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

Contenu

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

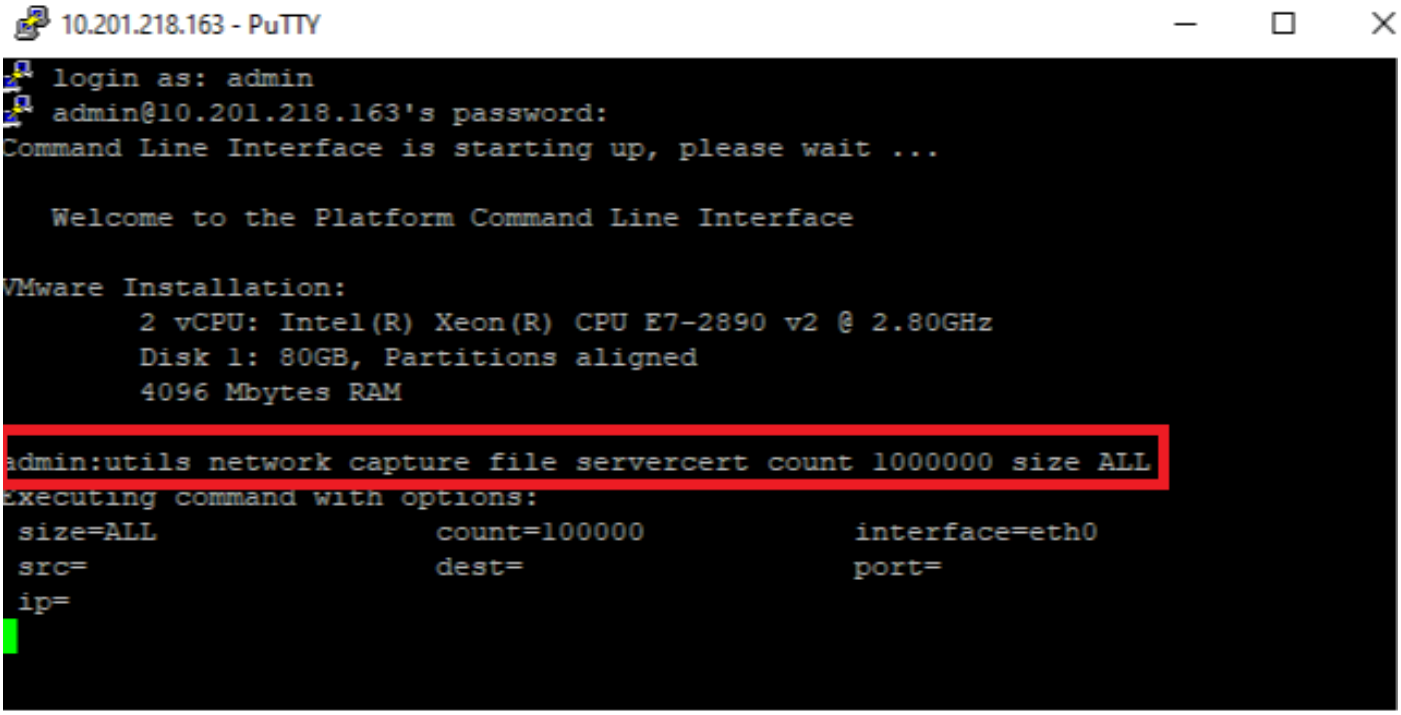
télécharger ou qui sont téléchargés vers CUCM Certificate Management.

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

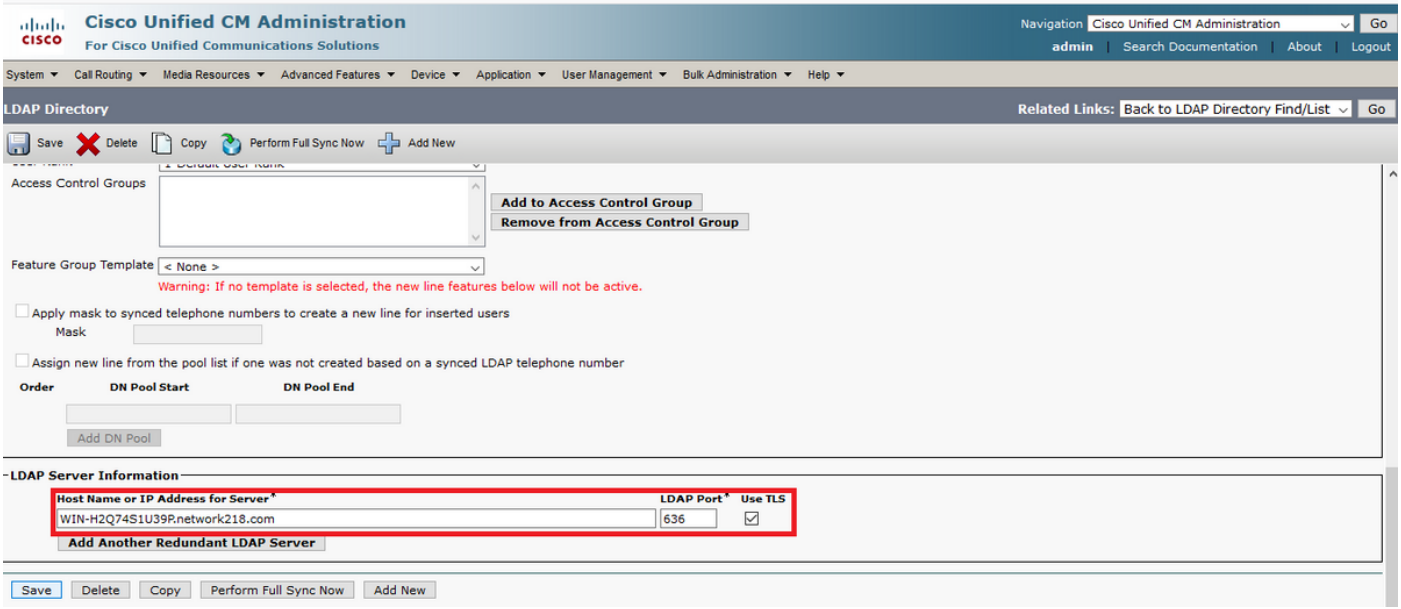
Étape 1. Démarrer la commande de capture de paquets sur CUCM

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 :



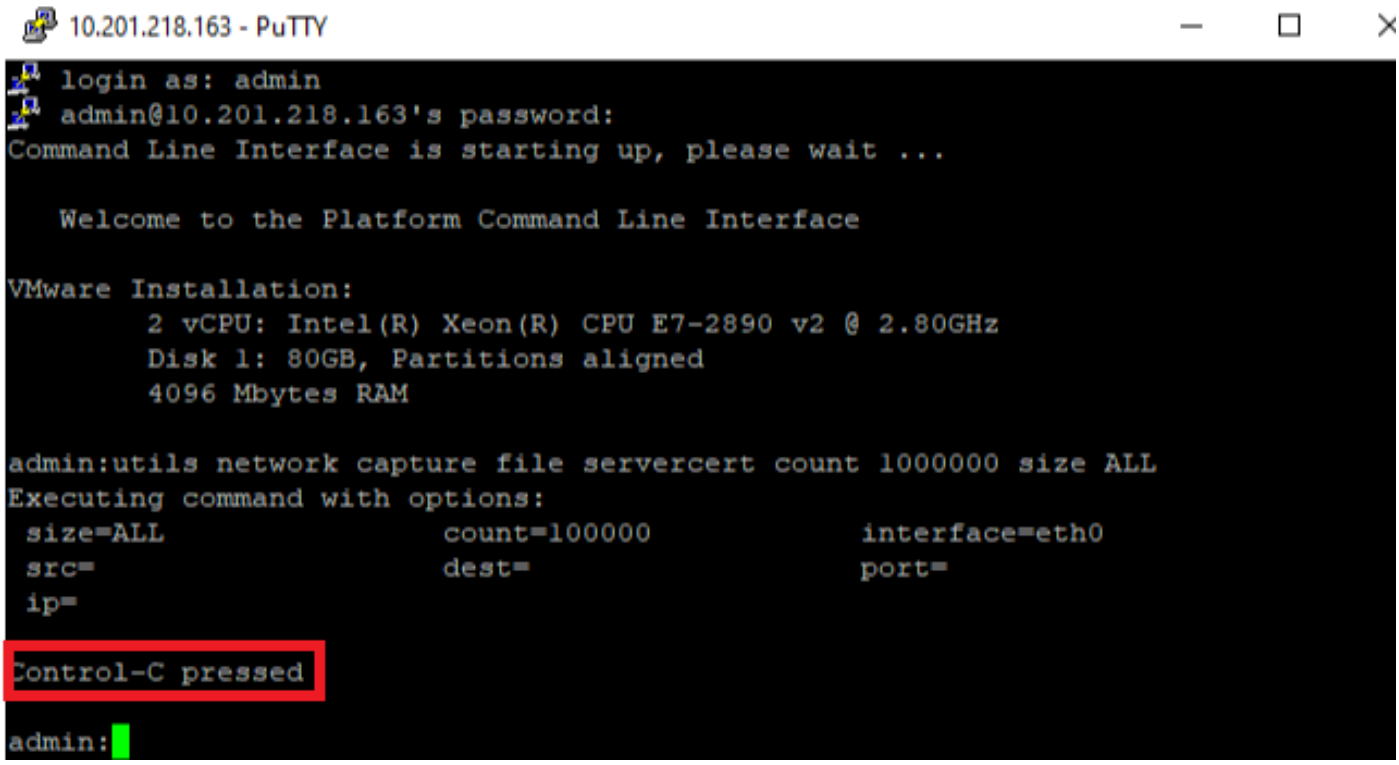
Étape 2. Démarrer une connexion TLS entre le serveur et CUCM

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 :



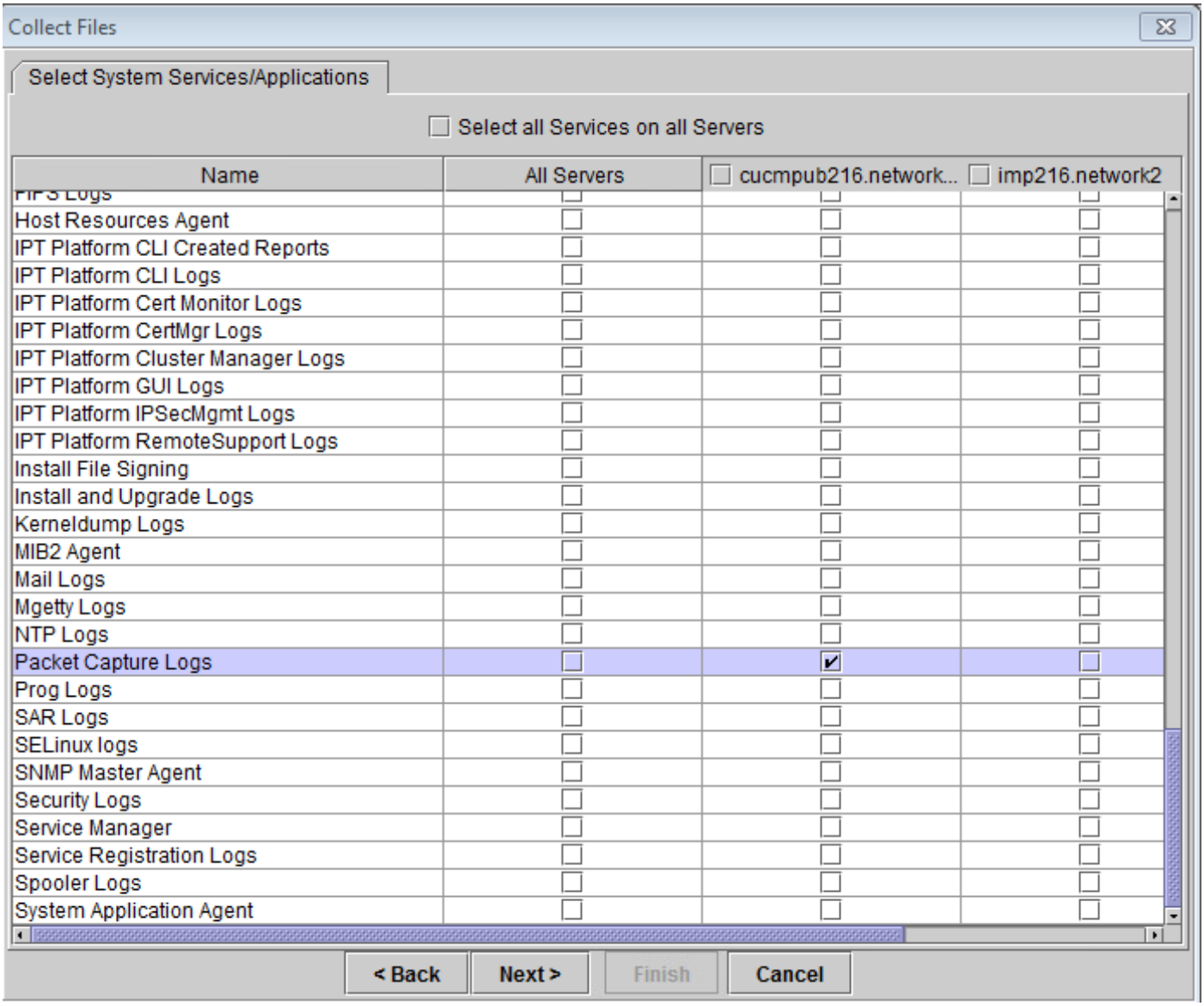
Étape 3. Arrêter CUCM PCAP une fois la connexion TLS terminée

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

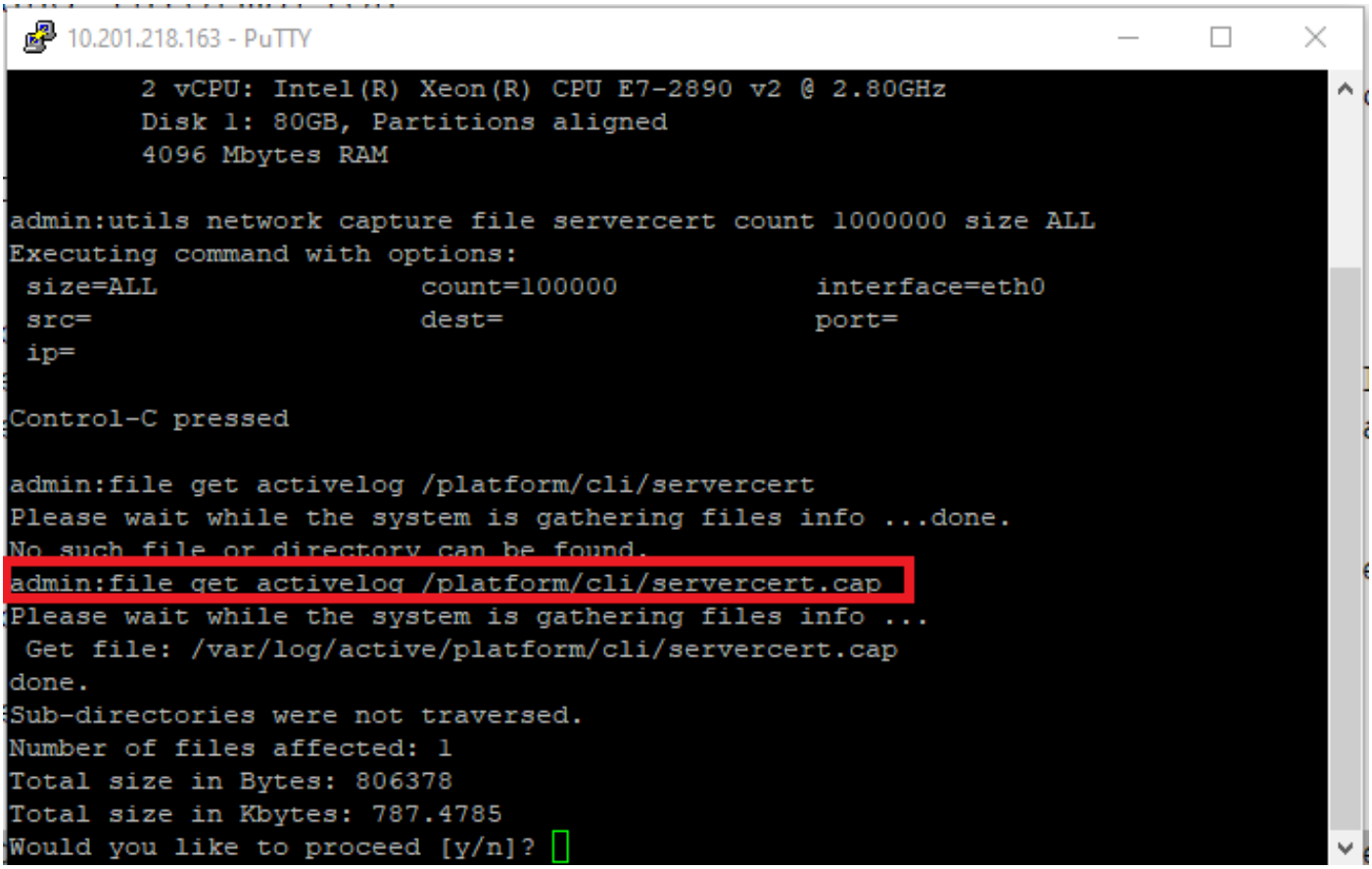


Étape 4. Téléchargez le fichier de capture du package selon l'une des deux méthodes répertoriées

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 :

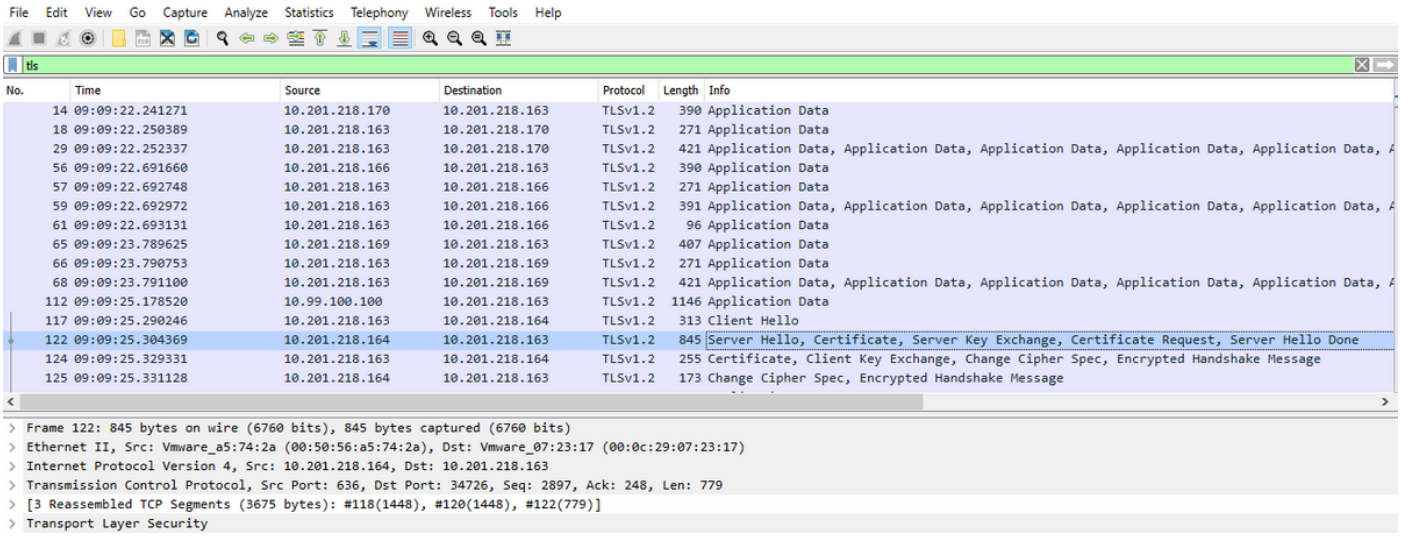


2. Démarrez un serveur SFTP (Secure File Transport Protocol) et dans la session CUCM SSH exécutez le **fichier** de commande **get activelog /patform/cli/<pcap filename>.cap** (passez par les invites afin de télécharger le PCAP sur le serveur SFTP), comme indiqué dans l'image :

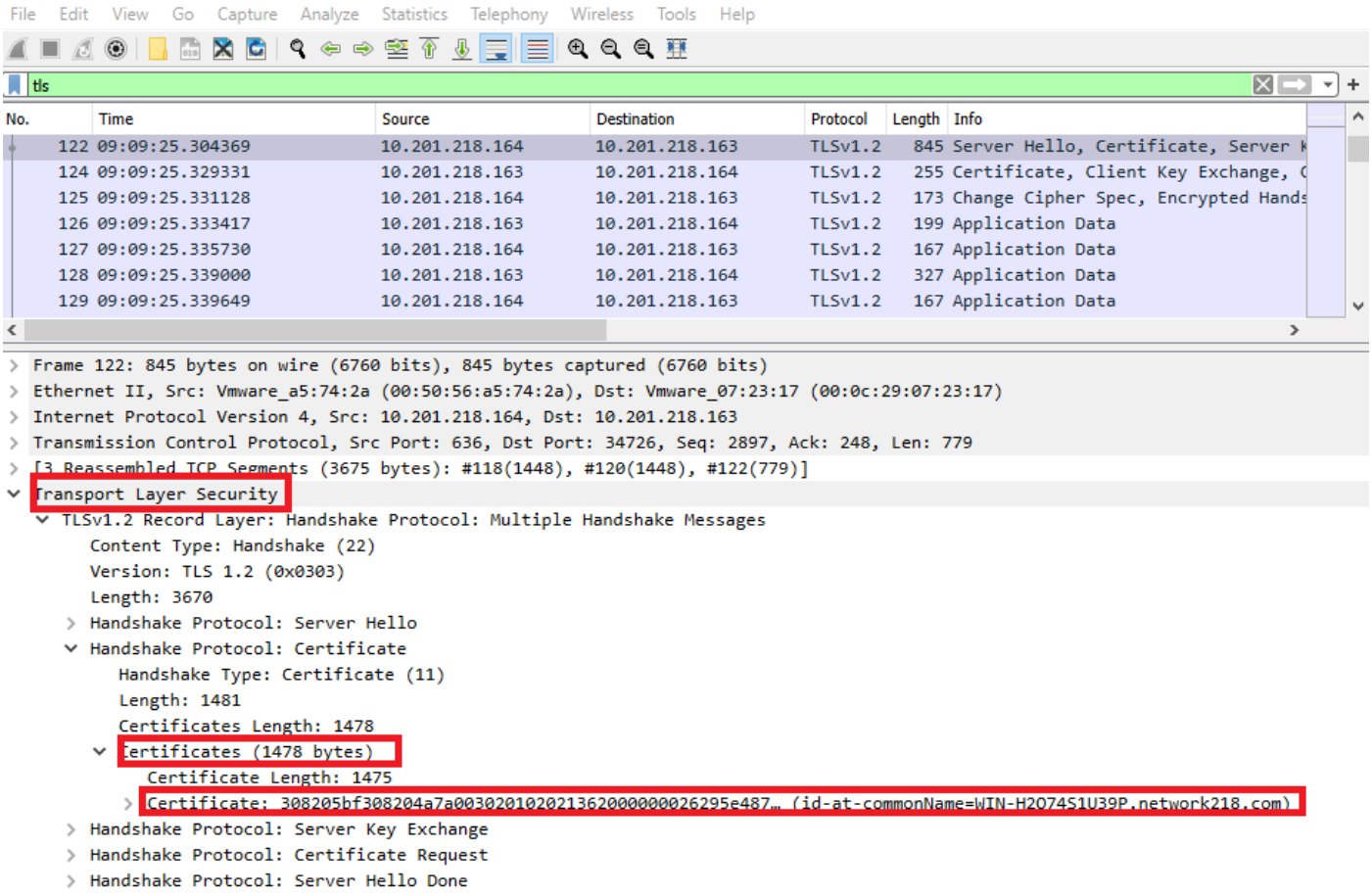


Étape 5. Déterminer le nombre de certificats présentés à CUCM par le serveur

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 :

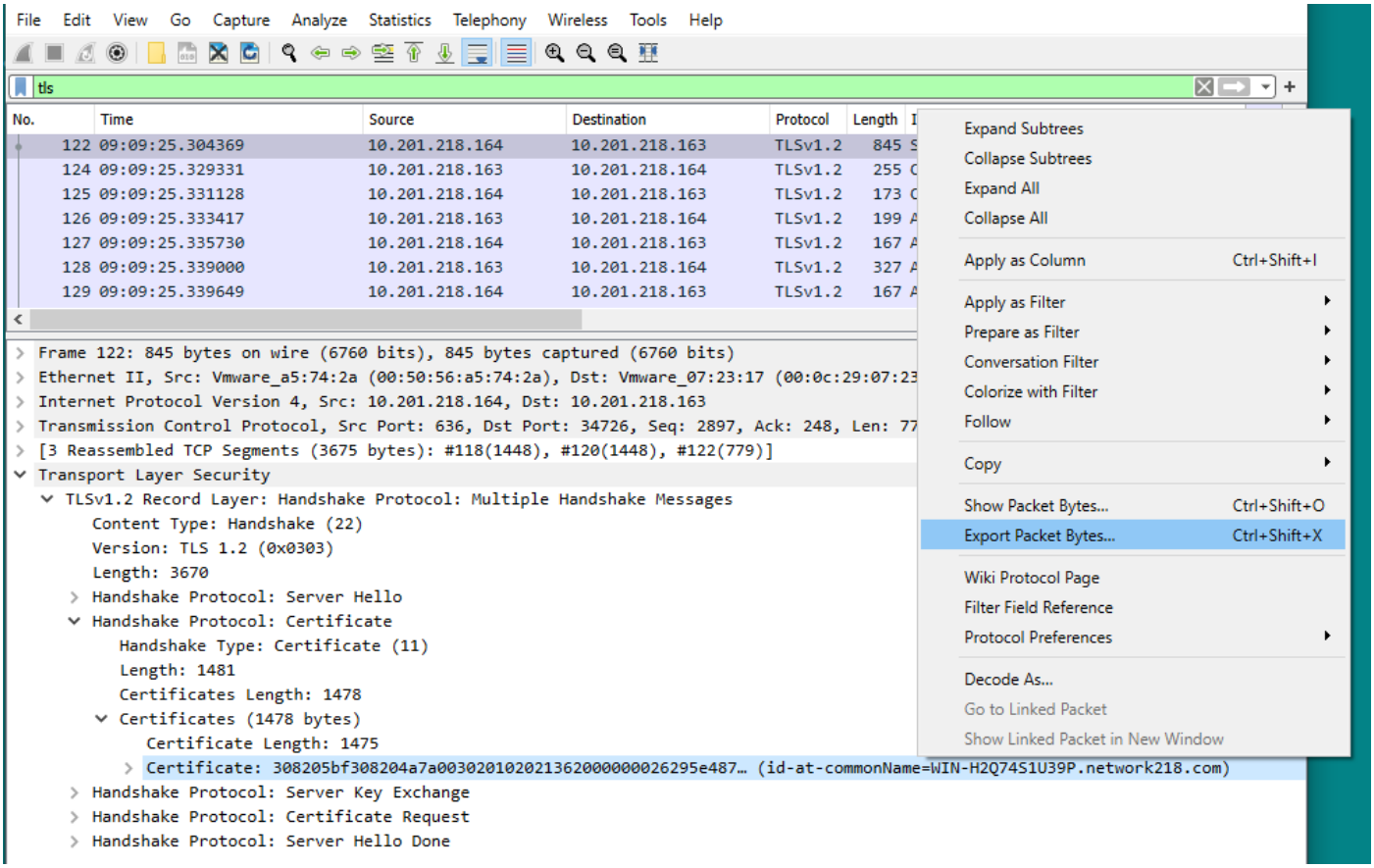


·développez **Transport Layer Security > Certificate** information from the Server Hello packet with certificate afin de déterminer le nombre de certificats présentés à CUCM. Le certificat supérieur est le certificat du serveur. Dans ce cas, seul un certificat, le certificat du serveur, est présenté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

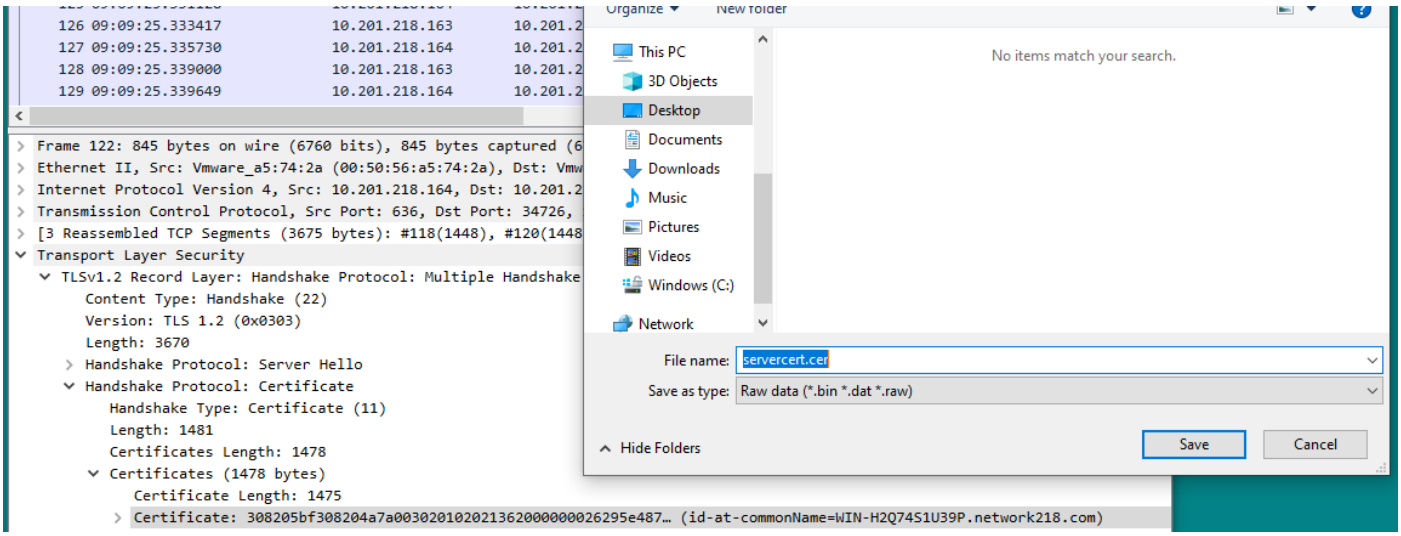


Étape 6. Exporter la chaîne de certificats/certificats du serveur à partir du PCAP CUCM

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 :

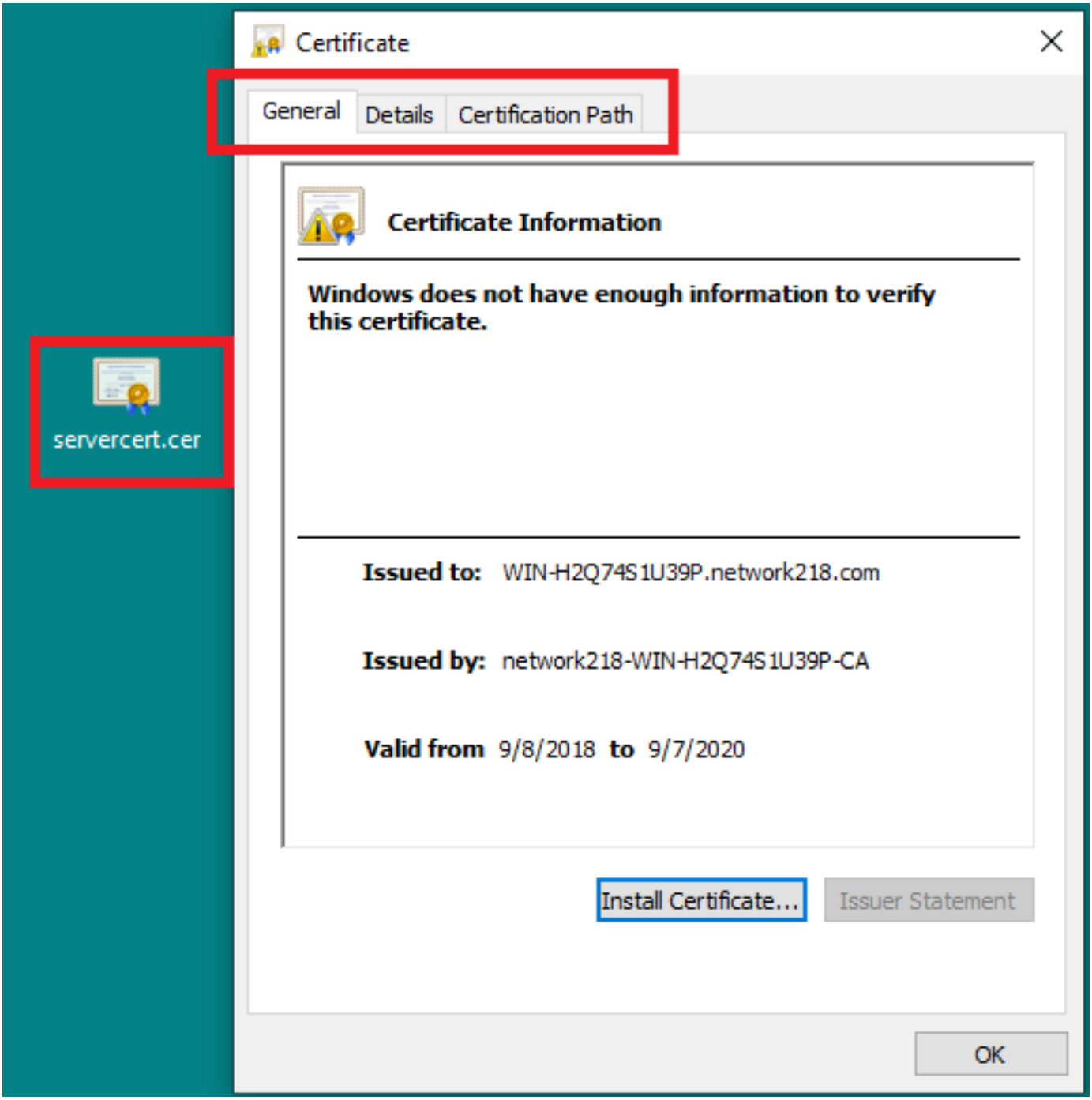


·Dans la fenêtre suivante, indiquez un nom de fichier .cer, puis cliquez sur Enregistrer. Le fichier qui a été enregistré (dans ce cas, sur le bureau) a été nommé servercert.cer, comme l'illustre l'image :



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.