Cisco视频Surveillance媒体服务器的数据包捕获

目录

简介

本文描述步骤收集到/从在Cisco视频Surveillance媒体服务器6.x/7.x的网络接口被发送的数据包。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据Cisco视频Surveillance媒体服务器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。

Cisco视频Surveillance媒体服务器数据包捕获

当您排除故障与Cisco视频Surveillance媒体服务器6.x/7.x时的问题，收集到/从在服务器的网络接口被发送的数据包是有时必要的。 执行下列步骤：

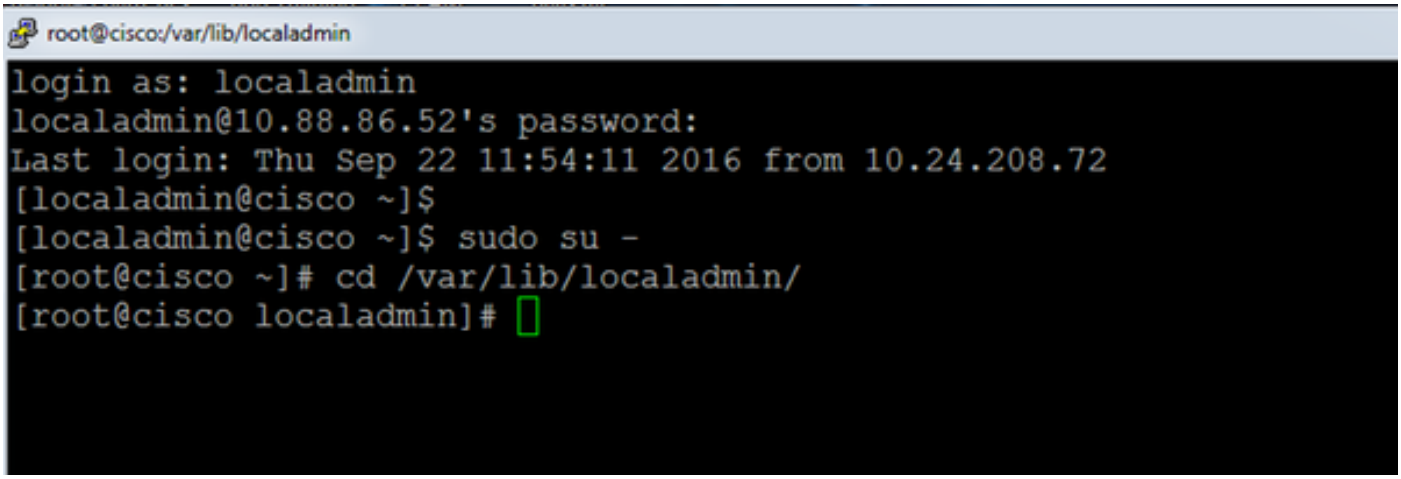
1. 开始捕获
2. 再生产问题症状或情况
3. 终止捕获
4. 收集从服务器的捕获

步骤1.开始捕获

为了开始捕获，建立安全壳SSH会话到Cisco视频Surveillance媒体服务器和验证与localadmin帐户

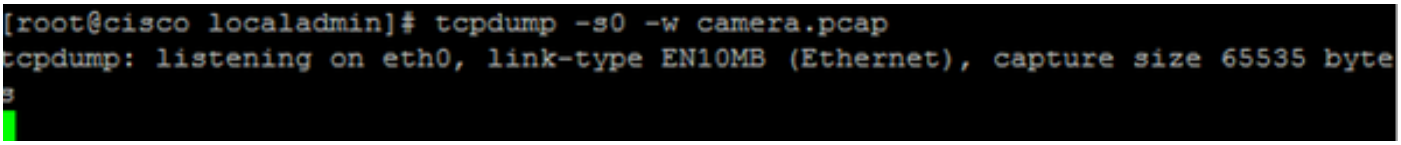
，如显示。

导航到有cd命令的/var/lib/localadmin/ /var/lib/localadmin文件夹



一个典型的捕获，收集所有信息包所有大小从和到所有地址和保存输出对呼叫**camera.pcap使用**以下命令的捕获文件：

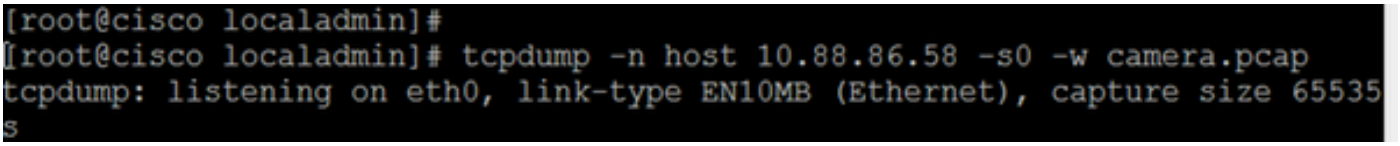
tcpdump -s0 - w camera.pcap



当您排除故障一个问题用Cisco视频Surveillance媒体服务器和特定主机时，您能使用**host选项**为了为流量过滤到/从特定主机，如显示：

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

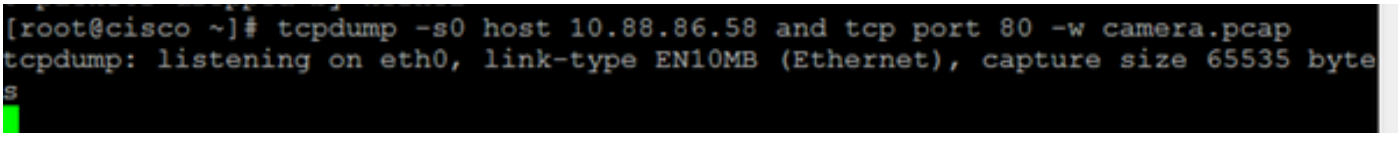
在这里10.88.86.58有问题的主机的IP



当您排除故障在思科时的平底锅掀动zoom(PTZ)摄像头相关问题或第三方ONVIF摄像头，使用TCP端口80 PTZ通信，请使用此命令：

tcmpdump -s0主机10.88.86.58和TCP端口80 - w camera.pcap

在这里10.88.86.58有问题的主机的IP



步骤2.再生产问题症状或情况

当捕获运行时，请再生产问题症状或情况，以便必要的数据包在捕获包括。如果问题断断续续，请作为扩展周期运行捕获。如果捕获结束，这是因为缓冲区被充满。在这些情况下重新启动捕获。如果捕获长时间必要，捕获在网络级通过其它方法，例如通过使用交换机的一个监控会话可以是值得的。

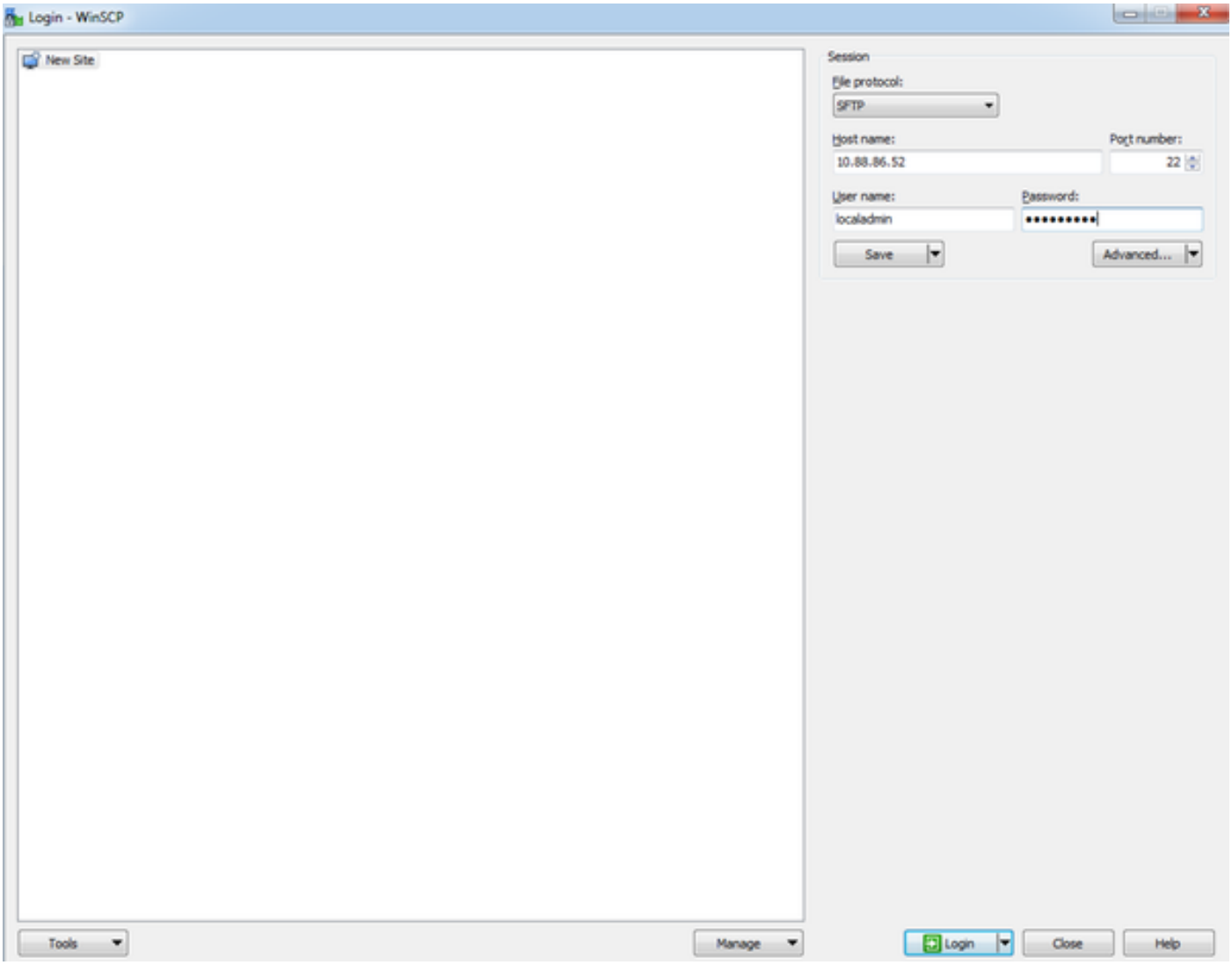
步骤3.终止捕获

为了终止捕获，请把握**控制键**并且按在键盘的**C**。这造成捕获进程结束，并且新的数据包没有被添加到捕获转储。

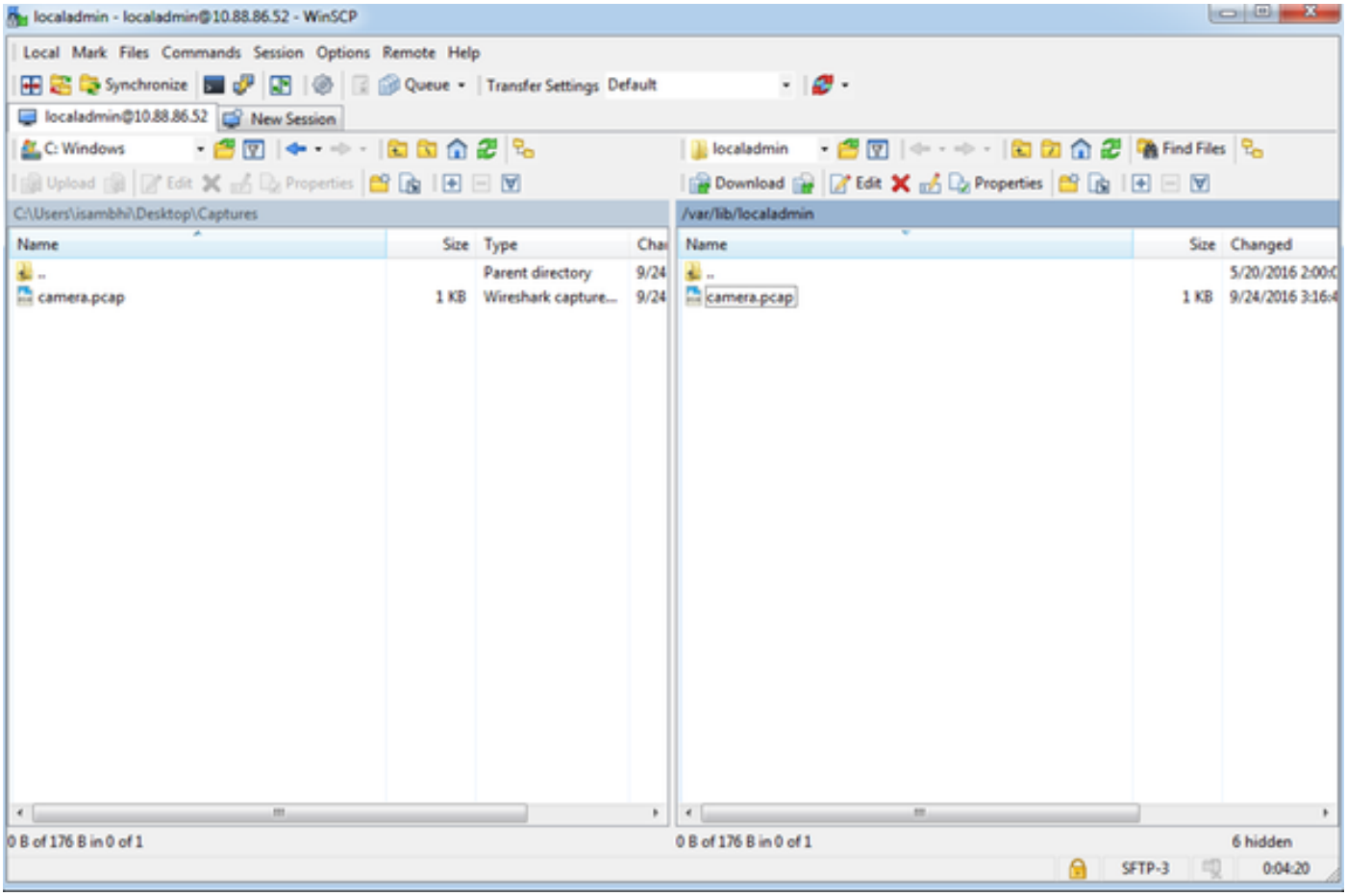
```
[root@cisco localadmin]# tcpdump -s0 -w camera.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byte
s
158 packets captured
158 packets received by filter
0 packets dropped by kernel
[root@cisco localadmin]#
```

步骤4.收集从服务器的捕获

请使用WinSCP应用程序对SFTP到服务器下载文件。



拖放从服务器的文件在您的计算机的所需位置上。



相关信息

- 如果日志由Cisco TAC工程师请求，他们可以上传到有在本文略述的其中一个的TAC案例方法：http://www.cisco.com/c/en/us/about/security-center/tac-customer-file-uploads.html
- [技术支持和文档 - Cisco Systems]