

회사 디렉터리 "호스트를 찾을 수 없음" 문제 해결

목차

[소개](#)

[배경 정보](#)

[중요 정보](#)

[작업 시나리오](#)

[전화 서비스 URL이 Application:Cisco/CorporateDirectory로 설정되어 있으며 전화기에서 HTTP를 사용합니다.](#)

[문제 해결](#)

["Host Not Found\(호스트를 찾을 수 없음\)" 문제가 발생하는 기타 시나리오](#)

소개

이 문서에서는 IP Phone의 기업 디렉터리 기능에서 "호스트를 찾을 수 없음" 문제를 해결하는 방법에 대해 설명합니다.

배경 정보

이 문서와 관련된 중요한 정보는 다음과 같습니다.

- Corporate Directory는 CUCM(Cisco Unified Communications Manager)과 함께 자동으로 설치되는 Cisco에서 제공하는 기본 IP 전화 서비스입니다.
- 다양한 전화 서비스에 대한 전화 가입에 대한 정보는 telecaterservice, telecaterserviceparameter, telecatersubscribedparameter, telecatersubscribedservice 테이블의 데이터베이스에 저장됩니다.
- 전화기에서 Corporate Directory(회사 디렉토리) 옵션을 선택하면 전화기가 CUCM 서버 중 하나에 HTTP 또는 HTTPS 요청을 전송하고 XML 객체로 HTTP(S) 응답으로 반환됩니다. HTTPS인 경우 이 역시 TVS 서비스에 연결하여 HTTPS용 인증서를 확인하는 전화기에 따라 달라집니다. 미드릿을 지원하는 전화기에서 이 기능은 전화기 미드릿에서 구현되고 [서비스](#) 프로비저닝 설정의 영향을 [받을](#) 수 있습니다.

중요 정보

- 디렉터리 또는 회사 디렉터리에 액세스할 때 문제가 발생하는지 확인합니다.
- Corporate Directory(회사 디렉토리) 서비스 아래에서 Service UR(서비스 UR) 필드를 무엇으로 설정합니까?
 - URL이 Application:Cisco/CorporateDirectory로 설정된 경우 전화기의 펌웨어 버전에 따라 전화기는 HTTP 또는 HTTPS 요청을 수행합니다.
 - 펌웨어 버전 9.3.3 이상을 사용하는 전화기는 기본적으로 HTTPS를 요청합니다.
- 서비스 URL이 Application:Cisco/CorporateDirectory로 설정된 경우 전화기는 CallManager(CM) 그룹의 첫 번째 서버인 서버에 HTTP(S) 요청을 보냅니다.

- HTTP(S) 요청이 전송되는 전화기와 서버 간의 네트워크 토폴로지를 식별합니다.
- HTTP(S) 트래픽을 삭제/방해할 수 있는 경로의 방화벽, WAN 최적화 프로그램 등에 유의하십시오.
- HTTPS를 사용 중인 경우 전화기와 TVS 서버 간의 연결 및 TVS가 작동하는지 확인합니다.

작업 시나리오

이 시나리오에서 전화 서비스 URL은 Application:Cisco/CorporateDirectory로 설정되며 전화기는 HTTPS를 사용합니다.

이 예에서는 올바른 URL이 있는 전화기의 컨피그레이션 파일을 보여줍니다.

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

전화기 콘솔 로그에서 이 단계를 확인할 수 있습니다.

1. 전화기에서 HTTPS URL을 사용합니다.

```
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. 디렉터리 서버에서 전화기에 제공된 Tomcat 웹 인증서를 전화기에서 사용할 수 없습니다. 따라서 전화기는 TVS(Trust Verification Service)를 통해 인증서를 인증하려고 시도합니다.

```
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. 전화기는 TVS 캐시에서 먼저 찾고, 찾지 못한 경우 TVS 서버에 연결합니다.

```
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. TVS와의 연결도 안전하므로 인증서 인증이 완료되며 이 메시지는 성공하면 인쇄됩니다.

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

5. 이제 전화기에서 인증서 인증 요청을 보냅니다.

```
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. TVS의 응답 "0"은(는) 인증이 성공했음을 의미합니다.

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

7. 이 메시지가 표시되면 응답이 표시됩니다.

```
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>
<FormItem><DisplayLabel>First Name</DisplayLabel>
<QueryStringParam>f</QueryStringParam><InputFlags>A</InputFlags>
<DefaultValue></DefaultValue></FormItem><FormItem>
<DisplayLabel>Last Name</DisplayLabel><QueryStringParam>l</QueryStringParam>
<InputFlags>A</InputFlags><DefaultValue></DefaultValue></FormItem></InputItem>
<DisplayLabel>
```

인증서 인증 프로세스는 알 수 없는 인증서에 대한 [전화 연락처 신뢰 확인 서비스에서 설명하는 것과 유사합니다.](#)

폰 엔드에서 수집한 패킷 캡처(PCAP)에서 이 필터 tcp.port==2445를 사용하여 TVS 통신을 확인할 수 있습니다.

동시 TVS 로그에서:

- 1. TLS(Transport Layer Security) 핸드 셰이크와 관련된 추적을 검토합니다.
- 2. 다음으로, 들어오는 16진수 덤프를 검토합니다.

```
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. TVS가 발급자 세부사항을 검색합니다.

```

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. TVS가 인증서를 확인합니다.

```

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. TVS가 전화기로 응답을 전송합니다.

```

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

```

전화 서비스 URL이 Application:Cisco/CorporateDirectory로 설정되어 있으며 전화기에서 HTTP를 사용합니다.

 참고: 이전 폰 펌웨어 버전을 사용하는 대신 서비스 및 보안 서비스 URL을 HTTP URL로 하드 코딩했습니다. 그러나 기본적으로 HTTP를 사용하는 전화기 펌웨어에 동일한 이벤트 시퀀스가 표시됩니다.

전화기의 구성 파일에 올바른 URL이 있습니다.

```

<phoneService type="1" category="0">
<name>Corporate Directory</name>

```

```
<url>Application: Cisco/CorporateDirectory</url>
<vendor></vendor>
<version></version>
</phoneService>
```

전화기 콘솔 로그에서 이 단계를 확인할 수 있습니다.

```
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
```

패킷 캡처에서 HTTP GET 요청 및 성공적인 응답을 볼 수 있습니다. 다음은 CUCM의 PCAP입니다.

No.	Time	Source	Destination	Protocol	Length	Info
87	2015-01-23 09:04:10.358018000	64.103.236.206	10.106.111.99	HTTP	472	GET /ccmcip/xmldirectoryinput.jsp?name=SEP00216C899172 HTTP/1.1
89	2015-01-23 09:04:10.368077000	10.106.111.99	64.103.236.206	HTTP/HTML	1173	HTTP/1.1 200 OK

문제 해결

트러블슈팅을 수행하기 전에 앞서 나열된 문제에 대한 세부 정보를 수집하십시오.

필요한 경우 수집할 로그

- IP 전화 및 CUCM 서버(HTTP(S)) 요청이 전송될 CM 그룹의 첫 번째 서버)에서 동시 패킷 캡처
- IP Phone 콘솔 로그

- Cisco TVS 로그(상세).

TVS 로그를 detailed로 설정하면 추적 수준 변경이 적용되려면 서비스를 다시 시작해야 합니다. 로그 수준이 변경될 때 서비스를 다시 시작해야 함을 알리는 개선 사항은 Cisco 버그 ID CSCuq22327을 참조하십시오.

문제를 격리하려면 다음 단계를 완료하십시오.

1단계.

다음 세부 정보를 사용하여 테스트 서비스를 만듭니다.

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

이제 영향을 받는 전화기 중 하나에 이 서비스를 등록합니다.

- a. 디바이스 컨피그레이션 페이지로 이동합니다.
- b. Related Links(관련 링크)에서 Subscribe/Unsubscribe Services(서비스 가입/가입 취소)를 선택합니다.
- c. 생성한 테스트 서비스를 구독합니다.
- d. 전화기를 저장하고 컨피그레이션을 적용하고 재설정합니다.
 - i. HTTP 또는 HTTPS URL 사용 여부를 결정하는 전화기의 FW 버전에 관계없이 사용자가 수행한 작업은 HTTP URL을 사용하도록 강제하는 것입니다.
 - ii. 전화기에서 회사 디렉터리 서비스에 액세스합니다.
 - iii. 작동하지 않을 경우 앞에서 설명한 로그를 수집한 다음 [작업 시나리오] 섹션에서 설명한 작업 시나리오와 비교하고 편차가 있는 위치를 식별합니다.
 - iv. 이 기능이 작동하면 CUCM IP Phone 서비스 관점에서 문제가 없음을 확인한 것입니다.
 - v. 이 단계에서는 HTTPS URL을 사용하는 전화기에서 문제가 발생할 가능성이 높습니다.
 - vi. 이제 작동하지 않는 전화기를 선택하고 다음 단계로 진행합니다.

이 변경과 함께 작동하는 경우 컨피그레이션을 HTTPS 대신 HTTP를 통해 작동하는 회사 디렉터리 요청/응답과 함께 남겨도 되는지 여부를 결정해야 합니다. HTTPS 통신이 작동하지 않는 이유는 다음에 논의되는 이유 중 하나입니다.

2단계.

앞에서 언급한 로그를 수집하여 작업 시나리오 섹션에서 설명한 작업 시나리오와 비교하고 편차가 있는 위치를 확인합니다.

다음 문제 중 하나일 수 있습니다.

- a. 전화기에서 TVS 서버에 연결할 수 없습니다.

- i. PCAPS에서 포트 2445의 통신을 확인합니다.
 - ii. 경로의 네트워크 장치가 이 포트를 차단하지 않는지 확인합니다.
- b. 전화기에서 TVS 서버에 연결하지만 TLS 핸드셰이크가 실패합니다.

이러한 라인은 전화기 콘솔 로그에 인쇄할 수 있습니다.

```
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,
svr<192.168.136.6>
```

자세한 내용은 Cisco 버그 ID [CSCua65618](#)을 참조하십시오.

- c. 전화기에서 TVS 서버에 연결하고 TLS 핸드셰이크에 성공했지만 TVS에서 전화기가 인증을 요청한 인증서의 서명자를 확인할 수 없습니다.

TVS 로그의 코드 조각은 다음과 같습니다.

전화기에서 TV에 연결합니다.

```
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
```

TVS는 발급자 이름을 가져옵니다.

```
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
```

인증서를 조회하지만 찾을 수 없습니다.

```
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 트래픽은 네트워크 어딘가에서 차단/삭제됩니다.

통신을 확인하기 위해 전화기와 CUCM 서버에서 동시 PCAP를 가져옵니다.

"Host Not Found(호스트를 찾을 수 없음)" 문제가 발생하는 기타 시나리오

1. CUCM 서버는 이름 확인 문제와 함께 호스트 이름으로 정의됩니다.
2. TVS 서버 목록이 xmldefault.cnf.xml 파일을 다운로드할 때 전화기에서 비어 있습니다. (버전 8.6.2에서는 Cisco 버그 ID CSCti64589로 인해 기본 컨피그레이션 파일에 TVS 항목이 없습니다.)
3. 전화기에서 xmldefault.cnf.xml 파일을 다운로드했으므로 컨피그레이션 파일의 TVS 항목을 사용할 수 없습니다. 기본 컨피그레이션 파일에서 TVS 정보를 구문 분석하려면 Cisco 버그 ID CSCuq33297 - Phone을 참조하십시오.
4. CUCM 업그레이드 후에는 회사 디렉토리가 작동하지 않습니다. 전화기 펌웨어가 이후 버전으로 업그레이드되기 때문에 결국 HTTPS 사용 동작이 기본적으로 변경됩니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.