

Comment exporter le certificat TLS à partir de CUCM Packet Capture (PCAP)

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Exporter le certificat TLS de CUCM PCAP](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit la procédure à suivre pour exporter un certificat à partir d'un PCAP Cisco Unified Communications Manager (CUCM).

Avec la collaboration d'Adrian Esquillo, ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

Prise de contact · TLS (Transport Layer Security)

Gestion des certificats · CUCM

· serveur SFTP (Secure File Transport Protocol)

Outil · de surveillance en temps réel (RTMT)

· application Wireshark

Components Used

· CUCM version 9.X et ultérieure

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Une chaîne de certificats/certificats de serveur peut être exportée afin de confirmer que le certificat/la chaîne de certificats de serveur fourni par le serveur correspond au(x) certificat(s) à

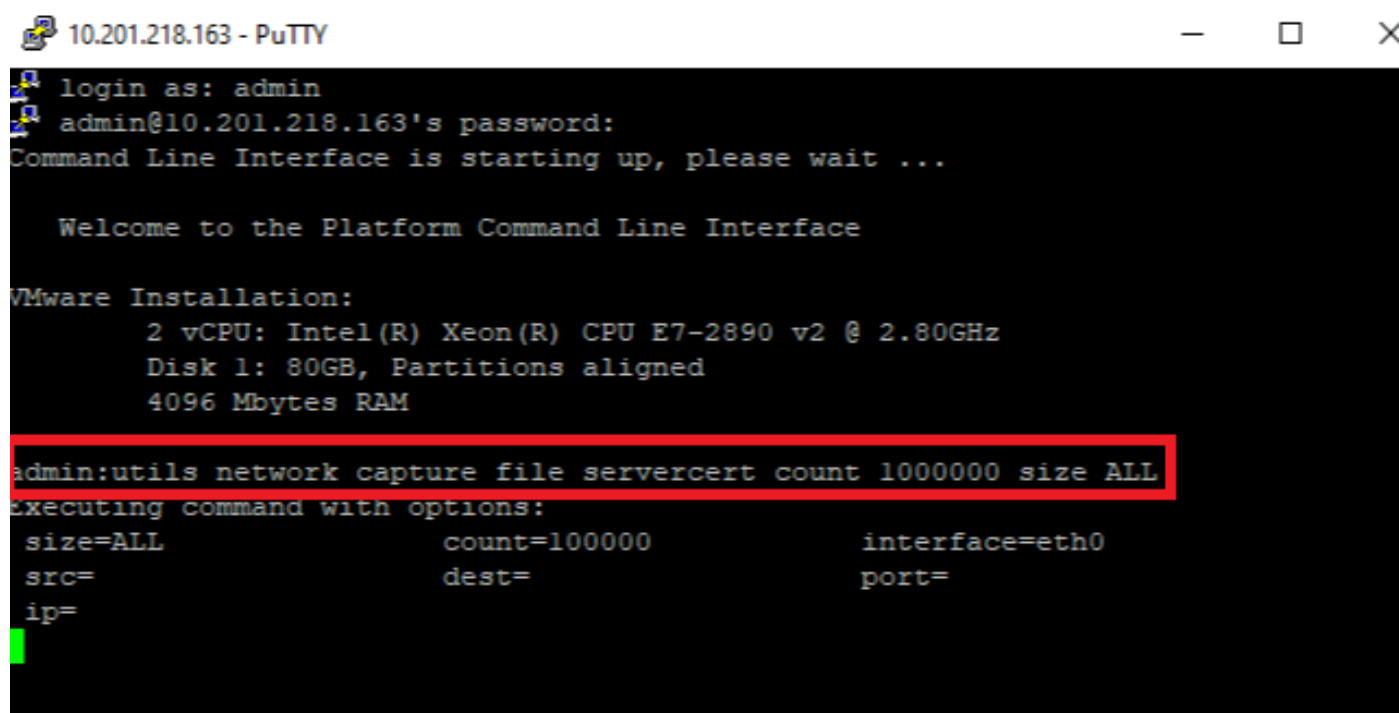
télécharger ou qui sont téléchargés vers CUCM Certificate Management.

Dans le cadre de la connexion TLS, le serveur fournit sa chaîne de certificats/certificats serveur à CUCM.

Exporter le certificat TLS de CUCM PCAP

Étape 1. Démarrer la commande de capture de paquets sur CUCM

Établissez une connexion Secure Shell (SSH) au noeud CUCM et exécutez la commande **utils network capture (ou capture-rotate) file <nom de fichier> count 1000000 size ALL**, comme illustré dans l'image :



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

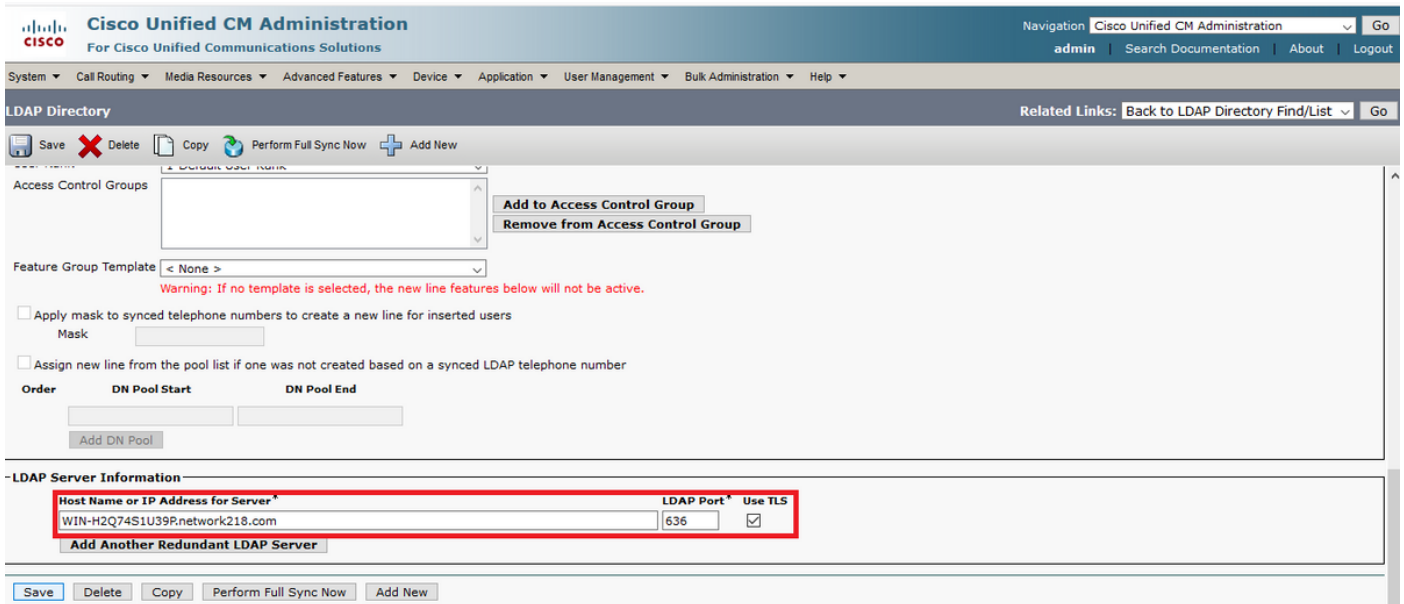
Welcome to the Platform Command Line Interface

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=
```

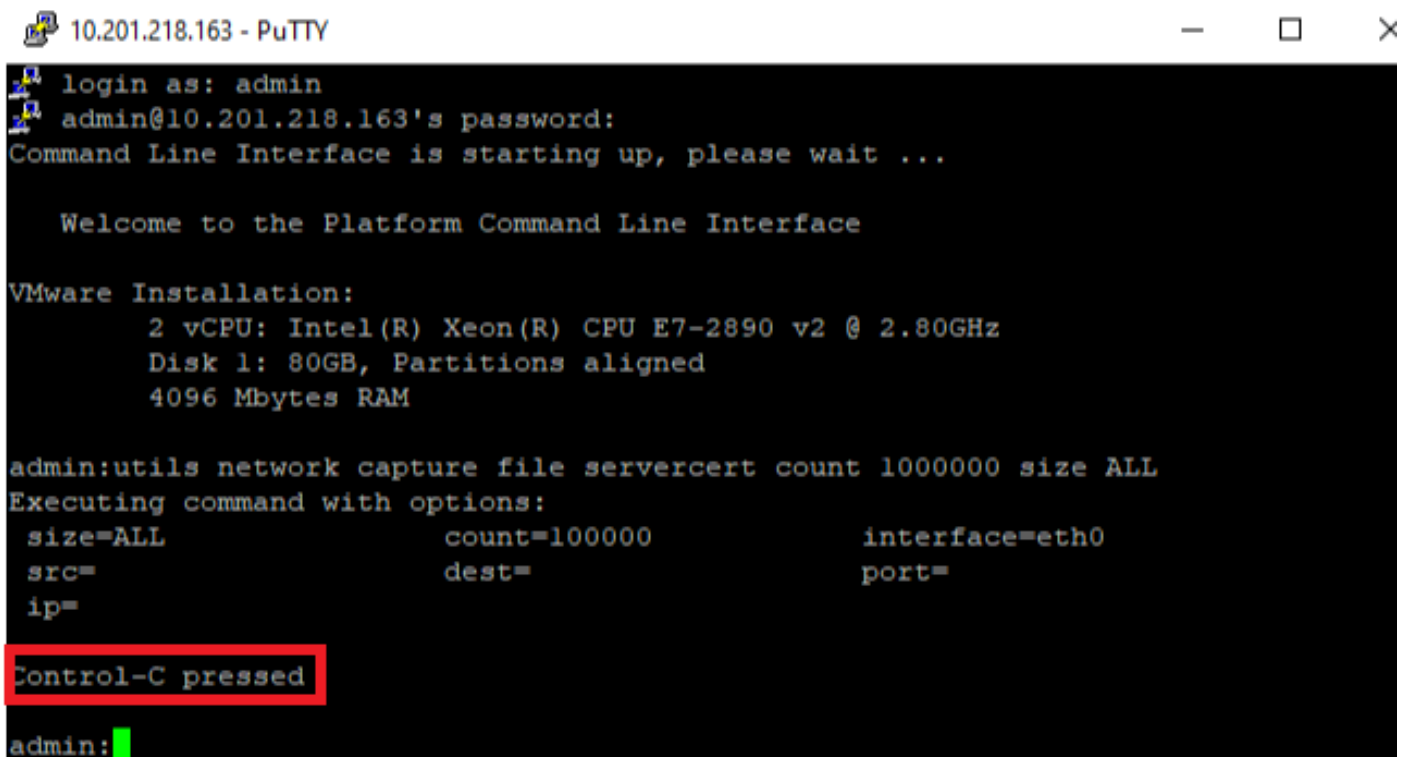
Étape 2. Démarrer une connexion TLS entre le serveur et CUCM

Dans cet exemple, vous démarrez une connexion TLS entre un serveur LDAPS (Secure Lightweight Directory Access Protocol) et CUCM en établissant une connexion sur le port TLS 636, comme illustré dans l'image :



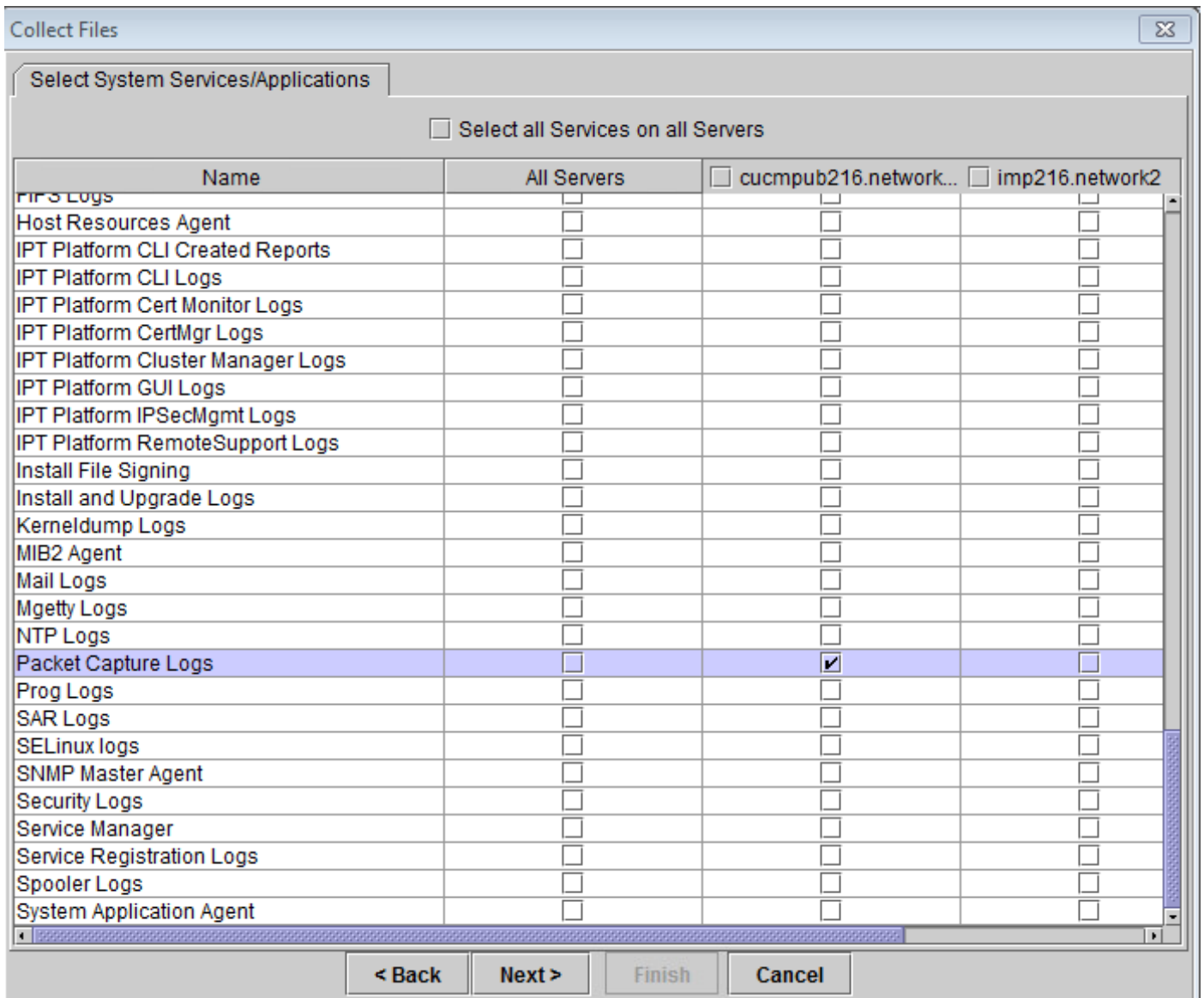
Étape 3. Arrêter CUCM PCAP une fois la connexion TLS terminée

Appuyez sur **Control-C** pour arrêter la capture de paquets, comme illustré dans l'image



Étape 4. Téléchargez le fichier de capture du package selon l'une des deux méthodes répertoriées

1. Lancez le noeud RTMT pour CUCM et accédez à **System > Tools > Trace > Trace & Log Central > Collect Files** et cochez la case **Packet Capture Logs** (passez par le processus RTMT afin de télécharger le pcap), comme indiqué dans l'image :



2. Démarrez un serveur SFTP (Secure File Transport Protocol) et dans la session CUCM SSH exécutez le **fichier de commande** `get activelog /patform/cli/<pcap filename>.cap` (passez par les invites afin de télécharger le PCAP sur le serveur SFTP), comme indiqué dans l'image :

```
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

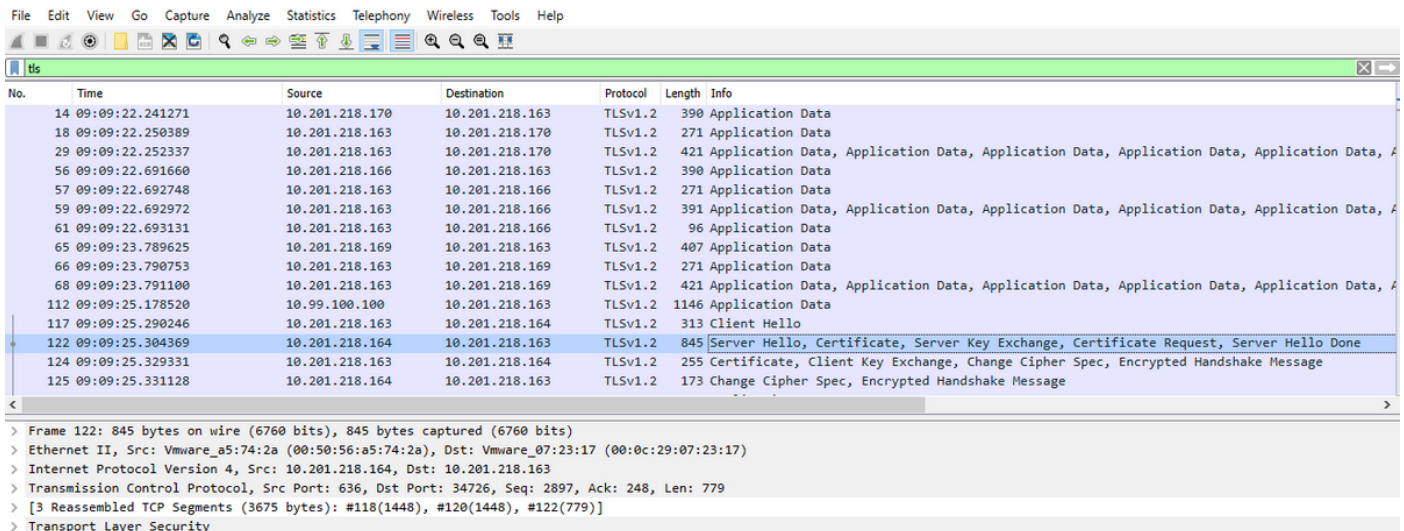
admin:utils network capture file servercert count 1000000 size ALL
Executing command with options:
size=ALL count=100000 interface=eth0
src= dest= port=
ip=

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]? [ ]
```

Étape 5. Déterminer le nombre de certificats présentés à CUCM par le serveur

Utilisez l'application Wireshark afin d'ouvrir le pcap et de filtrer sur **tls** pour déterminer le paquet avec **Server Hello** qui contient le certificat/la chaîne de certificats du serveur présenté à CUCM. Il s'agit de la trame 122, comme le montre l'image :



développez **Transport Layer Security > Certificate** information from the Server Hello packet with certificate afin de déterminer le nombre de certificats présentés à CUCM. Le certificat supérieur est le certificat du serveur. Dans ce cas, seul un certificat, le certificat du serveur, est présenté comme indiqué dans l'image :

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

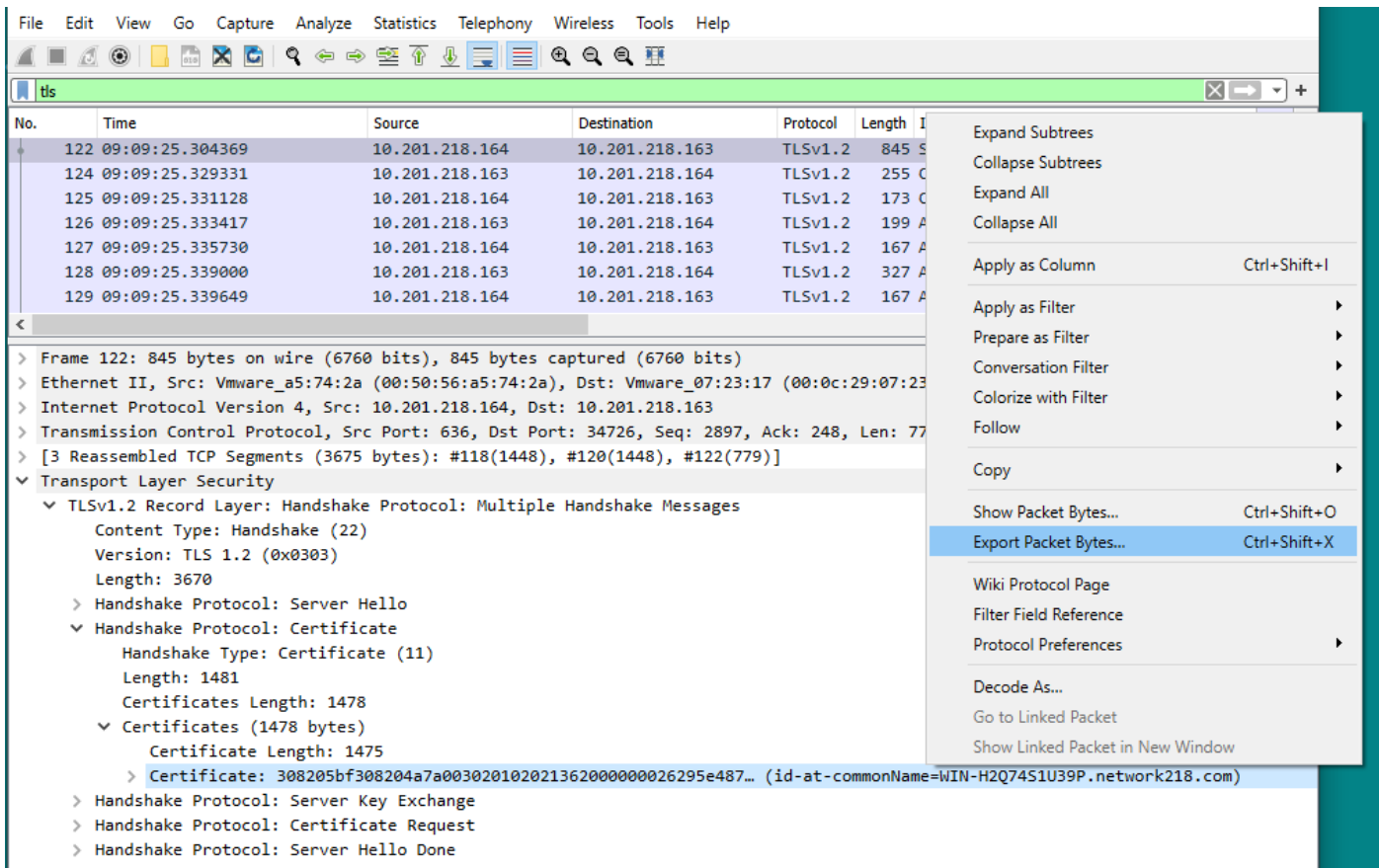
tls

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

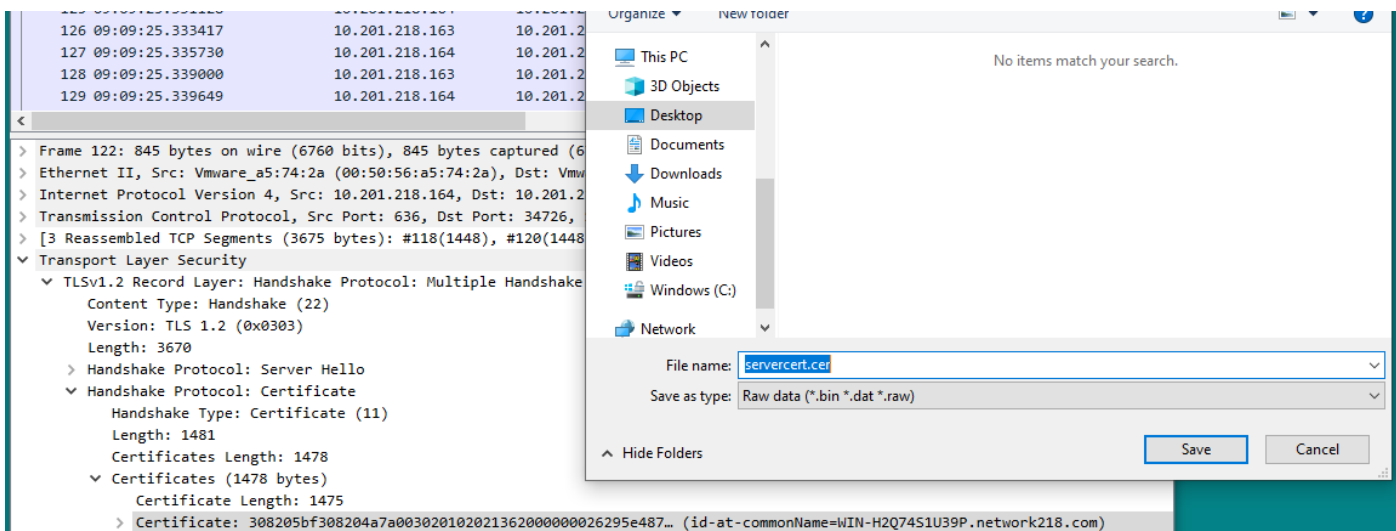
- > Frame 122: 845 bytes on wire (6760 bits), 845 bytes captured (6760 bits)
- > Ethernet II, Src: Vmware_a5:74:2a (00:50:56:a5:74:2a), Dst: Vmware_07:23:17 (00:0c:29:07:23:17)
- > Internet Protocol Version 4, Src: 10.201.218.164, Dst: 10.201.218.163
- > Transmission Control Protocol, Src Port: 636, 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

Étape 6. Exporter la chaîne de certificats/certificats du serveur à partir du PCAP CUCM

Dans cet exemple, seul le certificat de serveur est présenté. Vous devez donc examiner le certificat de serveur. Cliquez avec le bouton droit sur le certificat du serveur et sélectionnez **Exporter les octets de paquets** afin d'enregistrer en tant que certificat .cer, comme illustré dans l'image :

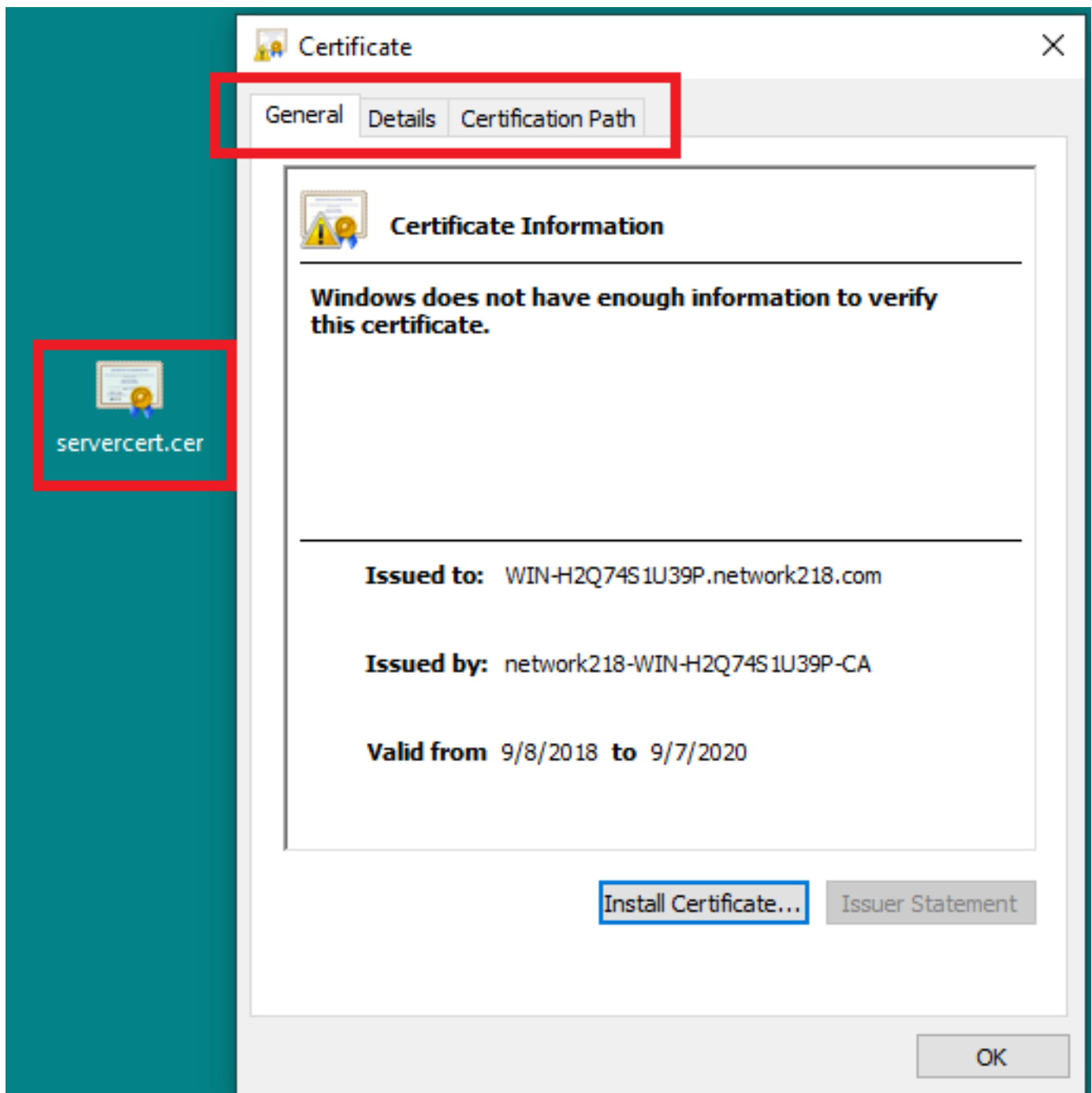


Dans la fenêtre suivante, indiquez un nom de fichier .cer, puis cliquez sur Enregistrer. Le fichier qui a été enregistré (dans ce cas, sur le bureau) a été nommé servercert.cer, comme l'illustre l'image :



Étape 7. Ouvrir le fichier .CER enregistré afin d'examiner le contenu

Double-cliquez sur le fichier .cer afin d'examiner les informations dans les onglets **General**, **Details** et **Certificate Path**, comme illustré dans l'image :



Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.