Probleemoplossing Corporate Directory "a;host niet gevonden" problemen

Inhoud

Inleiding

Dit document beschrijft hoe u problemen met "Host Not Found" kunt oplossen in de functie Corporate Directory van IP-telefoons.

Achtergrondinformatie

Belangrijke informatie over dit document is:

- De Corporate Directory is een door Cisco verstrekte standaard IP-telefoonservice die automatisch wordt geïnstalleerd met Cisco Unified Communications Manager (CUCM).
- Informatie over telefoonabonnement op de verschillende telefoondiensten wordt opgeslagen in de database in de telecasterservice, telecasterservice parameter, telecastersubscribedparameter, telecastersubscribedservice tabellen.
- Op de telefoon, wanneer u de optie Corporate Directory selecteert, verstuurt de telefoon een HTTP of HTTPS verzoek naar een van de CUCM servers en wordt teruggegeven als een XML object als een HTTP(S) respons. Als HTTPS, dan hangt dit ook af van de telefoon die met de dienst TVS verbindt om het certificaat voor HTTPS te verifiëren. Op telefoons die midlets ondersteunen, kan dit worden geïmplementeerd in de phone midlet en worden beïnvloed door Services Provisioning setting.

Belangrijke informatie

- Verklaar als het probleem zich voordoet wanneer u directory's of Corporate Directory opent.
- Wat is het veld Service UR ingesteld onder de Corporate Directory service?
  - Als de URL is ingesteld op Application:Cisco/CorporateDirectory en vervolgens is gebaseerd op de firmware-versie van de telefoon, doet de telefoon een HTTP- of HTTPS-verzoek.
  - Telefoons die firmware versie 9.3.3 en hoger gebruiken, dienen standaard een HTTPS-verzoek in.
- Wanneer de service-URL is ingesteld op Application:Cisco/Corporate Directory, verstuurt de telefoon het HTTP(S)-verzoek naar de server die als eerste in de CallManager (CM)-groep zit.
- Identificeer de netwerktopologie tussen de telefoon en de server waarnaar het HTTP(S)-verzoek wordt verzonden.
- Besteed aandacht aan firewalls, WAN-optimalisators., enzovoort op het pad dat HTTP(S)-verkeer kan laten vallen/hinderen.
- Als HTTPS wordt gebruikt, zorg dan voor de verbinding tussen de telefoon en de TVS-server, en dat de TVS functioneert.

Werkscenario

In dit scenario wordt de telefoonservice-URL ingesteld op Application:Cisco/Corporate Directory en de telefoon gebruikt HTTPS.

Dit voorbeeld toont het configuratiebestand van de telefoon met de juiste URL.

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

Van de logboeken van de telefoonconsole, kunt u deze stappen verifiëren.

1. De telefoon gebruikt de 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. Het Tomcat-webcertificaat dat aan de telefoon wordt getoond vanaf de server van Directories is niet beschikbaar op de telefoon. Vandaar dat de telefoon probeert om het certificaat te verifiëren via de 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. De telefoon kijkt eerst in het TVS cache, en als hij niet gevonden wordt, neemt hij contact op met de 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. Aangezien de verbinding met het TVS ook veilig is, is een certificaat-authenticatie voltooid en wordt dit bericht afgedrukt als het succesvol is.

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

5. De telefoon stuurt nu een verzoek om het certificaat te verifiëren.

   ```
   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. De respons "0" van de TVS betekent dat de authenticatie is geslaagd.

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

7. Dit bericht wordt weergegeven en je ziet het antwoord.

```
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>
```

Het proces voor de verificatie van certificaten is vergelijkbaar met wat wordt besproken in de Service voor de verificatie van contactgegevens van de telefoon voor onbekend certificaat.

Van de pakketopnamen (PCAPâ€™s) die aan het telefoonuiteinde worden verzameld, kunt u de communicatie van de TVS verifiëren met het gebruik van dit filter - tcp.port==2445.

In de gelijktijdige TVS-logboeken:

1. Bekijk de overtrekken met betrekking tot het TLS-handschudden (Transport Layer Security).
2. Daarna, herzie de inkomende hexadecimale 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. De TVS haalt de emittentengegevens op.

```
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. De TV verifieert het certificaat.

```
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. De TVS stuurt het antwoord naar de telefoon.

```
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 ingesteld op Application:Cisco/Corporate Directory en de telefoon gebruikt HTTP

> **Opmerking**: in plaats van het gebruik van een eerdere versie van de telefoon firmware, de service en beveiligde service-URL waren hard-gecodeerd naar de HTTP-URL. Echter, dezelfde volgorde van gebeurtenissen wordt gezien in de telefoon firmware die standaard gebruik maakt van HTTP.

Het configuratiebestand van de telefoon heeft de juiste URL.

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

Van de logboeken van de telefoonconsole, kunt u deze stappen verifiëren.

```
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
```

Van het pakket vangt, ziet u een HTTP GET verzoek, en een succesvolle REACTIE. Dit is de PCAP van CUCM:

Problemen oplossen

Alvorens u problemen oplost, verzamel de details van het probleem dat eerder wordt vermeld:

Logbestanden te verzamelen, indien vereist

- Het gelijktijdige pakket vangt van de IP telefoon, en van de server CUCM (de server die eerst in het is Cm groep is waar het HTTP(S) verzoek zou worden verzonden naar).
- Logboeken van IP-telefoonconsole.
- Cisco TVS-logbestanden (gedetailleerd).

  Wanneer u de TVS-logbestanden op gedetailleerd instelt, moet de service opnieuw worden opgestart om de wijzigingen op overtredingsniveau te laten plaatsvinden. Zie Cisco bug-id CSCuq2327 voor de verbetering om te melden dat een opnieuw opstarten van de service vereist is wanneer de logniveaus worden gewijzigd.

Voltooi de volgende stappen om het probleem te isoleren:

Stap 1.

Maak een testservice met deze gegevens:

```
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
```

Abonneer u nu op deze service voor een van de getroffen telefoons:

a. Ga naar de pagina met de apparaatconfiguratie.
b. Kies **Abonneren/Abonnement opzeggen** onder Verwante links.
c. **Abonneer u** op de testservice die u hebt gemaakt.
d. **Sla op**, pas de configuratie toe en stel de telefoon opnieuw in.
    i. Wat je hebt gedaan, ongeacht de FW-versie van de telefoon, die bepaalt of je de HTTP- of HTTPS-URL wilt gebruiken, is het dwingen om de HTTP-URL te gebruiken.
    ii. Ga telefonisch naar de Corporate Directory-service.
    iii. Als het niet werkt, verzamel dan de logbestanden die eerder zijn genoemd, en vergelijk ze met het werkscenario dat wordt genoemd onder het werkscenario sectie, en identificeer waar de afwijking is.
    iv. Als het werkt, dan hebt u ten minste bevestigd dat vanuit het perspectief van de CUCM IP-telefoon er geen problemen zijn.
    v. In dit stadium is het probleem waarschijnlijk met de telefoons die de HTTPS URL gebruiken.
    vi. Kies nu een telefoon die niet werkt en ga door naar de volgende stap.

Wanneer het met deze verandering werkt, moet u beslissen of het OK is om de configuratie te verlaten met de corporate directory aanvraag/antwoord die werkt via HTTP in plaats van HTTPS. HTTPS-communicatie werkt niet vanwege een van de volgende redenen.

Stap 2.

Verzamel de logbestanden die eerder zijn genoemd, vergelijk ze met het werkscenario dat wordt genoemd in het gedeelte Werkend scenario, en identificeer waar de afwijking is.

Het zou een van de volgende kwesties kunnen zijn:

a. De telefoon kan geen contact opnemen met de TVS-server.
    i. Controleer in de CAPS de communicatie op poort 2445.
    ii. Zorg ervoor dat geen van de netwerkapparaten in het pad deze poort blokkeert.
b. De telefoon neemt contact op met de TVS server, maar de TLS handdruk mislukt.

Deze lijnen kunnen in de logboeken van de telefoonconsole worden afgedrukt:

```
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>
```

Zie Cisco bug-id CSC65618 voor meer informatie.

c. De telefoon neemt contact op met de TVS-servers, en de TLS handdruk is succesvol, maar de TVS is niet in staat om de ondertekenaar van het certificaat te verifiëren dat de telefoon gevraagd heeft om te verifiëren.

Hier worden fragmenten uit TVS-logs vermeld:

De telefoon neemt contact op met de TV.

```
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
```

De TVS krijgt de naam van de emittent.

```
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
```

Het kijkt omhoog het certificaat, maar kan het niet vinden.

```
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-verkeer wordt ergens in het netwerk geblokkeerd/gedropt.

   Ontvang gelijktijdige PCAP's van de telefoon en de CUCM-server om de communicatie te verifiëren.

Andere scenario's wanneer het probleem "Host Not Found" optreedt

1. De CUCM-server wordt gedefinieerd door de hostnaam, samen met problemen in de naamresolutie.
2. De TVS serverlijst is leeg op de telefoon wanneer het het bestand xmldefault.cnf.xml downloadt. (In versie 8.6.2 bevat het standaardconfiguratiebestand de TVS-ingang niet vanwege Cisco bug-id CSC64589.)
3. De telefoon kan de TVS-ingang in het configuratiebestand niet gebruiken omdat het het bestand xmldefault.cnf.xml heeft gedownload. Zie Cisco bug-id CSCuq3297 - Telefoon om TVS-informatie te parseren uit het standaardconfiguratiebestand.
4. De Corporate Directory werkt niet na een CUCM upgrade omdat de telefoon firmware upgrades naar een latere versie die uiteindelijk het gedrag van het gebruik van HTTPS door standaard verandert.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.