텔레메트리 브로커 노드에서 패킷 캡처 수행

목차

소개

이 문서에서는 Cisco CTB(Telemetry Broker) 브로커 노드에서 패킷 캡처를 수행하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 Linux 관리
- 기본 Cisco Telemetry Broker 아키텍처
- SSH 기본 지식
- CLI(Command Line Interface) 액세스. **admin** root는 패킷 캡처를 수행하는 데 필요합니다.

사용되는 구성 요소

이 문서의 정보는 버전 2.0.1을 실행하는 CTB 브로커 노드를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

CTB Broker Node에는 Broker 노드의 텔레메트리 인터페이스에서 네트워크 캡처를 수행하는 데 사용되**ctb-pcap**는 라는 툴이 있습니다. CTB 관리자 노드에서는 이 툴을 사용할 수 없습니다.

명령을 사용하기 전에ctb-pcap,먼저 명령을 사용하여 사용자로 **root** 전환해야 합니다sudo su. root이 툴은 사용자에게만 제공됩니다.

이 도구에 사용 가능한 옵션을 보려면 Broker 노드의 CLI**ctb-pcap --help**에서 명령을 실행하십시오. 이 그림에는 옵션의 전체 목록이 표시됩니다.

```
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 패킷 캡처 툴에 사용 가능한 모든 옵션

출력에 표시된 대로 캡처된 패킷 수, 기간(초) 및 패킷 캡처 출력 파일 이름이 필요합니다. 또한 패킷

명령의 기반으로 사용할 수 있습니다. 이 명령은 이미 캡처된 패킷의 수, 패킷 캡처의 지속 시간 및 파일 이름, verbose 옵션 및 패킷 유형을 지정합니다.

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

다음을 확인합니다.

예를 들어, verbose 옵션을 사용하여 패킷 캡처를 수행할 수 있습니다. 수신된 패킷의 소스 10.10.10.10에서 필터링한 100개의 패킷을 30초 동안 캡처하고 출력을 이름과 함께 저장할 수 **received_packets.pcap**있습니다.

이러한 패킷 캡처를 수행하는 명령은 다음과 같습니다.

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

Broker 노드의 CLI에 명령을 입력하면 패킷 캡처가 시작됩니다. 패킷 캡처가 완료되면 파일이 자동으로 디렉토리에/var/lib/titan/pcap/저장됩니다.

다음은 packet capture 명령의 자세한 출력 예입니다.

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

example 명령의 자세한 정보 출력

패킷 옵션의 기간 및 수에 대해 첫 번째 옵션은 패킷 캡처를 중지합니다. 예를 들어, 30분의 3이 완료되지 않았는데도 총 100개의 패킷이 캡처되면 패킷 캡처가 중지됩니다. 이 예에서는 30초의 기간에 먼저 도달했으므로 66개의 패킷만 캡처되었습니다.)

패킷 캡처가 생성된 후 SCP 또는 SFTP를 사용하여 파일을 로컬 시스템으로 전송합니다. SFTP를 사용하는 경우 어플라이언스에 연결할 관리자 자격 증명을 입력합니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.