

# パケットキャプチャ on Cisco ビデオ監視 Media Server

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[Cisco ビデオ サーベイランス Media Server パケットキャプチャ](#)

[ステップ 1.キャプチャを開始して下さい](#)

[ステップ 2.問題の症状を再生するか、または状態](#)

[ステップ 3.キャプチャを停止して下さい](#)

[ステップ 4.サーバからキャプチャを集めて下さい](#)

[関連情報](#)

## 概要

この資料は Cisco ビデオ サーベイランス Media Server 6.x/7.x のネットワーク インターフェイスに出入して送信されるパケットを収集するためにプロシージャを記述したものです。

## 前提条件

### 要件

このドキュメントに関する固有の要件はありません。

### 使用するコンポーネント

この文書に記載されている情報は Cisco ビデオ サーベイランス Media Server 6.x/7.x に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## Cisco ビデオ サーベイランス Media Server パケットキャプチャ

Cisco ビデオ サーベイランス Media Server 6.x/7.x で問題を解決するとき、サーバのネットワーク インターフェイスに出入して送信されるパケットを収集することは時々必要です。次の手順に従ってください。

### 1. キャプチャの開始

2. 問題の症状を再生するか、または状態
3. キャプチャを停止して下さい
4. サーバからキャプチャを集めて下さい

## ステップ 1.キャプチャを開始して下さい

キャプチャを開始するため、セキュア シェル ( SSH ) セッション、および示されている localadmin アカウントの認証するを、Cisco ビデオ サーベイランス Media Server に確立するため。

コマンド `cd /var/lib/localadmin/` の `/var/lib/localadmin` フォルダにナビゲートして下さい

```
root@cisco:/var/lib/localadmin
login as: localadmin
localadmin@10.88.86.52's password:
Last login: Thu Sep 22 11:54:11 2016 from 10.24.208.72
[localadmin@cisco ~]$
[localadmin@cisco ~]$ sudo su -
[root@cisco ~]# cd /var/lib/localadmin/
[root@cisco localadmin]#
```

典型的なキャプチャに関しては、すべてのサイズのすべてのパケットをすべてのアドレスからおよびに収集し、出力を `camera.pcap` 使用を次のコマンドと呼ばれるキャプチャ ファイルに保存するため:

`tcpdump -s0 -w camera.pcap`

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

Cisco ビデオ サーベイランス Media Server およびあるホストで問題を解決するとき、示されているようにあるホストに出入してトラフィックのために、フィルタリングするためにホスト オプションを使用できます:

`tcpdump -n ホスト 10.88.86.58 -s0 -w camera.pcap`

ここに 10.88.86.58 は問題となるホストの IP です

```
[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 bytes
```

Cisco のパン傾き zoom ( PTZ ) カメラ関連 問題を解決するかまたは PTZ 通信のために TCP ポート 80 を使用するサードパーティ ONVIF カメラとき、このコマンドを使用して下さい:

tcpdump -s0 ホスト 10.88.86.58 および TCPポート 80 -w camera.pcap

ここに 10.88.86.58 は問題となるホストの IP です

```
[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
```

## ステップ 2.問題の症状を再生するか、または状態

キャプチャが動作する間、必要なパケットがキャプチャに含まれているように問題の症状を再生するか、または調節して下さい。問題が断続的である場合、キャプチャを長期間にわたって実行して下さい。キャプチャが終了する場合、バッファが充満するという理由によります。キャプチャをそのような場合再起動して下さい。キャプチャが長時間にわたって必要とされる場合、スイッチのモニタセッションの使用によってのような他の手段によってネットワークレベルで、キャプチャすることは価値があります。

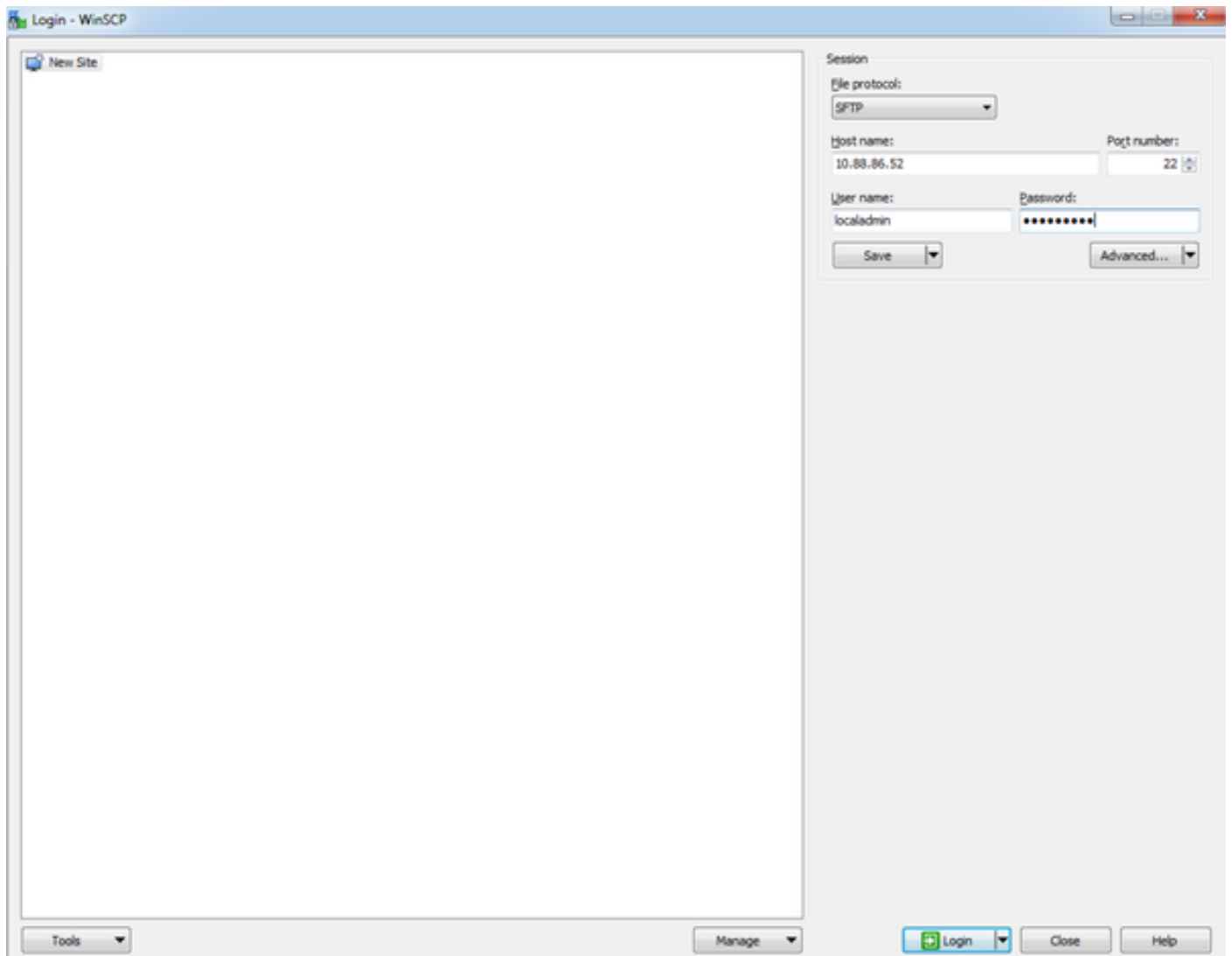
## ステップ 3.キャプチャを停止して下さい

キャプチャを停止するために、コントロール キーを握り、キーボードの C を押して下さい。これによりキャプチャ プロセスは終了します、新しいパケットはキャプチャ ダンプするに追加されません。

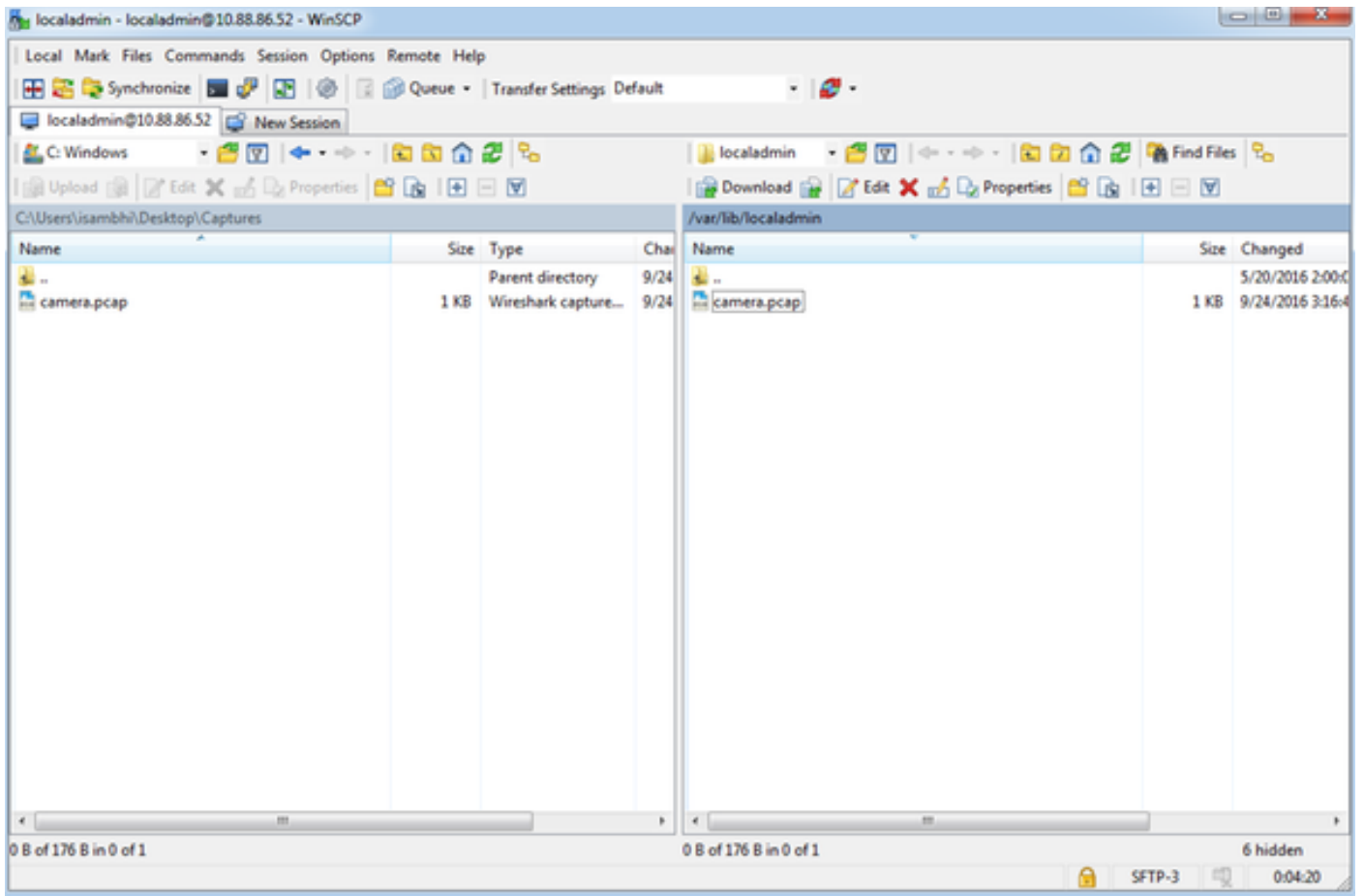
```
[root@cisco localadmin]# tcpdump -s0 -w camera.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byte
s
158 packets captured
158 packets received by filter
0 packets dropped by kernel
[root@cisco localadmin]#
```

## ステップ 4.サーバからキャプチャを集めて下さい

ファイルをダウンロードするのにサーバに SFTP に WinSCP アプリケーションを使用して下さい。



コンピュータの目的の場所にサーバからのファイルをドラッグ・アンド・ドロップして下さい。



## 関連情報

- ログが Cisco TAC エンジニアによって要求された場合、この資料で説明されているメソッドの 1 つの TAC ケースにアップロードすることができます  
: <http://www.cisco.com/c/en/us/about/security-center/tac-customer-file-uploads.html>
- [テクニカルサポートとドキュメント - Cisco Systems](#)