Capturas de pacote de informação na experiência móvel conectada (CMX)

Índice

Introdução

Este documento descreve em como recolher capturas de pacote de informação do CLI do server 10.x móvel conectado da experiência (CMX). Estas capturas de pacote de informação podem ajudar em pesquisar defeitos diversas encenações (por exemplo: Uma comunicação NMSP entre o controlador do Wireless LAN (WLC) e CMX server) para validar o fluxo de comunicação.

Requisitos

- Acesso do comando line interface(cli) ao server CMX.
- O computador com Wireshark instalou para ler em detalhe as captações.

Usando o TCPDUMP para captações

O TCPDUMP é um analisador de pacote que indique transmitido e os pacotes recebidos no server CMX. Serve como uma análise & uma ferramenta de Troubleshooting para a rede/administradores de sistema. O pacote é incorporado ao server CMX onde os dados brutos dos pacotes podem ser olhados.

O tcpdump running como o usuário do “cmxadmin” falharia com o seguinte erro: (o acesso da “raiz” é exigido)

```
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)
```

Comute “para enraizar” o usuário após a abertura como o usuário do “cmxadmin” ao CLI sobre o SSH ou o console.

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

Usando a relação direita

Faça a anotação da relação onde os pacotes seriam capturados. Pode ser obtida usando o “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 ~]$
```

Capturando 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 escrever a saída a 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]#
```

Uma vez o arquivo está pronto, você precisará de extrair o arquivo .pcap do CMX a seu computador para a análise em uma ferramenta mais confortável tal como o wireshark. Você pode usar todo o aplicativo SCP fazer assim. Por exemplo em Windows, o aplicativo de WinSCP permitirá que você conecte ao CMX usando as credenciais SSH e você pode então consultar o sistema de arquivos e encontrar o arquivo que .pcap você apenas criou. Para encontrar o trajeto atual, tipo “pwd” após ter executado o tcpdump para saber onde o arquivo salvar.

Para capturar o número específico de pacotes

Se um número específico de contagem de pacote de informação é desejado, utilização - a opção c filtra 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 captações escritas aos arquivos salvar no diretório atual no server e podem ser copiadas para fora para revisão detalhada usando Wireshark.