排除企业目录故障"；未找到主机"问题

目录

简介

背景信息

重要信息

工作场景

电话服务URL设置为Application:Cisco/CorporateDirectory，电话使用HTTP

故障排除

出现“Host Not Found”问题的其他场景

简介

本文档介绍如何排除IP电话公司目录功能中的“找不到主机”问题。

背景信息

与本文档相关的重要信息包括：

- 公司目录是思科提供的默认IP电话服务，可随Cisco Unified Communications Manager(CUCM)自动安装。
- 有关电话预订各种电话服务的信息存储在数据库中的telecasterservice、telecasterserviceparameter、telecastersubscribedparameter和telecastersubscribedservice表中。
- 在电话上，当您选择Corporate Directory选项时，电话会向其中一个CUCM服务器发送HTTP或HTTPS请求，并作为XML对象返回作为HTTP(S)响应。如果是HTTPS，则这还取决于连接到TVS服务的电话以验证HTTPS的证书。在支持Midlet的电话上，这可以在电话Midlet中实施，并受Services Provisioning设置的影响。

重要信息

- 当您访问目录或公司目录时，请澄清问题是否发生。
- Corporate Directory服务下的Service UR字段设置为什么？
  - 如果URL设置为Application:Cisco/CorporateDirectory，则根据电话的固件版本，电话会发出HTTP或HTTPS请求。
  - 默认情况下，使用固件版本9.3.3及更高版本的电话会发出HTTPS请求。
- 当服务URL设置为Application:Cisco/CorporateDirectory时，电话将HTTP(S)请求发送到其CallManager(CM)组中的第一个服务器。
- 确定电话与HTTP(S)请求发送到的服务器之间的网络拓扑。
- 注意路径中可能丢弃/阻止HTTP(S)流量的防火墙、WAN优化器等。
- 如果正在使用HTTPS，则确保电话和TVS服务器之间的连接，并且TVS正常工作。

工作场景

在这种情况下，电话服务URL设置为Application:Cisco/CorporateDirectory，并且电话使用HTTPS。

此示例显示具有正确URL的电话配置文件。

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

通过电话控制台日志，您可以验证这些步骤。

1. 电话使用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. 从目录服务器提供给电话的Tomcat Web证书在电话上不可用。因此，电话尝试通过信任验证服务(TVS)对证书进行身份验证。

   ```
   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. 电话首先在TVS缓存中查找，如果未找到，则会与TVS服务器联系。

   ```
   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. 由于与TVS的连接也是安全的，因此证书身份验证完成，如果成功，将打印此消息。

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

5. 电话现在会发送请求以对证书进行身份验证。

   ```
   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. TVS的响应“0”表示身份验证成功。

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

7. 系统将显示此消息，然后您会看到响应。

```
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>
```

证书身份验证过程类似于在Phone Contacts Trust Verification Service for Unknown Certificate中讨论的内容。

通过电话端收集的数据包捕获(PCAP)，您可以使用此过滤器 — tcp.port==2445验证TVS通信。

在同时TVS日志中：

1. 回顾传输层安全(TLS)握手的踪迹。
2. 接下来，查看传入的十六进制转储。

```
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. TVS检索颁发者详细信息。

```
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. TVS验证证书。

```
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. TVS将响应发送到电话。

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

电话服务URL设置为Application:Cisco/CorporateDirectory，电话使用HTTP

注意：服务和安全服务URL被硬编码为HTTP URL，而不是使用早期的电话固件版本。但是，在默认情况下使用HTTP的电话固件中可以看到相同的事件序列。

电话的配置文件具有正确的URL。

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

通过电话控制台日志，您可以验证这些步骤。

```
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
```

从数据包捕获中，您会看到HTTP GET请求和成功的RESPONSE。这是CUCM的PCAP:



故障排除

在排除故障之前，请收集之前列出的问题的详细信息：

要收集的日志（如果需要）

- 同时从IP电话和CUCM服务器(其CM组中的第一个服务器，HTTP(S)请求将发送到该服务器)捕获数据包。
- IP电话控制台日志。
- 思科TVS日志（详细）。

  将TVS日志设置为detailed时，需要重新启动服务才能进行跟踪级别更改。请参阅Cisco Bug ID CSCuq22327，了解更改日志级别时通知需要重新启动服务的增强功能。

完成以下步骤以隔离问题：

步骤1:

使用以下详细信息创建测试服务：

```
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
```

现在，请将此服务订用到受影响的电话之一：

a. 导航到设备配置页面。
b. 选择Related Links下的Subscribe/Unsubscribe Services。
c. 订阅您创建的测试服务。
d. 保存、应用配置并重置电话。
    i. 无论电话的FW版本如何（确定是使用HTTP还是HTTPS URL），您所做的都是强制使用HTTP URL。
    ii. 通过电话访问公司目录服务。
    iii. 如果它不起作用，则收集之前提到的日志，将其与“工作场景”部分中提到的工作场景进行比较，并确定偏差的位置。
    iv. 如果正常工作，则您至少已确认，从CUCM IP电话服务的角度而言，不存在问题。
    v. 在此阶段，使用HTTPS URL的电话最有可能出现问题。
    vi. 现在，请选择不工作的电话，然后继续下一步。

当它处理此更改时，您需要确定保留通过HTTP而不是HTTPS处理的企业目录请求/响应的配置是否正常。HTTPS通信不起作用，原因如下。

Step 2.

收集之前提到的日志，将其与“工作场景”部分中提到的工作场景进行比较，并确定偏差的位置。

这可能属于以下问题之一：

a. 电话无法联系TVS服务器。
    i. 在PCAPS中，验证端口2445上的通信。
    ii. 确保路径中的所有网络设备均不会阻塞此端口。
b. 电话与TVS服务器联系，但TLS握手失败。

电话控制台日志中可打印以下行：

```
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>
```

有关详细信息，请参阅Cisco Bug ID CSCua65618。

c. 电话联系TVS服务器，并且TLS握手成功，但是TVS无法验证电话请求进行身份验证的证书的签名者。

TVS日志的代码段如下所示：

电话与TVS联系。

```
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
```

TVS获取颁发者名称。

```
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
```

它查找证书，但找不到该证书。

```
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流量在网络中的某处被阻止/丢弃。

从电话和CUCM服务器同时获取PCAP以验证通信。

出现“Host Not Found”问题的其他场景

1. CUCM服务器由主机名以及名称解析中的问题定义。
2. 下载xmldefault.cnf.xml文件时，电话上的TVS服务器列表为空。(在版本8.6.2中，由于Cisco Bug ID CSCti64589，默认配置文件没有TVS条目。)
3. 电话无法使用配置文件中的TVS条目，因为它已下载xmldefault.cnf.xml文件。请参阅Cisco bug ID CSCuq33297 — 电话，以解析默认配置文件中的TVS信息。
4. 企业目录在CUCM升级后不起作用，因为电话固件会升级到更高版本，最终会更改默认情况下使用HTTPS的行为。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。