

CUCMパケットキャプチャ(PCAP)からTLS証明書 をエクスポートする方法

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[CUCM PCAPからのTLS証明書のエクスポート](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Cisco Unified Communications Manager(CUCM)PCAPから証明書をエクスポートする手順について説明します。

著者 : Cisco TACエンジニア、Adrian Esquillo

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ・ Transport Layer Security(TLS)ハンドシェイク
- ・ CUCM証明書管理
- ・ セキュアファイル転送プロトコル(SFTP)サーバ
- ・ リアルタイム監視ツール(RTMT)

- ・ Wiresharkアプリケーション

使用するコンポーネント

- ・ CUCMリリース9.X以降

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

サーバ証明書/証明書チェーンは、サーバから提供されたサーバ証明書/証明書チェーンが、アップ

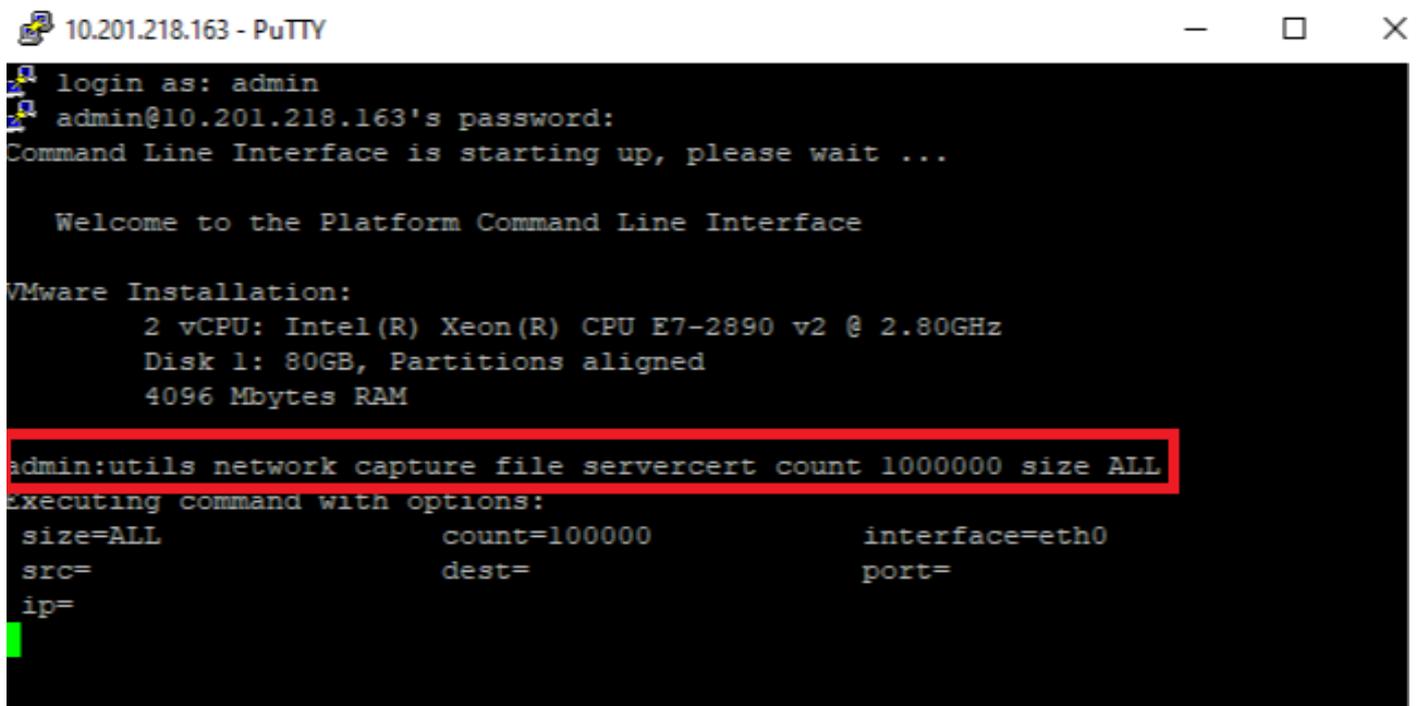
ロードする証明書またはCUCM証明書管理にアップロードされた証明書と一致することを確認するためにエクスポートできます。

TLSハンドシェイクの一部として、サーバはサーバ証明書/証明書チェーンをCUCMに提供します。

CUCM PCAPからのTLS証明書のエクスポート

ステップ1:CUCMでpacket captureコマンドを開始します

CUCMノードへのセキュアシェル(SSH)接続を確立し、図に示すように、`utils network capture (or capture-rotate) file <filename> count 1000000 size ALL`コマンドを実行します。



```
10.201.218.163 - PuTTY
login as: admin
admin@10.201.218.163's password:
Command Line Interface is starting up, please wait ...

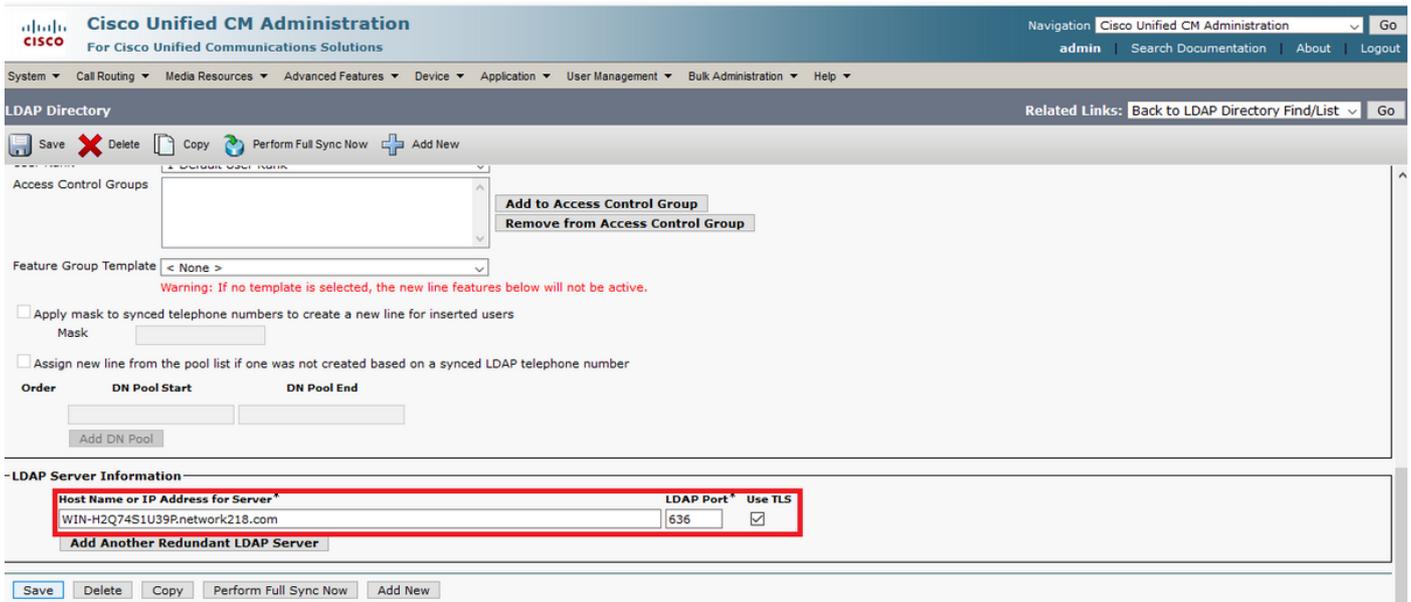
Welcome to the Platform Command Line Interface

VMware Installation:
  2 vCPU: Intel(R) Xeon(R) CPU E7-2890 v2 @ 2.80GHz
  Disk 1: 80GB, Partitions aligned
  4096 Mbytes RAM

admin:utils network capture file servercert count 1000000 size ALL
executing command with options:
size=ALL          count=100000          interface=eth0
src=              dest=                port=
ip=
```

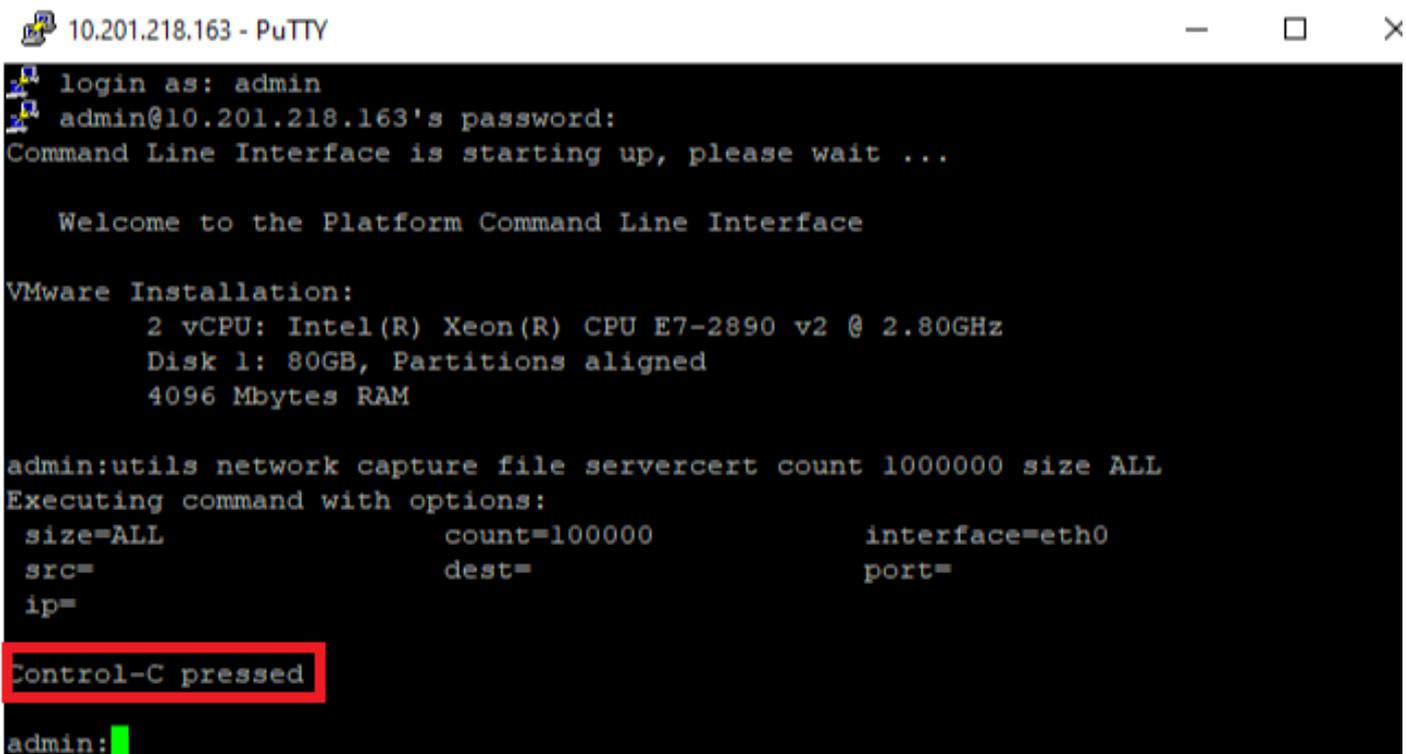
ステップ2 : サーバとCUCM間のTLS接続を開始します

この例では、図に示すように、TLSポート636で接続を確立することで、Secure Lightweight Directory Access Protocol(LDAPS)サーバとCUCM間のTLS接続を開始します。



ステップ3:TLSハンドシェイク完了後にCUCM PCAPを停止する

図に示すように、Control-Cを押してパケットキャプチャを停止します



ステップ4 : 次の2つの方法のいずれかでパッカーキャプチャファイルをダウンロードします

1. CUCMノードのRTMTを起動し、[System] > [Tools] > [Trace] > [Trace & Log Central] > [Collect Files]に移動し、[Packet Capture Logs]ボックスをオンにします (pcapをダウンロードするには RTMTプロセスをします)。

Collect Files

Select System Services/Applications

Select all Services on all Servers

Name	All Servers	<input type="checkbox"/> cucmpub216.network...	<input type="checkbox"/> imp216.network2
PIPS Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Host Resources Agent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform CLI Created Reports	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform CLI Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform Cert Monitor Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform CertMgr Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform Cluster Manager Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform GUI Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform IPSecMgmt Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform RemoteSupport Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Install File Signing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Install and Upgrade Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerneldump Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MIB2 Agent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mail Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mgetty Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NTP Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Packet Capture Logs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Prog Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SAR Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SELinux logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SNMP Master Agent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Service Manager	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Service Registration Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Spooler Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System Application Agent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

< Back Next > Finish Cancel

2. SFTP (Secure File Transport Protocol)サーバを起動し、CUCM SSHセッションでfile get activelog /patform/cli/<pcap filename>.capコマンドを実行します(プロンプトに従ってSFTPサーバにPCAPをダウンロードします)。

```
10.201.218.163 - PuTTY
2 vCPU: Intel(R) Xeon(R) CPU E7-2890 v2 @ 2.80GHz
Disk 1: 80GB, Partitions aligned
4096 Mbytes RAM

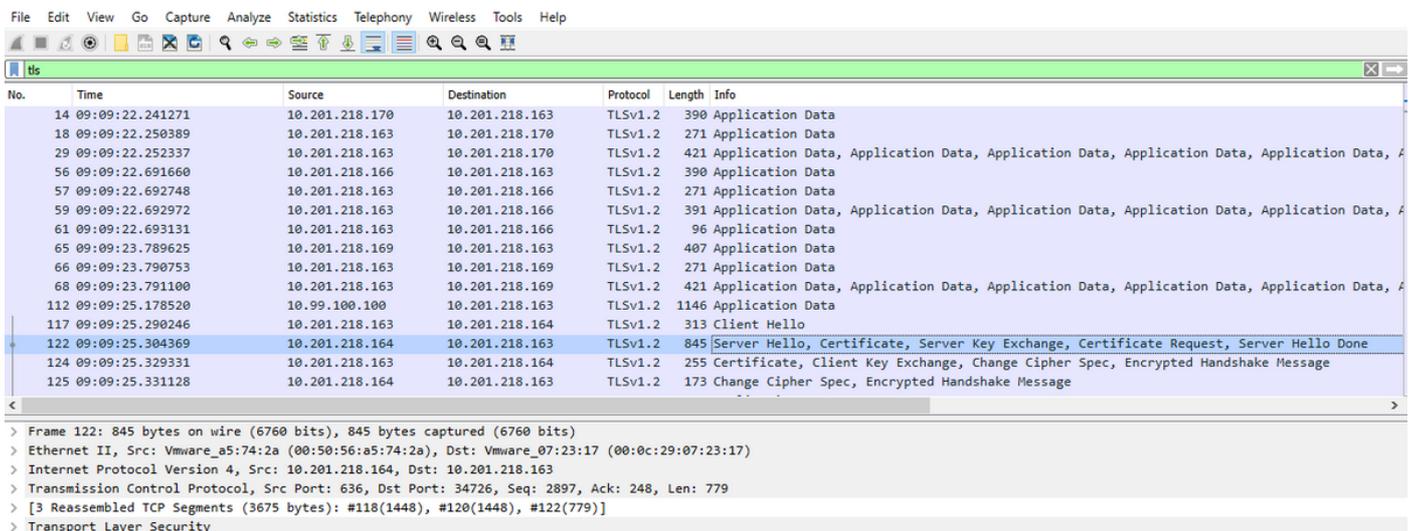
admin:utils network capture file servercert count 1000000 size ALL
Executing command with options:
  size=ALL          count=100000          interface=eth0
  src=              dest=              port=
  ip=

Control-C pressed

admin:file get activelog /platform/cli/servercert
Please wait while the system is gathering files info ...done.
No such file or directory can be found.
admin:file get activelog /platform/cli/servercert.cap
Please wait while the system is gathering files info ...
  Get file: /var/log/active/platform/cli/servercert.cap
done.
Sub-directories were not traversed.
Number of files affected: 1
Total size in Bytes: 806378
Total size in Kbytes: 787.4785
Would you like to proceed [y/n]? [ ]
```

ステップ5：サーバがCUCMに提示する証明書の数を決める

Wiresharkアプリケーションを使用してpcapを開き、tlsでフィルタを実行し、CUCMに提示されるサーバ証明書/証明書チェーンを含むServer Helloパケットを判別します。これは、図に示すように、フレーム122です。



・ CUCMに提示される証明書の数を確認するには、証明書を含まServer Helloパケットから [Transport Layer Security] > [Certificate]の情報を展開します。一番上の証明書はサーバ証明書です。この場合、サーバ証明書である1つの証明書だけが図のように表示されます。

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls

No.	Time	Source	Destination	Protocol	Length	Info
122	09:09:25.304369	10.201.218.164	10.201.218.163	TLSv1.2	845	Server Hello, Certificate, Server K
124	09:09:25.329331	10.201.218.163	10.201.218.164	TLSv1.2	255	Certificate, Client Key Exchange, C
125	09:09:25.331128	10.201.218.164	10.201.218.163	TLSv1.2	173	Change Cipher Spec, Encrypted Hands
126	09:09:25.333417	10.201.218.163	10.201.218.164	TLSv1.2	199	Application Data
127	09:09:25.335730	10.201.218.164	10.201.218.163	TLSv1.2	167	Application Data
128	09:09:25.339000	10.201.218.163	10.201.218.164	TLSv1.2	327	Application Data
129	09:09:25.339649	10.201.218.164	10.201.218.163	TLSv1.2	167	Application Data

> Frame 122: 845 bytes on wire (6760 bits), 845 bytes captured (6760 bits)

> Ethernet II, Src: Vmware_a5:74:2a (00:50:56:a5:74:2a), Dst: Vmware_07:23:17 (00:0c:29:07:23:17)

> Internet Protocol Version 4, Src: 10.201.218.164, Dst: 10.201.218.163

> Transmission Control Protocol, Src Port: 636, Dst Port: 34726, Seq: 2897, Ack: 248, Len: 779

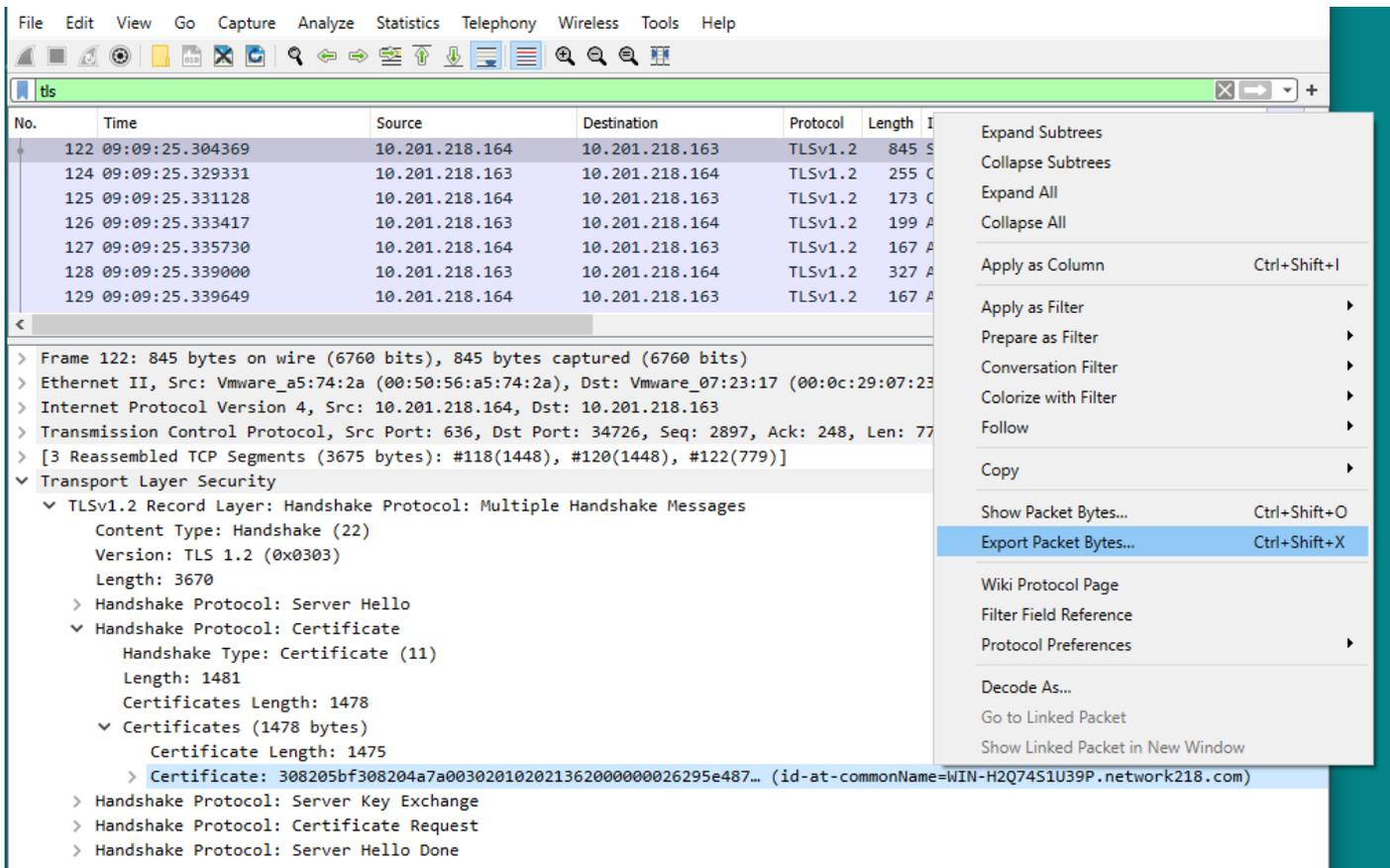
> [3 Reassembled TCP Segments (3675 bytes): #118(1448), #120(1448), #122(779)]

▼ Transport Layer Security

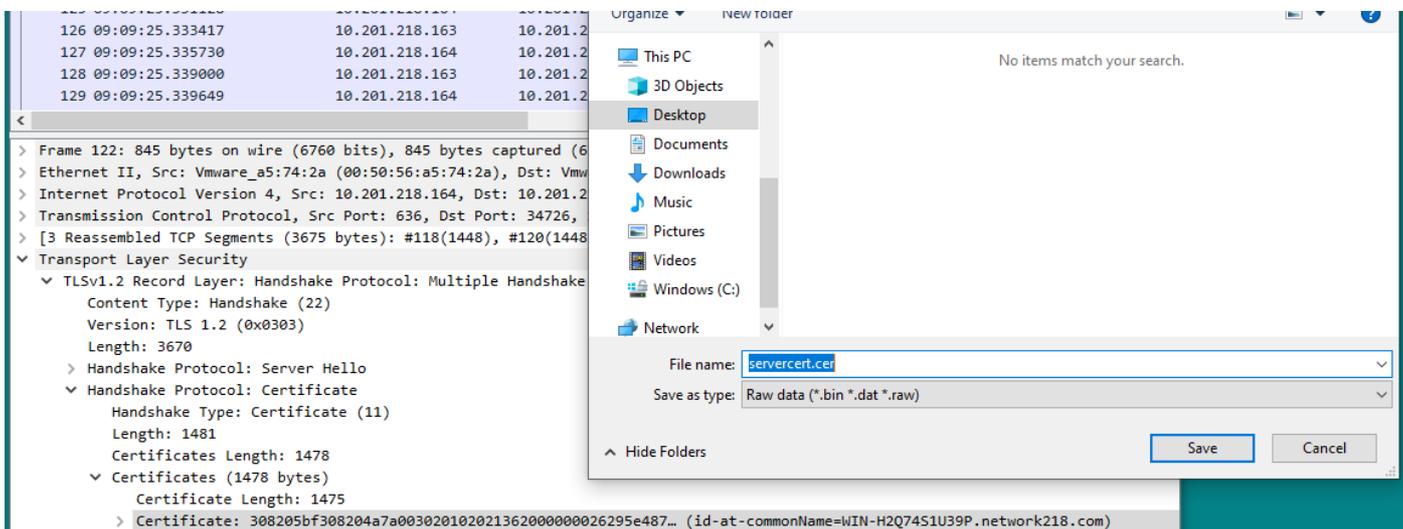
- ▼ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 3670
 - > Handshake Protocol: Server Hello
 - ▼ Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 1481
 - Certificates Length: 1478
 - ▼ Certificates (1478 bytes)
 - Certificate Length: 1475
 - > Certificate: 308205bf308204a7a00302010202136200000026295e487... (id-at-commonName=WIN-H207451U39P.network218.com)
 - > Handshake Protocol: Server Key Exchange
 - > Handshake Protocol: Certificate Request
 - > Handshake Protocol: Server Hello Done

ステップ6: CUCM PCAPからサーバ証明書/証明書チェーンをエクスポートします

この例では、サーバ証明書だけが示されているため、サーバ証明書を調べる必要があります。図に示すように、サーバ証明書を右クリックし、[Export Packet Bytes]を選択して.cer証明書として保存します。

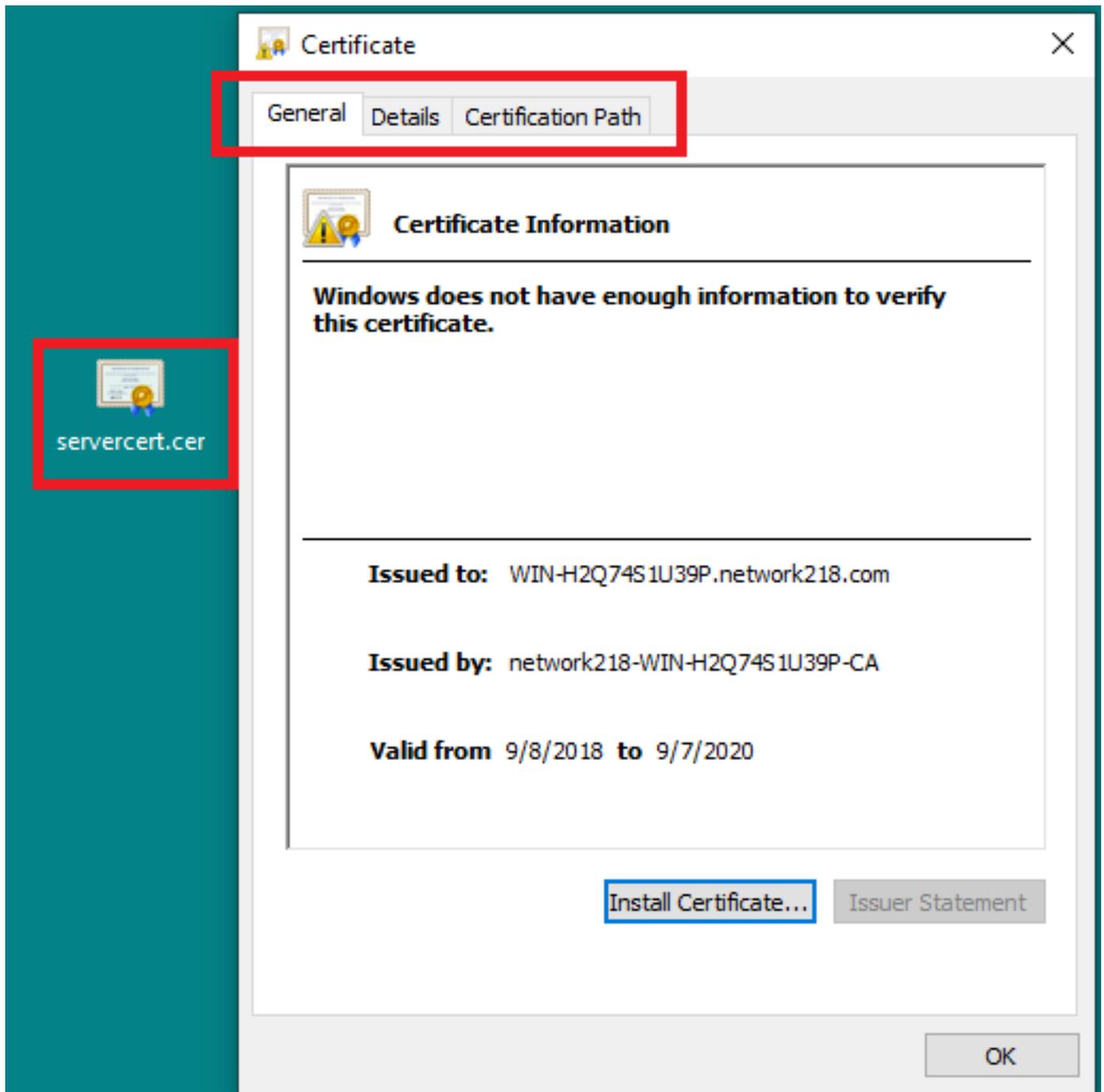


・ 後続のウィンドウで、.cerファイル名を入力し、[保存]をクリックします。次の図に示すように、デスクトップに保存されたファイルの名前はservercert.cerです（この場合はデスクトップに保存されます）。



ステップ7：保存した.CERファイルを開いて内容を確認する

.cerファイルをダブルクリックして、[General]、[Details]、および[Certificate Path]タブの情報を確認します（図を参照）。



確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。