Paketerfassung auf Cisco Video Surveillance Media Server

Inhalt

Einführung

Dieses Dokument beschreibt das Verfahren zum Sammeln der Pakete, die an die Netzwerkschnittstelle eines Cisco Video Surveillance Media Server 6.x/7.x gesendet werden.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco Video Surveillance Media Server 6.x/7.x.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Paketerfassung für Cisco Video Surveillance Media Server

Wenn Sie Probleme mit dem Cisco Video Surveillance Media Server 6.x/7.x beheben, ist es manchmal notwendig, die an die Netzwerkschnittstelle des Servers und von dieser gesendeten Pakete zu erfassen. Gehen Sie folgendermaßen vor:

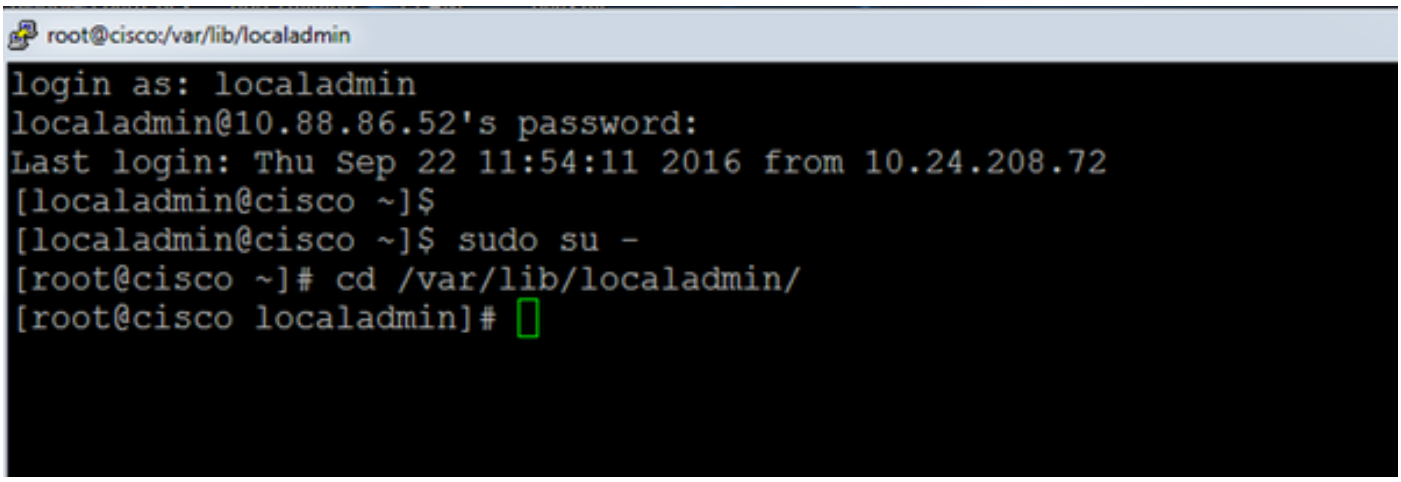
1. Erfassen starten

2. Reproduzieren des Problemsymptoms oder -zustands
3. Erfassen beenden
4. Erfassen der Erfassung vom Server

Schritt 1: Erfassen starten

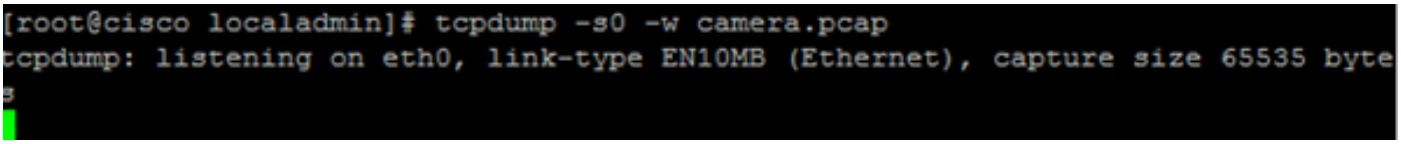
Um die Erfassung zu starten, richten Sie eine Secure Shell (SSH)-Sitzung zum Cisco Video Surveillance Media-Server ein, und authentifizieren Sie sich wie gezeigt mit dem lokalen Admin-Konto.

Navigieren Sie zum Ordner **/var/lib/localadmin** mit dem Befehl **cd /var/lib/localadmin/**



Um eine typische Erfassung durchzuführen, müssen Sie alle Pakete aller Größen von und zu allen Adressen erfassen und die Ausgabe in einer Erfassungsdatei mit dem Namen **camera.pcap** speichern. Verwenden Sie den folgenden Befehl:

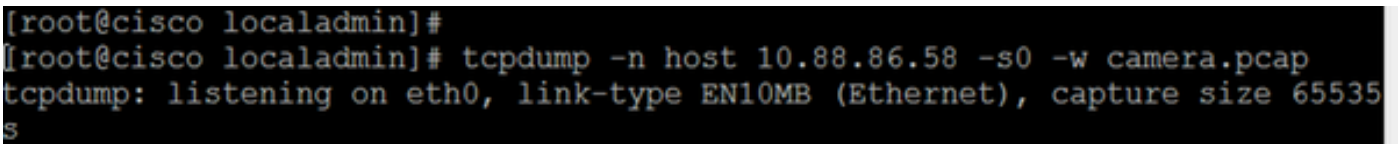
tcpdump -s0 -w camera.pcap



Wenn Sie ein Problem mit dem Cisco Video Surveillance Media Server und einem bestimmten Host beheben, können Sie die **Host-**Option verwenden, um den Datenverkehr zu und von einem bestimmten Host zu filtern, wie folgt:

tcpdump -n host 10,88,86,58 -s0 -w camera.pcap

Hier ist 10.88.86.58 die IP des problematischen Hosts



Wenn Sie ein Problem mit einer PTZ-Kamera (Schwenk-/Neigefunktion und optischem Zoom) bei einer ONVIF-Kamera von Cisco oder einem Drittanbieter, die TCP-Port 80 für die PTZ-Kommunikation verwendet, beheben, verwenden Sie den folgenden Befehl:

tcmpdump -s0 host 10,88,86,58 und tcp port 80 -w camera.pcap

Hier ist 10.88.86.58 die IP des problematischen Hosts

```
[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
```

Schritt 2: Reproduzieren des Problemsymptoms oder -zustands

Reproduzieren Sie während der Erfassung das Problem-Symptom oder den Zustand, sodass die erforderlichen Pakete in die Erfassung einbezogen werden. Wenn das Problem nur gelegentlich auftritt, führen Sie die Erfassung für einen längeren Zeitraum aus. Wenn die Erfassung beendet ist, liegt dies daran, dass der Puffer gefüllt ist. Starten Sie die Erfassung in solchen Fällen neu. Wenn eine Erfassung über einen längeren Zeitraum benötigt wird, kann es sich lohnen, sie auf Netzwerkebene auf andere Weise zu erfassen, z. B. durch die Verwendung einer Überwachungssitzung auf einem Switch.

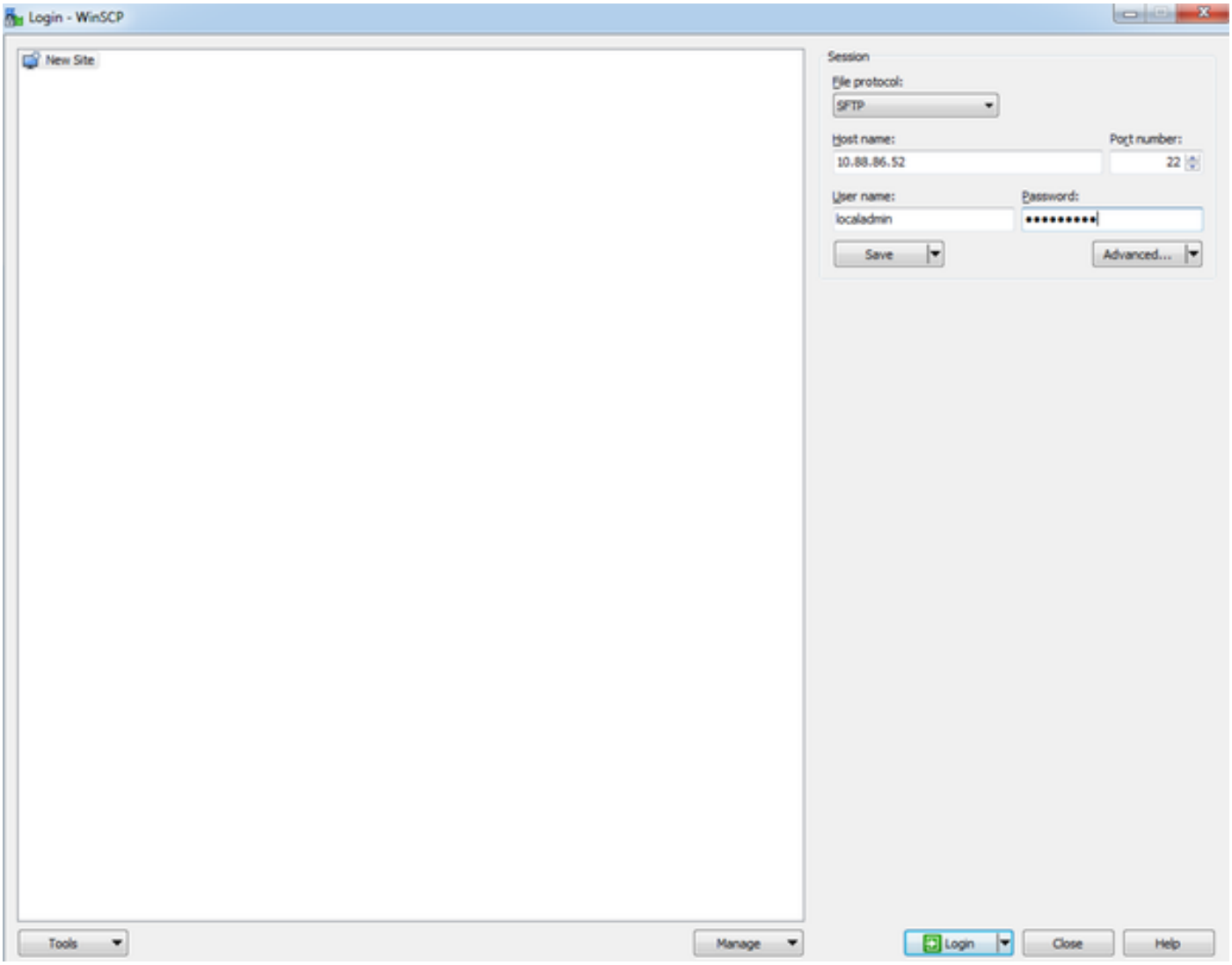
Schritt 3: Erfassen beenden

Um die Erfassung zu stoppen, halten Sie die **Strg**-Taste gedrückt und drücken Sie **C** auf der Tastatur. Dadurch wird der Erfassungsprozess beendet, und es werden keine neuen Pakete zum Erfassungsdump hinzugefügt.

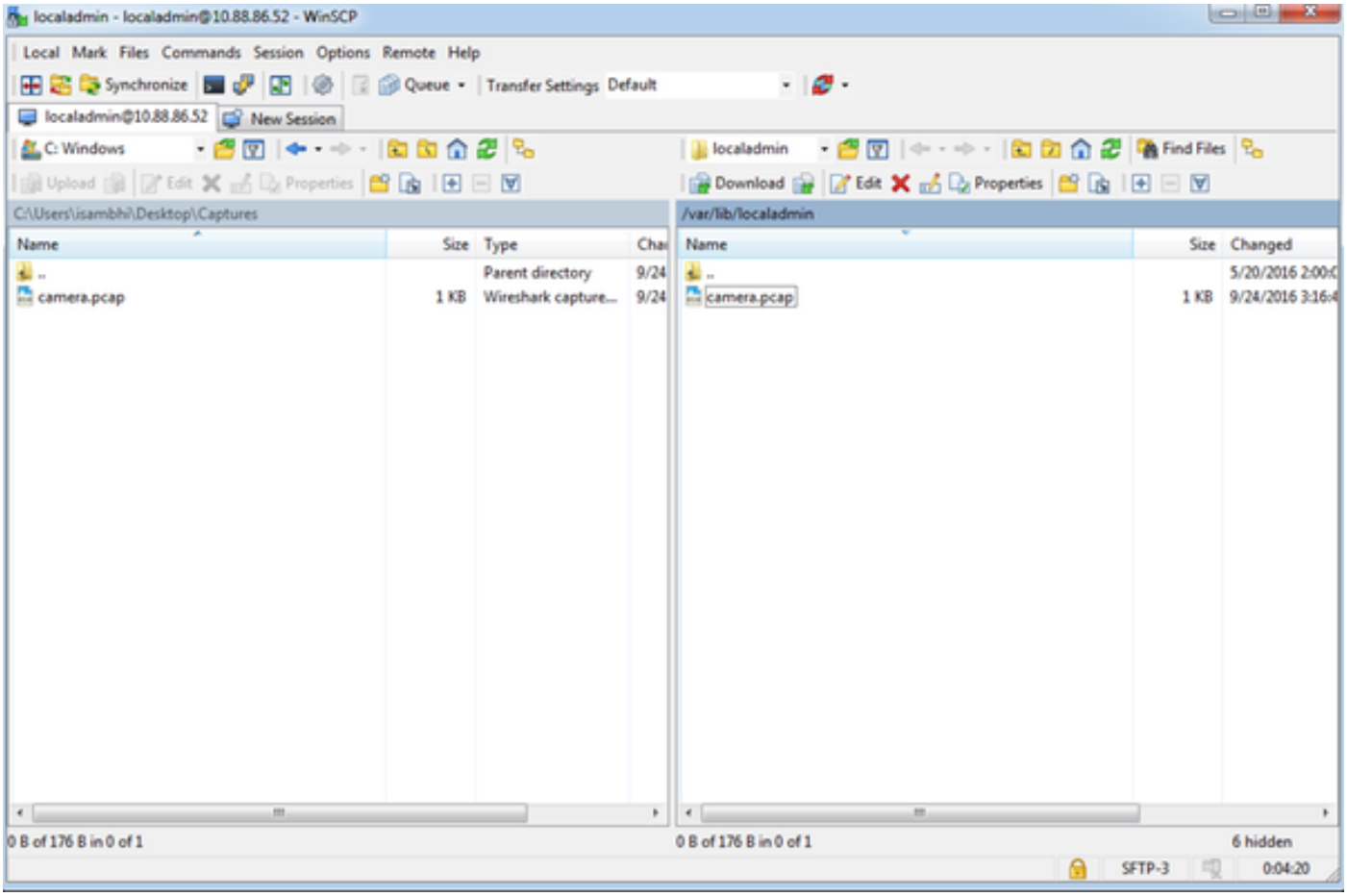
```
[root@cisco localadmin]# tcpdump -s0 -w camera.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byte
s
158 packets captured
158 packets received by filter
0 packets dropped by kernel
[root@cisco localadmin]#
```

Schritt 4: Erfassen der Erfassung vom Server

Verwenden Sie die WinSCP-Anwendung, um die Datei über SFTP auf den Server herunterzuladen.



Ziehen Sie die Datei vom Server auf den gewünschten Speicherort auf Ihrem Computer.



Zugehörige Informationen

- Wenn die Protokolle von einem Cisco TAC-Techniker angefordert wurden, können sie mit einer der in diesem Dokument beschriebenen Methoden in den TAC-Fall hochgeladen werden: http://www.cisco.com/c/en/us/about/security-center/tac-customer-file-uploads.html
- Technischer Support und Dokumentation - Cisco Systems