Packet Capture op Cisco Video Surveillance Media Server

Inhoud

Inleiding

Dit document beschrijft de procedure om de pakketten te verzamelen die naar en van de netwerkinterface op een Cisco Video Surveillance Media Server 6.x/7.x worden verzonden.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Video Surveillance Media Server 6.x/7.x.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Cisco Video Surveillance Media Server-pakketvastlegging

Wanneer u problemen oplossen met Cisco Video Surveillance Media Server 6.x/7.x, is het soms nodig om de pakketten te verzamelen die naar en van de netwerkinterface op de server worden verzonden. Volg deze stappen:

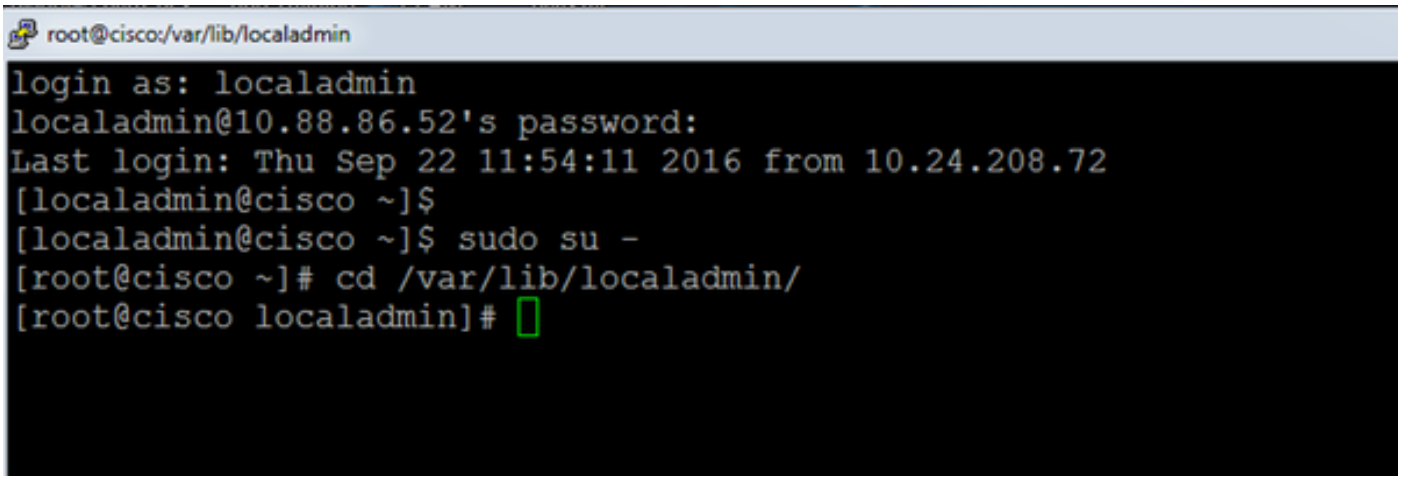
1. Start de Capture
2. Reproduceren van het probleem Symptoom of de conditionering

3. Opname stoppen
4. Verzamel de Capture from the Server

Stap 1. Start de Capture

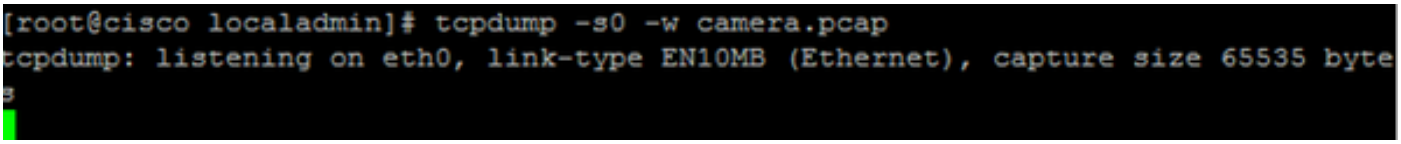
Om de opname te starten, stelt u een beveiligde shelf (SSH) sessie in op de Cisco Video Surveillance Media server en authenticeert u de lokale admin account zoals getoond.

Navigeer naar de map **/var/lib/localadmin** met de opdracht **cd /var/lib/localadmin/**



Voor een typische opname, om alle pakketten van alle groottes van en op alle adressen te verzamelen en de uitvoer naar een opnamebestand op te slaan dat **camera.pcap** heet, gebruik de volgende opdracht:

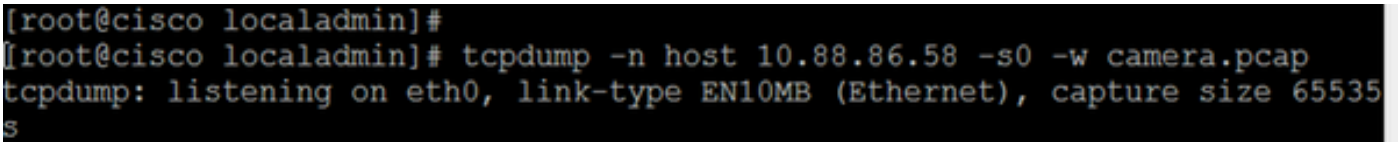
pomp -s0-w camera.pcap



Wanneer u een probleem met Cisco Video Surveillance Media Server en een bepaalde host oplossen, kunt u de **host-**optie gebruiken om voor verkeer naar en van een bepaalde host te filteren, zoals wordt weergegeven:

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

Hier is 10.8.86.58 het IP van de problematische host



Wanneer u een probleem met een Pan tilt zoom (PTZ)-camera (kanteling zoom) oplossen op een Cisco- of 3rd-partij ONVIF-camera, die TCP poort 80 voor PTZ-communicatie gebruikt, gebruikt u deze opdracht:

TCP -s0-host 10.88.86.58 en TCP-poort 80-w camera.pcap

Hier is 10.8.86.58 het IP van de problematische host

```
[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
s
```

Stap 2. Reproduceren van het probleem of de aandoening

Tijdens de vangst lopen, reproduceren de probleemsymptoom of de toestand zodat de noodzakelijke pakketten in de opname zijn opgenomen. Als het probleem zich voordoet, voert u de opname voor een langere periode uit. Als de opname stopt, komt de buffer op gang. Start de opname in dergelijke gevallen opnieuw. Als een opname voor een langere periode nodig is, kan het de moeite waard zijn om op het netwerkniveau op andere manieren op te nemen, zoals door het gebruik van een monitor sessie op een switch.

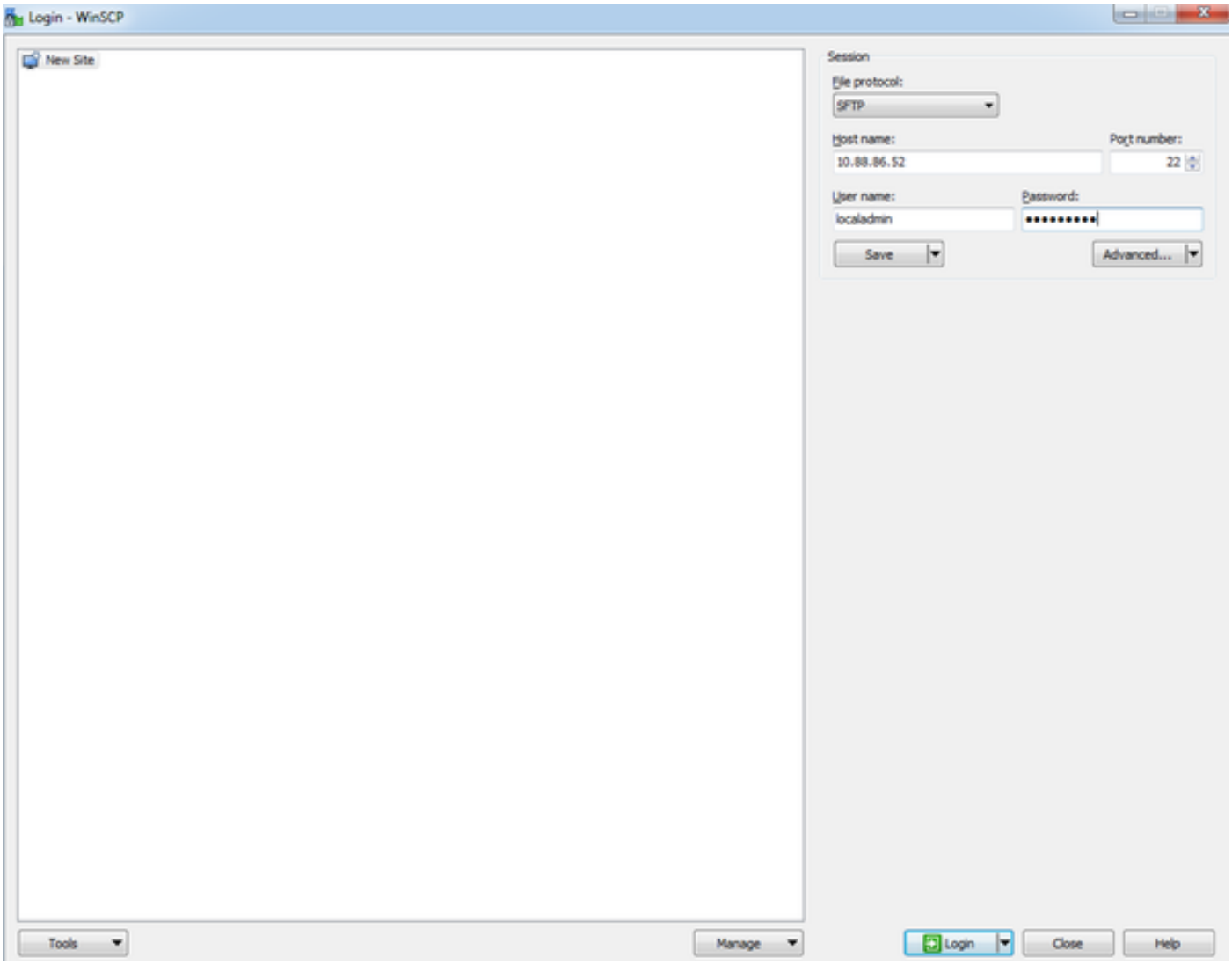
Stap 3. Stop de opname

Houd de **Control**-toets ingedrukt en druk **op** het toetsenbord om **de** opname te stoppen. Hierdoor wordt het proces van opname gestopt en worden er geen nieuwe pakketten toegevoegd aan het afvaldumpen.

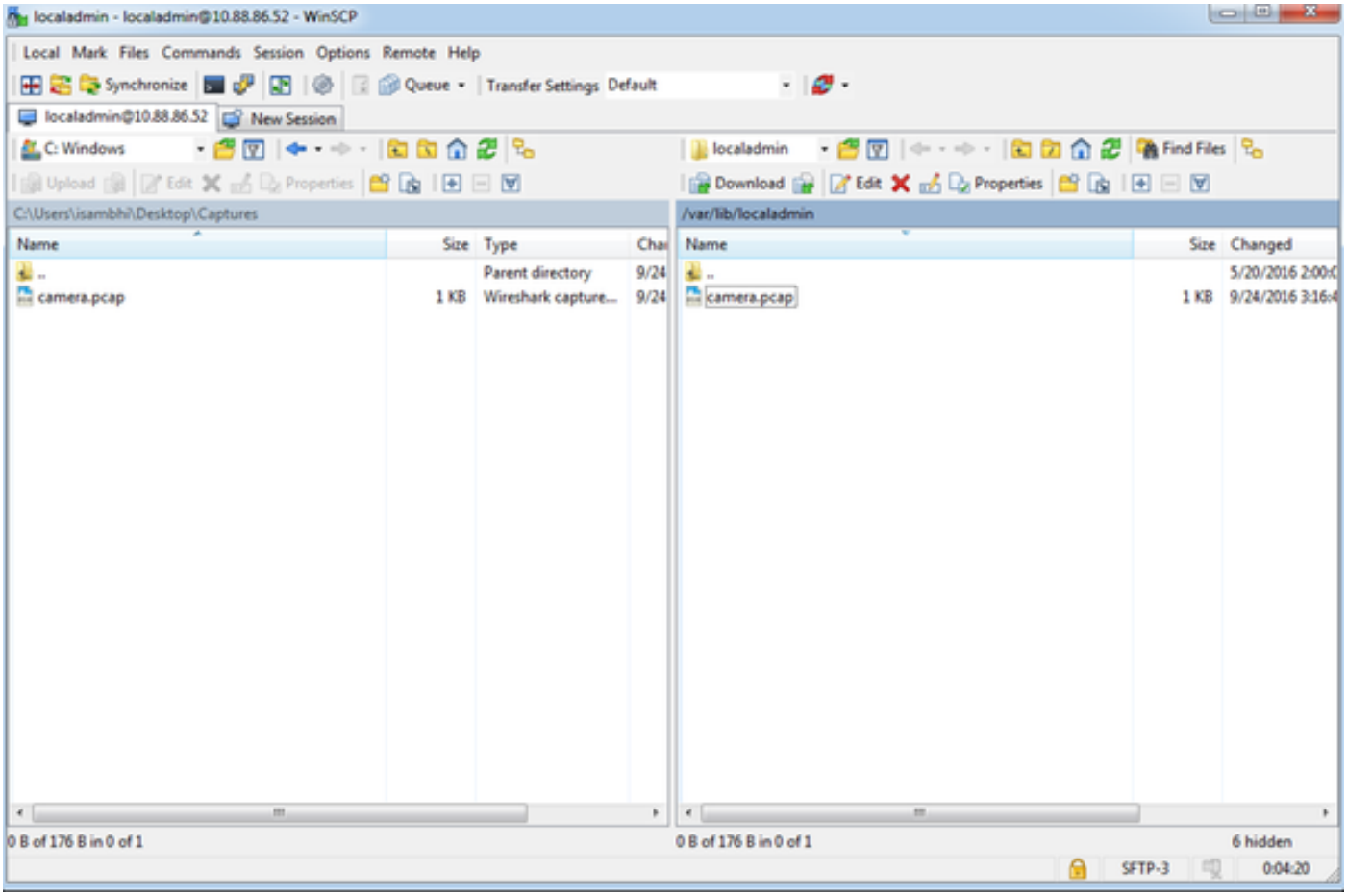
```
[root@cisco localadmin]# tcpdump -s0 -w camera.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byte
s
158 packets captured
158 packets received by filter
0 packets dropped by kernel
[root@cisco localadmin]#
```

Stap 4. Verzamel de Opname vanaf de server

Gebruik de WinSCP-toepassing van SFTP op de server om het bestand te downloaden.



Sleep het bestand van de server naar de gewenste locatie op de computer.



Gerelateerde informatie

- Als de logbestanden door een Cisco TAC-engineer zijn aangevraagd, kunnen ze met een van de in dit document beschreven methoden naar de TAC-case worden geüpload: http://www.cisco.com/c/en/us/about/security-center/tac-customer-file-uploads.html
- Technische ondersteuning en documentatie – Cisco Systems