互联移动体验(CMX)上的数据包捕获

目录

简介

(CMX)10.xCLI((WLC)CMXNMSP

要求

- (CLI)CMX
- Wireshark

使用TCPDUMP捕获

TCPDUMP是一种数据包分析器，它显示CMX服务器上发送和接收的数据包。它用作网络/系统管理员的分析和故障排除工具。该包内置到CMX服务器，在该服务器中可以查看来自数据包的原始数据。

以“cmxadmin”用户身份运行tcpdump将失败，并出现以下错误：（需要“根”访问权限）

```
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)
```

以“cmxadmin”用户身份登录到CLI over SSH或控制台后，切换到“root”用户。

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

使用正确的接口

记录要捕获数据包的接口。可使用“ifconfig -a”获取

```
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 ~]$
```

捕获数据包

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 ~]#
```

将输出写入文件

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]#
```

文件准备就绪后，您需要将.pcap文件从CMX提取到计算机，以便使用更舒适的工具（如wireshark）进行分析。您可以使用任何SCP应用执行此操作。例如，在Windows中，WinSCP应用允许您使用SSH凭证连接到CMX，然后您可以浏览文件系统并找到刚创建的.pcap文件。要查找当

前路径，请在运行tcpdump后键入“pwd”，以了解文件的保存位置。

捕获特定数量的数据包

如果需要特定数量的数据包计数，则使用 — c选项完全过滤该计数。

```
[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 ~]#
```

其他过滤选项

```
[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)
```

写入文件的捕获将保存在服务器的当前目录中，并可以使用Wireshark复制出来以进行详细检查。