Fehlerbehebung bei Problemen mit dem Firmenverzeichnis "Host nicht gefunden"

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Probleme mit dem Eintrag "Host nicht gefunden" in der Funktion "Firmenverzeichnis" von IP-Telefonen beheben.

Hintergrundinformationen

Wichtige Informationen zu diesem Dokument:

- Das Firmenverzeichnis ist ein von Cisco bereitgestellter Standard-IP-Telefondienst, der automatisch mit Cisco Unified Communications Manager (CUCM) installiert wird.
- Informationen über Telefonabonnements für die verschiedenen Telefondienste werden in der Datenbank in den Tabellen für den Telecasterservice, den Telecasterserviceparameter, den Telecastersubscribedparameter und den Telecastersubscribedservice gespeichert.
- Wenn Sie auf dem Telefon die Option Firmenverzeichnis auswählen, sendet das Telefon entweder eine HTTP- oder HTTPS-Anforderung an einen der CUCM-Server und wird als XML-Objekt als HTTP(S)-Antwort zurückgegeben. Bei HTTPS hängt dies auch vom Telefon ab, das sich mit dem TVS-Dienst verbindet, um das Zertifikat für HTTPS zu überprüfen. Bei Telefonen, die Midlets unterstützen, kann dies im Telefon-Midlet implementiert werden und von den Services Provisioning-Einstellungen beeinflusst werden.

Wichtige Informationen

- Klärung, ob das Problem beim Zugriff auf Verzeichnisse oder Firmenverzeichnisse auftritt
- Wie lautet die Service-URL im Corporate Directory-Dienst?
  - Wenn die URL auf Application:Cisco/CorporateDirectory festgelegt ist, sendet das Telefon basierend auf der Firmware-Version des Telefons eine HTTP- oder HTTPS-Anforderung.
  - Telefone, die die Firmware-Version 9.3.3 oder höher verwenden, stellen standardmäßig eine HTTPS-Anforderung.
- Wenn die Service-URL auf Application:Cisco/CorporateDirectory festgelegt ist, sendet das Telefon die HTTP(S)-Anforderung an den Server, der sich zuerst in der CallManager (CM)-Gruppe befindet.
- Identifizieren Sie die Netzwerktopologie zwischen dem Telefon und dem Server, an den die HTTP(S)-Anforderung gesendet wird.
- Achten Sie auf Firewalls, WAN-Optimierer usw. in dem Pfad, der HTTP(S)-Datenverkehr verwerfen/behindern kann.

- Wenn HTTPS verwendet wird, stellen Sie die Verbindung zwischen dem Telefon und dem TVS-Server sicher, und stellen Sie sicher, dass der TVS funktioniert.

Arbeitsszenario

In diesem Szenario wird die Telefondienst-URL auf Application:Cisco/CorporateDirectory festgelegt, und das Telefon verwendet HTTPS.

Dieses Beispiel zeigt die Konfigurationsdatei des Telefons mit der richtigen URL.

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

Aus den Telefonkonsolenprotokollen können Sie diese Schritte überprüfen.

1. Das Telefon verwendet die 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. Das Tomcat-Webzertifikat, das dem Telefon vom Verzeichnisserver übermittelt wird, ist auf dem Telefon nicht verfügbar. Daher versucht das Telefon, das Zertifikat über den Trust Verification Service (TVS) zu authentifizieren.

   ```
   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. Das Telefon sucht zuerst im TVS-Cache und kontaktiert den TVS-Server, falls es nicht gefunden wird.

   ```
   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. Da die Verbindung zum TVS ebenfalls sicher ist, ist eine Zertifikatsauthentifizierung abgeschlossen, und diese Nachricht wird ausgegeben, wenn sie erfolgreich ist.

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

5. Das Telefon sendet jetzt eine Anforderung zur Authentifizierung des Zertifikats.

   ```
   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. Die Antwort "0" vom TVS bedeutet, dass die Authentifizierung erfolgreich war.

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

7. Diese Meldung wird angezeigt, und dann wird die Antwort angezeigt.

```
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>
```

Der Zertifikatauthentifizierungsprozess ähnelt dem unter Telefonkontakte - Vertrauensverifizierungsdienst für unbekanntes Zertifikat beschriebenen Prozess.

Aus den telefonisch erfassten Paketerfassungen (PCAPs) können Sie die TVS-Kommunikation mithilfe dieses Filters überprüfen - tcp.port==2445.

Bei gleichzeitigen TVS-Protokollen:

1. Überprüfen Sie die Rückverfolgungen hinsichtlich des TLS-Handshakes (Transport Layer Security).
2. Überprüfen Sie anschließend den eingehenden 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. Der TVS ruft die Details zum Aussteller ab.

```
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. Der TVS verifiziert das Zertifikat.

```
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. Der TVS sendet die Antwort an das Telefon.

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

Die Telefondienst-URL ist auf "Application:Cisco/Corporate Directory" (Anwendung:Cisco/Firmenverzeichnis) festgelegt, und das Telefon verwendet HTTP.

> **Hinweis**: Anstatt eine frühere Telefon-Firmware-Version zu verwenden, wurden der Service und die sichere Service-URL als feste Codes für die HTTP-URL festgelegt. Die gleiche Ereignissequenz tritt jedoch auch in der Telefon-Firmware auf, die standardmäßig HTTP verwendet.

Die Konfigurationsdatei des Telefons hat die richtige URL.

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

Aus den Telefonkonsolenprotokollen können Sie diese Schritte überprüfen.

```
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
```

Bei der Paketerfassung werden eine HTTP GET-Anforderung und eine erfolgreiche ANTWORT angezeigt. Dies ist das PCAP vom CUCM:

Fehlerbehebung

Bevor Sie die Fehlerbehebung durchführen, sollten Sie die Details zu dem zuvor aufgeführten Problem ermitteln:

Bei Bedarf zu erfassende Protokolle

- Simultane Paketerfassung vom IP-Telefon und vom CUCM-Server (dem Server, der sich zuerst in seiner CM-Gruppe befindet, an den die HTTP(S)-Anforderung gesendet werden würde).
- Konsolenprotokolle des IP-Telefons
- Cisco TVS-Protokolle (detailliert).

  Wenn Sie die TVS-Protokolle auf "detailliert" festlegen, muss der Dienst neu gestartet werden, damit die Änderungen der Ablaufverfolgungsebene stattfinden. Unter der Cisco Bug-ID CSCuq22327 finden Sie Informationen zur Erweiterung, um anzuzeigen, dass ein Neustart des Service erforderlich ist, wenn die Protokollstufen geändert werden.

Gehen Sie wie folgt vor, um das Problem zu isolieren:

Schritt 1:

Erstellen Sie einen Testservice mit folgenden 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
```

Jetzt abonnieren Sie diesen Service für eines der betroffenen Telefone:

a. Gehen Sie zur Seite für die Gerätekonfiguration.
b. Wählen Sie **Services abonnieren/abbestellen** unter Zugehörige Links.
c. **Abonnieren** Sie den von Ihnen erstellten Testservice.
d. **Speichern**, Konfiguration übernehmen und Telefon zurücksetzen
    i. Unabhängig von der FW-Version des Telefons, die bestimmt, ob die HTTP- oder HTTPS-URL verwendet werden soll, müssen Sie die Verwendung der HTTP-URL erzwingen.
    ii. Greifen Sie auf das Firmenverzeichnis am Telefon zu.
    iii. Wenn es nicht funktioniert, sammeln Sie die oben genannten Protokolle, vergleichen Sie sie mit dem im Abschnitt "Arbeitsszenario" genannten Arbeitsszenario, und geben Sie an, wo die Abweichung liegt.
    iv. Wenn es funktioniert, haben Sie zumindest bestätigt, dass es aus Sicht des CUCM-IP-Telefondienstes keine Probleme gibt.
    v. In dieser Phase ist das Problem am wahrscheinlichsten bei Telefonen, die die HTTPS-URL verwenden.
    vi. Wählen Sie nun ein Telefon aus, das nicht funktioniert, und fahren Sie mit dem nächsten Schritt fort.

Wenn diese Änderung durchgeführt wird, müssen Sie entscheiden, ob es in Ordnung ist, die Konfiguration mit der Anforderung/Antwort des Unternehmensverzeichnisses zu belassen, die über HTTP statt HTTPS funktioniert. Die HTTPS-Kommunikation funktioniert aus einem der im Folgenden genannten Gründe nicht.

Schritt 2:

Sammeln Sie die oben genannten Protokolle, und vergleichen Sie sie mit dem im Abschnitt "Arbeitsszenario" genannten Arbeitsszenario. Ermitteln Sie, wo die Abweichung liegt.

Dabei könnte es sich um eines der folgenden Themen handeln:

a. Das Telefon kann keine Verbindung zum TVS-Server herstellen.
    i. Überprüfen Sie im PCAPS die Kommunikation an Port 2445.
    ii. Stellen Sie sicher, dass keines der Netzwerkgeräte im Pfad diesen Port blockiert.
b. Das Telefon kontaktiert den TVS-Server, aber der TLS-Handshake schlägt fehl.

Die folgenden Zeilen können in den Telefonkonsolenprotokollen ausgegeben werden:

```
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>
```

Weitere Informationen finden Sie unter Cisco Bug-ID CSCua65618.

c. Das Telefon kontaktiert die TVS-Server, und der TLS-Handshake ist erfolgreich, aber der TVS kann den Unterzeichner des Zertifikats, das das Telefon authentifizieren soll, nicht überprüfen.

Ausschnitte aus TVS-Protokollen werden hier aufgelistet:

Das Telefon kontaktiert den 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
```

Der TVS ruft den Namen des Ausstellers ab.

```
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
```

Er sucht nach dem Zertifikat, kann es jedoch nicht finden.

```
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-Datenverkehr wird im Netzwerk blockiert/blockiert.

   Rufen Sie gleichzeitig PCAPs vom Telefon und vom CUCM-Server ab, um die Kommunikation zu überprüfen.

Andere Szenarien, in denen das Problem "Host nicht gefunden" auftritt

1. Der CUCM-Server wird durch den Hostnamen und die Probleme bei der Namensauflösung definiert.
2. Die TVS-Serverliste ist auf dem Telefon leer, wenn die Datei "xmldefault.cnf.xml" heruntergeladen wird. (In Version 8.6.2 enthält die Standardkonfigurationsdatei aufgrund der Cisco Bug-ID CSCti64589 keinen TVS-Eintrag.)
3. Das Telefon kann den TVS-Eintrag in der Konfigurationsdatei nicht verwenden, da es die Datei "xmldefault.cnf.xml" heruntergeladen hat. Siehe Cisco Bug-ID CSCuq3297 - Phone, um TVS-Informationen aus der Standardkonfigurationsdatei zu analysieren.
4. Das Firmenverzeichnis funktioniert nach einem CUCM-Upgrade nicht, da die Telefon-Firmware auf eine neuere Version aktualisiert wird, die das Verhalten der Verwendung von HTTPS standardmäßig ändert.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.