Captures de paquet sur l'expérience de la mobilité connectée (CMX)

Contenu

Introduction

Ce document décrit sur la façon dont collecter des captures de paquet du CLI du serveur 10.x connecté d'expérience de la mobilité (CMX). Ces captures de paquet peuvent faciliter en dépannant plusieurs scénarios (par exemple : Transmission NMSP entre le contrôleur LAN Sans fil (WLC) et CMX serveur) pour valider l'écoulement de transmission.

Conditions requises

- Accès de l'interface de ligne de commande (CLI) au serveur CMX.
- L'ordinateur avec Wireshark a installé pour indiquer les captures en détail.

Utilisant TCPDUMP pour des captures

TCPDUMP est un analyseur de paquet qui affiche les paquets transmis et reçus sur le serveur CMX. Il sert d'outil d'analyse et de dépannage au réseau/aux administrateurs système. Le module est intégré au serveur CMX où les données brutes des paquets peuvent être regardées.

Le tcpdump courant en tant qu'utilisateur de « cmxadmin » échouerait avec l'erreur suivante : ("accès de racine le » est exigé)

```
In this example, tcpdump is attempted to be run as a 'cmxadmin' user.

[cmxadmin@laughter ~]$ tcpdump -i eth0 port 16113
tcpdump: eth0: You don't have permission to capture on that device (socket: Operation not
permitted)
```

Commutez « pour enraciner » l'utilisateur après avoir ouvert une session en tant qu'utilisateur de « cmxadmin » au CLI au-dessus du SSH ou de la console.

```
[cmxadmin@laughter ~]$ su - root
Password:
[root@laughter ~]#
```

Utilisant la bonne interface

Notez l'interface où les paquets seraient capturés. Il peut être obtenu utilisant le « ifconfig - »

```
In this example, 10.10.10.25 is the IP address of CMX server and 'eth0' is the interface it's
tied to on the server.
[cmxadmin@laughter ~]$ ifconfig -a eth0 Link encap:Ethernet HWaddr 00:50:56:A1:38:BB inet
addr:10.10.10.25 Bcast:10.10.10.255 Mask:255.255.255.0 inet6 addr:
2003:a04::250:56ff:fea1:38bb/64 Scope:Global inet6 addr: fe80::250:56ff:fea1:38bb/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:32593118 errors:0 dropped:0
overruns:0 frame:0 TX packets:3907086 errors:0 dropped:0 overruns:0 carrier:0 collisions:0
txqueuelen:1000 RX bytes:3423603633 (3.1 GiB) TX bytes:603320575 (575.3 MiB) lo Link encap:Local
Loopback inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUNNING
MTU:65536 Metric:1 RX packets:1136948442 errors:0 dropped:0 overruns:0 frame:0 TX
packets:1136948442 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX
bytes:246702302162 (229.7 GiB) TX bytes:246702302162 (229.7 GiB) [cmxadmin@laughter ~]$
```

Capturer des paquets

```
This example captures and displays all packets that are sourced from port - 16113 and enter the
CMX server on the eth0 interface.

[root@laughter ~]# tcpdump -i eth0 src port 16113 tcpdump: verbose output suppressed, use -v or
-vv for full protocol decode listening on eth0, link-type EN10MB (Ethernet), capture size 65535
bytes 09:50:29.530824 IP 172.18.254.249.16113 > laughter.cisco.com.40020: Flags [P.], seq
983381312:983382645, ack 2483597279, win 191, options [nop,nop,TS val 1792647414 ecr
1148435777], length 1333 09:50:31.507118 IP 172.18.254.249.16113 > laughter.cisco.com.40020:
Flags [.], seq 1333:2715, ack 1, win 191, options [nop,nop,TS val 1792647908 ecr 1148437650],
length 1382 09:50:31.507186 IP 172.18.254.249.16113 > laughter.cisco.com.40020: Flags [P.], seq
2715:2890, ack 1, win 191, options [nop,nop,TS val 1792647908 ecr 1148437650], length 175
09:50:33.483166 IP 172.18.254.249.16113 > laughter.cisco.com.40020: Flags [P.], seq 2890:4239,
ack 1, win 191, options [nop,nop,TS val 1792648402 ecr 1148439626], length 1349 09:50:35.459584
IP 172.18.254.249.16113 > laughter.cisco.com.40020: Flags [P.], seq 4239:5396, ack 1, win 191,
options [nop,nop,TS val 1792648896 ecr 1148441603], length 1157 ^C 5 packets captured 5 packets
received by filter 0 packets dropped by kernel [root@laughter ~]#
```

Pour écrire la sortie à un fichier

```
In this example, tcpdump would capture packets that are from 10.10.20.5 received on it's eth0
interface and write it to a file named TEST_NMSP_WLC.pcap.

[root@laughter cmxadmin]# tcpdump -i eth0 src 10.10.20.5 -w TEST_NMSP_WLC.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
^C7 packets captured
7 packets received by filter
0 packets dropped by kernel
[root@laughter cmxadmin]#
```

Une fois le fichier est prêt, vous devra extraire le fichier .pcap du CMX à votre ordinateur pour l'analyse dans un outil plus confortable tel que le wireshark. Vous pouvez employer n'importe quelle application SCP pour faire ainsi. Par exemple dans Windows, l'application de WinSCP te permettra pour se connecter au CMX utilisant les qualifications de SSH et vous pouvez alors parcourir le système de fichiers et trouver le fichier .pcap que vous avez juste créé. Pour trouver le chemin en cours, type « pwd » après qu'exécutant le tcpdump pour savoir où le fichier a été enregistré.

Pour capturer le nombre spécifique de paquets

Si un nombre spécifique de compte de paquet est désiré, utilisant - l'option c filtre exactement pour ce compte.

```
[root@laughter ~]# tcpdump -Z root -i eth0 -c 5 src 10.10.20.5 -w CMX_WLC_Capture.pcap tcpdump:
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes 5 packets captured 6
packets received by filter 0 packets dropped by kernel [root@laughter ~]#
```

D'autres options de filtrage

```
[root@laughter cmxadmin]# tcpdump -i eth0 dst 10.10.20.5 (filtered based on destination IP
address)
[root@laughter cmxadmin]# tcpdump -i eth0 src 10.10.20.4 (filtered based on Source IP address)

[root@laughter cmxadmin]# tcpdump -i eth0 port 80  (filtered for packets on port 80 in both
directions)
[root@laughter cmxadmin]# tcpdump -i eth0 port 443  (filtered for packets on port 443 in both
directions)
```

Les captures écrites aux fichiers seraient enregistrées dans le répertoire courant sur le serveur et peuvent être copiées pour l'examen détaillé utilisant Wireshark.