Collecter les captures de paquets sur le système d'exploitation client et serveur Windows

Table des matières

Introduction

Ce document décrit comment collecter des captures de paquets sur la plate-forme Windows à l'aide de l'utilitaire pktmon de Windows dans un environnement client hautement sécurisé. Par exemple, la banque, la défense, la marine, etc.

Problème

Un environnement gouvernemental hautement sécurisé (banques, défense, marine, etc.) limite l'installation d'outils tiers. En particulier, l'outil de capture de paquets Wireshark afin de dépanner la voix, la vidéo et les paquets de données. Les approbations de la gestion des modifications prennent du temps et sont inutilement retardées pour résoudre un problème. L'utilitaire par défaut disponible avec Windows peut aider à éviter le retard.

Solution

Par défaut, le nom de l'outil PKTMON est un utilitaire d'extrait de paquet par défaut fourni avec les systèmes d'exploitation client et serveur Microsoft Windows. PKTMON est disponible sur Windows Server 2022, Windows Server 2019, Windows 10, Azure Stack HCI, Azure Stack Hub et Azure. La configuration est très facile et prend moins de temps. L'utilitaire est exécuté à l'aide de l'utilitaire d'invite de commandes Windows (cmd) avec des privilèges d'administrateur.

Répertoire exécutable : C:\Windows\System32\PktMon.exe

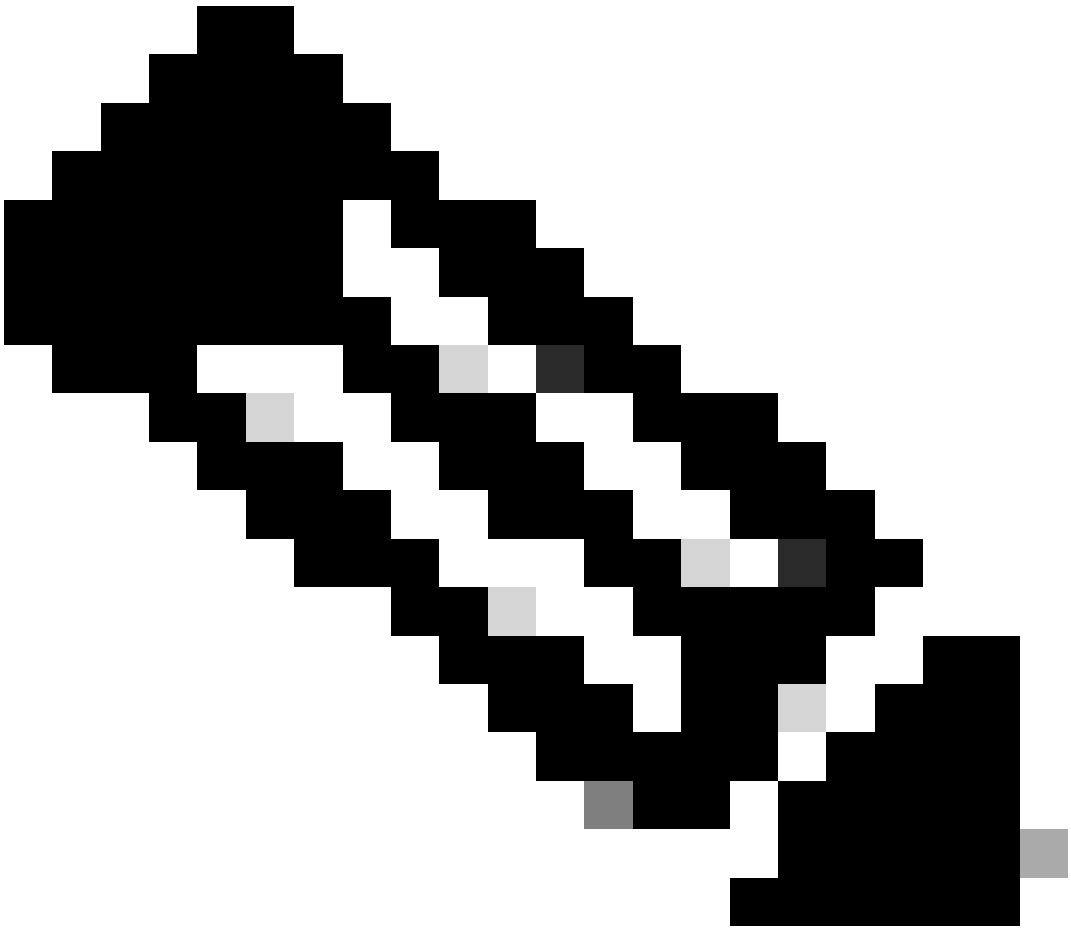
Ici, il est supposé suivre la capture de paquets entre System-1 (PG-A) et System-2 (Logger-A).

Vous devez d'abord identifier l'ID d'interface ou l'ID de contrôleur d'interface réseau ou de carte réseau sur le système/la machine virtuelle.

pktmon list - Cette commande répertorie les interfaces sur le système/la machine virtuelle.

Sortie :

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



Remarque : pour obtenir de l'aide, utilisez le suffixe help à la fin de la commande. C'est-à-dire pktmon list aider.

Tableau 1 . Tables d'interface.

Une fois l’ID d’interface identifié, la capture de paquets démarre. La commande active les captures de paquets et les compteurs de paquets.

Méthode 1. pktmon start --capture

Cette commande commence à capturer les paquets au niveau du chemin d'accès utilisateur Windows connecté par défaut.

Sortie :

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

Tableau 2 . Indication de début de capture de paquet.

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

Cette commande commence à capturer les paquets au niveau du chemin personnalisé.

Sortie :

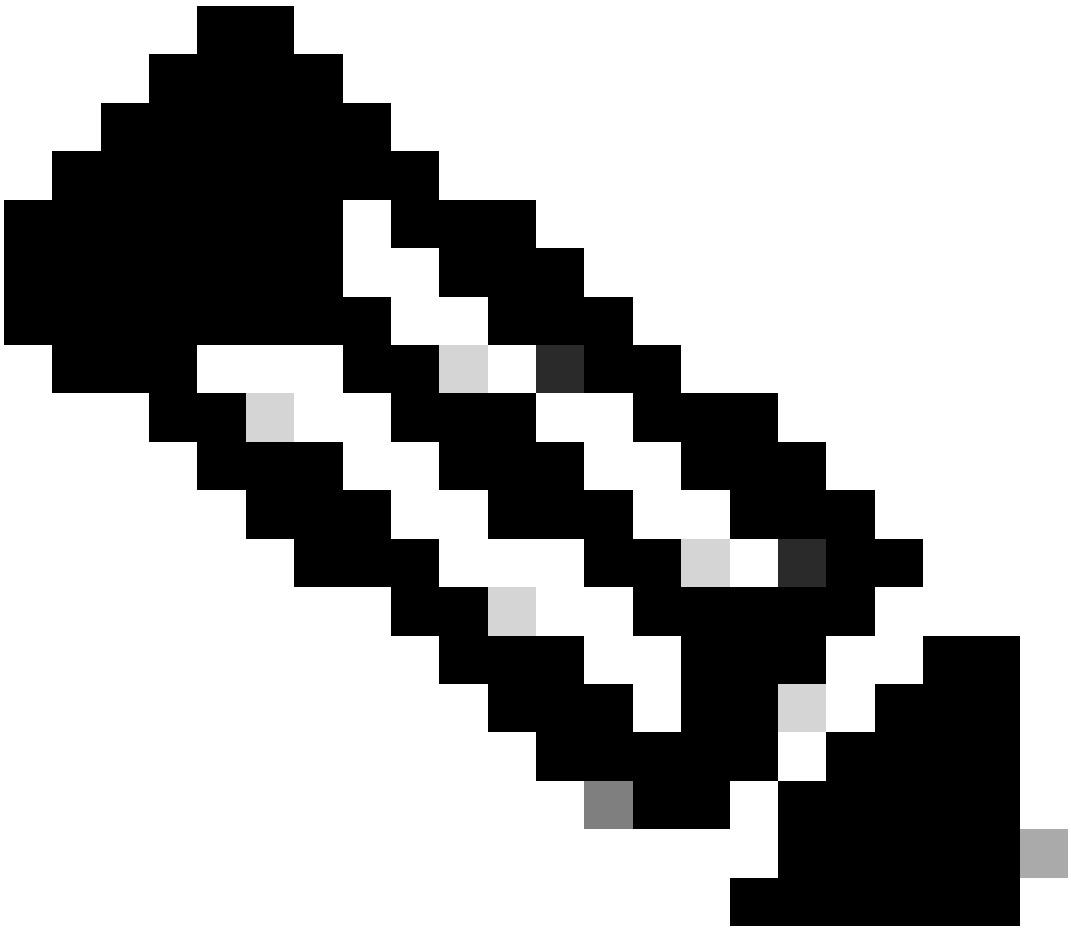
Logger Parameters:
Logger name: PktMon
Logging mode: Circular
Log file: C:\Cisco\Campaigninactive\pga.etl
Max file size: 512 MB
Memory used: 64 MB

Collected Data:
Packet counters, packet capture

Capture Type:
All packets

Monitored Components:
All

Packet Filters:
None



Remarque : par défaut, il capture toutes les interfaces et tous les types de paquets.

Tableau 3 . Capture de paquets avec l'adresse du chemin afin de stocker le fichier de capture.

Au milieu de la capture, l'état de capture des paquets peut également être validé.

pktmon status- Cette commande affiche la capture de paquets active **pktmon** exécutée en cours.

Sortie :

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>

Tableau 4 . Validez l'état de capture des paquets.

Une fois le problème reproduit, arrêtez la capture de paquets à l’aide de la commandepktmon stop .

Sortie :

Flushing logs...
Merging metadata...

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

Tableau 5 . Arrêtez la capture de paquets.

Par défaut, **pktmon** stocke dans le format par défaut.etl et il y a un moyen de le convertir en **pcapng** afin de réviser à l'aide de Wireshark.

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

Cette commande convertit au format **pcapng** le fichier par défaut enregistré dansPktMon.etl le répertoire par défaut.

Sortie :

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>

Tableau 6 .

Méthode 1. Pour convertir la capture de paquets de l'extension native **.etl** au format lisible Wireshark **.pcapng**.

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

Sortie :

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>

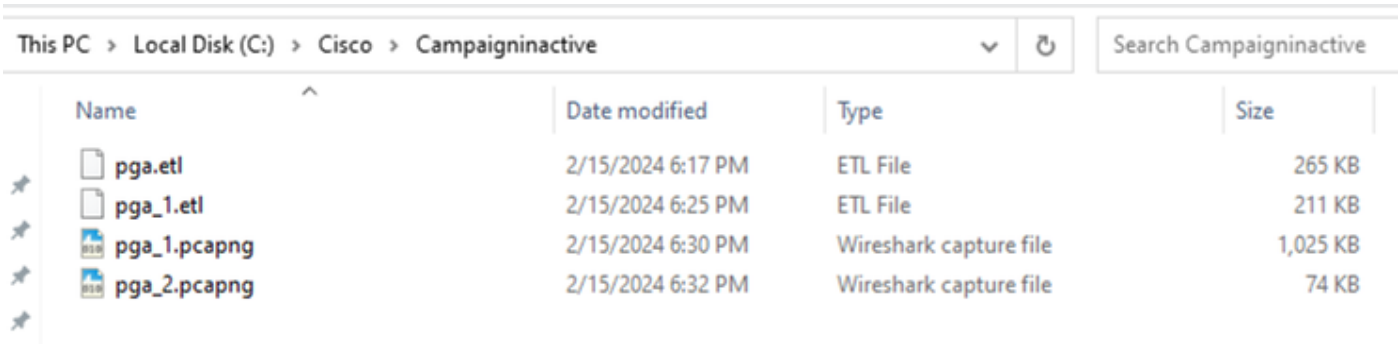


Image 1.

Méthode 2. pour convertir la capture de paquets de l’extension native **.etl** au format lisible Wireshark **.pcapng**.

Ces commandes de base permettent de collecter les fichiers et sont utiles pour le dépannage du centre d'assistance technique.

Informations connexes

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

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.