如何从CUCM数据包捕获(PCAP)导出TLS证书

目录

简介

本文档介绍从思科统一通信管理器(CUCM)PCAP导出证书的过程。

作者：思科TAC工程师Adrian Esquillo。

先决条件

要求

Cisco 建议您了解以下主题：
·传输层安全(TLS)握手
·CUCM证书管理
·安全文件传输协议(SFTP)服务器
·实时监控工具(RTMT)

·Wireshark应用

使用的组件

·CUCM 9.X及更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

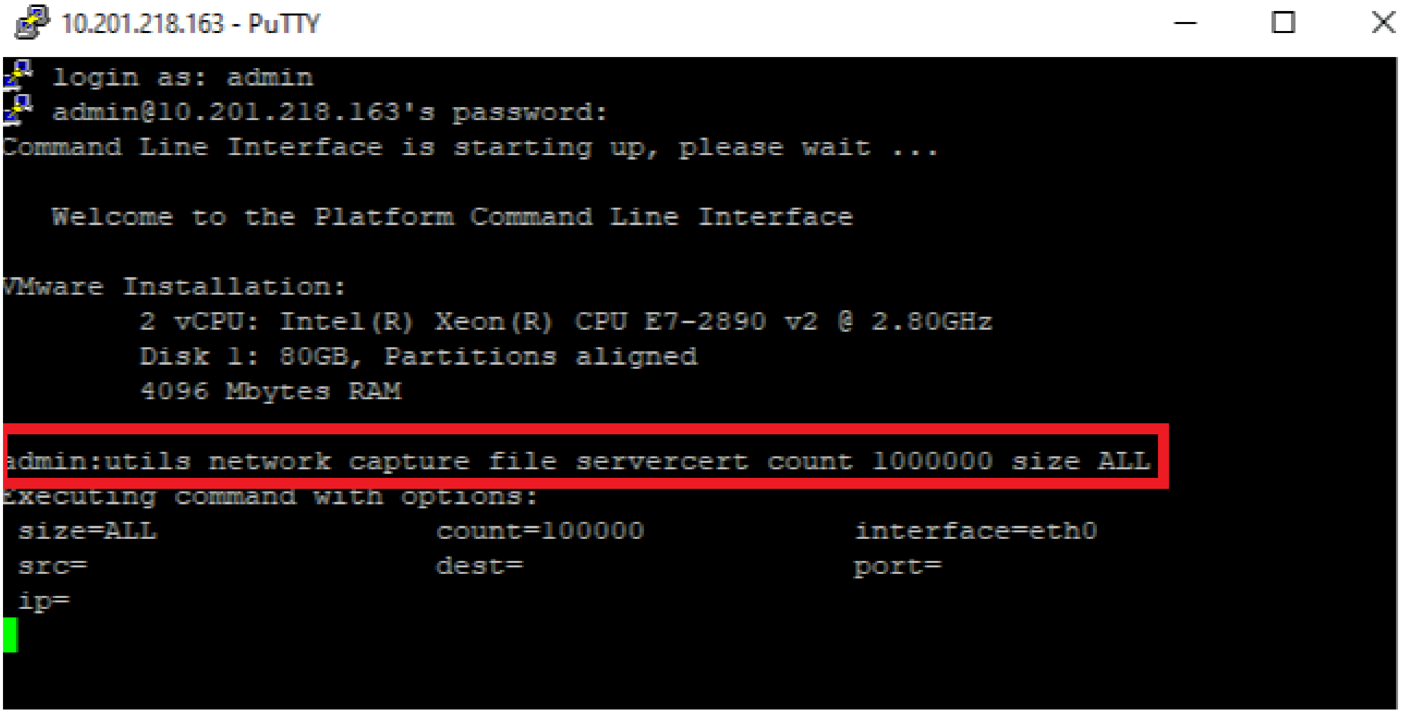
可以导出服务器证书/证书链，以确认服务器提供的服务器证书/证书链与要上传或已上传到CUCM证书管理的证书相匹配。

作为TLS握手的一部分，服务器将其服务器证书/证书链提供给CUCM。

从CUCM PCAP导出TLS证书

步骤1.在CUCM上启动数据包捕获命令

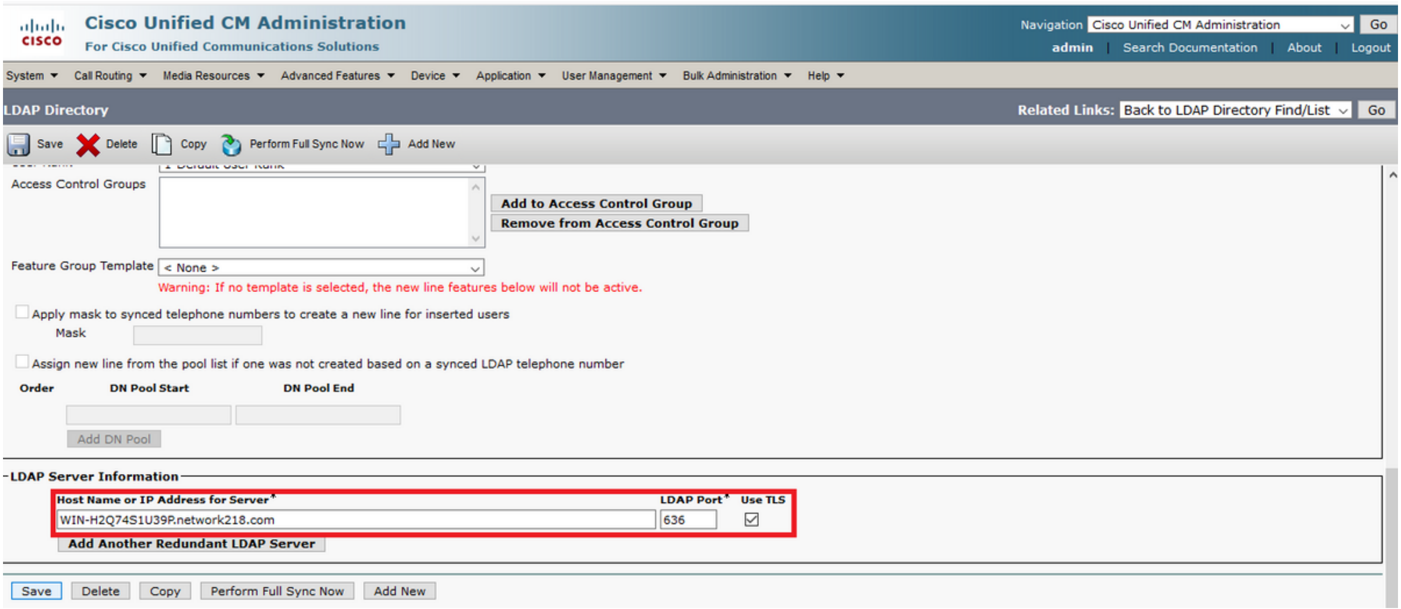
与CUCM节点建立安全外壳(SSH)连接并运行命令**utils network capture（或capture-rotate） file <filename> count 1000000 size ALL，如图所示：**



```
 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=
```

步骤2.启动服务器与CUCM之间的TLS连接

在本示例中，通过在TLS端口636上建立连接，在安全轻量目录访问协议(LDAPS)服务器和CUCM之间启动TLS连接，如图所示：


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

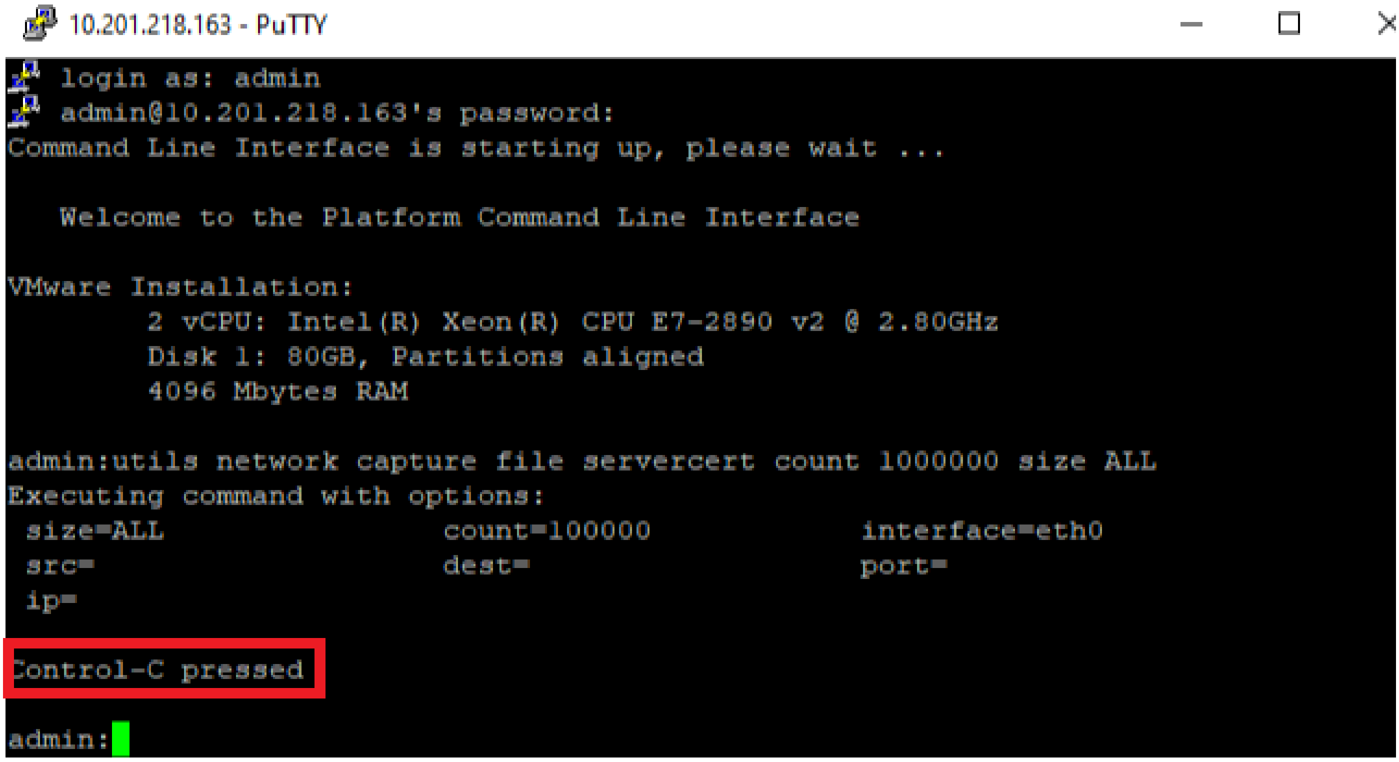
Order	DN Pool Start	DN Pool End

LDAP Server Information

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

步骤3.在TLS握手完成后停止CUCM PCAP

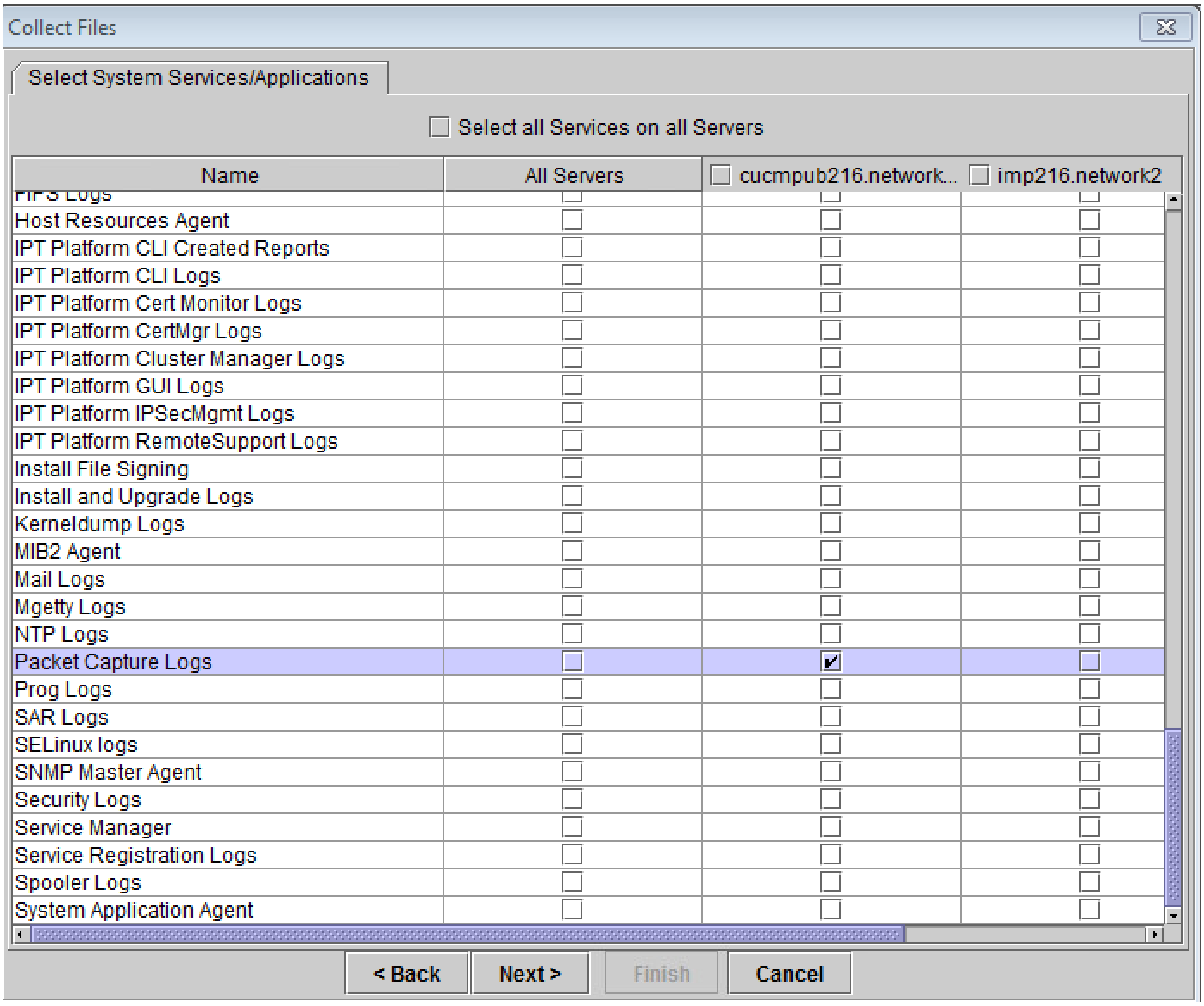
按**Control-C**停止数据包捕获，如图所示



```
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:
```

步骤4.通过列出的两种方法之一下载打包程序捕获文件

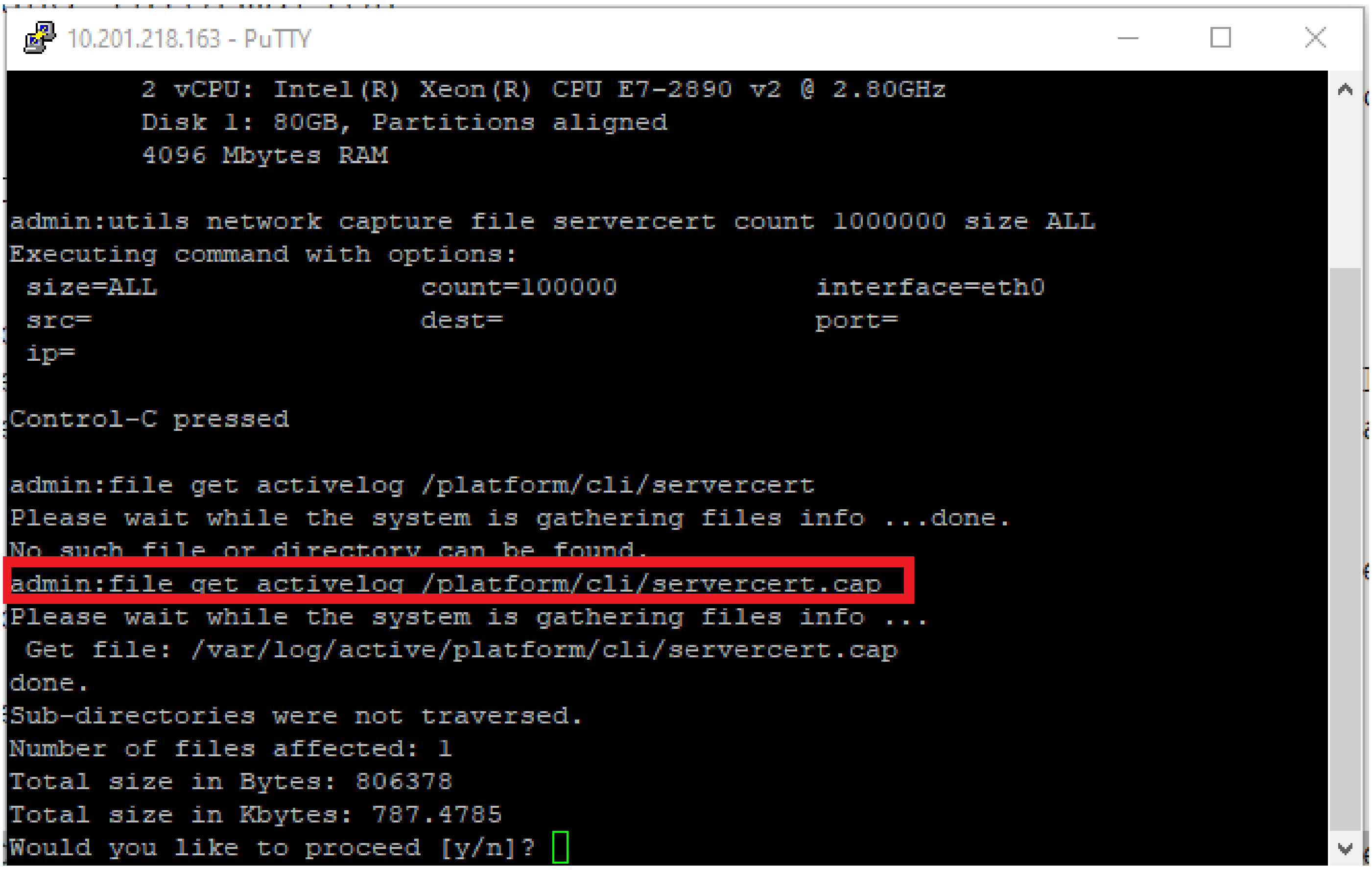
1.启动CUCM节点的RTMT并导航到**System > Tools > Trace > Trace & Log Central > Collect Files**并选中**Packet Capture Logs**框（继续执行RTMT过程以下载pcap），如图所示：



☐ 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	☐	☐	☐

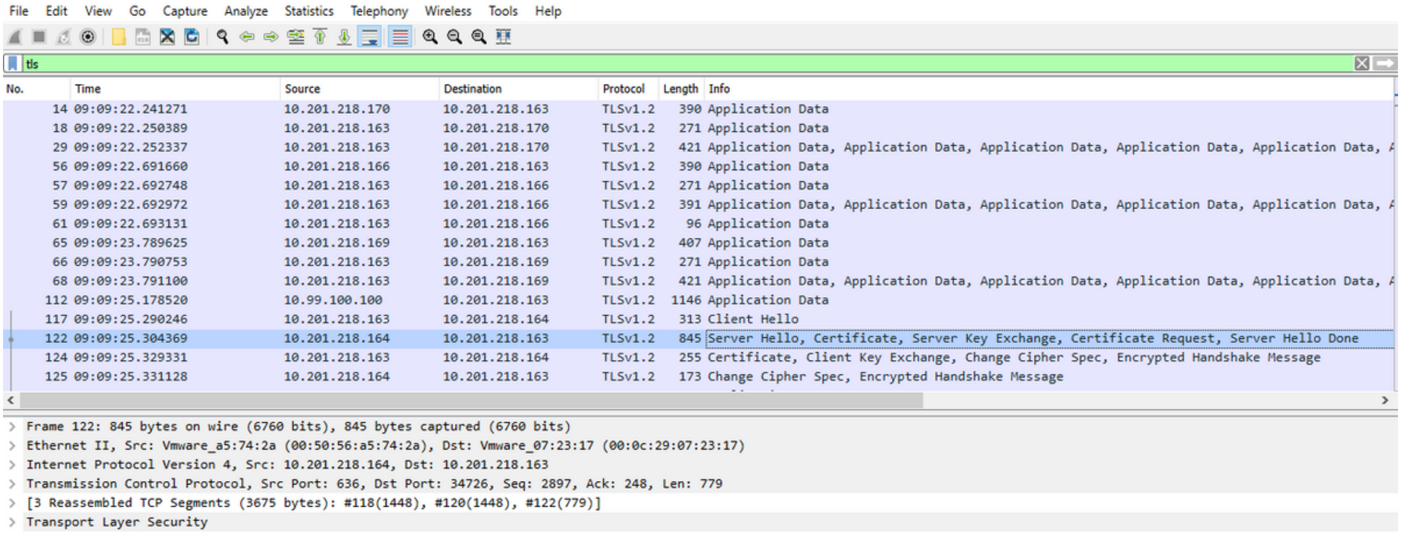
2.启动安全文件传输协议(SFTP)服务器，在CUCM SSH会话中运行命令**file get activelog /patform/cli/<pcap filename>.cap**（通过提示继续下载SFTP服务器上的PCAP），如图所示：



```
        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]?
```

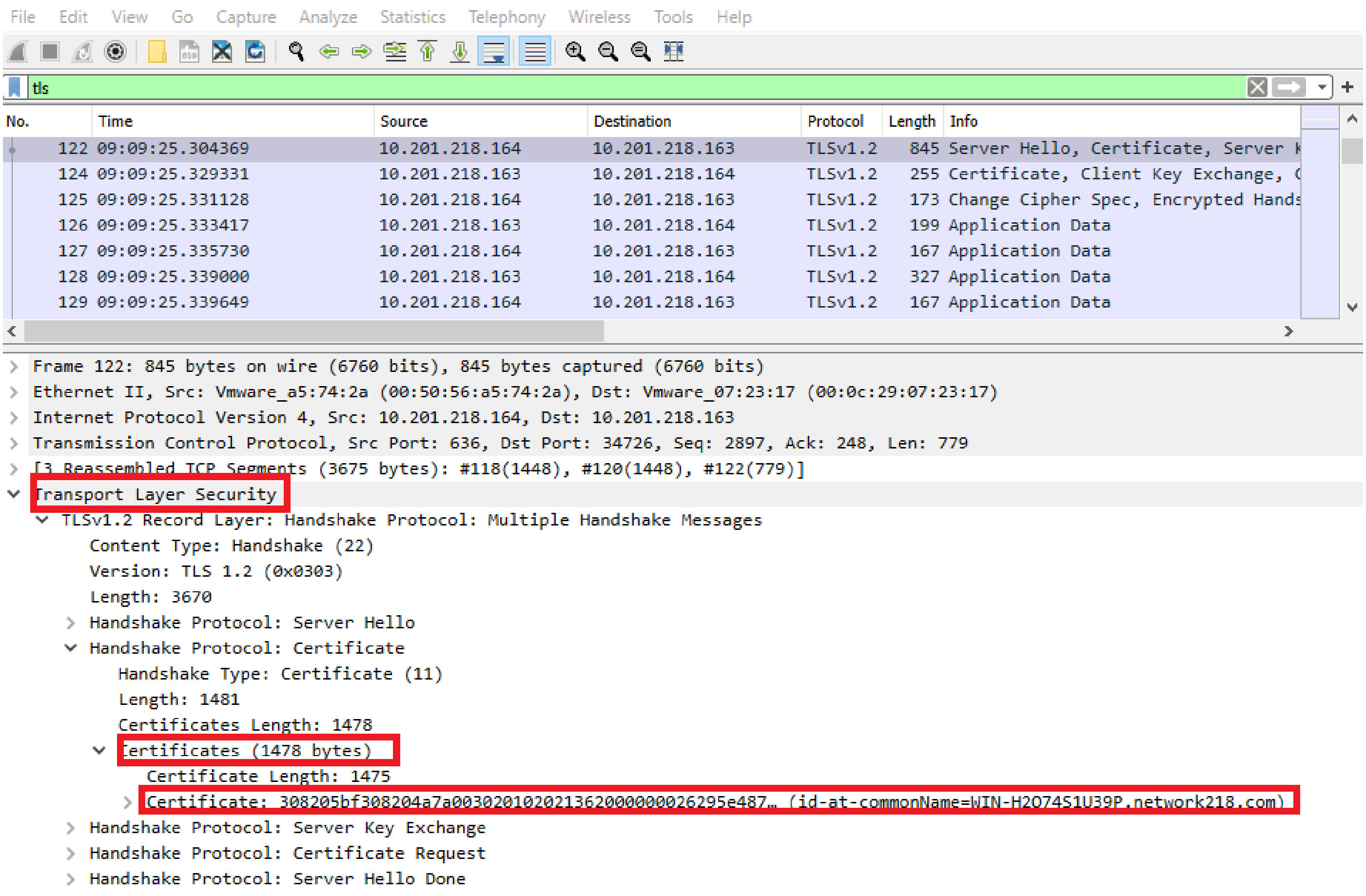
步骤5.确定服务器向CUCM提供的证书数

使用Wireshark应用程序打开pcap并在**tls**上进行过滤，以使用包含向CUCM提供的服务器证书/证书链的**Server Hello**确定数据包。如图所示，这是帧122:



```
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
```

·展开带证**书的Server Hello数据包的**Transport Layer Security > Certificate信息，以确定提供给CUCM的证书数。排名靠前的证书是服务器证书。在本例中，仅显示1个证书，即服务器证书，如图所示：

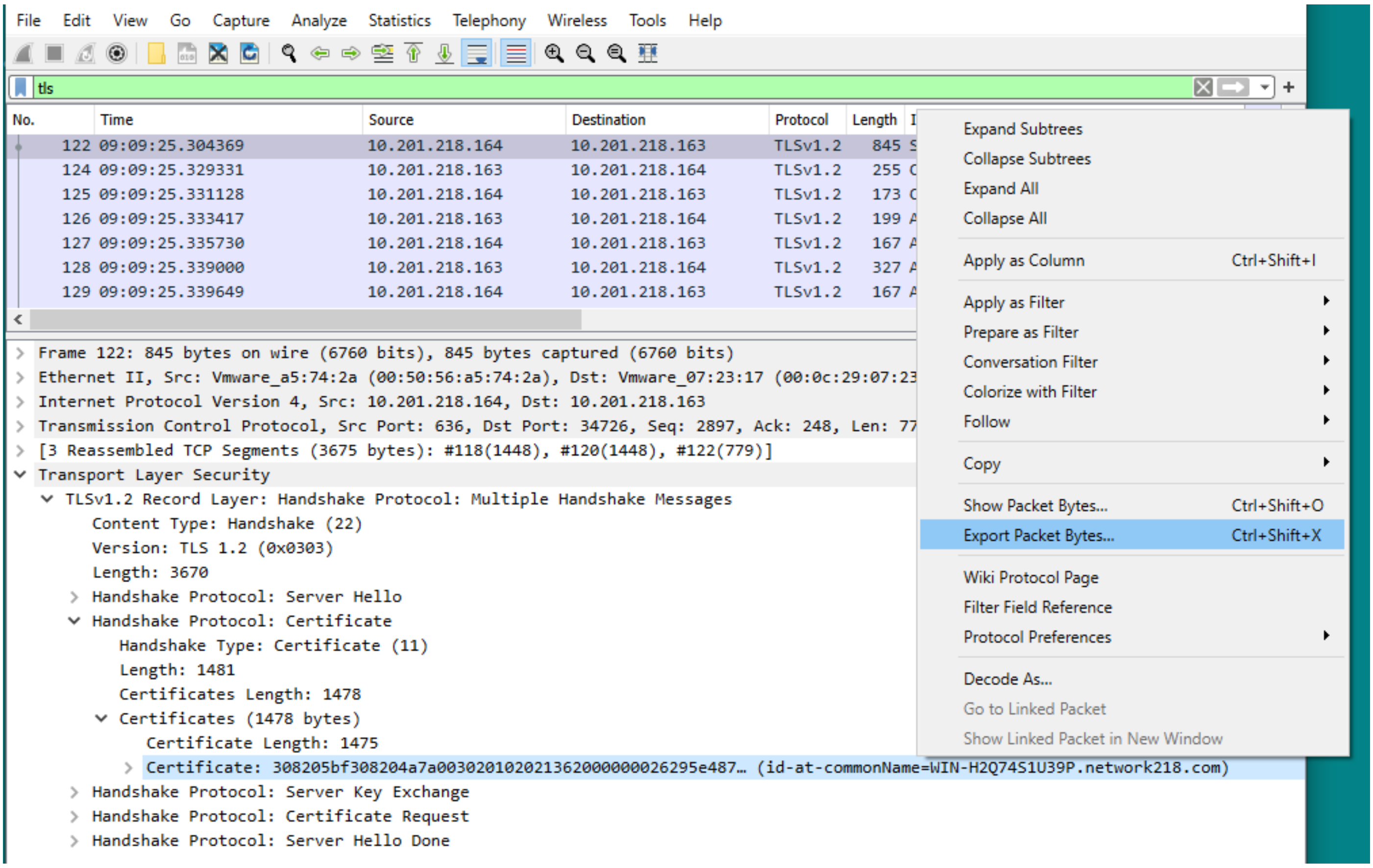


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
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)]
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
```

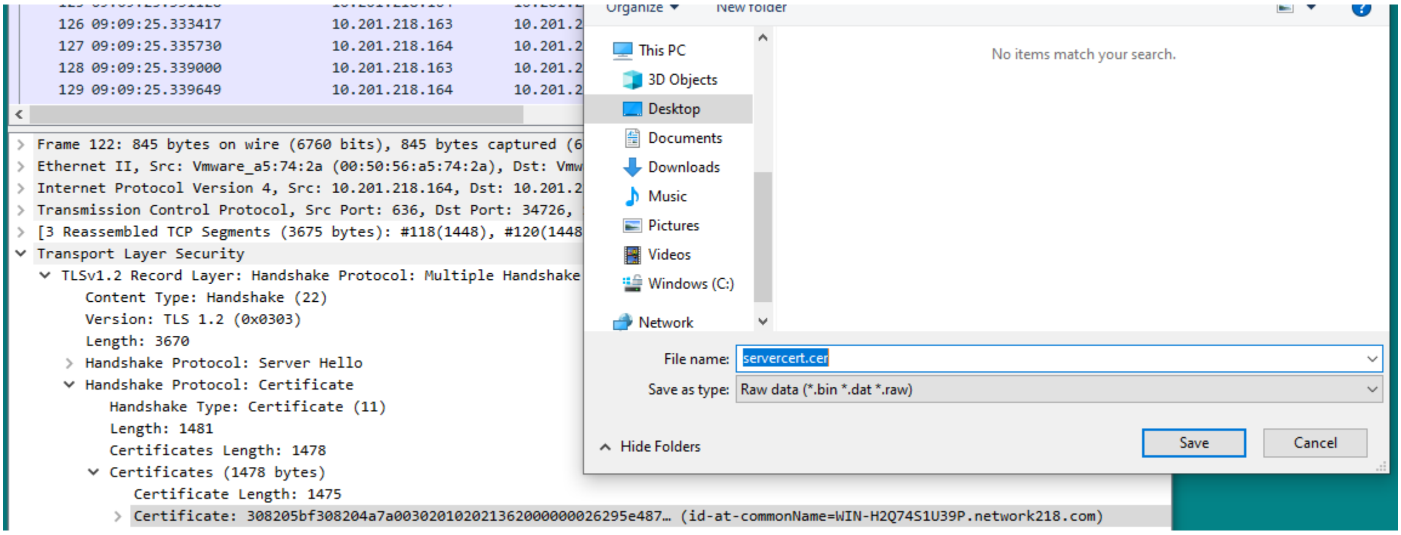
步骤6.从CUCM PCAP导出服务器证书/证书链

在本例中，仅显示服务器证书，因此您需要检查服务器证书。右键单击服务器证书并选择**导出数据包字节**以另存为.cer证书，如图所示：



```
tls

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
```

·在后续窗口中，提供.cer文件名，然后单击“保存”。保存的文件（在本例中，保存到桌面）命名为servercert.cer，如图所示：



```
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)
```

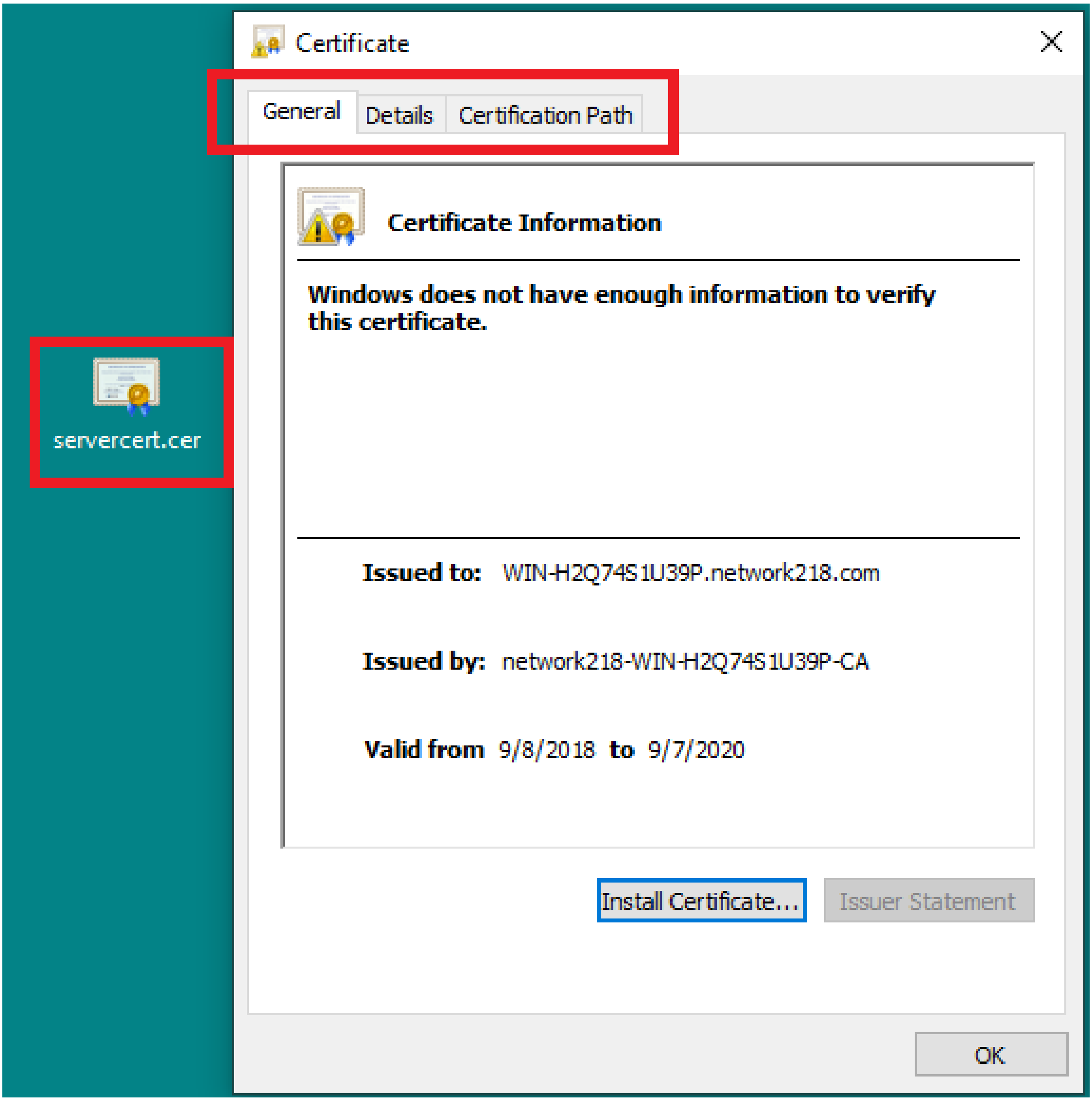
No items match your search.

File name: servercert.cer

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

步骤7.打开保存的.CER文件以检查内容

双击.cer文件以检查“常规”、“详细信息”和“证书路径”选项卡中的信息，如图所示：



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

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。