Effectuer une capture de paquets sur un noeud Telemetry Broker

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configurer

Exemples

Informations connexes

Introduction

Ce document décrit comment effectuer une capture de paquets sur un noeud Cisco Telemetry Broker (CTB) Broker.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration Linux de base
- Architecture de base de Cisco Telemetry Broker
- Connaissances de base SSH
- L'accès à l'interface de ligne de commande (CLI) est nécessaire **admin** root et nécessaire pour capturer les paquets.

Composants utilisés

Les informations de ce document sont basées sur le noeud CTB Broker exécutant la version 2.3.3.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Le noeud du courtier CTB dispose d'un outil appelé **ctb-pcap** qui est utilisé pour effectuer une

capture réseau à partir de l’interface de télémétrie du noeud du courtier. Notez que cet outil n'est pas disponible au niveau du noeud Gestionnaire CTB.

- Avant d'utiliser la commande ctb-pcap,, assurez-vous d'abord de passer à l' **root** utilisateur à l'aide de la commande sudo su. Cet outil est disponible uniquement pour l' root utilisateur.
- Pour afficher les options disponibles pour cet outil, exécutez la commande **ctb-pcap --help** dans l'interface de ligne de commande du noeud Broker. Cette image affiche la liste complète des options :
- Si vous tentez d'effectuer une capture réseau sur une paire de courtiers HA, assurez-vous que vous tentez d'effectuer la commande ctb-pcap à partir du courtier CTB actif.

```
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).

-T, --transport <tcp|udp>
  Transport protocol, udp or tcp.

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

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

Comme l'indique la sortie, le nombre de paquets capturés, la durée en secondes et le nom du fichier de sortie de capture de paquets sont requis. En outre, le type de paquet, qu'il s'agisse de paquets reçus, envoyés ou abandonnés, doit être indiqué dans la commande.

Il existe une autre dépendance qui n'est pas également répertoriée : lorsque vous tentez de capturer le port source (-p) ou le port de destination (-P), l'option Protocole de transport (-T) est également requise.

Vous pouvez utiliser la syntaxe suivante comme base de la commande de capture de paquets, qui spécifie déjà le nombre de paquets capturés, la durée et le nom de fichier de la capture de paquets, ainsi que l'option détaillée et le type de paquet :

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

Exemples

1. Capturez tout le trafic rx sans filtre :
sudo ctb-pcap -n 10000 -t 30 -o rx-no-filter.pcap -V rx

2. Capture rx pour le sous-réseau src ipv4 (utilisez ip/32 pour src unique) :
sudo ctb-pcap -n 10000 -t 30 -o rx-ipv4-src-subnet.pcap -s 10.0.81.0/24 -V rx

3. Capture rx pour ipv6 src ip :
sudo ctb-pcap -n 10000 -t 30 -o rx-ipv6-srcip.pcap -s fc00:f53b:82e4::1000 -v ip6 -V rx

4. Capture rx pour ipv4 udp
sudo ctb-pcap -n 10000 -t 30 -o rx-ipv4-udp.pcap -T udp -V rx

5. Capture tx pour ipv4 tcp
sudo ctb-pcap -n 10000 -t 30 -o tx-ipv4-tcp.pcap -T tcp -V tx

6. Capture rx pour ipv6 udp
sudo ctb-pcap -n 10000 -t 30 -o rx-ipv6-udp.pcap -T udp -v ip6 -V rx

7. Capture rx pour ipv6 tcp
sudo ctb-pcap -n 10000 -t 30 -o rx-ipv6-tcp.pcap -T tcp -v ip6 -V rx

8. Capture rx pour ipv4 udp dstport
sudo ctb-pcap -n 10000 -t 30 -o rx-ipv4-udp-dstport.pcap -T udp -P 2055 -V rx

9. Capture tx pour ipv4 tcp dstport
sudo ctb-pcap -n 10000 -t 30 -o tx-ipv4-tcp-dstport.pcap -T tcp -P 443 -V tx

10. Capture rx pour ipv6 udp dstport
sudo ctb-pcap -n 10000 -t 30 -o rx-ipv6-udp-dstport.pcap -v ip6 -T udp -P 2055 -V rx

11. Capture rx pour ipv6 tcp dstport
sudo ctb-pcap -n 10000 -t 30 -o rx-ipv6-tcp-dstport.pcap -v ip6 -T tcp -P 443 -V rx

12. Capture rx pour ipv4 srcip et udp dstport
sudo ctb-pcap -n 10000 -t 30 -o rx-ipv4-srcip-udp-dstport.pcap -s 10.0.81.171/32 -T udp -P 2055 -V rx

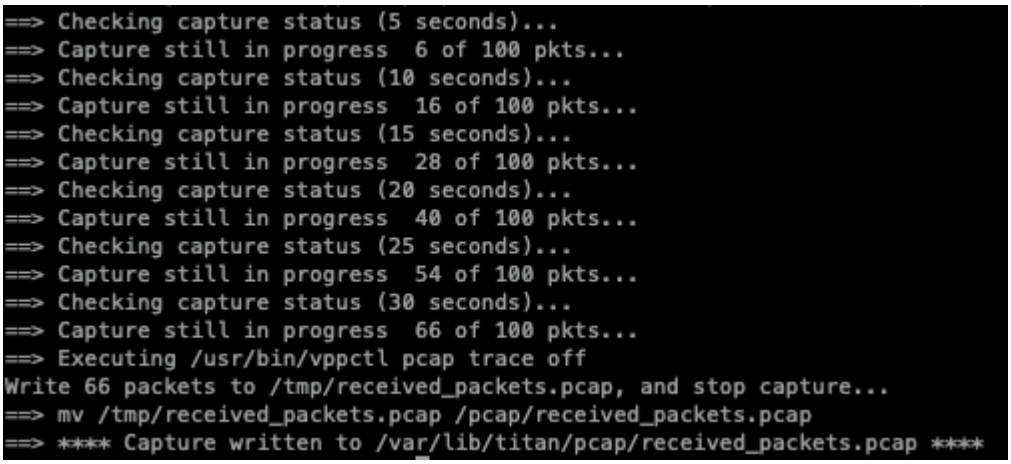
13. Capture rx pour ipv4 srcip et tcp dstport
sudo ctb-pcap -n 10000 -t 30 -o rx-ipv4-srcip-tcp-dstport.pcap -s 10.0.81.171/32 -T tcp -P 443 -V rx

14. Capture rx pour ipv6 srcip et udp dstport
sudo ctb-pcap -n 10000 -t 30 -o rx-ipv6-srcip-udp-dstport.pcap -s fc00:f53b:82e4::1000 -v ip6 -T udp -P 2055 -V rx

15. Capture rx pour ipv6 srcip et tcp dstport
sudo ctb-pcap -n 10000 -t 30 -o rx-ipv6-srcip-tcp-dstport.pcap -s fc00:f53b:82e4::1000 -v ip6 -T tcp -P 443 -V rx

Entrez la commande dans l'interface de ligne de commande du noeud Broker et la capture de paquets commence. Lorsque la capture de paquets est terminée, le fichier est automatiquement enregistré dans le /var/lib/titan/pcap/ répertoire.

Voici un exemple du résultat détaillé de la commande packet capture :

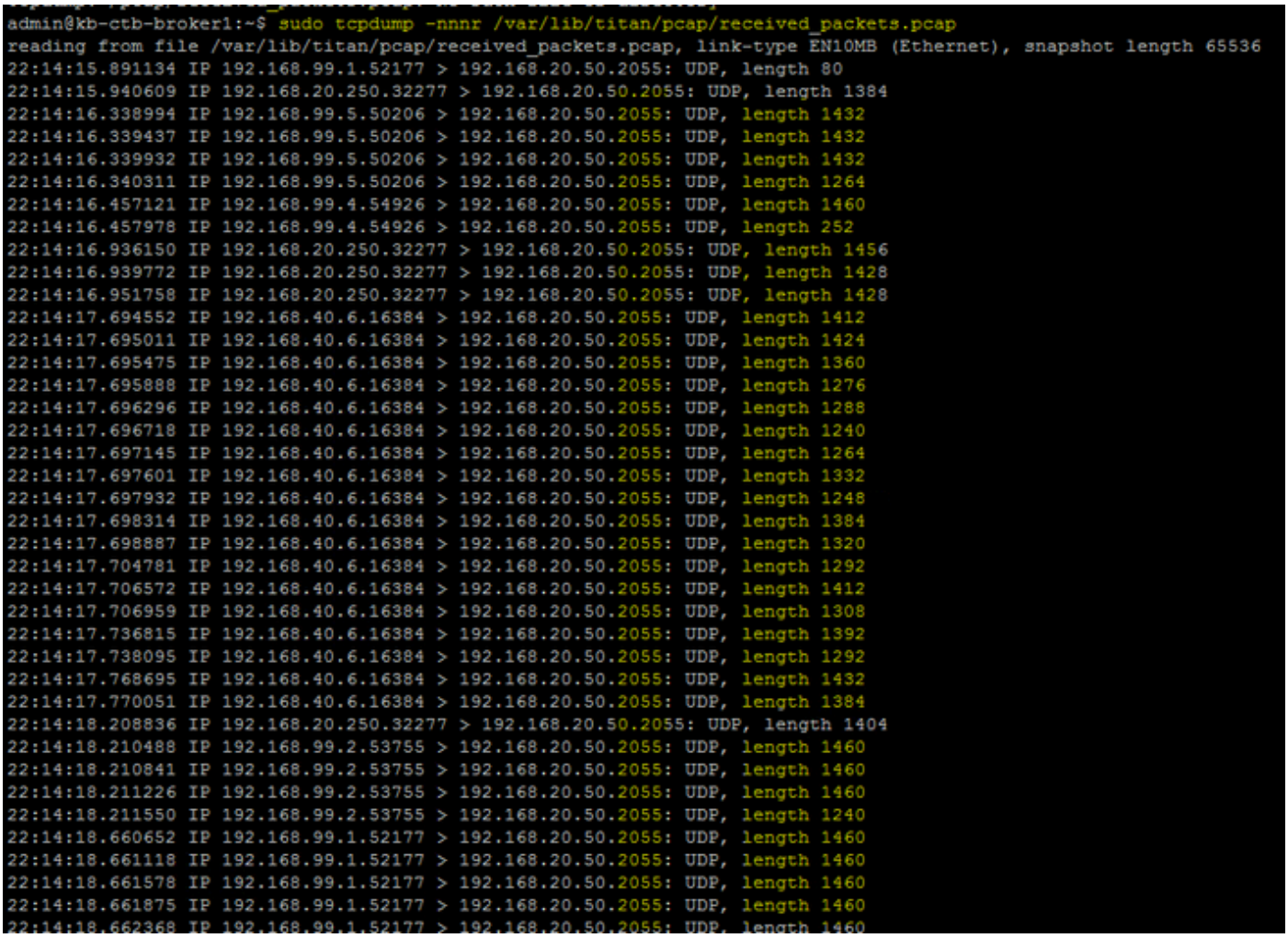


Sortie détaillée de la commande exemple

Notez que pour la durée et le nombre d'options de paquet, la première arrête la capture de paquet. (Par exemple, si un total de 100 paquets ont été capturés alors que les trente paquets de la durée n'ont pas été terminés, la capture des paquets est arrêtée. Dans cet exemple, la durée de trente secondes a été atteinte en premier, de sorte que seuls 66 paquets ont été capturés.)

Une fois la capture de paquets générée, utilisez SCP ou SFTP pour transférer le fichier vers votre machine locale. Si vous utilisez le protocole SFTP, saisissez les informations d'identification d'administrateur pour vous connecter à l'appliance.

Vous pouvez également utiliser > sudo tcpdump -nnr </lavar/lib/titan/pcap/<pcap_filename> afin de relire le pcap sur la console. Ceci est utile si vous voulez juste voir rapidement si les paquets de capture ont des données en eux



Informations connexes

- [Assistance et documentation techniques - Cisco Systems]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.