تجميع التقاط الحزم على عميل Windows ونظام تشغيل الخادم

المحتويات

المقدمة

يوضح هذا المستند كيفية تجميع التقاط الحزم على النظام الأساسي ل Windows باستخدام الأداة المساعدة Windows PKTMON في بيئة خاصة بالعملاء تتسم بقدر كبير من الأمان. على سبيل المثال، البنوك، والدفاع، والبحرية، وغير ذلك.

المشكلة

لمعظم البيئة الحكومية التي تتسم بقدر كبير من الأمان، مثل البنوك والدفاع والبحرية، وغير ذلك، على تقييد عملية تركيب أدوات الطرف الثالث. خصوصا، الربط أداة التقاط الحزم in order to تحريت الصوت، الفيديو، وحزم البيانات. تخضع الموافقات على إدارة التغيير للاستهلاك الوقت والتأخيرات غير الضرورية في حل إحدى المشكلات. يمكن أن تساعد الأداة المساعدة المتوفرة بشكل افتراضي مع Windows في تجنب التأخير.

الحل

بشكل افتراضي، اسم الأداة PKTMON هو أداة قصاصة ربط افتراضية يتم تجميعها مع عميل Microsoft Windows وأنظمة تشغيل الخادم. يتوفر PKTMON على Windows Server 2022 و Windows Server 2019 و Windows 10 و Azure Stack HCI و Azure Stack Hub و Azure. الإعداد المساعدة باستخدام الأداة المساعدة الأداة تشغيل يتم .لقأ اتقو كلهتسيو ةياغلل لهس المطالبة للأوامر في Windows (CMD) مع امتيازات المسؤول.

الدليل القابل للتنفيذ: C:\Windows\System32\PktMon.exe

هنا يفترض أن يتتبع التقاط الحزمة بين النظام 1 (PG-A) والنظام 2 (المسجل-A).

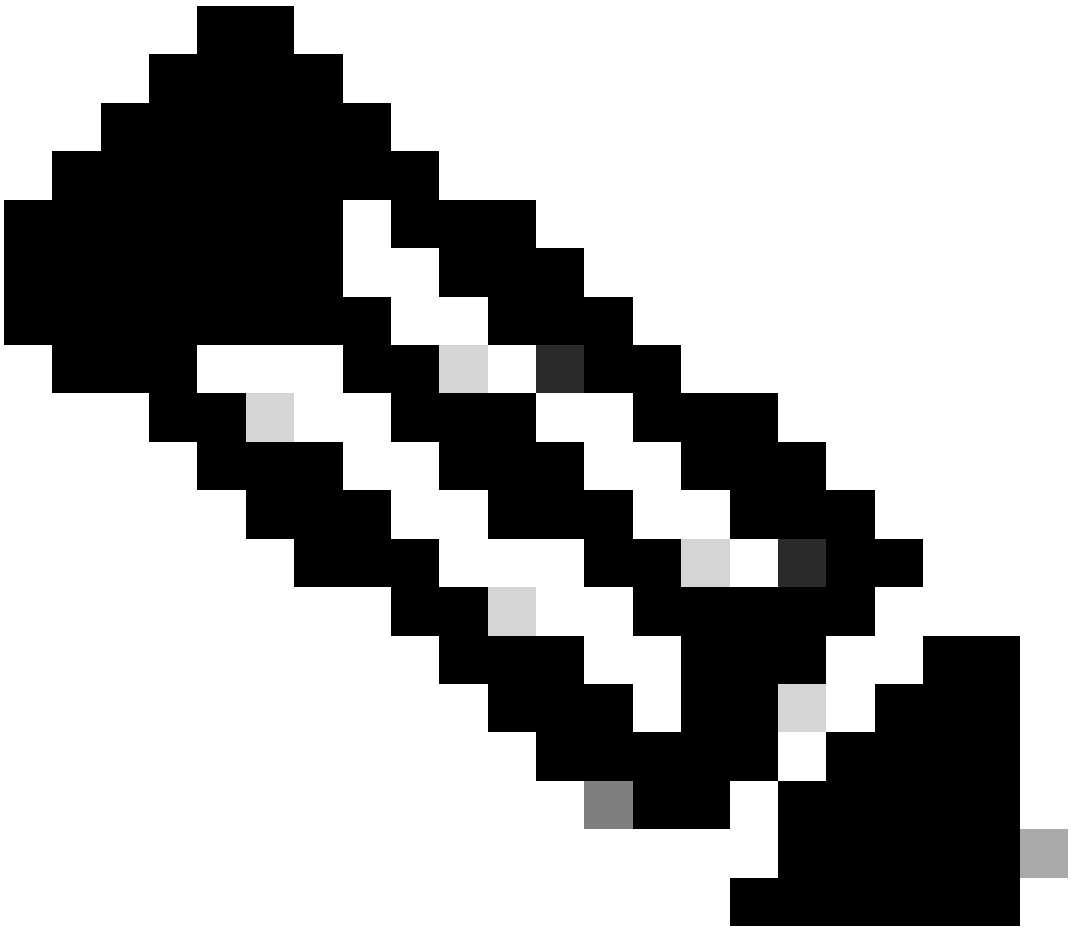
يجب عليك أولا تحديد معرف الواجهة أو معرف بطاقة (NIC) وحدة تحكم واجهة الشبكة أو معرف البطاقة على النظام/الجهاز الظاهري.

pktmon list - يسرد هذا الأمر الواجهات على النظام/الجهاز الظاهري.

الناتج:

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
```



ملاحظة: للحصول على تعليمات، أستخدم التعليمات اللاحقة في نهاية الأمر. هذه هي، pktmon list المساعدة.

الجدول 1. جداول الواجهة.

ما إن عينت القارن id، الربط يدأ التقاط. يتيح الأمر التقاط الحزمة وعدادات الحزم.

الطريقة 1. pktmon start --capture

يبدأ هذا الأمر في التقاط الحزم في مسار المستخدم الافتراضي الذي قام Windows بتسجيل الدخول إليه.

الناتج:

```
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
```

الجدول 2. مؤشر بدء التقاط الحزمة.

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

يبدأ هذا الأمر في التقاط الحزم في المسار المخصص المعرف.

الناتج:

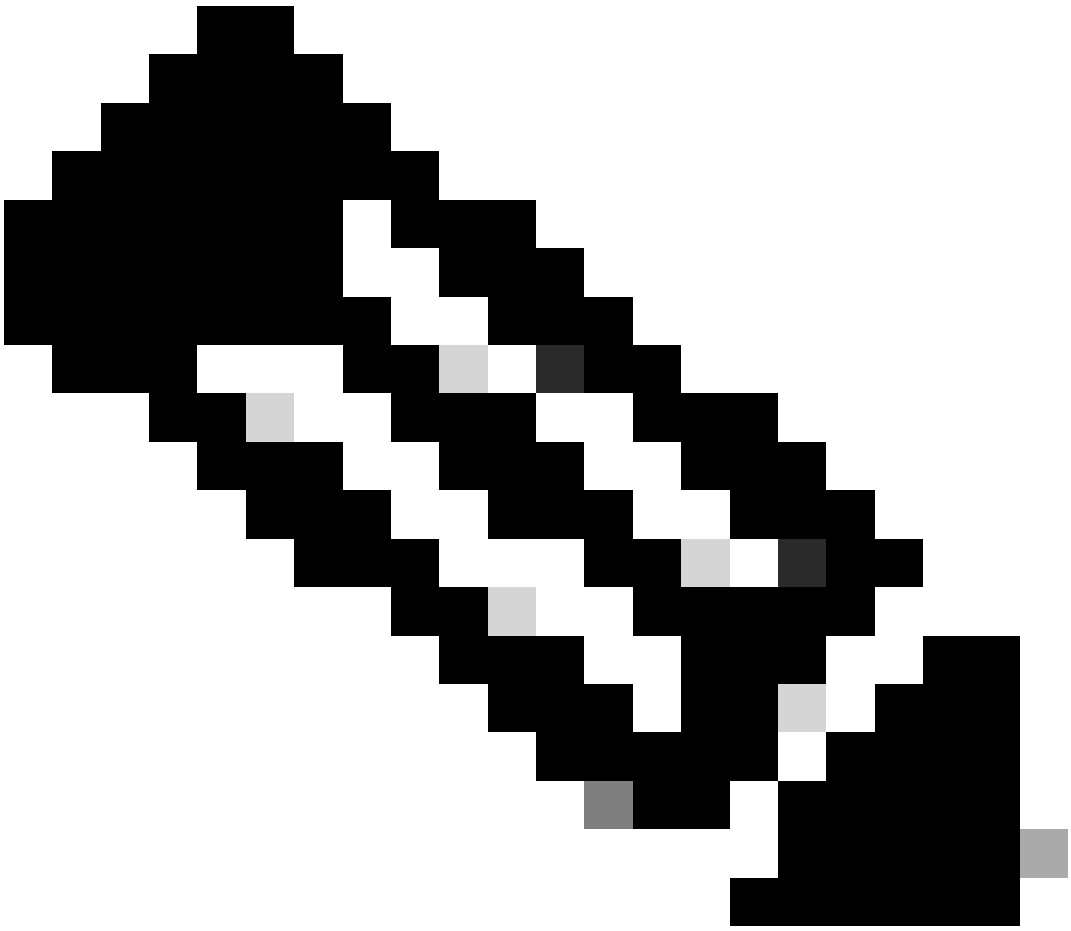
```
Logger Parameters:
Logger name: PktMon
Logging mode: Circular
Log file: C:\Cisco\Campaigninactive\pga.etl
Max file size: 512 MB
Memory used: 64 MB

Collected Data:
Packet counters, packet capture

Capture Type:
All packets

Monitored Components:
All

Packet Filters:
None
```



ملاحظة: بشكل افتراضي، يلتقط كل الواجهات وجميع أنواع الحزم.

الجدول 3. التقاط الحزمة باستخدام عنوان المسار لتخزين ملف الالتقاط.

في وسط الالتقاط، يمكن أيضا التحقق من حالة التقاط الحزمة.

pktmon status- يعرض هذا الأمر التقاط الحزمة الجاري تنفيذها بواسطة PKTMON.

الناتج:

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>

الجدول 4. التحقق من حالة التقاط الحزمة.

ام إن استنسخت الإصدار، أوقف الربط التقاط مع pktmon stop الأمر.

الناتج:

Flushing logs...
Merging metadata...

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

الجدول 5. إيقاف التقاط الحزمة.

بشكل افتراضي، يتم تخزين **PKTMON** بالتنسيق الافتراضي .etl وهناك طريقة لتحويله إلى **PCAPNG** للرجوع باستخدام Wireshark.

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

يحول هذا الأمر الإعداد الافتراضي المحفوظ في PktMon.etl الملف في الدليل الافتراضي إلى تنسيق **PCAPNG**.

الناتج:

```
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>
```

الجدول 6.

الطريقة 1. لتحويل التقاط الحزم من extension **.etl** الأصلي إلى تنسيق Wireshark القابل للقراءة **.pcapng**.

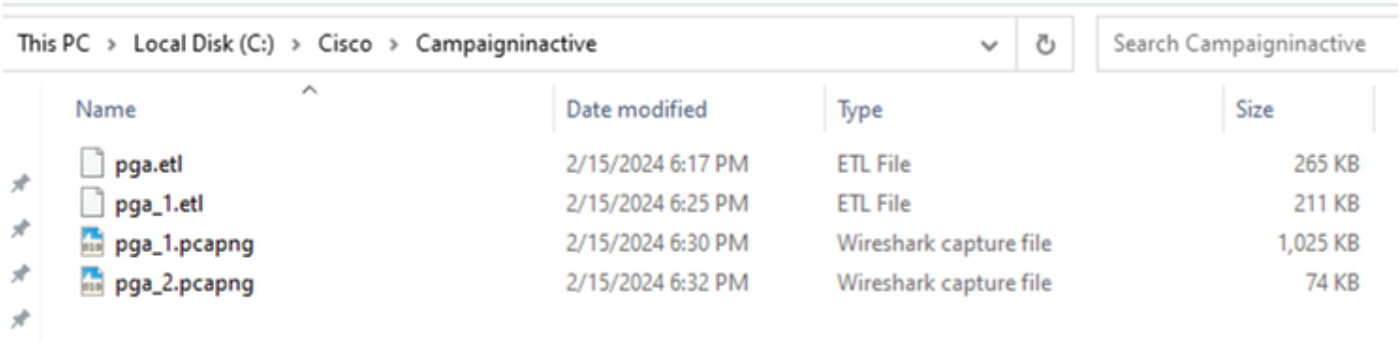
الطريقة 2. pktmonetl2pcapC:\Cisco\Campaigninactive\pga_1.etl --out C:\Cisco\Campaigninactive\pga.pcapng

الناتج:

```
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>
```



الصورة 1.

الطريقة 2. لتحويل التقاط الحزم من الملحق الأصلي **.etl** إلى تنسيق Wireshark القابل للقراءة **.pcapng**.

تساعد هذه الأوامر الأساسية في تجميع الملفات وتكون مفيدة في أستكشاف أخطاء TAC وإصلاحها.

معلومات ذات صلة

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

- الدعم الفني والتنزيلات من Cisco

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).