

# 收集Windows客户端和服务端操作系统上的数据包捕获

## 目录

---

[简介](#)

[问题](#)

[解决方案](#)

[相关信息](#)

---

## 简介

本文档介绍如何在高度安全的客户环境中使用Windows pktmon 实用程序在Windows平台上收集数据包捕获信息。例如，银行、国防、海军等。

## 问题

高度安全的政府环境（如银行、国防、海军等）限制安装第三方工具。特别是数据包捕获工具Wireshark，用于对语音、视频和数据数据包进行故障排除。变更管理审批会耗费大量时间，而且会在解决问题时造成不必要的延迟。默认情况下，Windows提供的实用程序可以帮助避免延迟。

## 解决方案

默认情况下，工具名称PKTMON是与Microsoft Windows客户端和服务端操作系统捆绑在一起的数据包片段实用程序。PKTMON可用于Windows Server 2022、Windows Server 2019、Windows 10、Azure堆栈HCI、Azure堆栈中心和Azure。设置非常简单且耗时较少。该实用程序使用具有管理员权限的Windows命令提示符(cmd)实用程序运行。

可执行目录：C:\Windows\System32\PktMon.exe

此处假设跟踪系统1 (PG-A)和系统2 (Logger-A)之间的数据包捕获。

您必须首先确定系统/虚拟机上的接口ID或网络接口控制器或卡(NIC) ID。

**pktmon list** - 此命令列出系统/虚拟机上的接口。

输出：

```
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
```

---

注意：如需帮助，请使用命令末尾的后缀帮助。也就是说，帮pktmon list 助。

---

表 1. 接口表。

一旦确定接口ID，便开始捕获数据包。命令启用数据包捕获和数据包计数器。

方法 1. pktmon start --capture

此命令开始捕获默认Windows登录用户路径上的数据包。

输出：

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

表 2. 数据包捕获开始指示。

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

此命令开始在自定义路径上捕获数据包。

输出 :

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:

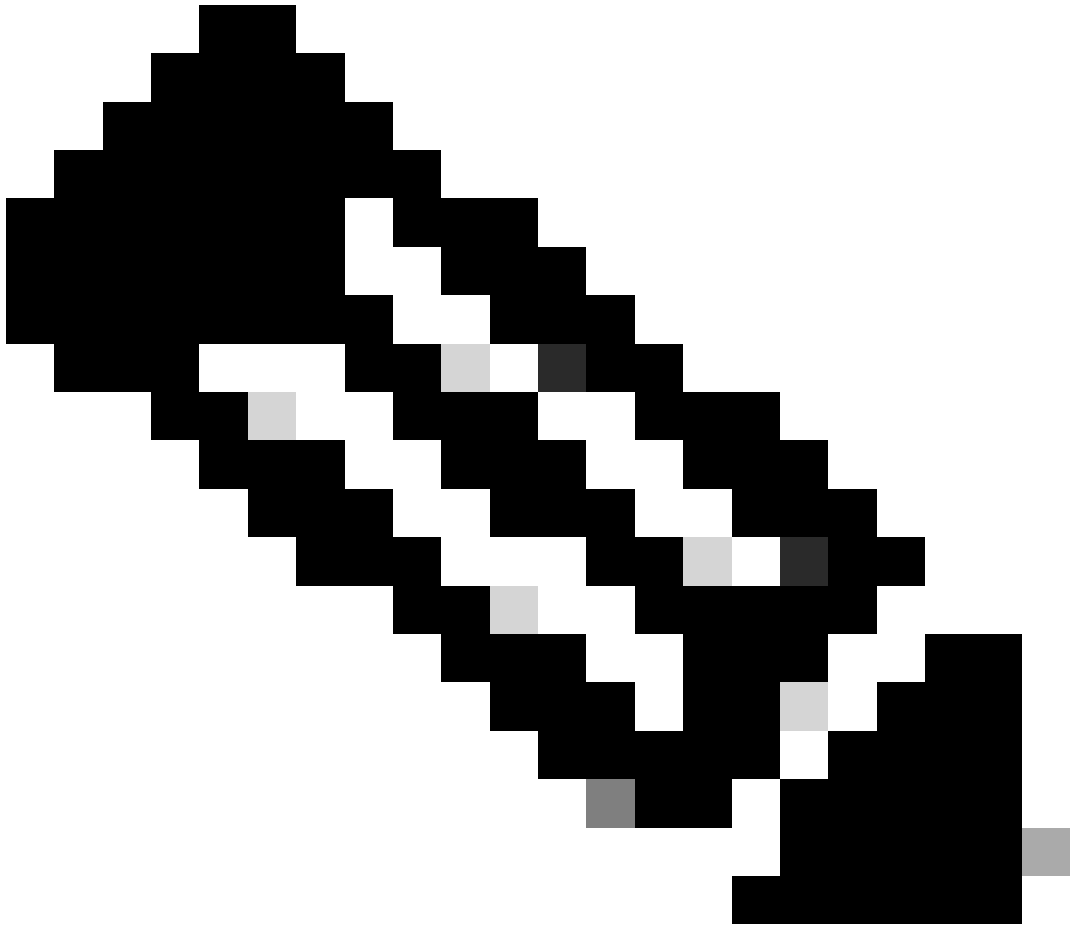
All packets

Monitored Components:

All

Packet Filters:

None



注意：默认情况下，它会捕获所有接口和所有数据包类型。

---

表 3. 包含路径地址的数据包捕获，用于存储捕获文件。

在捕获过程中，还可以验证数据包捕获状态。

pktmon status- 此命令显示正在进行的活动pktmon执行的数据包捕获。

输出：

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>

表 4. 验证数据包捕获的状态。

重现问题后，使用pktmon stop命令停止数据包捕获。

输出：

Flushing logs...  
Merging metadata...

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

表 5. 停止数据包捕获。

默认情况下，pktmon以默认.etl格式存储，并且可以通过将其转换为pcapng来使用Wireshark进行查看。

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

此命令将默认目录的PktMon.etl文件中保存的默认格式转换为pcapng格式。

输出：

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>

表 6.

方法 1. 将数据包捕获从本地扩展.etl转换为Wireshark可读格式.pcapng。

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

输出 :

```
C:\Users\Administrator>pktmon etl2pcap C:\Cisco\Campaigninactive\pga_1.etl --out C:\Cisco\Campaigninactive\pga_1.pcapng
Processing...
```

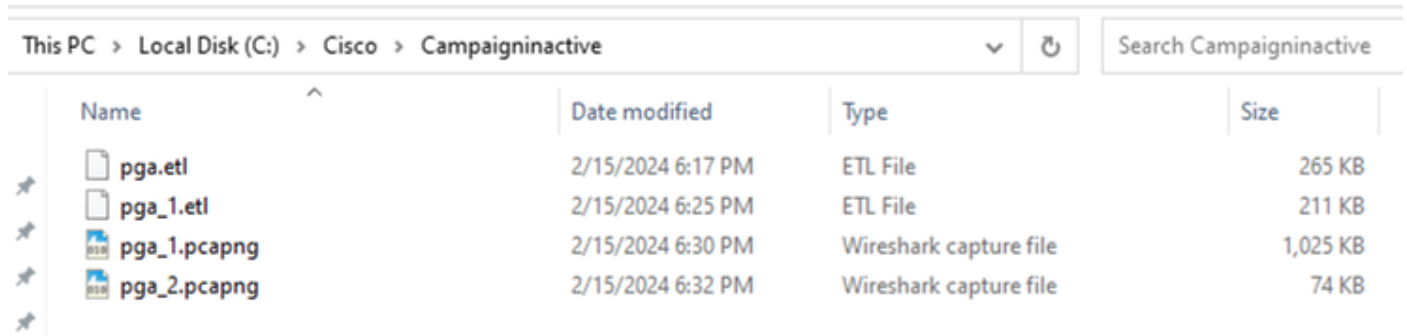
Packets total: 8964

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

图 1.

方法2. 将数据包捕获从本地扩展.etl转换为Wireshark可读格式.pcapng。

这些基本命令有助于收集文件并有助于排除TAC故障。

相关信息

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

- [思科技术支持和下载](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。