# Cisco Video Surveillance Media Server上的資料 包捕獲

## 目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>思科視訊監視媒體伺服器封包擷取</u> <u>步驟1.開始捕獲</u> <u>步驟2.重現問題症狀或狀況</u> <u>步驟3.停止擷取</u> <u>步驟4.從伺服器收集捕獲</u> 相關資訊

# 簡介

本檔案將說明收集傳送至Cisco Video Surveillance Media Server 6.x/7.x上的網路介面或自該介面傳送的封包的程式。

## 必要條件

#### 需求

本文件沒有特定需求。

#### 採用元件

本檔案中的資訊是根據思科視訊監視媒體伺服器6.x/7.x。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

### 思科視訊監視媒體伺服器封包擷取

當您對Cisco Video Surveillance Media Server 6.x/7.x問題進行故障排除時,有時需要收集從伺服器 上的網路介面傳送和傳送的資料包。請執行以下步驟:

- 1. 開始捕獲
- 2. 重現問題症狀或狀況
- 3. 停止擷取
- 4. 從伺服器收集捕獲

#### 步驟1.開始捕獲

若要開始擷取,請建立與Cisco Video Surveillance Media伺服器的安全殼層(SSH)作業階段,並使 用localadmin帳戶進行驗證,如圖所示。

使用命令cd /var/lib/localadmin/導航到/var/lib/localadmin資料夾



對於典型的捕獲,要收集所有地址之間所有大小的所有資料包,並將輸出儲存到名為camera.pcap 的捕獲檔案,請使用以下命令:

tcpdump -s0 -w camera.pcap

[root@cisco localadmin]# tcpdump -s0 -w camera.pcap tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byte s

排查Cisco Video Surveillance Media Server和特定主機的故障時,可以使用**host**選項來過濾進出特 定主機的流量,如下所示:

tcpdump -n host 10.88.86.58 -s0 -w camera.pcap

10.88.86.58是有問題的主機的IP

```
[root@cisco localadmin]#
[root@cisco localadmin]# tcpdump -n host 10.88.86.58 -s0 -w camera.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535
```

對使用TCP埠80進行PTZ通訊的思科或第三方ONVIF監視器上的雲台變焦(PTZ)監視器相關問題進 行故障排除時,請使用以下命令:

tcmpdump -s0 host 10.88.86.58和tcp port 80 -w camera.pcap

10.88.86.58是有問題的主機的IP

[root@cisco ~]# tcpdump -s0 host 10.88.86.58 and tcp port 80 -w camera.pcap tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byte

### 步驟2.重現問題症狀或狀況

捕獲運行時,重現問題症狀或狀況,以便將必要的資料包包含在捕獲中。如果問題間歇性出現,請 運行更長的捕獲時間。如果捕獲結束,則是因為緩衝區已滿。在這些情況下重新啟動捕獲。如果捕 獲需要較長時間,則最好在網路級別通過其他方法(例如通過在交換機上使用監控會話)進行捕獲 。

#### 步驟3.停止擷取

若要停止捕獲,請按住Control鍵並按鍵盤上的C。這會導致捕獲進程結束,並且不會向捕獲轉儲中 新增任何新資料包。

| [root@cisco localadmin]# topdump -s0 -w camera.pcap                              |   |  |  |  |  |  |  |
|----------------------------------------------------------------------------------|---|--|--|--|--|--|--|
| tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byte |   |  |  |  |  |  |  |
|                                                                                  |   |  |  |  |  |  |  |
| 158 packets captured                                                             |   |  |  |  |  |  |  |
| 158 packets received by filter                                                   |   |  |  |  |  |  |  |
| 0 packets dropped by kernel                                                      |   |  |  |  |  |  |  |
| [root@cisco localadmin]#                                                         | • |  |  |  |  |  |  |

#### 步驟4.從伺服器收集捕獲

使用WinSCP應用程式將SFTP傳送到伺服器以下載檔案。

| 🐜 Login - WinSCP |                                                 | X            |
|------------------|-------------------------------------------------|--------------|
| New Site         | Session<br>Elle protocol:<br>SFTP<br>Host name: | Pogt number: |
|                  | 10.88.86.52                                     | 22 👷         |
|                  | User name:                                      | Password:    |
|                  | localadmin                                      |              |
|                  | Save 💌                                          | Advanced 🔻   |
|                  | Manage                                          | Close Help   |
| Tools 💌          | Manage 💌 🔁 Login 💌                              | Close Help   |

### 將檔案從伺服器拖放到電腦上的所需位置。

| Sa localadmin - localadmin@10.88.86.52 - WinSCP |             |                      |       |                                          |            |                  |  |  |
|-------------------------------------------------|-------------|----------------------|-------|------------------------------------------|------------|------------------|--|--|
| Local Mark Files Commands Session Options R     | lemote Help | )                    |       |                                          |            |                  |  |  |
| 🕀 🎇 🣚 Synchronize 🔤 🦑 💽 🛞 🗟                     | 🖗 Queue 🔹   | Transfer Settings De | fault | - I 🥔 -                                  |            |                  |  |  |
| Iocaladmin@10.88.86.52 See New Session          |             |                      |       |                                          |            |                  |  |  |
| 🐇 C: Windows 🔹 🥂 🚰 😨   🗢 • 🔶 •   [              | 🖬 🕼 🏦       | 2%                   |       | 🏭 localadmin 🔹 🥶 😨   💠 - 🐡 -   🔂 🔂 🏠 🥭   | Rind Files | ₽ <mark>6</mark> |  |  |
| 🕼 Upload 🏢 📝 Edit 🗶 🛃 😡 Properties              |             |                      |       | 🔐 Download 🎲 📝 Edit 🗙 🛃 😡 Properties 📑 🕞 | • - 🗑      |                  |  |  |
| C:\Users\isambhi\Desktop\Captures               |             |                      |       | /var/lib/localadmin                      |            |                  |  |  |
| Name                                            | Size        | Туре                 | Cha   | Name                                     | Size       | Changed          |  |  |
| 🔐                                               |             | Parent directory     | 9/24  | <u>*</u>                                 |            | 5/20/2016 2:00:0 |  |  |
| amera.pcap                                      | 1 KB        | Wireshark capture    | 9/24  | amera.pcap                               | 1 KB       | 9/24/2016 3:16:4 |  |  |
|                                                 |             |                      |       |                                          |            |                  |  |  |
|                                                 |             |                      |       |                                          |            |                  |  |  |
|                                                 |             |                      |       |                                          |            |                  |  |  |
|                                                 |             |                      |       |                                          |            |                  |  |  |
|                                                 |             |                      |       |                                          |            |                  |  |  |
|                                                 |             |                      |       |                                          |            |                  |  |  |
|                                                 |             |                      |       |                                          |            |                  |  |  |
|                                                 |             |                      |       |                                          |            |                  |  |  |
|                                                 |             |                      |       |                                          |            |                  |  |  |
|                                                 |             |                      |       |                                          |            |                  |  |  |
|                                                 |             |                      |       |                                          |            |                  |  |  |
|                                                 |             |                      |       |                                          |            |                  |  |  |
|                                                 |             |                      |       |                                          |            |                  |  |  |
|                                                 |             |                      |       |                                          |            |                  |  |  |
|                                                 |             |                      |       |                                          |            |                  |  |  |
| K                                               |             |                      | •     | × [                                      |            | •                |  |  |
| 0 B of 176 B in 0 of 1                          |             |                      |       | 0 B of 176 B in 0 of 1                   |            | 6 hidden         |  |  |
| 🔒 SFTP-3 🦞 0.04:20                              |             |                      |       |                                          |            |                  |  |  |

# 相關資訊

- •如果日誌是思科TAC工程師要求的,可以使用本文檔中概述的方法之一將其上傳到TAC案例
  - : <u>http://www.cisco.com/c/en/us/about/security-center/tac-customer-file-uploads.html</u>
- 技術支援與文件 Cisco Systems