Recopilar capturas de paquetes en el sistema operativo de cliente y servidor de Windows

Contenido

Introducción

Este documento describe cómo recopilar capturas de paquetes en la plataforma Windows mediante la utilidad pktmon de Windows en un entorno de cliente altamente seguro. Por ejemplo, banca, defensa, marina y más.

Problema

Entorno gubernamental altamente seguro, como bancos, defensa, marina, etc., que restringe la instalación de herramientas de terceros. En especial, la herramienta de captura de paquetes Wireshark para solucionar problemas de paquetes de voz, vídeo y datos. Las aprobaciones de administración de cambios consumen tiempo y se producen retrasos innecesarios en la resolución de un problema. Utilidad disponible de forma predeterminada con Windows puede ayudar a evitar el retraso.

Solución

De forma predeterminada, el nombre de herramienta PKTMON es una utilidad de fragmento de paquete predeterminada que se incluye con los sistemas operativos cliente y servidor de Microsoft Windows. PKTMON está disponible en Windows Server 2022, Windows Server 2019, Windows 10, Azure Stack HCI, Azure Stack Hub y Azure. La configuración es muy sencilla y requiere menos tiempo. La utilidad se ejecuta mediante la utilidad del símbolo del sistema de Windows (cmd) con privilegios de administrador.

Directorio ejecutable: C:\Windows\System32\PktMon.exe

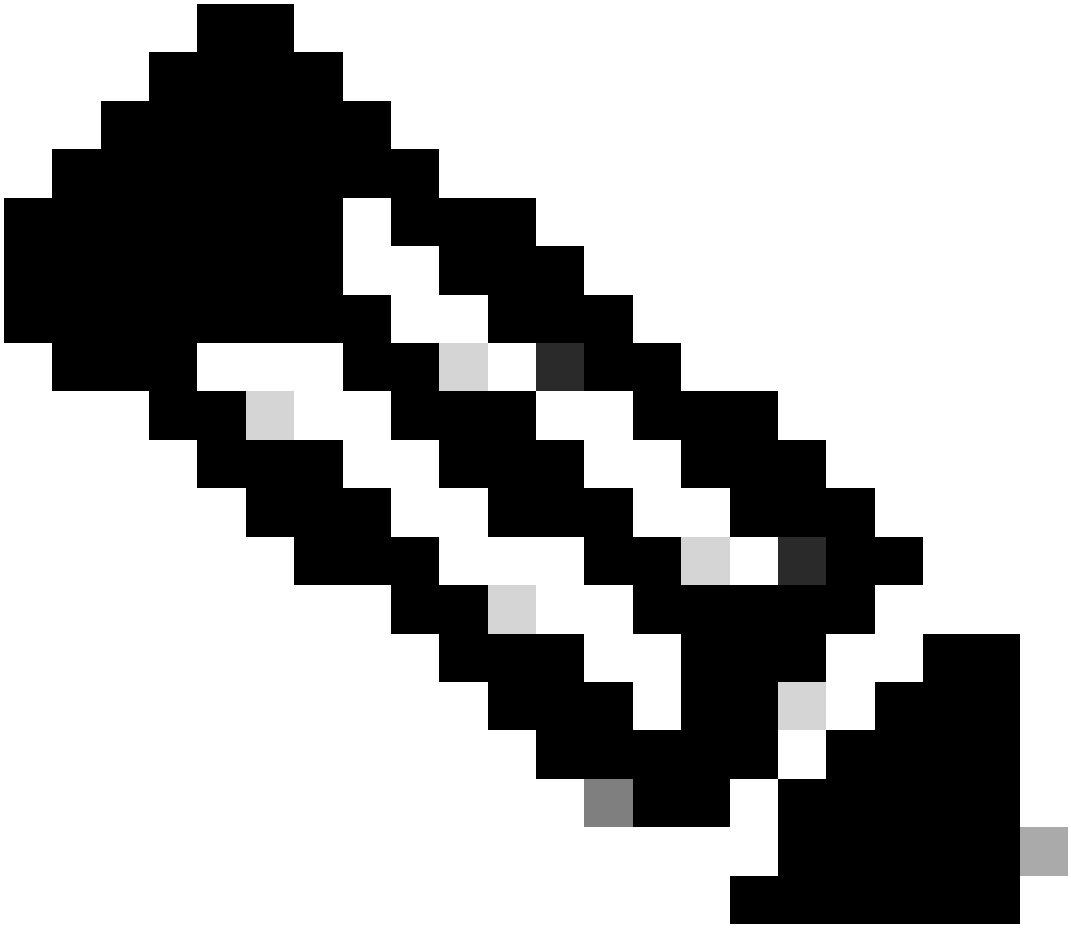
Aquí se supone que se realiza un seguimiento de la captura de paquetes entre el sistema 1 (PG-A) y el sistema 2 (Logger-A).

Primero debe identificar el ID de la interfaz o el ID del controlador de interfaz de red o de la tarjeta (NIC) en el sistema o la máquina virtual.

pktmon list - Este comando enumera las interfaces en el sistema/máquina virtual.

Salida:

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



Nota: Para obtener ayuda, utilice el sufijo help al final del comando. Es decir, pktmon list ayuda.

Tabla 1. Tablas de interfaz.

Una vez que se identifica el ID de interfaz, se inicia la captura de paquetes. El comando habilita las capturas de paquetes y los contadores de paquetes.

Método 1. pktmon start --capture

Este comando inicia la captura de los paquetes en la ruta de acceso de usuario de inicio de sesión predeterminada de Windows.

Salida:

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

Tabla 2. Indicación de inicio de captura de paquetes.

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

Este comando comienza a capturar los paquetes en la trayectoria definida personalizada.

Salida:

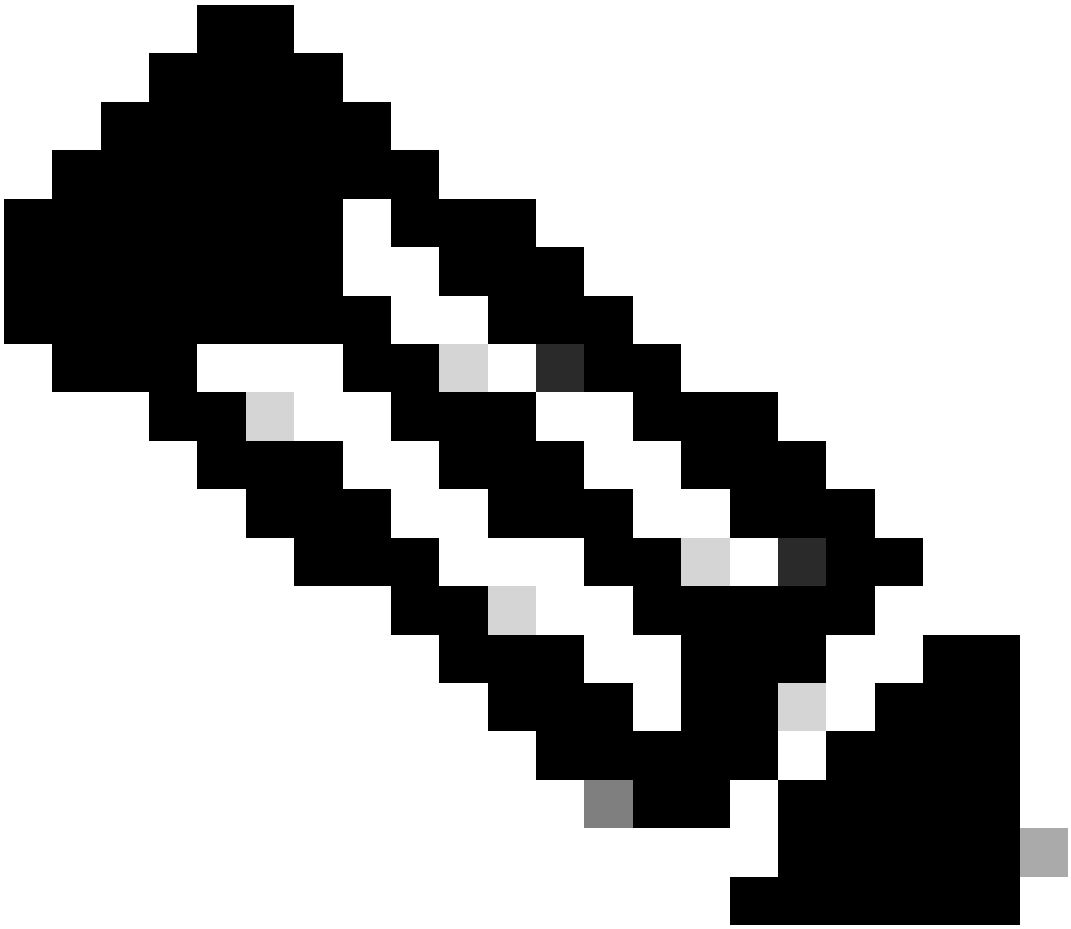
Logger Parameters:
Logger name: PktMon
Logging mode: Circular
Log file: C:\Cisco\Campaigninactive\pga.etl
Max file size: 512 MB
Memory used: 64 MB

Collected Data:
Packet counters, packet capture

Capture Type:
All packets

Monitored Components:
All

Packet Filters:
None



Nota: De forma predeterminada, captura todas las interfaces y todos los tipos de paquetes.

Tabla 3. Captura de paquetes con dirección de ruta para almacenar el archivo de captura.

En el medio de la captura, el estado de la captura de paquetes también se puede validar.

pktmon status- Este comando muestra la captura de paquetes ejecutada activa **pktmon** en curso.

Salida:

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>

Tabla 4. Valide el estado de la captura de paquetes.

Una vez que se reproduzca el problema, detenga la captura de paquetes con el pktmon stop comando.

Salida:

Flushing logs...
Merging metadata...

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

Tabla 5. Detenga la captura de paquetes.

De forma predeterminada, **pktmon** almacena en el formato predeterminado.etl y existe una manera de convertirlo en **pcapng** para poder revisarlo mediante Wireshark.

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

Este comando convierte el valor predeterminado guardado en el PktMon.etl archivo del directorio predeterminado al formato **pcapng**.

Salida:

```
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>
```

Tabla 6.

Método 1. Para convertir la captura de paquetes de la extensión nativa **.etl** al formato legible de Wireshark **.pcapng**.

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

Salida:

```
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>
```

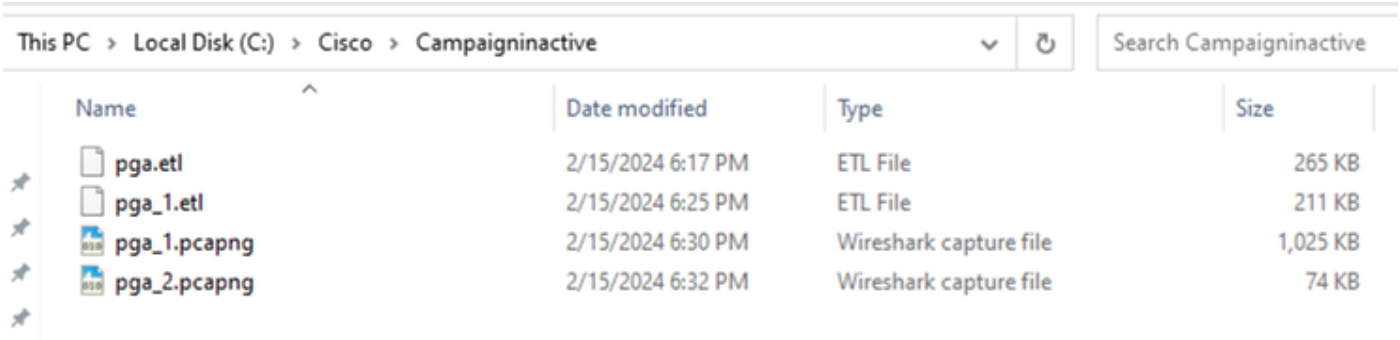


Imagen 1.

Método 2. para convertir la captura de paquetes de la extensión nativa **.etl** al formato legible de Wireshark **.pcapng**.

Estos comandos básicos ayudan a recopilar los archivos y son útiles para solucionar problemas de TAC.

Información Relacionada

- https://learn.microsoft.com/en-us/windows-server/networking/technologies/pktmon/pktmon
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).