# Raccogli acquisizioni pacchetti nel sistema operativo client e server Windows

## Sommario



## Introduzione

In questo documento viene descritto come raccogliere i pacchetti acquisiti sulla piattaforma Windows utilizzando l'utilità pktmon di Windows in un ambiente altamente protetto. Ad esempio, le banche, la difesa, la marina e altro ancora.

## Problema

Ambienti governativi altamente protetti, come banche, difesa, marina e altro ancora, limitano l'installazione di strumenti di terze parti. In particolare, lo strumento di acquisizione dei pacchetti Wireshark per la risoluzione dei problemi relativi a pacchetti voce, video e dati. Le approvazioni di gestione delle modifiche sono soggette a un consumo di tempo e a inutili ritardi nella risoluzione di un problema. Per impostazione predefinita, l'utilità disponibile in Windows consente di evitare il ritardo.

## Soluzione

Per impostazione predefinita, il nome dello strumento PKTMON è un'utilità di frammento di pacchetto predefinita fornita con i sistemi operativi client e server di Microsoft Windows. PKTMON è disponibile in Windows Server 2022, Windows Server 2019, Windows 10, Azure Stack HCI, Azure Stack Hub e Azure. La configurazione è molto semplice e richiede meno tempo. L'utilità viene eseguita dal prompt dei comandi di Windows (cmd) con privilegi di amministratore.

Directory eseguibile: C:\Windows\System32\PktMon.exe

**Qui si presume che venga tracciata l'acquisizione del pacchetto tra System-1 (PG-A) e System-2 (Logger-A).**

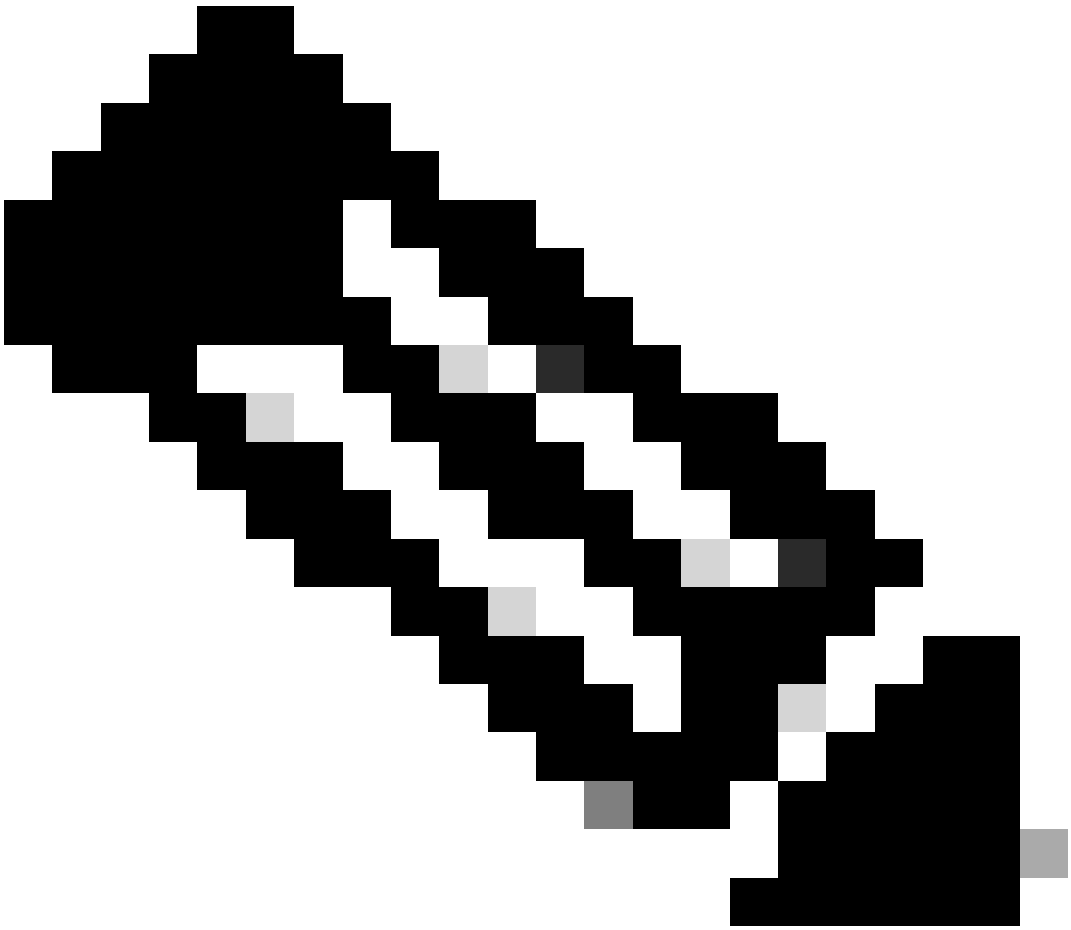
**È necessario innanzitutto identificare l'ID interfaccia o l'ID NIC (Network Interface Controller) nel sistema o nella macchina virtuale.**

**pktmon list** - Questo comando elenca le interfacce nel sistema/macchina virtuale.

**Uscita:**

```
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**: per la Guida, utilizzare il suffisso help alla fine del comando. Cioè, pktmon list  aiuto.

---

Tabella 1.  Tabelle di interfaccia.

Dopo aver identificato l'ID interfaccia, l'acquisizione del pacchetto viene avviata. Il comando abilita le acquisizioni e i contatori dei pacchetti.

Metodo 1. pktmon start --capture

Questo comando avvia l'acquisizione dei pacchetti nel percorso utente predefinito per l'accesso a Windows.

Uscita:

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

Tabella 2. Indicazione di avvio acquisizione pacchetti.

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

Con questo comando viene avviata l'acquisizione dei pacchetti nel percorso personalizzato.

Uscita:

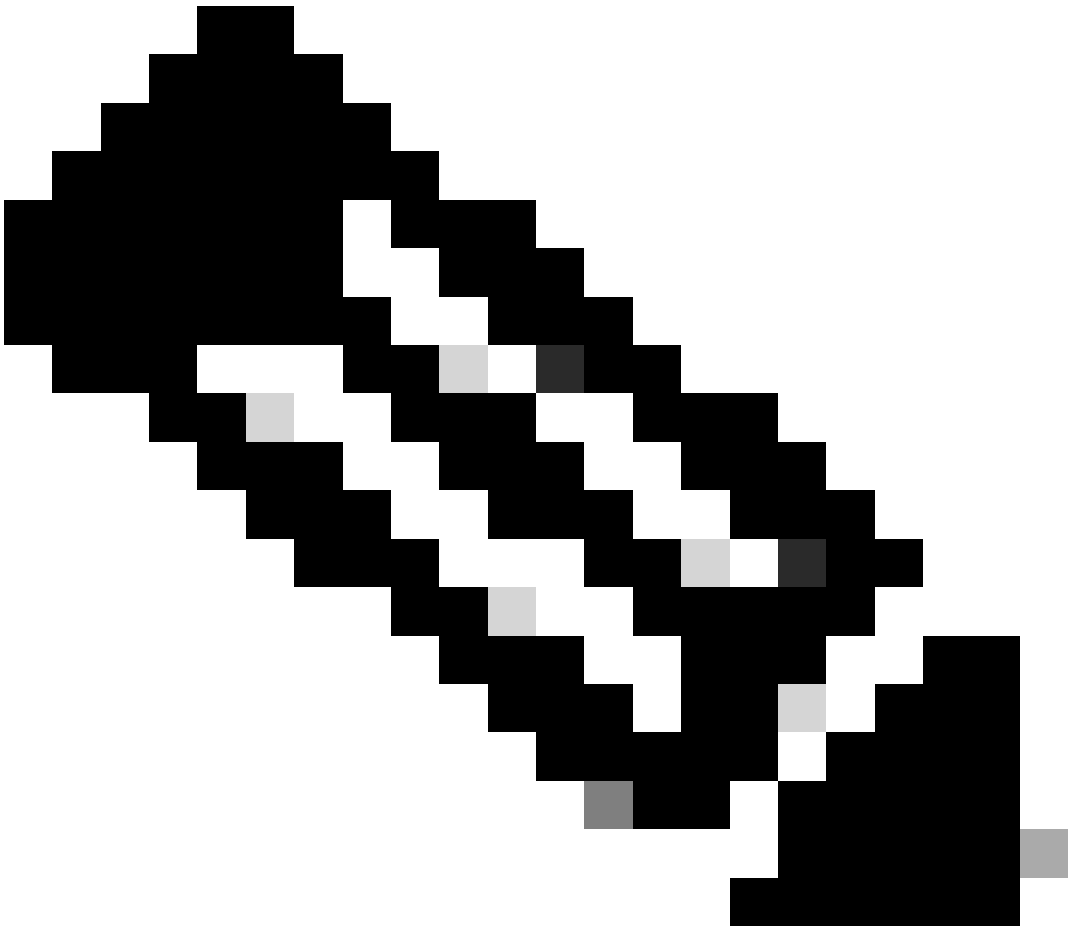
Logger Parameters:
Logger name: PktMon
Logging mode: Circular
Log file: C:\Cisco\Campaigninactive\pga.etl
Max file size: 512 MB
Memory used: 64 MB

Collected Data:
Packet counters, packet capture

Capture Type:
All packets

Monitored Components:
All

Packet Filters:
None



**Nota**: per impostazione predefinita, acquisisce tutte le interfacce e tutti i tipi di pacchetto.

Tabella 3. Acquisizione del pacchetto con indirizzo del percorso per archiviare il file di acquisizione.

Durante l'acquisizione, è possibile verificare anche lo stato di acquisizione del pacchetto.

pktmon status- Questo comando visualizza l'acquisizione del pacchetto **pktmon** attivo in corso.

Uscita:

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>

Tabella 4. Convalida lo stato dell'acquisizione dei pacchetti.

Una volta riprodotto il problema, arrestare l'acquisizione del pacchetto con il pktmon stop comando.

Uscita:

Flushing logs...
Merging metadata...

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

Tabella 5. Arrestare l'acquisizione dei pacchetti.

Per impostazione predefinita, il comando **pktmon** viene memorizzato nel formato predefinito.etl ed è disponibile un metodo per convertirlo in **pcapng** per la revisione tramite Wireshark.

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

Questo comando converte nel formato **pcapng** l'impostazione predefinita salvata nelPktMon.etl file nella directory predefinita.

Uscita:

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>

Tabella 6.

Metodo 1. Per convertire l'acquisizione dei pacchetti dall'estensione nativa **.etl** al formato leggibile Wireshark **.pcapng**.

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

Uscita:

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>

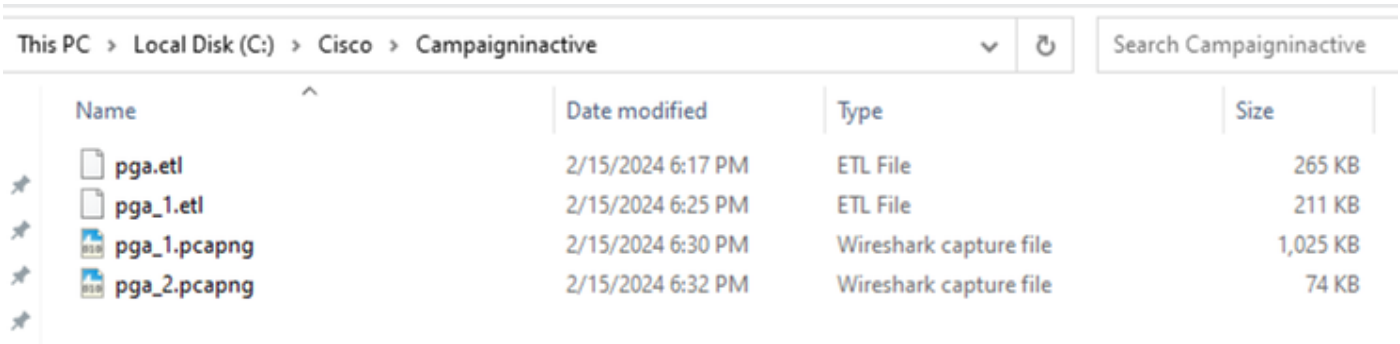



Immagine 1.

Metodo 2. per convertire l'acquisizione dei pacchetti dall'estensione nativa **.etl** al formato leggibile Wireshark **.pcapng**.

Questi comandi di base aiutano a raccogliere i file e sono utili per la risoluzione dei problemi di TAC.

Informazioni correlate

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

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).