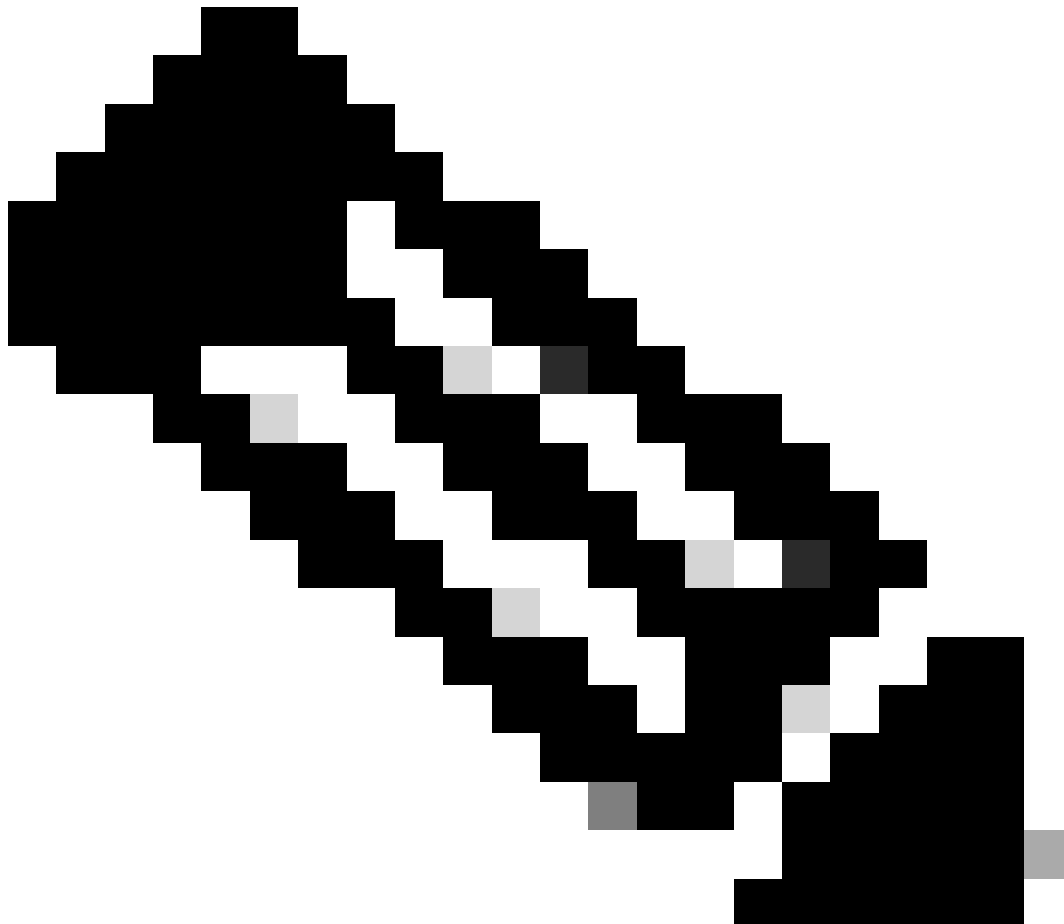
Network Adapters:

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



Hinweis: Verwenden Sie für Hilfe das Suffix help am Ende des Befehls. Das heißt, pktmon list Hilfe.

Sobald die Schnittstellen-ID identifiziert ist, beginnt die Paketerfassung. Der Befehl aktiviert die Paketerfassung und die Paketzähler.

Methode 1: pktmon start --capture

Mit diesem Befehl werden die Pakete auf dem Windows-Standardpfad für angemeldete Benutzer erfasst.

Ausgabe:

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

Tabelle 2. Startanzeige für die Paketerfassung.

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

Mit diesem Befehl werden die Pakete über den benutzerdefinierten Pfad erfasst.

Ausgabe:

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

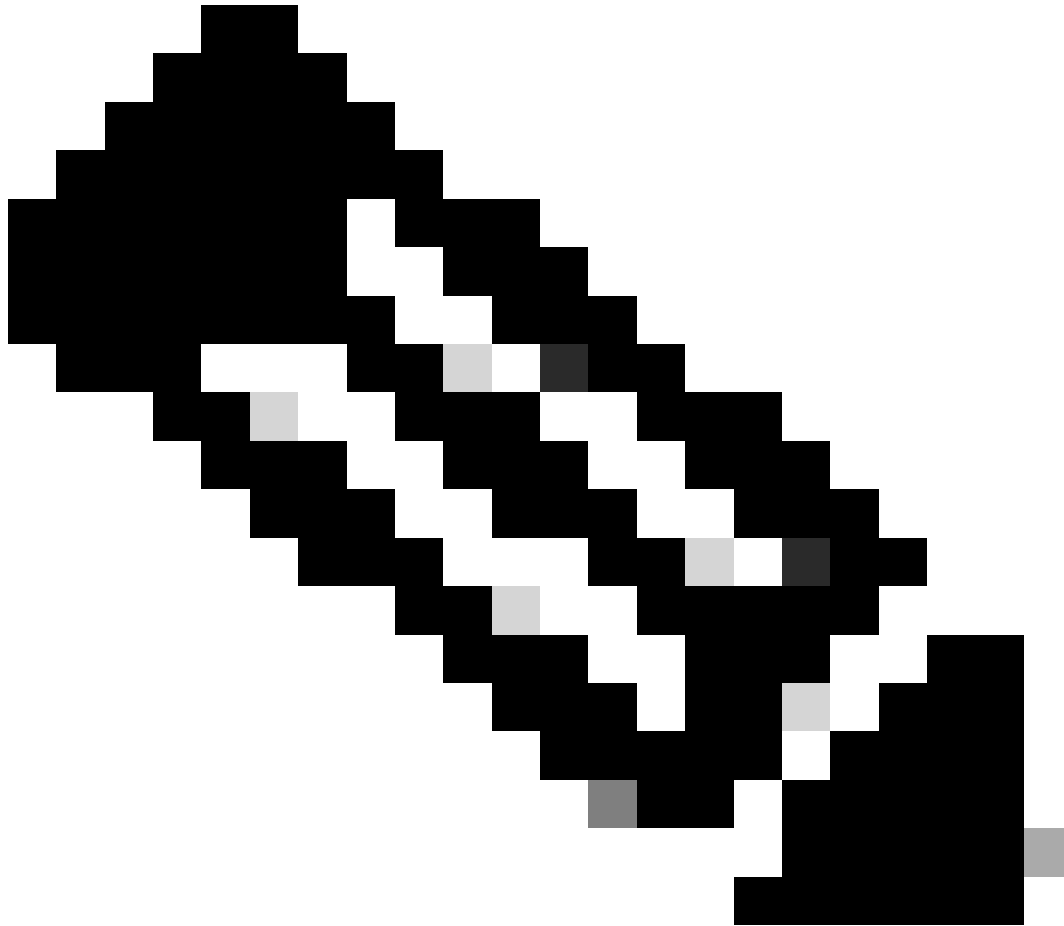
Capture Type:

All packets

Monitored Components:

All

Packet Filters:
None



Hinweis: Standardmäßig werden alle Schnittstellen und Pakettypen erfasst.

Tabelle 3. Paketerfassung mit Pfadadresse zum Speichern der Erfassungsdatei.

Während der Erfassung kann auch der Paketerfassungstatus validiert werden.

pktmon status- Dieser Befehl zeigt die laufende aktive Paketerfassung von **pktmon** an.

Ausgabe:

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>

Tabelle 4. Validiert den Status der Paketerfassung.

Sobald das Problem reproduziert wurde, stoppen Sie die Paketerfassung mit dem pktmon stop Befehl.

Ausgabe:

Flushing logs...

Merging metadata...

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

Tabelle 5. Beenden Sie die Paketerfassung.

pktmon speichert standardmäßig im Standardformat .etl und es gibt eine Möglichkeit, es in **pcapng** zu konvertieren, um Wireshark zu verwenden.

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

Mit diesem Befehl wird die Standarddatei, die im Standardverzeichnis gespeichert ist, in das **pcapng**-Format konvertiert PktMon.etl.

Ausgabe:

```
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>
```

Tabelle 6.

Methode 1: So konvertieren Sie die Paketerfassung von der nativen Erweiterung **.etl** in das für Wireshark lesbare Format **.pcapng**.

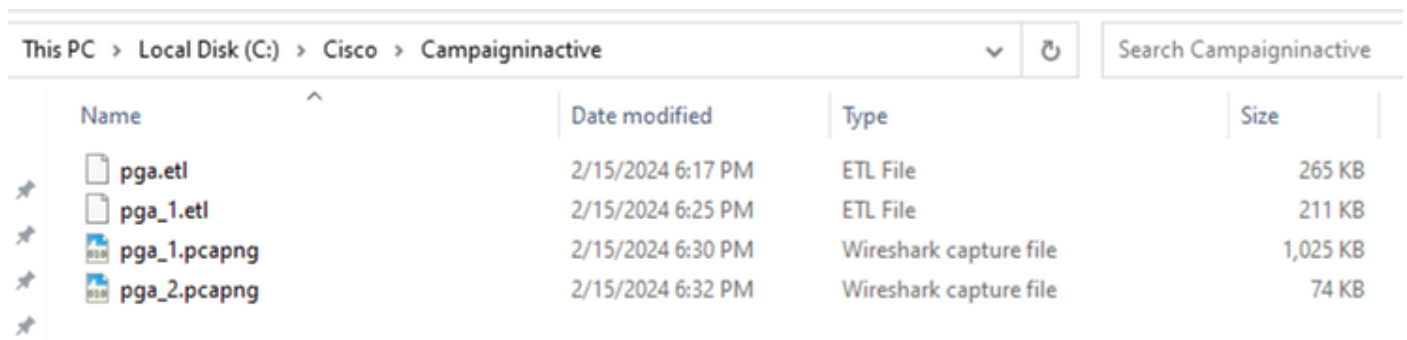
```
Methode 2. pktmonetl2pcap C:\Cisco\Campaigninactive\pga_1.etl --out C:\Cisco\Campaigninactive\pga.pcapng
```

Ausgabe:

```
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>
```



Name	Date modified	Type	Size
pga.etl	2/15/2024 6:17 PM	ETL File	265 KB
pga_1.etl	2/15/2024 6:25 PM	ETL File	211 KB
pga_1.pcapng	2/15/2024 6:30 PM	Wireshark capture file	1,025 KB
pga_2.pcapng	2/15/2024 6:32 PM	Wireshark capture file	74 KB

Bild 1.

Methode 2. zum Konvertieren der Paketerfassung von der nativen Erweiterung **.etl** in das Wireshark-lesbare Format **.pcapng**.

Diese einfachen Befehle helfen beim Sammeln der Dateien und sind bei der Fehlerbehebung für das TAC hilfreich.

Zugehörige Informationen

- <https://learn.microsoft.com/en-us/windows-server/networking/technologies/pktmon/pktmon>
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.