在遥测代理节点中执行数据包捕获

目录

简介

本文档介绍如何在思科遥测代理(CTB)代理节点中执行数据包捕获。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本Linux管理
- 基本思科遥测代理架构
- SSH基础知识
- 执行数据包捕获时需要使用**admin**root命令行界面(CLI)访问。

使用的组件

本文档中的信息基于运行版本2.0.1的CTB Broker节点。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

CTB代理节点有一个称为**ctb-pcap**的工具，用于从代理节点的遥测接口执行网络捕获。请注意，此工具在CTB管理器节点不可用。

使用命令之前ctb-pcap,，请确保首先使用命令**root**切换到用sudo su户。此工具仅对用户可用root。

要查看此工具的可用选项，请在Broker节**ctb-pcap --help**点的CLI上运行命令。此图像显示了选项的完整列表：

```
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数据包捕获工具的所有可用选项

如输出所示，需要捕获的数据包数量、持续时间（以秒为单位）和数据包捕获输出文件名。此外，

命令的基础，该命令已指定捕获的数据包数量、数据包捕获的持续时间和文件名，以及详细选项和数据包类型：

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

验证

例如，您可以使用冗余选项100个数据包（30秒）执行数据包捕获，按接收数据包的源10.10.10.10进行过滤，并将输出保存为名**received_packets.pcap**称。

执行此类数据包捕获的命令为：

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

在Broker节点的CLI中输入命令，数据包捕获随即开始。数据包捕获完成后，文件将自动保存到目/var/lib/titan/pcap/录。

以下是packet capture命令的详细输出示例：

```
==> 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 ****
```

示例命令的详细输出

请注意，对于数据包选项的持续时间和数量，第一个选项会停止数据包捕获。(例如，如果总共捕获了100个数据包，即使持续时间的30个尚未完成，数据包捕获也会停止。在本例中，首先达到三十秒的持续时间，因此只捕获了66个数据包。)

生成数据包捕获后，使用SCP或SFTP将文件传输到本地计算机。如果使用SFTP，请输入管理员凭证以连接到设备。

相关信息

- 技术支持和文档 - Cisco Systems

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）。