如何從CUCM資料包捕獲(PCAP)匯出TLS證書

目錄

簡介

本檔案介紹從思科整合通訊管理員(CUCM)PCAP匯出憑證的程式。

作者：思科TAC工程師Adrian Esquillo。

必要條件

需求

思科建議您瞭解以下主題：
·傳輸層安全(TLS)握手
·CUCM證書管理
·安全檔案傳輸通訊協定(SFTP)伺服器
·即時監控工具(RTMT)

·Wireshark應用程式

採用元件

·CUCM 9.X及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

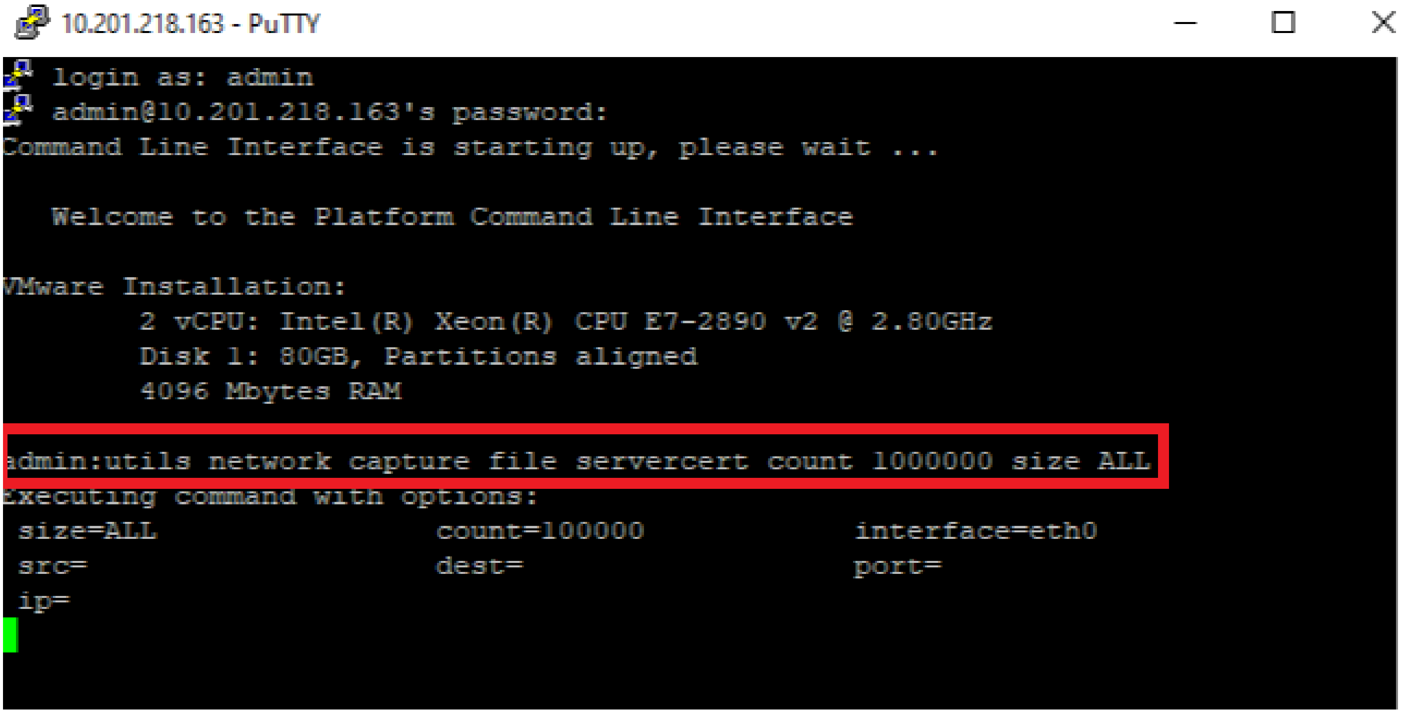
可以匯出伺服器證書/證書鏈，以確認伺服器提供的伺服器證書/證書鏈與要上傳的證書或上傳到CUCM證書管理的證書相匹配。

作為TLS握手的一部分，伺服器將其伺服器證書/證書鏈提供給CUCM。

從CUCM PCAP匯出TLS證書

步驟1.在CUCM上啟動packet capture命令

建立與CUCM節點的安全外殼(SSH)連線，並運行**utils network capture(or capture-rotate)file <filename> count 1000000 size ALL**命令，如下圖所示：

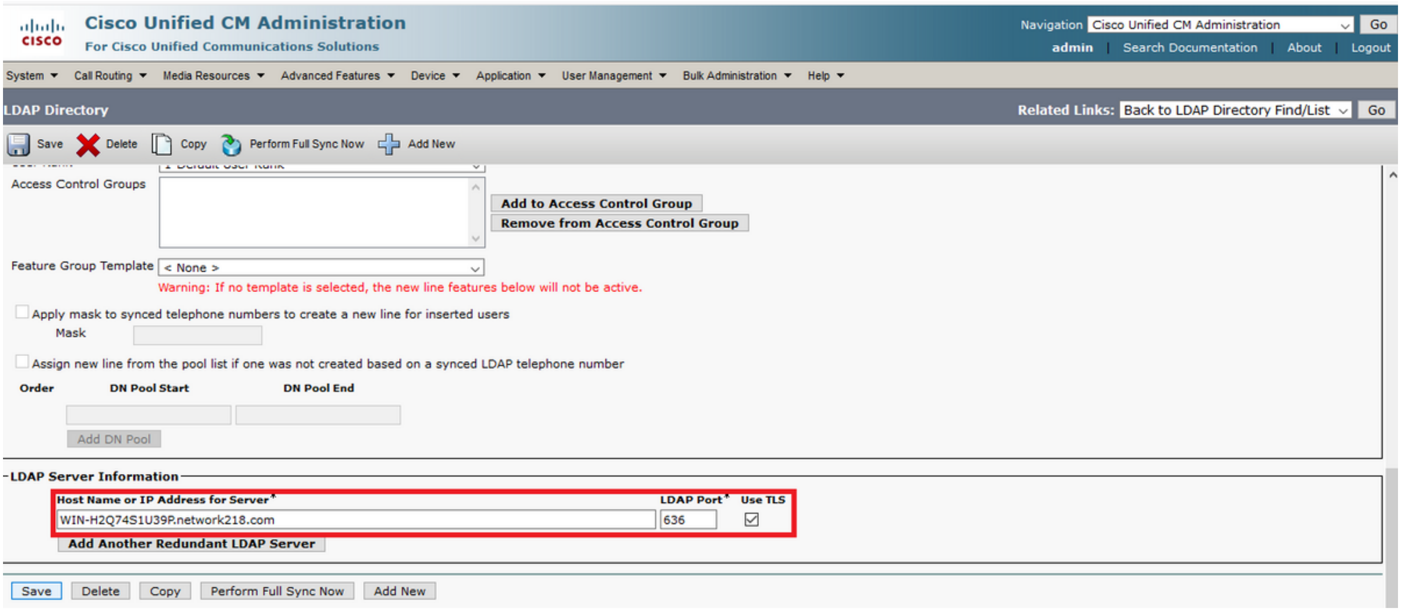


10.201.218.163 - PuTTY

```
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=
```

步驟2.啟動伺服器和CUCM之間的TLS連線

在本示例中，通過在TLS埠636上建立連線，可以在安全輕量級目錄訪問協定(LDAPS)伺服器和CUCM之間啟動TLS連線，如下圖所示：



Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾
LDAP Directory
Related Links: Back to LDAP Directory Find/List Go
Save Delete Copy Perform Full Sync Now Add New
Add to Access Control Group
Remove from Access Control Group
Add DN Pool
Add Another Redundant LDAP Server
Save Delete Copy Perform Full Sync Now Add New

Access Control Groups

Feature Group Template < None >

Warning: If no template is selected, the new line features below will not be active.

□ Apply mask to synced telephone numbers to create a new line for inserted users

Mask

□ Assign new line from the pool list if one was not created based on a synced LDAP telephone number

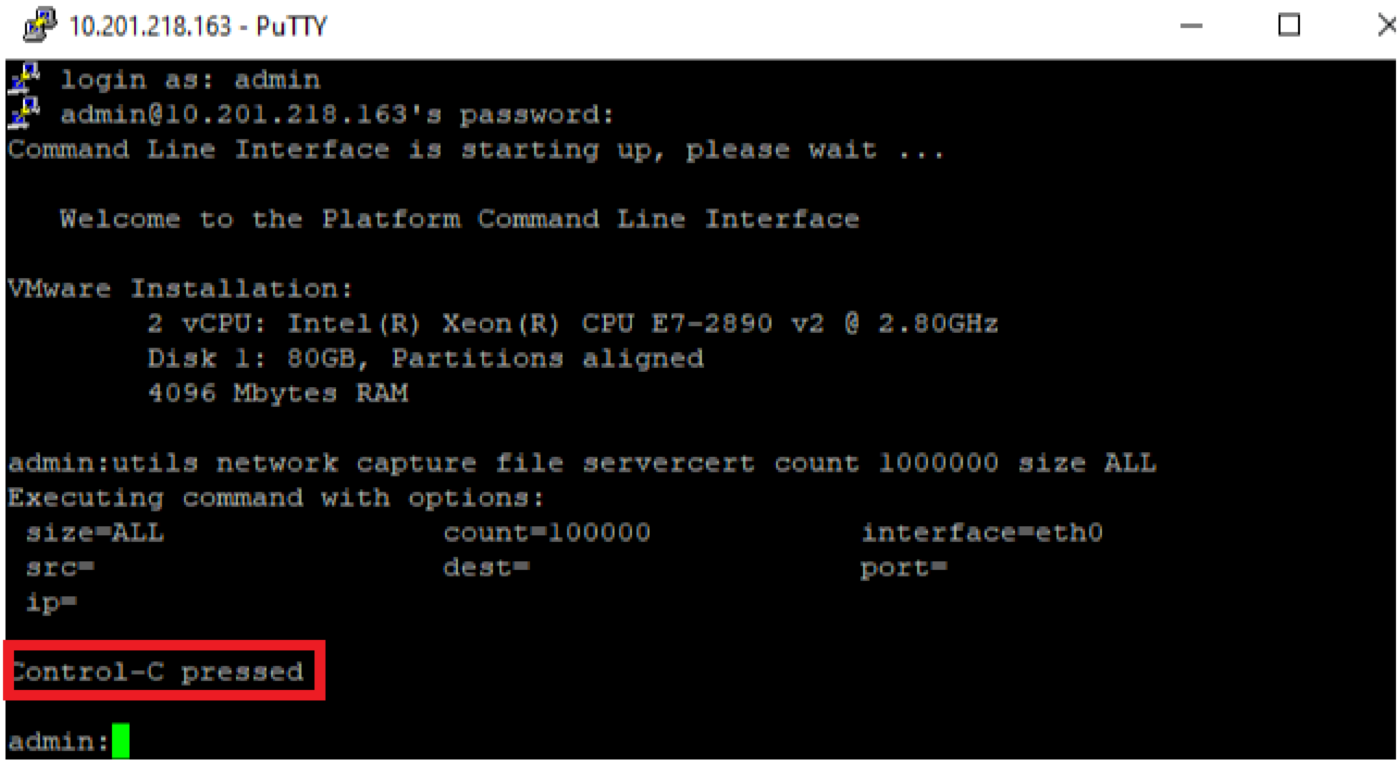
Order DN Pool Start DN Pool End

LDAP Server Information

Host Name or IP Address for Server*	LDAP Port*	Use TLS
WIN-H2Q74S1U39P.network218.com	636	☑

步驟3.完成TLS握手後停止CUCM PCAP

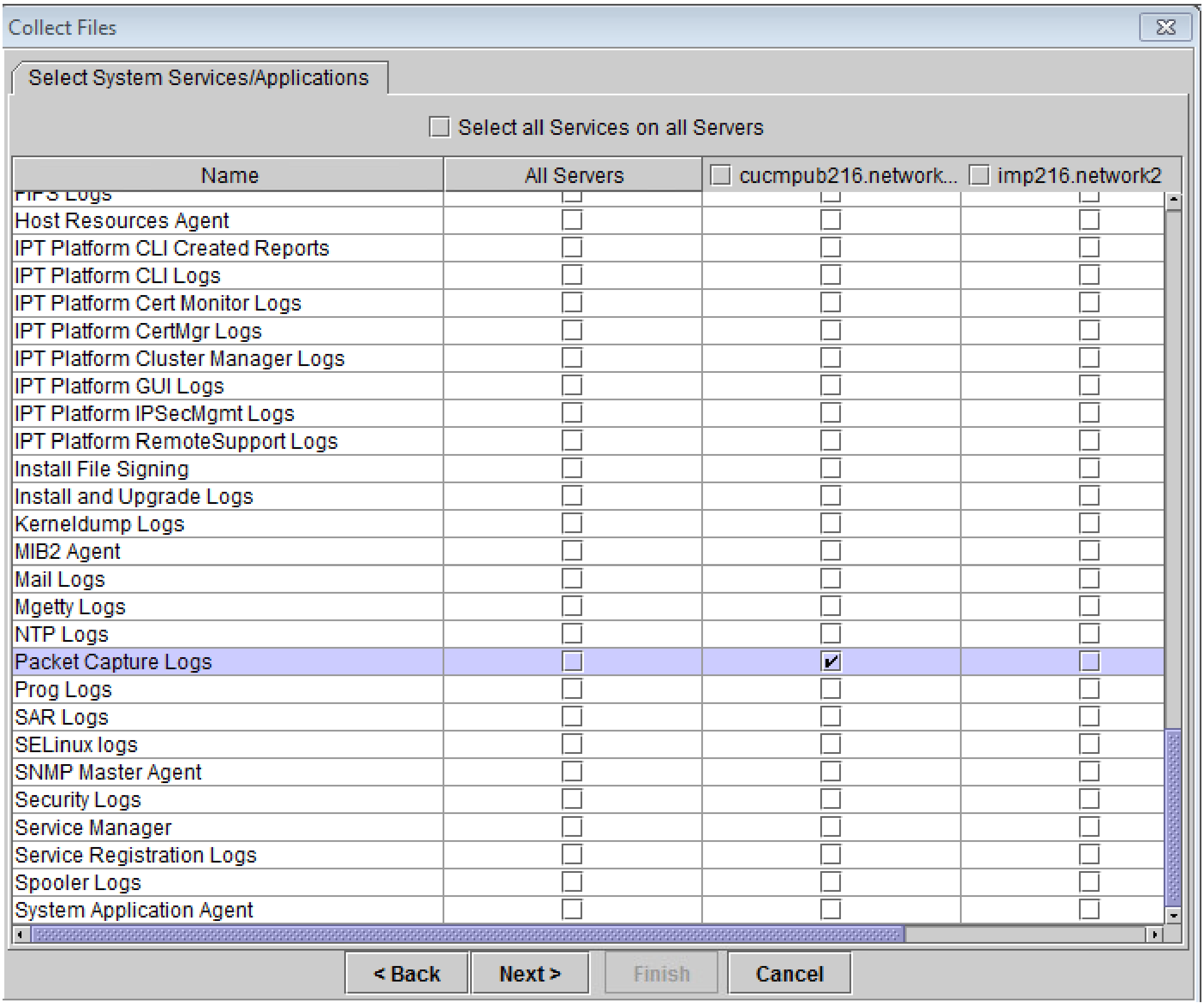
按**Control-C**以停止資料包捕獲，如下圖所示



```
  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=

Control-C pressed

admin:
```

步驟4.使用列出的兩種方法中的任一種下載打包程式捕獲檔案

1.啟動CUCM節點的RTMT，然後導航到**System > Tools > Trace > Trace & Log Central > Collect Files**，並選中**Packet Capture Logs**框（繼續通過RTMT過程下載pcap），如下圖所示：



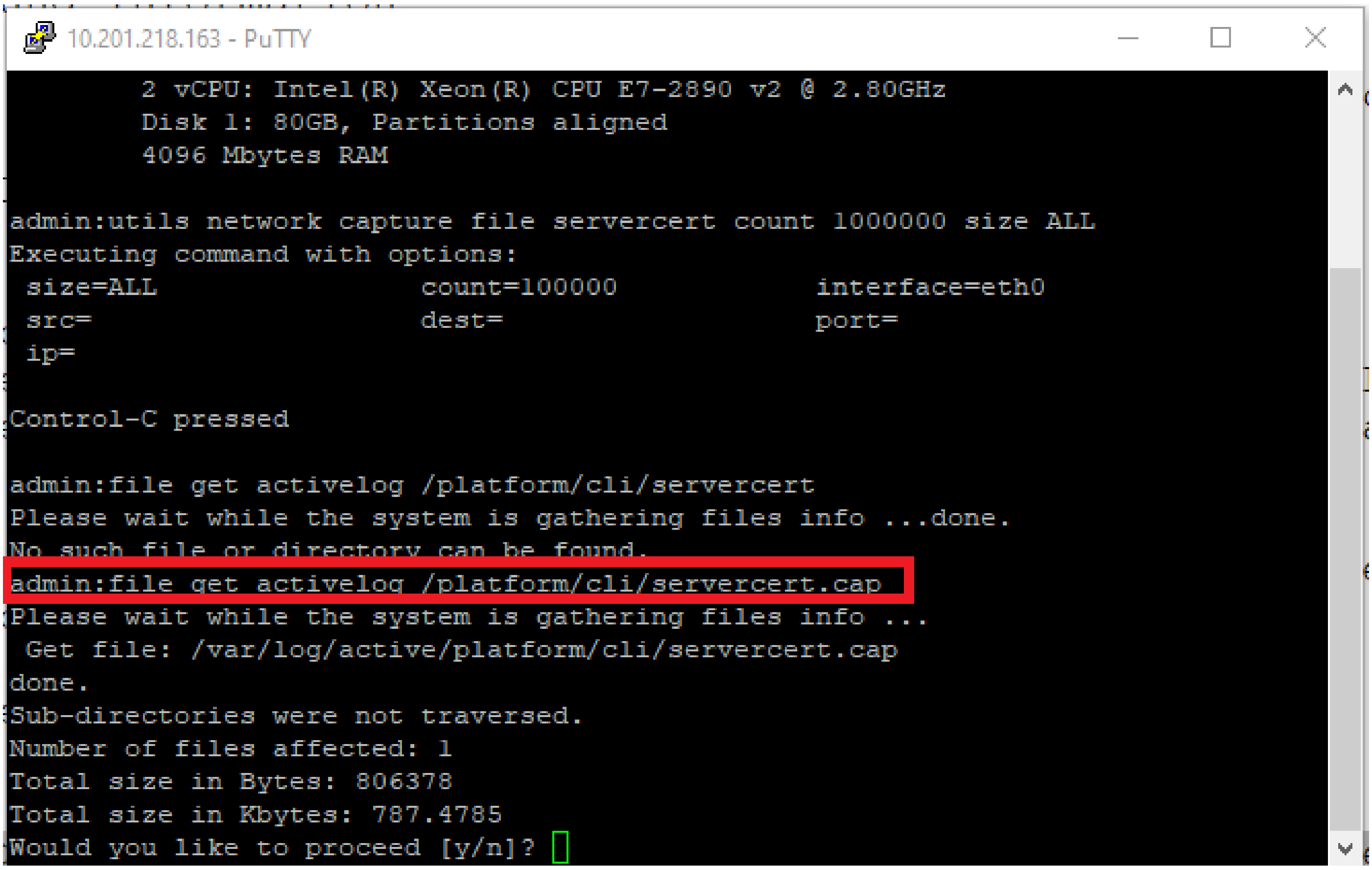
Collect Files

Select System Services/Applications

□ Select all Services on all Servers

Name	All Servers	□ cucmpub216.network...	□ imp216.network2
FIPS Logs	□	□	□
Host Resources Agent	□	□	□
IPT Platform CLI Created Reports	□	□	□
IPT Platform CLI Logs	□	□	□
IPT Platform Cert Monitor Logs	□	□	□
IPT Platform CertMgr Logs	□	□	□
IPT Platform Cluster Manager Logs	□	□	□
IPT Platform GUI Logs	□	□	□
IPT Platform IPSecMgmt Logs	□	□	□
IPT Platform RemoteSupport Logs	□	□	□
Install File Signing	□	□	□
Install and Upgrade Logs	□	□	□
Kerneldump Logs	□	□	□
MIB2 Agent	□	□	□
Mail Logs	□	□	□
Mgetty Logs	□	□	□
NTP Logs	□	□	□
Packet Capture Logs	□	☑	□
Prog Logs	□	□	□
SAR Logs	□	□	□
SELinux logs	□	□	□
SNMP Master Agent	□	□	□
Security Logs	□	□	□
Service Manager	□	□	□
Service Registration Logs	□	□	□
Spooler Logs	□	□	□
System Application Agent	□	□	□

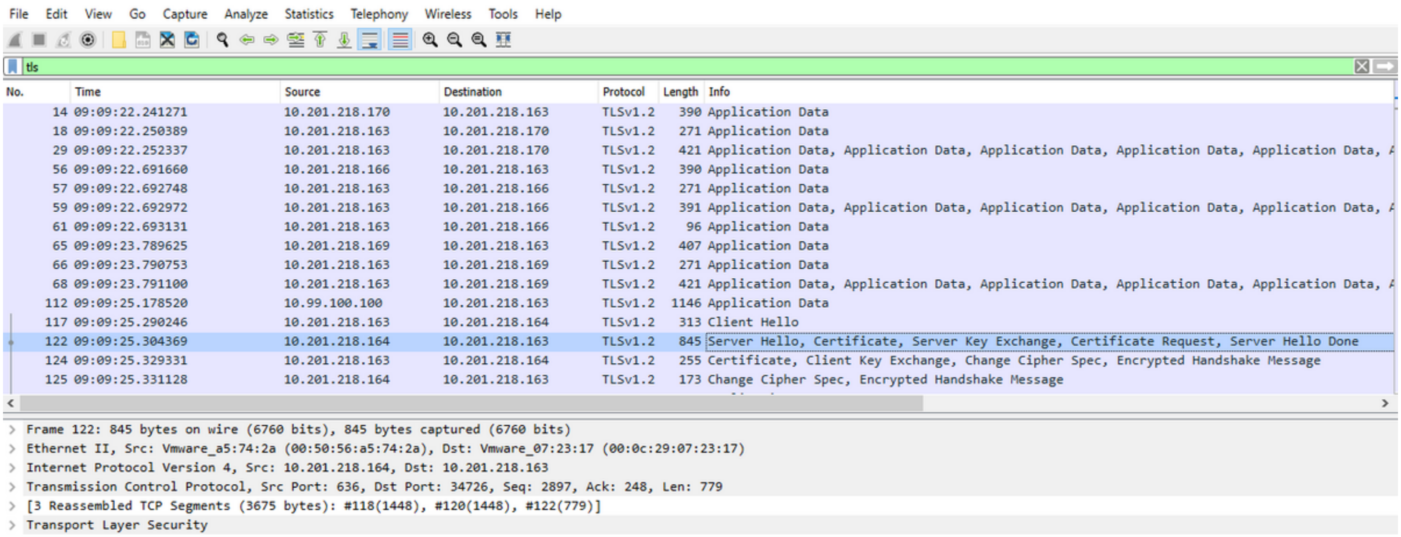
2.啟動安全檔案傳輸通訊協定(SFTP)伺服器，然後在CUCM SSH作業階段中執行命令**file get activelog /patform/cli/<pcap filename>.cap**（繼續按照提示在SFTP伺服器上下載PCAP），如下圖所示：



```
        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]?
```

步驟5.確定伺服器向CUCM提供的證書數量

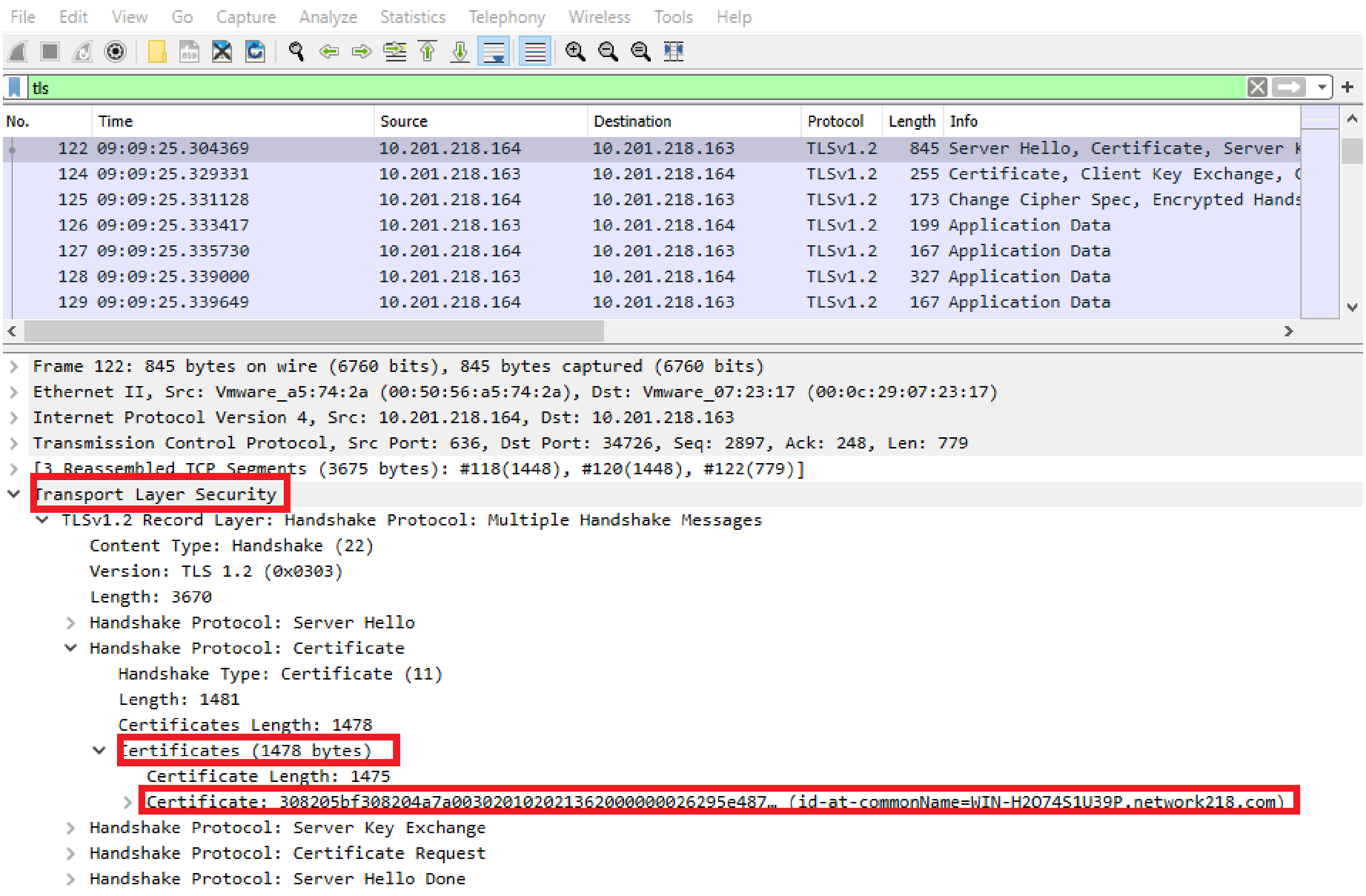
使用Wireshark應用程式開啟pcap並過濾**tls**，以確定包含**向CUCM提供的伺服器證書/證書鏈的Server Hello**的資料包。這是第122幀，如下圖所示：



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tls

No.  Time             Source          Destination     Protocol  Length Info
  14 09:09:22.241271  10.201.218.170  10.201.218.163  TLSv1.2    390 Application Data
  18 09:09:22.250389  10.201.218.163  10.201.218.170  TLSv1.2    271 Application Data
  29 09:09:22.252337  10.201.218.163  10.201.218.170  TLSv1.2    421 Application Data, Application Data, Application Data, Application Data, Application Data, A
  56 09:09:22.691660  10.201.218.166  10.201.218.163  TLSv1.2    390 Application Data
  57 09:09:22.692748  10.201.218.163  10.201.218.166  TLSv1.2    271 Application Data
  59 09:09:22.692972  10.201.218.163  10.201.218.166  TLSv1.2    391 Application Data, Application Data, Application Data, Application Data, Application Data, A
  61 09:09:22.693131  10.201.218.163  10.201.218.166  TLSv1.2     96 Application Data
  65 09:09:23.789625  10.201.218.169  10.201.218.163  TLSv1.2    407 Application Data
  66 09:09:23.790753  10.201.218.163  10.201.218.169  TLSv1.2    271 Application Data
  68 09:09:23.791100  10.201.218.163  10.201.218.169  TLSv1.2    421 Application Data, Application Data, Application Data, Application Data, Application Data, A
 112 09:09:25.178520  10.99.100.100   10.201.218.163  TLSv1.2   1146 Application Data
 117 09:09:25.290246  10.201.218.163  10.201.218.164  TLSv1.2    313 Client Hello
 122 09:09:25.304369  10.201.218.164  10.201.218.163  TLSv1.2    845 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
 124 09:09:25.329331  10.201.218.163  10.201.218.164  TLSv1.2    255 Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 125 09:09:25.331128  10.201.218.164  10.201.218.163  TLSv1.2    173 Change Cipher Spec, Encrypted Handshake Message

> 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
```

·從包含證書的Server Hello資料包中展開**Transport Layer Security > Certificate**資訊，以確定提供給CUCM的證書數量。首要憑證是伺服器憑證。在此案例中，只會顯示1個憑證（伺服器憑證），如下圖所示：

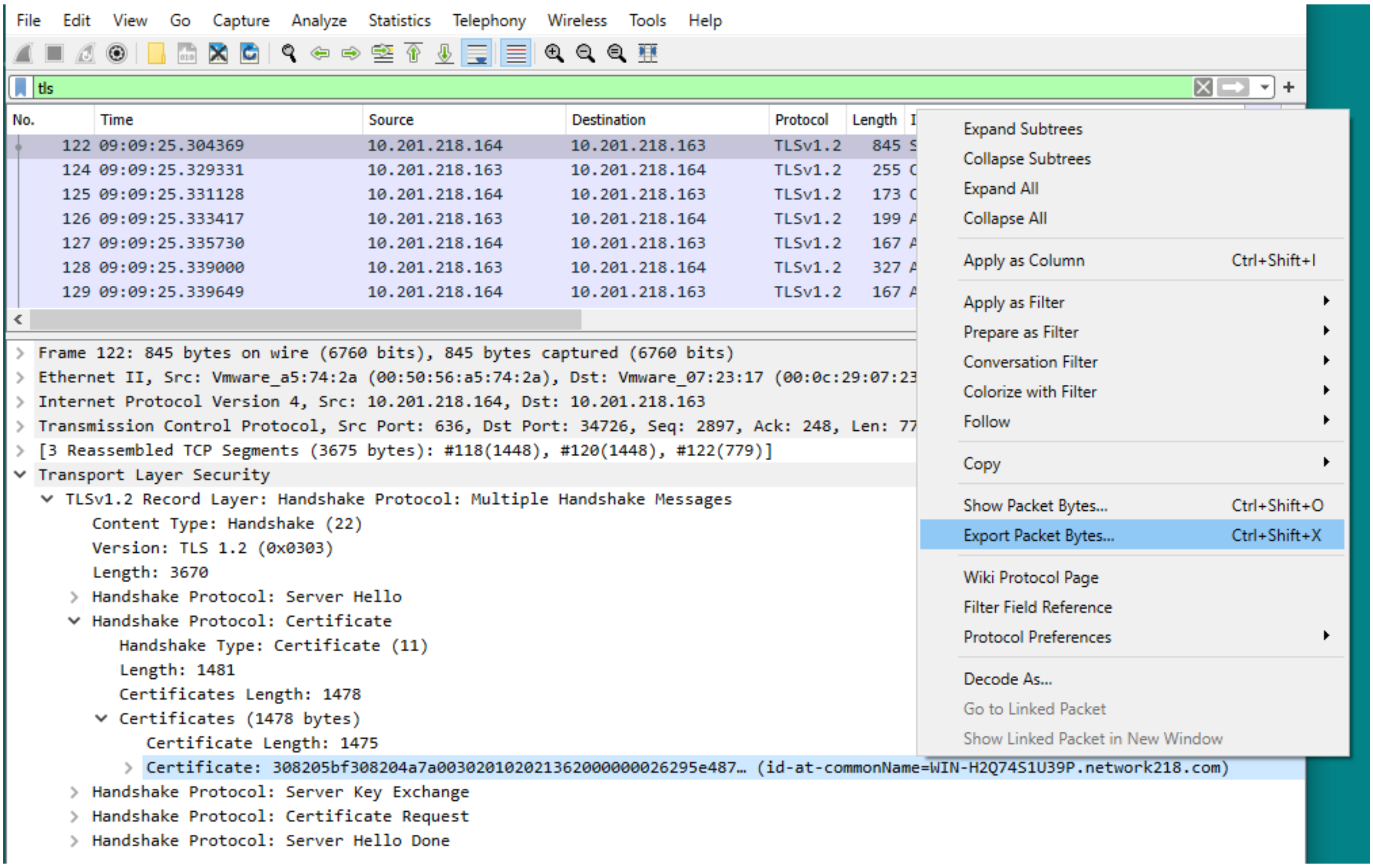


```
No.   Time             Source          Destination     Protocol Length Info
  122 09:09:25.304369  10.201.218.164  10.201.218.163  TLSv1.2  845 Server Hello, Certificate, Server K
  124 09:09:25.329331  10.201.218.163  10.201.218.164  TLSv1.2  255 Certificate, Client Key Exchange, C
  125 09:09:25.331128  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)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 3670
    > Handshake Protocol: Server Hello
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 1481
        Certificates Length: 1478
      v Certificates (1478 bytes)
          Certificate Length: 1475
        > Certificate: 308205bf308204a7a003020102021362000000026295e487… (id-at-commonName=WIN-H2O74S1U39P.network218.com)
    > Handshake Protocol: Server Key Exchange
    > Handshake Protocol: Certificate Request
    > Handshake Protocol: Server Hello Done
```

步驟6.從CUCM PCAP匯出伺服器證書/證書鏈

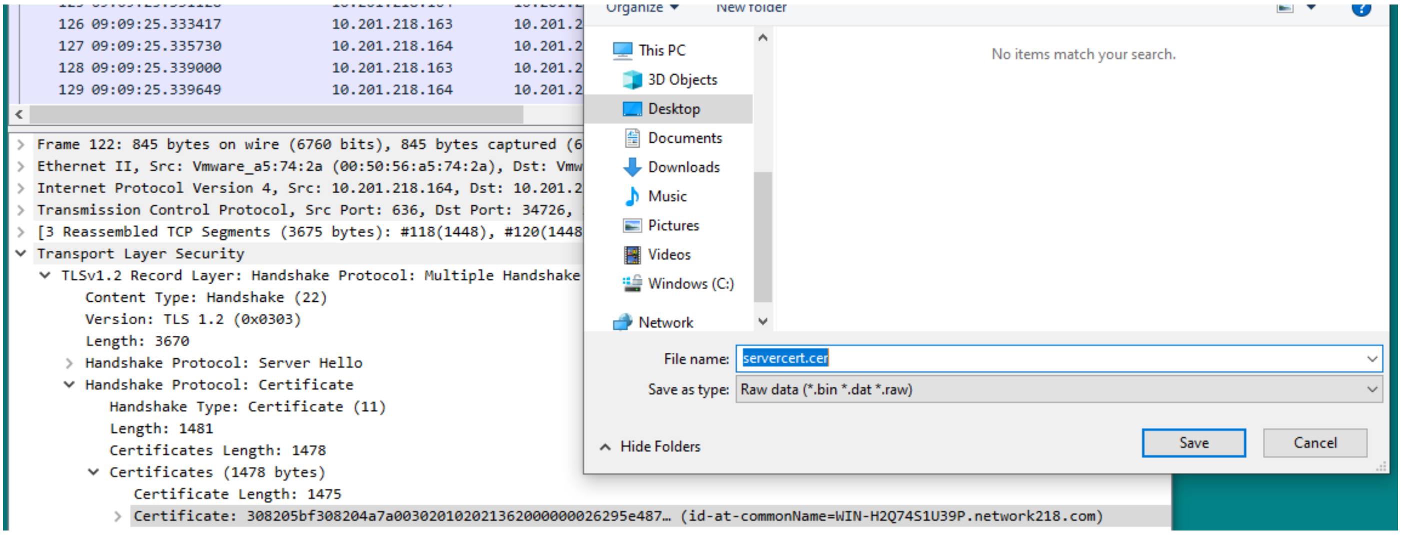
在此示例中，只顯示伺服器證書，因此您需要檢查伺服器證書。按一下右鍵伺服器證書，然後選擇**Export Packet Bytes**以另存為.cer證書，如下圖所示：



```
No.   Time             Source          Destination     Protocol Length I
  122 09:09:25.304369  10.201.218.164  10.201.218.163  TLSv1.2  845 S
  124 09:09:25.329331  10.201.218.163  10.201.218.164  TLSv1.2  255 C
  125 09:09:25.331128  10.201.218.164  10.201.218.163  TLSv1.2  173 C
  126 09:09:25.333417  10.201.218.163  10.201.218.164  TLSv1.2  199 A
  127 09:09:25.335730  10.201.218.164  10.201.218.163  TLSv1.2  167 A
  128 09:09:25.339000  10.201.218.163  10.201.218.164  TLSv1.2  327 A
  129 09:09:25.339649  10.201.218.164  10.201.218.163  TLSv1.2  167 A
```

```
> 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
> 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: 77
> [3 Reassembled TCP Segments (3675 bytes): #118(1448), #120(1448), #122(779)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 3670
    > Handshake Protocol: Server Hello
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 1481
        Certificates Length: 1478
      v Certificates (1478 bytes)
          Certificate Length: 1475
        > Certificate: 308205bf308204a7a003020102021362000000026295e487… (id-at-commonName=WIN-H2Q74S1U39P.network218.com)
    > Handshake Protocol: Server Key Exchange
    > Handshake Protocol: Certificate Request
    > Handshake Protocol: Server Hello Done
```

·在後續視窗中，提供.cer檔名，然後按一下「儲存」。儲存的檔案（在本案例中是儲存到案頭）命名為servercert.cer，如下圖所示：



```
126 09:09:25.333417   10.201.218.163   10.201.2
127 09:09:25.335730   10.201.218.164   10.201.2
128 09:09:25.339000   10.201.218.163   10.201.2
129 09:09:25.339649   10.201.218.164   10.201.2

> Frame 122: 845 bytes on wire (6760 bits), 845 bytes captured (6
> Ethernet II, Src: Vmware_a5:74:2a (00:50:56:a5:74:2a), Dst: Vmw
> Internet Protocol Version 4, Src: 10.201.218.164, Dst: 10.201.2
> Transmission Control Protocol, Src Port: 636, Dst Port: 34726,
> [3 Reassembled TCP Segments (3675 bytes): #118(1448), #120(1448
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 3670
    > Handshake Protocol: Server Hello
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 1481
        Certificates Length: 1478
      v Certificates (1478 bytes)
          Certificate Length: 1475
        > Certificate: 308205bf308204a7a003020102021362000000026295e487… (id-at-commonName=WIN-H2Q74S1U39P.network218.com)
```

File name: servercert.cer

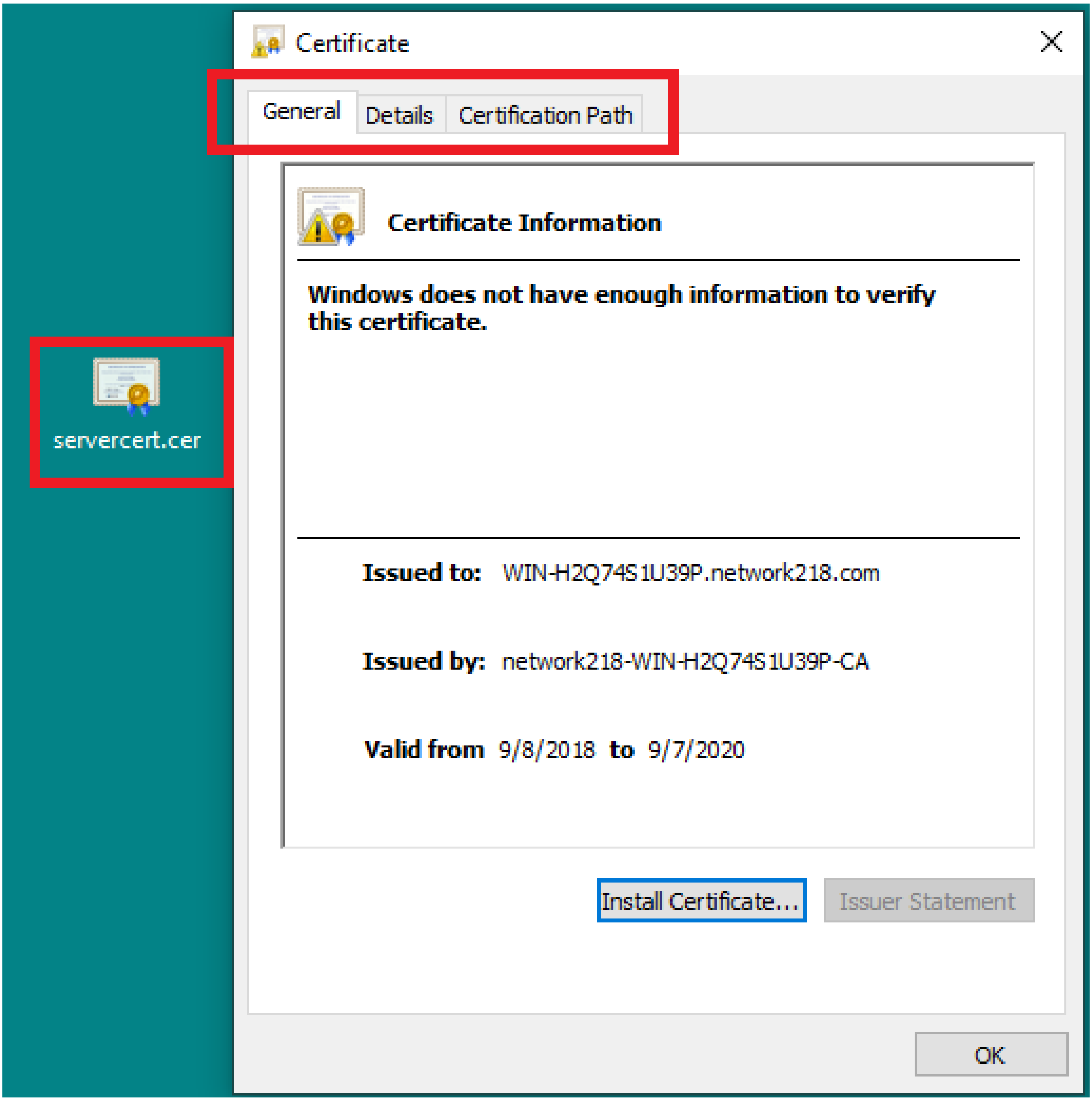
Save as type: Raw data (*.bin *.dat *.raw)

No items match your search.

步驟7.開啟儲存的.CER檔案以檢查內容

按兩下.cer檔案以檢查**General**、**Details**和**Certificate Path**頁籤中的資訊，如下圖所示：

目前尚無適用於此組態的具體疑難排解資訊。



Certificate Information

Windows does not have enough information to verify this certificate.

Issued to: WIN-H2Q74S1U39P.network218.com

Issued by: network218-WIN-H2Q74S1U39P-CA

Valid from 9/8/2018 to 9/7/2020

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。