在遙測代理節點中執行資料包捕獲

目錄

簡介

本檔案介紹如何在思科遙測代理(CTB)代理節點中執行封包擷取。

必要條件

需求

思科建議您瞭解以下主題：

- 基本Linux管理
- 基本思科遙測代理架構
- SSH基礎知識
- 執行封包擷取時需要使用**admin**命令root行介面(CLI)存取許可權。

採用元件

本文檔中的資訊基於運行版本2.0.1的CTB代理節點。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

CTB代理節點有一個名為**ctb-pcap**的工具，用於從Broker節點的遙測介面執行網路捕獲。請注意，此工具在CTB管理器節點上不可用。

使用命令ctb-pcap,之前，請確保首先使用命令**root**切換到使用者sudo su。此工具僅對使用者可用root。

要檢視此工具的可用選項，請在**ctb-pcap --help**Broker節點的CLI上運行命令。此圖顯示了選項的完整清單：

```
Cisco Telemetry Broker Packet Capture Tool

This tool can be used to capture packets that fit a specific filter
criteria that are specified using the Packet Type and the OPIONS below.

NOTE: The following options are required and MUST be specified.

-n, --num-pkgts
-t, --max-duration
-o, --output-file

Usage: ctb-pcap OPTIONS <packet type> [<packet type>] [<packet_type>] ..

<Packet Type>
  This specifies the direction/status of packets and can be one of the
  following:
    rx    Receive packets
    tx    Sent packets
    drop  Dropped packets

OPTIONS

-v, --ip-version <ip version>
  The IP version of packets to capture. It can be either ip4 or ip6.
  Default: ip4

-s, --src-ip <source ip address>
  The source IP address of packets to capture. In Address/Mask format.
  E.g. 10.0.81.10/24.

-d, --dst-ip <destination ip address>
  The destination IP address of the packets to capture.In Address/Mask
  format. E.g. 10.0.81.10/24.

-p, --src-port <port>
  The source port number.

-P, --dst-port <port>
  The destination port number.

-n, --num-pkts <count>
  The number of packets to capture.

-t, --max-duration <seconds>
  The max duration in seconds after which capture will stop.

-o, --output-file <path>
  File to send output to (default is stdout).

-V, --verbose
  Print verbose output when the tool runs.

-h, --help
  Show this help screen.
```

CTB資料包捕獲工具的所有可用選項

如輸出所示，需要捕獲的資料包數、持續時間（秒）和資料包捕獲輸出檔名。此外，必須在命令中

命令的基礎，該命令已指定捕獲的資料包數量、資料包捕獲的持續時間和檔名，以及詳細選項和資料包型別：

```
ctb-pcap -V -n [number_pkts] -t [duration] -o [filename] [rx/tx/drop]
```

驗證

例如，您可以使用冗餘選項100個資料包（30秒）執行資料包捕獲，按接收資料包的源10.10.10.10進行過濾，然後使用名稱儲存輸**received_packets.pcap**出。

執行此類資料包捕獲的命令為：

```
ctb-pcap -V -n 100 -t 120 -s 10.10.10.10 -o received_packets.pcap rx
```

在Broker節點的CLI中輸入命令，資料包捕獲即開始。資料包捕獲完成後，檔案將自動儲存到目/var/lib/titan/pcap/錄。

以下是packet capture命令詳細輸出的範例：

```
==> Checking capture status (5 seconds)...
==> Capture still in progress  6 of 100 pkts...
==> Checking capture status (10 seconds)...
==> Capture still in progress  16 of 100 pkts...
==> Checking capture status (15 seconds)...
==> Capture still in progress  28 of 100 pkts...
==> Checking capture status (20 seconds)...
==> Capture still in progress  40 of 100 pkts...
==> Checking capture status (25 seconds)...
==> Capture still in progress  54 of 100 pkts...
==> Checking capture status (30 seconds)...
==> Capture still in progress  66 of 100 pkts...
==> Executing /usr/bin/vppctl pcap trace off
Write 66 packets to /tmp/received_packets.pcap, and stop capture...
==> mv /tmp/received_packets.pcap /pcap/received_packets.pcap
==> **** Capture written to /var/lib/titan/pcap/received_packets.pcap ****
```

示例命令的詳細輸出

請注意，對於資料包選項的持續時間和數量，第一個選項會停止資料包捕獲。(例如，即使尚未完成三十個持續時間，仍捕獲了總共100個資料包，則資料包捕獲將停止。在此範例中，首先到達三十秒的持續時間，因此只擷取66個封包。)

生成資料包捕獲後，使用SCP或SFTP將檔案傳輸到本地電腦。如果使用SFTP，請輸入管理員憑據以連線到裝置。

相關資訊

- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。