Troubleshoot Corporate Directory "Host Not Found" Issues

Contents

Introduction

This document describes how to troubleshoot "Host Not Found" issues in the Corporate Directory feature of IP Phones.

Background Information

Important information relevant to this document is:

- The Corporate Directory is a Cisco-provided default IP phone service which installs automatically with Cisco Unified Communications Manager (CUCM).
- Information about phone subscription to the various phone services are stored in the database in the telecasterservice, telecasterserviceparameter, telecastersubscribedparameter, telecastersubscribedservice tables.
- On the phone, when you select the option Corporate Directory, the phone sends either an HTTP or HTTPS request to one of the CUCM servers and is returned as an XML object as an HTTP(S) response. If HTTPS, then this also depends on the phone connecting to TVS service to verify the certificate for HTTPS. On phones that support midlets, this can be implemented in the phone midlet, and affected by Services Provisioning setting.

Important Information

- Clarify if the issue occurs when you access Directories or Corporate Directory.
- What is the Service UR field set to under the Corporate Directory service?
  - If the URL is set to Application:Cisco/CorporateDirectory, then based on the phone's firmware version, the phone makes either an HTTP or HTTPS request.
  - Phones that use firmware version 9.3.3 and later by default make an HTTPS request.
- When the service URL is set to Application:Cisco/CorporateDirectory, the phone sends the HTTP(S) request to the server which is first in it's CallManager (CM) group.
- Identify the network topology between the phone and the server to which the HTTP(S) request is sent.
- Pay attention to firewalls, WAN optimizers., and so on in the path which can drop/hamper HTTP(S) traffic.
- If HTTPS is in use, then ensure connectivity between the phone and TVS server, and that TVS is

functioning.

Working Scenario

In this scenario, the phone service URL is set to Application:Cisco/CorporateDirectory, and the phone uses HTTPS.

This example shows the configuration file of the phone with the correct URL.

```
<phoneService  type="1" category="0">
<name>Corporate Directory</name>
<url>Application:Cisco/CorporateDirectory</url>
<vendor></vendor>
<version></version>
</phoneService>
```

From the phone console logs, you are able to verify these steps.

1. The phone uses the HTTPS URL.

   ```
   7949 NOT 11:04:14.765155  CVM-appLaunchRequest: [thread=AWT-EventQueue-0]
   [class=cip.app.G4ApplicationManager] Creating application module -
    Corporate Directory
   7950 ERR 11:04:14.825312  CVM-XsiAppData&colon;:getCdUrl:
   [thread=appmgr MQThread]
   [class=xxx.xxx.xx] Using HTTPS URL
   ```

2. The Tomcat web certificate presented to the phone from the Directories server is not available on the phone. Hence, the phone attempts to authenticate the certificate via the Trust Verification Service (TVS).

   ```
   7989 ERR 11:04:15.038637  SECD: -HTTPS cert not in CTL, <10.106.111.100:8443>
   7990 NOT 11:04:15.038714  SECD: -TVS service available, can attempt via TVS
   ```

3. The phone looks in the TVS cache first, and if not found, it contacts the TVS server.

   ```
   7995 NOT 11:04:15.039286  SECD: -TVS Certificate Authentication request
   7996 NOT 11:04:15.039394  SECD: -No matching entry found at cache
   ```

4. Since the connection to the TVS is also secure, a certificate authentication is completed, and this message is printed, if it is successful.

   ```
   8096 NOT 11:04:15.173585  SECD: -Successfully obtained a TLS connection
    to the TVS server
   ```

5. The phone now sends a request to authenticate the certificate.

```
8159 NOT 11:04:15.219065  SECD: -Successfully sent the certificate Authentication
 request to TVS server, bytes written : 962
8160 NOT 11:04:15.219141  SECD: -Done sending Certificate Validation request
8161 NOT 11:04:15.219218  SECD: -Authenticate Certificate : request sent to
 TVS server - waiting for response
```

6. The response "0" from the TVS means the authentication was successful.

```
8172 NOT 11:04:15.220060  SECD: -Authentication Response received, status : 0
```

7. This message is displayed, and then you see the response.

```
8185 NOT 11:04:15.221043  SECD: -Authenticated the HTTPS conn via TVS

8198 NOT 11:04:15.296173  CVM-[truncated] Received
         HTTP/1.1 200 OK^M
        X-Frame-Options: SAMEORIGIN^M
        Set-Cookie: JSESSIONID=660646D3655BB00734D3895606BCE76F;
 Path=/ccmcip/; Secure; HttpOnly^M
        Content-Type: text/xml;charset=utf-8^M
        Content-Length: 966^M
        Date: Tue, 30 Sep 2014 11:04:15 GMT^M
        Server:  ^M
        ^M
        <?xml version="1.0" encoding="UTF-8" standalone="yes"?><CiscoIPPhoneInput>
<Title>Directory Search</Title><Prompt>Enter search criteria</Prompt><SoftKeyItem>
<Name>Search</Name><Position>1</Position><URL>SoftKey:Submit</URL></SoftKeyItem>
<SoftKeyItem><Name>&lt;&lt;</Name><Position>2</Position><URL>SoftKey:&lt;&lt;</URL>
</SoftKeyItem><SoftKeyItem><Name>Cancel</Name><Position>3</Position>
<URL>SoftKey:Cancel</URL></SoftKeyItem>
<URL>https://10.106.111.100:8443/ccmcip/xmldirectorylist.jsp</URL>
<InputItem><DisplayName>First Name</DisplayName>
<QueryStringParam>f</QueryStringParam><InputFlags>A</InputFlags>
<DefaultValue></DefaultValue></InputItem><InputItem>
<DisplayName>Last Name</DisplayName><QueryStringParam>l</QueryStringParam>
<InputFlags>A</InputFlags><DefaultValue></DefaultValue></InputItem><InputItem>
<DisplayName>
```

The certificate authentication process is similar to what is discussed in Phone Contacts Trust Verification Service for Unknown Certificate.

From the packet captures (PCAPs) collected at the phone end, you are able to verify the TVS communication with the use of this filter - tcp.port==2445.

In the simultaneous TVS logs:

1. Review traces in regards to the Transport Layer Security (TLS) hand shake.
2. Next, review the incoming hex dump.

```
04:04:15.270 |   debug ipAddrStr (Phone) 10.106.111.121
04:04:15.270 |<--debug
04:04:15.270 |-->debug
04:04:15.270 |   debug 2:UNKNOWN:Incoming Phone Msg:
.
.
04:04:15.270 |   debug
HEX_DUMP: Len = 960:

04:04:15.270 |<--debug
04:04:15.270 |-->debug
04:04:15.270 |   debug 57 01 01 00 00 00 03 ea
.
<< o/p omitted >>
.
04:04:15.271 |   debug     MsgType               : TVS_MSG_CERT_VERIFICATION_REQ
```

3. The TVS retrieves the issuer details.

```
04:04:15.272 |-->CDefaultCertificateReader::GetIssuerName
04:04:15.272 |   CDefaultCertificateReader::GetIssuerName got issuer name
04:04:15.272 |<--CDefaultCertificateReader::GetIssuerName
04:04:15.272 |-->debug
04:04:15.272 |   debug tvsGetIssuerNameFromX509 - issuerName :
 CN=cucm10;OU=TAC;O=Cisco;L=Blore;ST=KN;C=IN and Length: 43
04:04:15.272 |<--debug
```

4. The TVS verifies the certificate.

```
04:04:15.272 |   debug tvsGetSerialNumberFromX509 - serialNumber :
 6F969D5B784D0448980F7557A90A6344 and Length: 16
04:04:15.272 |   debug CertificateDBCache::getCertificateInformation -
 Looking up the certificate cache using Unique MAP ID :
 6F969D5B784D0448980F7557A90A6344CN=cucm10;OU=TAC;O=Cisco;L=Blore;ST=KN;C=IN
04:04:15.272 |   debug CertificateDBCache::getCertificateInformation -
 Certificate compare return =0
04:04:15.272 |   debug CertificateDBCache::getCertificateInformation -
 Certificate found and equal
```

5. The TVS sends the response to the phone.

```
04:04:15.272 |   debug 2:UNKNOWN:Sending CERT_VERIF_RES msg
04:04:15.272 |   debug     MsgType               : TVS_MSG_CERT_VERIFICATION_RES
```

Phone Service URL is Set to Application:Cisco/CorporateDirectory and the Phone Uses HTTP

Note: Instead of the use of an earlier phone firmware version, the service and secure service URL were hard-coded to the HTTP URL. However, the same sequence of events is seen in phone firmware which makes use of HTTP by default.

The configuration file of the phone has the correct URL.

```
<phoneService  type="1" category="0">
<name>Corporate Directory</name>
<url>Application:Cisco/CorporateDirectory</url>
<vendor></vendor>
<version></version>
</phoneService>
```

From the phone console logs, you are able to verify these steps.

```
7250 NOT 11:44:49.981390  CVM-appLaunchRequest: [thread=AWT-EventQueue-0]
[class=cip.app.G4ApplicationManager] Creating application module -
 Corporate Directory/-838075552
7254 NOT 11:44:50.061552  CVM-_HTTPMakeRequest1: Processing Non-HTTPS URL
7256 NOT 11:44:50.061812  CVM-_HTTPMakeRequest1() theHostname: 10.106.111.100:8080


7265 NOT 11:44:50.233788  CVM-[truncated] Received
         HTTP/1.1 200 OK^M
        X-Frame-Options: SAMEORIGIN^M
        Set-Cookie: JSESSIONID=85078CC96EE59CA822CD607DDAB28C91;
 Path=/ccmcip/; HttpOnly^M
        Content-Type: text/xml;charset=utf-8^M
        Content-Length: 965^M
        Date: Tue, 30 Sep 2014 11:44:50 GMT^M
        Server:  ^M
        ^M
        <?xml version="1.0" encoding="UTF-8" standalone="yes"?><CiscoIPPhoneInput>
<Title>Directory Search</Title><Prompt>Enter search criteria</Prompt><SoftKeyItem>
<Name>Search</Name><Position>1</Position><URL>SoftKey:Submit</URL></SoftKeyItem>
<SoftKeyItem><Name>&lt;&lt;</Name><Position>2</Position><URL>SoftKey:&lt;&lt;</URL>
</SoftKeyItem><SoftKeyItem><Name>Cancel</Name><Position>3</Position>
<URL>SoftKey:Cancel</URL></SoftKeyItem>
<URL>http://10.106.111.100:8080/ccmcip/xmldirectorylist.jsp</URL><InputItem>
<DisplayName>First Name</DisplayName><QueryStringParam>f</QueryStringParam>
<InputFlags>A</InputFlags><DefaultValue></DefaultValue></InputItem><InputItem>
<DisplayName>Last Name</DisplayName><QueryStringParam>l</QueryStringParam>
<InputFlags>A</InputFlags><DefaultValue></DefaultValue></InputItem><InputItem>
<DisplayName>Number</D
```

From the packet captures, you see an HTTP GET request, and a successful RESPONSE. This is the PCAP from CUCM:

Troubleshoot

Before you troubleshoot, gather the details of the issue listed earlier:

Logs to Collect, if Required

- Simultaneous packet captures from the IP phone, and from the CUCM server (the server which is first in it's CM group where the HTTP(S) request would be sent to).
- IP phone console logs.
- Cisco TVS logs (detailed).

  When you set the TVS logs to detailed, the service needs to be restarted for the trace level changes to take place. See Cisco bug ID CSCuq22327 for the enhancement to notify that a service restart is required when log levels are changed.

Complete these steps in order to isolate the issue:

Step 1.

Create a test service with these details:

```
Service Name : <Any Name>
        Service URL :  http://<CUCM_IP_Address>:8080/ccmcip/xmldirectoryinput.jsp
        Secure-Service URL : http://<CUCM_IP_Address>:8080/ccmcip/xmldirectoryinput.jsp
        Service Category : XML Service
        Service Type : Directories
        Enable : CHECK
        Enterprise Subscription : DO NOT CHECK
```

Now, subscribe this service to one of the affected phones:

a. Navigate to the device configuration page.
b. Choose **Subscribe/Unsubscribe Services** under Related Links.
c. **Subscribe** the test service you created.
d. **Save**, apply the **configuration**, and reset the **phone**.
    i. What you have done, irrespective of the phone's FW version, which determines whether to use the HTTP or HTTPS URL, is force it to use the HTTP URL.
    ii. Access the Corporate Directory service on the phone.
    iii. If it does not work, then collect the logs mentioned previously, and compare them with the working scenario mentioned under the Working Scenario section, and identify where the deviation is.
    iv. If it works, then you have at least confirmed that from CUCM IP Phone service perspective

there are no issues.

v. At this stage, the issue is most likely with the phones that use the HTTPS URL.
vi. Now, pick a phone that does not work, and proceed to next step.

When it works with this change, you need to decide if it is OK to leave the configuration with the corporate directory request/response that works over HTTP instead of HTTPS. HTTPS communication does not work due to one of the reasons discussed next.

Step 2.

Collect the logs mentioned previously, and compare them with the working scenario mentioned under the Working Scenario section, and identify where the deviation is.

It could be one of these issues:

a. The phone is unable to contact the TVS server.
    i. In the PCAPS, verify the communication on port 2445.
    ii. Ensure that none of the network devices in the path block this port.
b. The phone contacts the TVS server, but the TLS handshake fails.

These lines can be printed in the phone console logs:

```
5007: NOT 10:25:10.060663 SECD: clpSetupSsl: Trying to connect to IPV4,
 IP: 192.168.136.6, Port : 2445
5008: NOT 10:25:10.062376 SECD: clpSetupSsl: TCP connect() waiting,
 <192.168.136.6> c:14 s:15 port: 2445
5009: NOT 10:25:10.063483 SECD: clpSetupSsl: TCP connected,
 <192.168.136.6> c:14 s:15
5010: NOT 10:25:10.064376 SECD: clpSetupSsl: start SSL/TLS handshake,
 <192.168.136.6> c:14 s:15
5011: ERR 10:25:10.068387 SECD: EROR:clpState: SSL3 alert
 read:fatal:handshake failure:<192.168.136.6>
5012: ERR 10:25:10.069449 SECD: EROR:clpState: SSL_connect:failed in SSLv3
 read server hello A:<192.168.136.6>
5013: ERR 10:25:10.075656 SECD: EROR:clpSetupSsl: ** SSL handshake failed,
 <192.168.136.6> c:14 s:15
5014: ERR 10:25:10.076664 SECD: EROR:clpSetupSsl: SSL/TLS handshake failed,
 <192.168.136.6> c:14 s:15
5015: ERR 10:25:10.077808 SECD: EROR:clpSetupSsl: SSL/TLS setup failed,
 <192.168.136.6> c:14 s:15
5016: ERR 10:25:10.078771 SECD: EROR:clpSndStatus: SSL CLNT ERR,
 srvr<192.168.136.6>
```

See Cisco bug ID CSCua65618 for more information.

c. The Phone contacts the TVS servers, and the TLS handshake is successful, but the TVS is unable to verify the signer of the certificate that the phone requested to authenticate.

Snippets from TVS logs are listed here:

The Phone contacts the TVS.

```
05:54:47.779 |   debug 7:UNKNOWN:Got a new ph conn 10.106.111.121 on 10, Total Acc = 6..
.
.
05:54:47.835 |   debug     MsgType               : TVS_MSG_CERT_VERIFICATION_REQ
```

The TVS gets the issuer name.

```
05:54:47.836 |-->CDefaultCertificateReader::GetIssuerName
05:54:47.836 |   CDefaultCertificateReader::GetIssuerName got issuer name
05:54:47.836 |<--CDefaultCertificateReader::GetIssuerName
05:54:47.836 |-->debug
05:54:47.836 |   debug tvsGetIssuerNameFromX509 - issuerName :
 CN=cucmpub9;OU=TAC;O=Cisco;L=Bangalore;ST=KN;C=IN and Length: 49
```

It looks up the certificate, but cannot find it.

```
05:54:47.836 |   debug CertificateCTLCache::getCertificateInformation
 - Looking up the certificate cache using Unique MAP ID :
 62E09123B09A61D20E77BE5BF5A82CD4CN=cucmpub9;OU=TAC;O=Cisco;L=Bangalore;ST=KN;C=IN
05:54:47.836 |<--debug
05:54:47.836 |-->debug
05:54:47.836 |   debug ERROR:CertificateCTLCache::getCertificateInformation
 - Cannot find the certificate in the cache
05:54:47.836 |<--debug
05:54:47.836 |-->debug
05:54:47.836 |   debug getCertificateInformation(cert) : certificate not found
```

d. HTTPS traffic is blocked/dropped somewhere in the network.

   Get simultaneous PCAPs from the phone and the CUCM server in order to verify the communication.

Other Scenarios When the "Host Not Found" Issue Occurs

1. The CUCM server is defined by the hostname along with issues in name resolution.
2. The TVS server list is empty on the phone when it downloads the xmldefault.cnf.xml file. (In Version 8.6.2 the default configuration file does not have the TVS entry in it due to Cisco bug ID CSCti64589.)
3. The phone is unable to use the TVS entry in the configuration file because it downloaded the xmldefault.cnf.xml file. See Cisco bug ID CSCuq33297 - Phone to parse TVS information from the default configuration file.
4. The Corporate Directory does not work after a CUCM upgrade because the phone firmware upgrades to a later version which eventually changes the behavior of the use of HTTPS by default.