Cisco Video Surveillance Media Server上的数据包捕获

目录

简介

本文档介绍收集在Cisco Video Surveillance Media Server 6.x/7.x网络接口上发送和接收的数据包的过程。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco Video Surveillance Media Server 6.x/7.x。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

思科视频监控媒体服务器数据包捕获

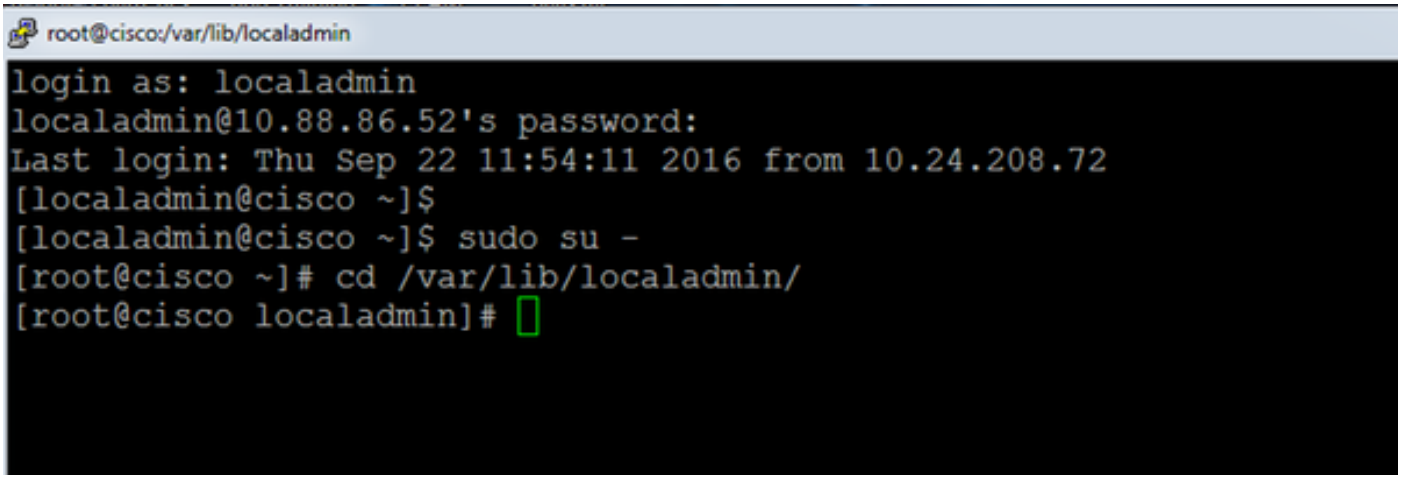
当您对Cisco Video Surveillance Media Server 6.x/7.x的问题进行故障排除时，有时需要收集发送到服务器网络接口和从服务器网络接口发送的数据包。请执行以下步骤：

1. 开始捕获
2. 重现问题症状或情况
3. 停止捕获
4. 从服务器收集捕获

步骤1.开始捕获

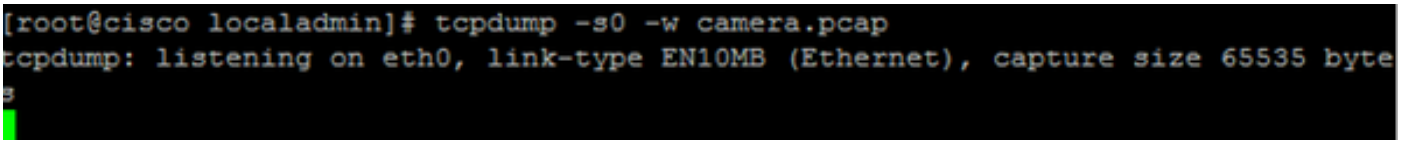
要开始捕获，请建立到Cisco Video Surveillance Media服务器的安全外壳(SSH)会话，并使用localadmin帐户进行身份验证，如图所示。

使用命令**cd /var/lib/localadmin/**导航**到/var/lib/localadmin/**



对于典型捕获，要收集来自和发往所有地址的所有大小的所有数据包并将输出保存到名为camera.pcap的捕获文件，请使**用以**下命令：

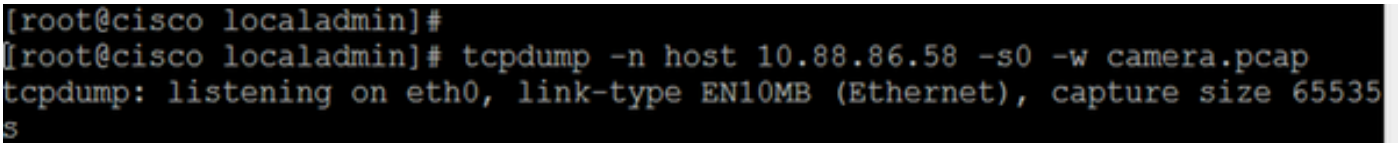
tcpdump -s0 -w camea.pcap



当您对Cisco Video Surveillance Media Server和特定主机的问题进行故障排除时，可以使用**host**选项过滤进出特定主机的流量，如下所示：

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

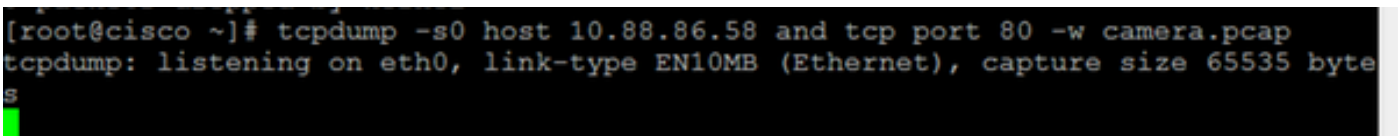
此处10.88.86.58是有问题主机的IP



当您对思科或第三方ONVIF摄像头（使用TCP端口80进行PTZ通信）上的云台倾斜变焦(PTZ)摄像头相关问题进行故障排除时，请使用以下命令：

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

此处10.88.86.58是有问题主机的IP



步骤2.重现问题症状或状况

捕获运行时，重现问题症状或情况，以便在捕获中包含必要的数据包。如果问题间歇性出现，请在较长的时间段内运行捕获。如果捕获结束，则是因为缓冲区已填充。在这种情况下，请重新启动捕获。如果需要捕获一段较长的时间，则可以通过其他方法（例如在交换机上使用监控会话）在网络级别捕获。

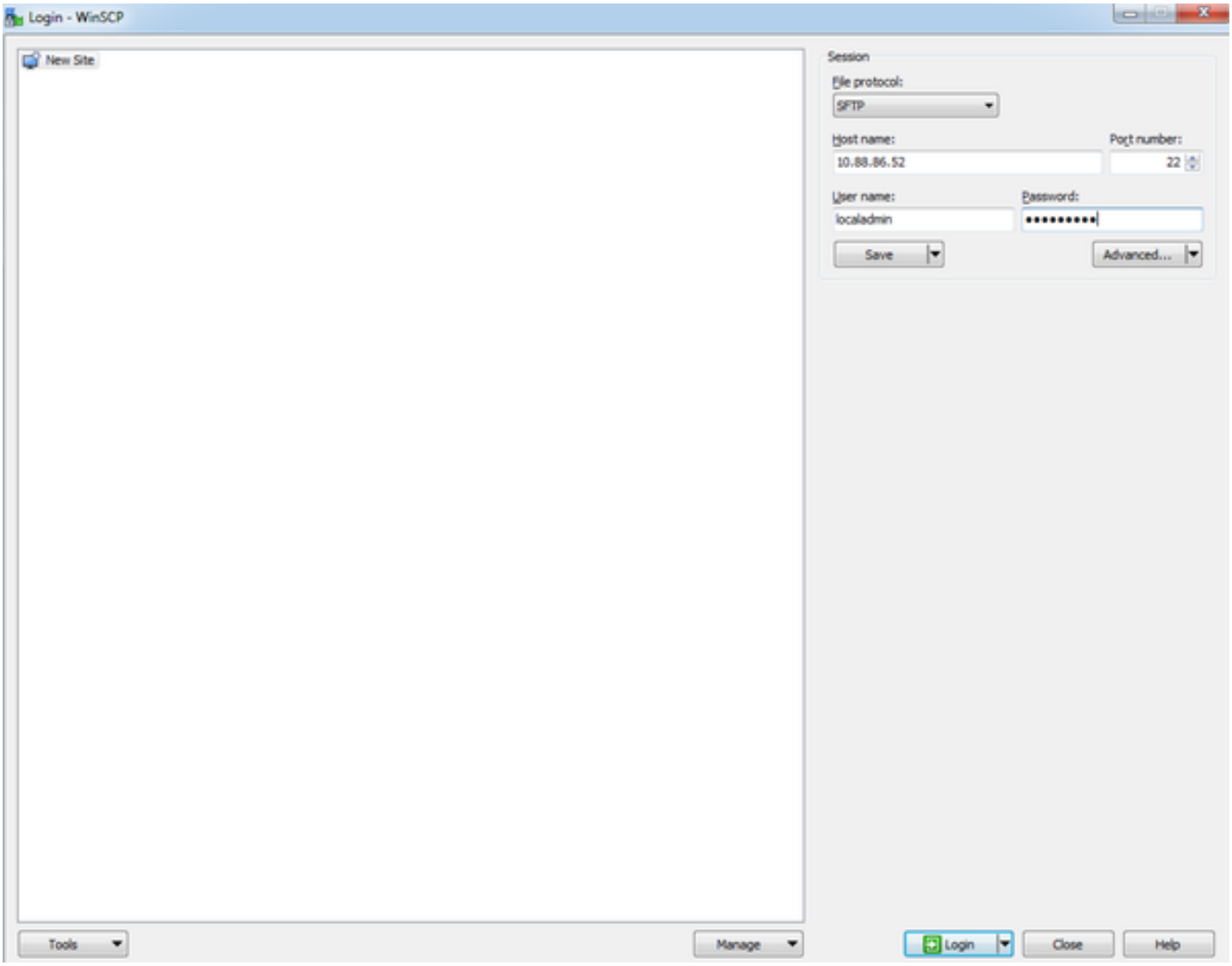
步骤3.停止捕获

要停止捕获，请按住Control键并按C键。这会导致捕获进程结束，并且不会向捕获转储添加新数据包。

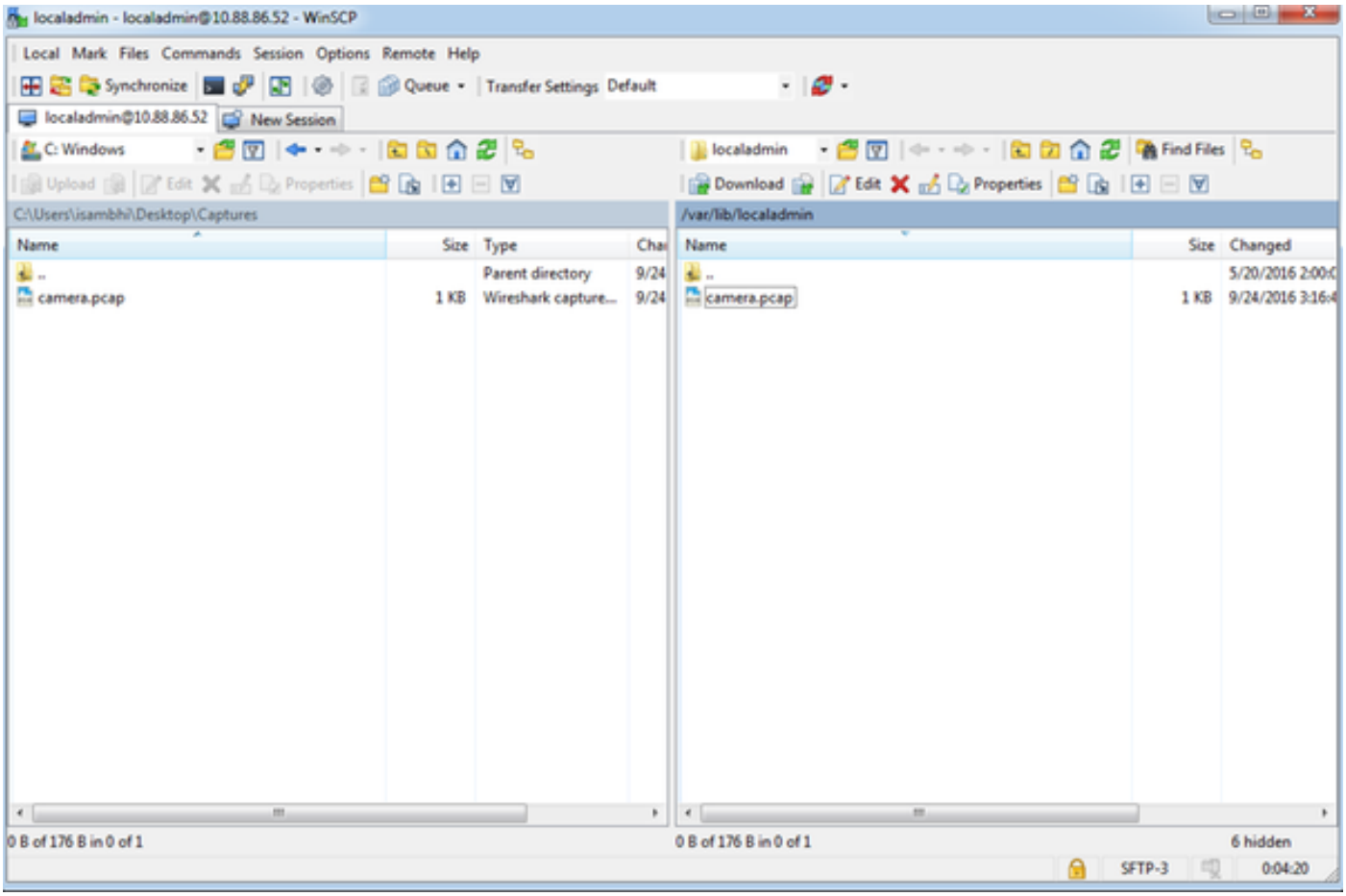
```
[root@cisco localadmin]# tcpdump -s0 -w camera.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byte
s
158 packets captured
158 packets received by filter
0 packets dropped by kernel
[root@cisco localadmin]#
```

步骤4.从服务器收集捕获

使用WinSCP应用将SFTP下载到服务器以下载文件。



将文件从服务器拖放到计算机上的所需位置。



相关信息

- 如果日志是由Cisco TAC工程师请求的，可以使用本文档中概述的方法之一将其上传到TAC案例：http://www.cisco.com/c/en/us/about/security-center/tac-customer-file-uploads.html
- 技术支持和文档 - Cisco Systems