

Verzamel pakketvastlegging op Windows-client en -serverbesturingssysteem

Inhoud

[Inleiding](#)

[Probleem](#)

[Oplossing](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe pakketopnamen op het Windows-platform moeten worden verzameld met behulp van het Windows pktmon-hulpprogramma in een sterk beveiligde klantomgeving. Bijvoorbeeld, het bankwezen, de defensie, de marine, en meer.

Probleem

Sterk beveiligde overheidsomgeving, zoals banken, defensie, marine en meer, beperken het installeren van tools van derden. Vooral, het pakketopnamegereedschap Wireshark om spraak-, video- en gegevenspakketten problemen op te lossen. Goedkeuringen voor wijzigingsbeheer gaan gepaard met tijdsverbruik en onnodige vertragingen bij het oplossen van een probleem. Het hulpprogramma dat standaard beschikbaar is in Windows kan vertragingen voorkomen.

Oplossing

Standaard is de gereedschapsnaam PKTMON een standaard pakketfragmenthulpprogramma dat is gebundeld met Microsoft Windows-client- en serverbesturingssystemen. PKTMON is beschikbaar op Windows Server 2022, Windows Server 2019, Windows 10, Azure Stack HCI, Azure Stack Hub en Azure. Installatie is zeer eenvoudig en minder tijdrovend. Het hulpprogramma wordt uitgevoerd met de Windows-opdrachtprompt (cmd) met beheerdersrechten.

Uitvoerbare map: `C:\Windows\System32\PktMon.exe`

Hier wordt aangenomen dat het pakket wordt opgenomen tussen systeem-1 (PG-A) en systeem-2 (Logger-A).

U moet eerst de interface-ID of de Network Interface Controller of Card (NIC)-ID op het systeem/de virtuele machine identificeren.

pktmon list - Deze opdracht geeft een lijst van de interfaces op het systeem/de virtuele machine.

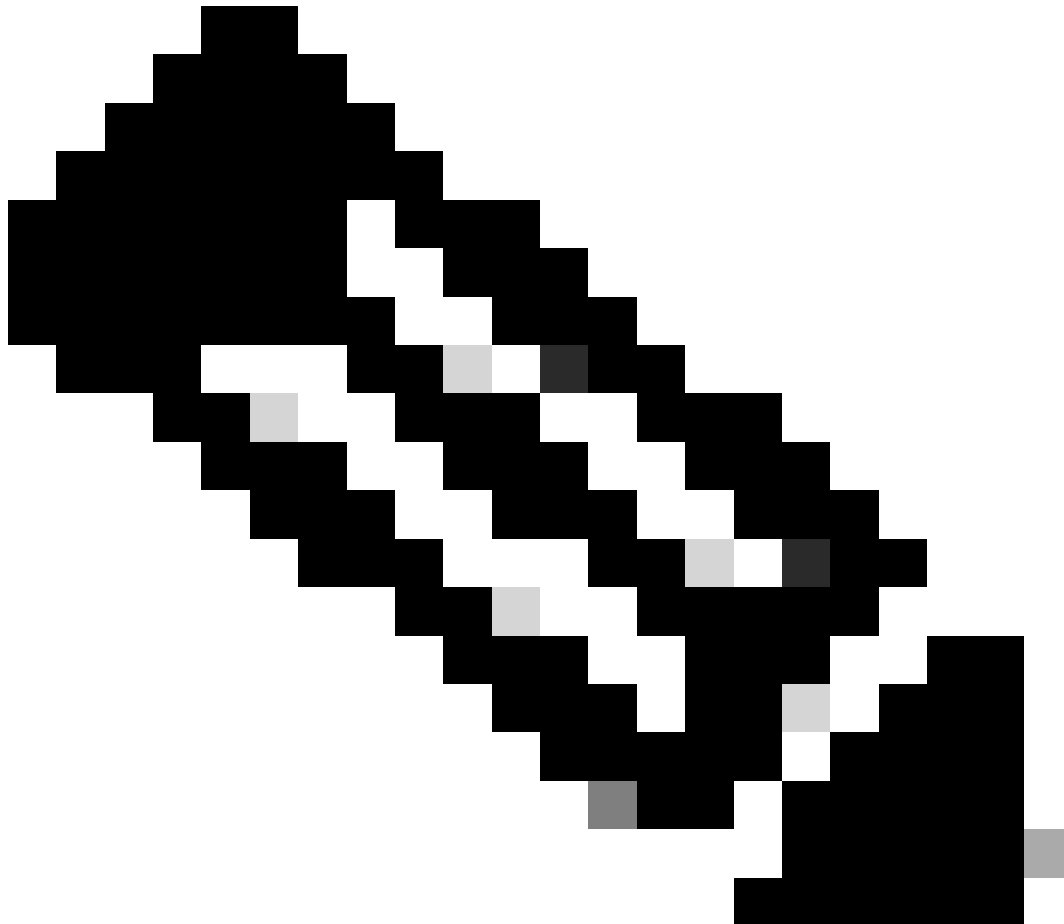
Uitvoer:

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



Opmerking: gebruik de achtervoegselhulp aan het einde van de opdracht als hulp. Dat wil zeggen, pktmon list hulp.

Tabel 1. Interfacetabellen.

Zodra de interface-ID is geïdentificeerd, wordt de pakketopname gestart. De opdracht schakelt de pakketopnamen en pakkettellers in.

Methode 1. pktmon start --capture

Deze opdracht begint met het opnemen van de pakketten op het standaard inlogpad van de Windows-gebruiker.

Uitvoer:

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

Tabel 2. Beginindicatie pakketvastlegging.

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

Deze opdracht begint met het opnemen van de pakketten op het op maat gedefinieerde pad.

Uitvoer:

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:

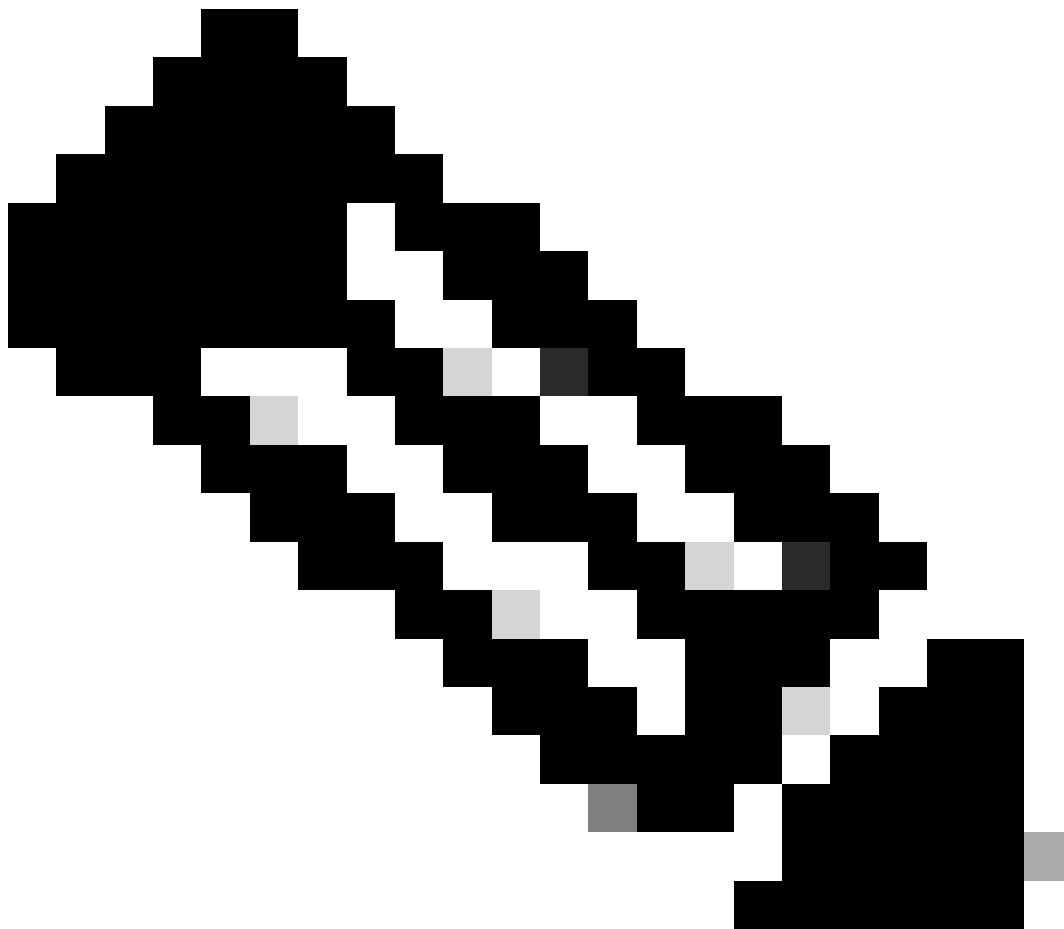
All packets

Monitored Components:

All

Packet Filters:

None



Opmerking: standaard worden alle interfaces en alle pakkettypen vastgelegd.

Tabel 3. Packet-opname met padadres om het opnamebestand op te slaan.

In het midden van de opname kan de pakketopnamestatus ook worden gevalideerd.

pktmon status- Deze opdracht geeft de lopende actieve **pktmon** uitgevoerde pakketopname weer.

Uitvoer:

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>

Tabel 4. Bevestig de status van pakketvastlegging.

Zodra de kwestie wordt gereproduceerd, stop het pakket met het pktmon stop bevel vangen.

Uitvoer:

Flushing logs...

Merging metadata...

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

Tabel 5. Stop de pakketopname.

Standaard slaat **pktmon** in het standaard .etl formaat op, en er is een manier om het om te zetten in **pcapng** om het gebruik van Wireshark te kunnen bekijken.

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

Met deze opdracht wordt de standaardinstelling die in het PktMon.etl bestand in de standaardmap is opgeslagen, geconverteerd naar de **paginanummer**.

Uitvoer:

```
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>
```

Tabel 6.

Methode 1. Om pakketopname van native extension **.nl** naar Wireshark readable formaat **.pcapng** om te zetten.

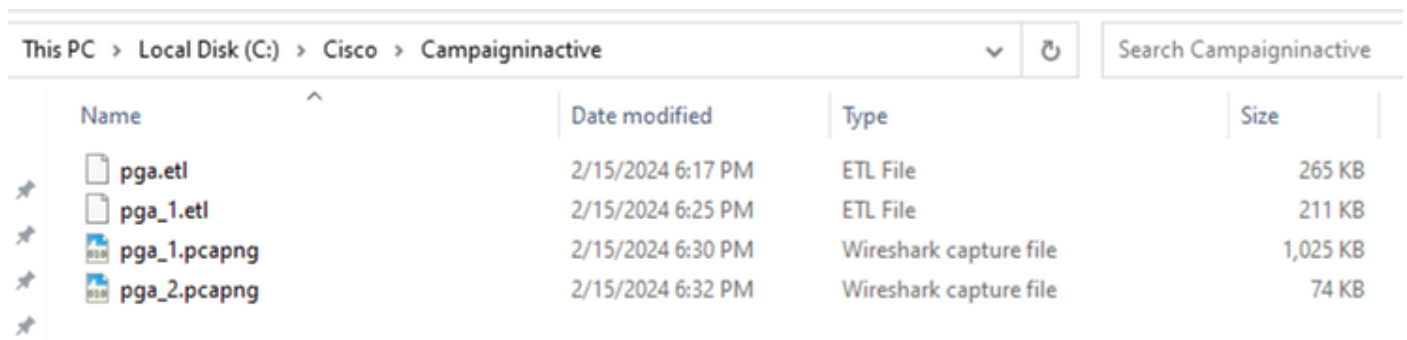
Methode 2. `pktmonetl2pcap C:\Cisco\Campaigninactive\pga_1.etl --out C:\Cisco\Campaigninactive\pga.pcapng`

Uitvoer:

```
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

Afbeelding 1.

Methode 2. om pakketopname van native extension **.nl** naar Wireshark readable formaat **.pcapng** om te zetten.

Deze basisopdrachten helpen bij het verzamelen van bestanden en zijn handig bij het oplossen van problemen voor TAC.

Gerelateerde informatie

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.