Capturas de pacotes na experiência móvel conectada (CMX)

Contents

Introduction

Este documento descreve como coletar capturas de pacotes do CLI do servidor Connected Mobile Experience (CMX) 10.x. Essas capturas de pacotes podem ajudar na solução de problemas em vários cenários (por exemplo: Comunicação NMSP entre Wireless LAN Controller (WLC) e servidor CMX) para validar o fluxo de comunicação.

Requirements

- Acesso à Interface de Linha de Comando (CLI - Command Line Interface) para o servidor CMX.
- Computador com Wireshark instalado para ler as capturas em detalhes.

Usando o TCPDUMP para Capturas

TCPDUMP é um analisador de pacotes que exibe os pacotes transmitidos e recebidos no servidor CMX. Ele serve como uma ferramenta de análise e solução de problemas para administradores de rede/sistema. O pacote é integrado ao servidor CMX, onde os dados brutos dos pacotes podem ser vistos.

A execução do tcpdump como usuário 'cmxadmin' falharia com o seguinte erro: (o acesso 'raiz' é obrigatório)

```
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)
```

Mude para o usuário 'root' depois de fazer login como usuário 'cmxadmin' no CLI sobre SSH ou console.

```
[cmxadmin@laughter ~]$ su - root
```

```
Password:
[root@laughter ~]#
```

Usando a interface correta

Anote a interface onde os pacotes seriam capturados. Ele pode ser obtido usando o comando 'ifconfig -a'

```
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 ~]$
```

Captura de pacotes

```
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 ~]#
```

Para gravar a saída em um arquivo

```
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]#
```

Quando o arquivo estiver pronto, você precisará extrair o arquivo .pcap do CMX para o computador para análise em uma ferramenta mais confortável, como o wireshark. Você pode usar qualquer aplicativo SCP para fazer isso. Por exemplo, no Windows, o aplicativo WinSCP permitirá que você se conecte ao CMX usando as credenciais SSH e você poderá navegar pelo sistema de arquivos e encontrar o arquivo .pcap que acabou de criar. Para localizar o caminho atual, digite "pwd" após executar o tcpdump para saber onde o arquivo foi salvo.

Para capturar um número específico de pacotes

Se um número específico de contagem de pacotes for desejado, use os filtros de opção -c exatamente para essa contagem.

```
[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 ~]#
```

Outras opções de filtragem

```
[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)
```

As Capturas gravadas em arquivos seriam salvas no diretório atual no servidor e podem ser copiadas para análise detalhada usando o Wireshark.