Résoudre les problèmes liés au répertoire d'entreprise " ; Hôte introuvable" ;

Table des matières

Introduction

Ce document décrit comment dépanner les problèmes « Hôte introuvable » dans la fonctionnalité de répertoire d'entreprise des téléphones IP.

Informations générales

Les informations importantes relatives à ce document sont les suivantes :

- Le répertoire d'entreprise est un service de téléphone IP par défaut fourni par Cisco qui s'installe automatiquement avec Cisco Unified Communications Manager (CUCM).
- Des informations concernant l'abonnement téléphonique aux divers services téléphoniques sont stockées dans la base de données dans les tables telecasterservice, telecasterserviceparameter, telecastersubscribedparameter, telecastersubscribedservice.
- Sur le téléphone, lorsque vous sélectionnez l'option Répertoire d'entreprise, le téléphone envoie une requête HTTP ou HTTPS à l'un des serveurs CUCM et est renvoyé en tant qu'objet XML sous forme de réponse HTTP(S). Si HTTPS, cela dépend également de la connexion du téléphone au service TVS pour vérifier le certificat pour HTTPS. Sur les téléphones qui prennent en charge les midlets, cela peut être mis en oeuvre dans le midlet du téléphone et affecté par le paramètre Services Provisioning.

Informations importantes

- Précisez si le problème se produit lorsque vous accédez aux répertoires ou au répertoire d'entreprise.
- Sur quoi le champ Service UR est-il défini dans le service d'annuaire d'entreprise ?
    - Si l'URL est définie sur Application:Cisco/CorporateDirectory, en fonction de la version du micrologiciel du téléphone, celui-ci émet une requête HTTP ou HTTPS.

    - Les téléphones qui utilisent le microprogramme version 9.3.3 et ultérieure par défaut effectuent une requête HTTPS.
- Lorsque l'URL du service est définie sur Application:Cisco/CorporateDirectory, le téléphone envoie la requête HTTP(S) au serveur qui se trouve en premier dans son groupe CallManager (CM).
- Identifiez la topologie du réseau entre le téléphone et le serveur auquel la requête HTTP(S) est envoyée.
- Faites attention aux pare-feu, aux optimiseurs WAN, etc., dans le chemin qui peut interrompre/entraver le trafic HTTP(S).
- Si le protocole HTTPS est utilisé, vérifiez la connectivité entre le téléphone et le serveur TVS et assurez-vous que le serveur TVS fonctionne.

Scénario de travail

Dans ce scénario, l'URL du service téléphonique est définie sur Application:Cisco/CorporateDirectory et le téléphone utilise HTTPS.

Cet exemple montre comment afficher le fichier de configuration du téléphone avec l'URL correcte.

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

Vous pouvez vérifier ces étapes à partir des journaux de la console téléphonique.

1. Le téléphone utilise l'URL HTTPS.

   ```
   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. Le certificat Web Tomcat présenté au téléphone à partir du serveur Répertoires n'est pas disponible sur le téléphone. Par conséquent, le téléphone tente d'authentifier le certificat via le service de vérification de la confiance (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. Le téléphone recherche d'abord dans le cache TVS et, s'il ne le trouve pas, il contacte le serveur TVS.

```
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. Comme la connexion au TVS est également sécurisée, une authentification de certificat est effectuée et ce message est imprimé s'il aboutit.

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

5. Le téléphone envoie maintenant une demande d'authentification du certificat.

```
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. La réponse « 0 » du TVS signifie que l'authentification a réussi.

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

7. Ce message s'affiche, puis vous voyez la réponse.

```
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>
```

Le processus d'authentification du certificat est similaire à ce qui est abordé dans le Service de vérification de l'approbation des contacts téléphoniques pour Certificat inconnu.

À partir des captures de paquets (PCAP) collectées à l'extrémité du téléphone, vous pouvez

vérifier la communication TVS à l'aide de ce filtre - tcp.port==2445.

Dans les journaux TVS simultanés :

1. Examiner les traces en ce qui concerne la poignée de main TLS (Transport Layer Security).
2. Ensuite, examinez le vidage hexadécimal entrant.

```
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. Le TVS récupère les détails de l'émetteur.

```
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. Le TVS vérifie le certificat.

```
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. Le TVS envoie la réponse au téléphone.

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

L'URL du service téléphonique est définie sur

Application:Cisco/CorporateDirectory et le téléphone utilise HTTP

> Remarque : au lieu d'utiliser une version antérieure du micrologiciel du téléphone, les URL de service et de service sécurisé ont été codées en dur sur l'URL HTTP. Cependant, la même séquence d'événements est visible dans le micrologiciel du téléphone qui utilise HTTP par défaut.

L'URL du fichier de configuration du téléphone est correcte.

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

Vous pouvez vérifier ces étapes à partir des journaux de la console téléphonique.

```
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
```

À partir des captures de paquets, vous voyez une requête HTTP GET et une RÉPONSE réussie. Voici le PCAP de CUCM :

Dépannage

Avant de procéder au dépannage, collectez les détails du problème répertorié précédemment :

Journaux à collecter, si nécessaire

- Captures simultanées de paquets à partir du téléphone IP et du serveur CUCM (le serveur qui est le premier dans son groupe CM où la requête HTTP(S) serait envoyée).
- Journaux de console du téléphone IP.
- Journaux Cisco TVS (détaillés).

  Lorsque vous définissez les journaux TVS sur détaillé, le service doit être redémarré pour que les modifications du niveau de suivi aient lieu. Reportez-vous à l'ID de bogue Cisco CSCuq22327 pour l'amélioration afin de notifier qu'un redémarrage du service est nécessaire lorsque les niveaux de journalisation sont modifiés.

Complétez ces étapes afin d'isoler le problème :

Étape 1.

Créez un service de test avec les détails suivants :

```
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
```

À présent, abonnez ce service à l'un des téléphones concernés :

a. Accédez à la page de configuration du périphérique.
b. Choisissez Subscribe/Unsubscribe Services sous Related Links.
c. Abonnez le service de test que vous avez créé.
d. Enregistrez, appliquez la configuration et réinitialisez le téléphone.
    i. Ce que vous avez fait, quelle que soit la version du logiciel du téléphone, qui détermine si l'URL HTTP ou HTTPS doit être utilisée, est de la forcer à utiliser l'URL HTTP.
    ii. Accédez au service d'annuaire d'entreprise sur le téléphone.
    iii. Si cela ne fonctionne pas, collectez les journaux mentionnés précédemment et comparez-les au scénario de travail mentionné dans la section Scénario de travail,

puis identifiez l'emplacement de l'écart.

iv. Si cela fonctionne, alors vous avez au moins confirmé que du point de vue du service de téléphone IP CUCM il n'y a pas de problèmes.

v. À ce stade, le problème se situe très probablement au niveau des téléphones qui utilisent l'URL HTTPS.

vi. Maintenant, choisissez un téléphone qui ne fonctionne pas, et passez à l'étape suivante.

Lorsque cette modification est prise en compte, vous devez décider s'il est acceptable de laisser la configuration avec la requête/réponse de répertoire d'entreprise qui fonctionne sur HTTP au lieu de HTTPS. La communication HTTPS ne fonctionne pas pour l'une des raisons décrites ci-dessous.

Étape 2.

Collectez les journaux mentionnés précédemment et comparez-les au scénario de travail mentionné dans la section Scénario de travail, puis identifiez l'emplacement de l'écart.

Il pourrait s'agir de l'une des questions suivantes :

a. Le téléphone ne parvient pas à contacter le serveur TVS.
   i. Dans le PCAPS, vérifiez la communication sur le port 2445.
   ii. Assurez-vous qu'aucun des périphériques réseau du chemin ne bloque ce port.

b. Le téléphone contacte le serveur TVS, mais la connexion TLS échoue.

Ces lignes peuvent être imprimées dans les journaux de la console téléphonique :

```
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>
```

Consultez l'ID de bogue Cisco CSCua65618 pour plus d'informations.

c. Le téléphone contacte les serveurs TVS et la connexion TLS a réussi, mais le TVS ne peut pas vérifier le signataire du certificat que le téléphone a demandé à authentifier.

Les extraits des journaux TVS sont répertoriés ici :

Le téléphone contacte le 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
```

Le TVS obtient le nom de l'émetteur.

```
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
```

Il recherche le certificat, mais ne le trouve pas.

```
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. Le trafic HTTPS est bloqué/abandonné quelque part sur le réseau.

Obtenez des PCAP simultanés du téléphone et du serveur CUCM afin de vérifier la communication.

Autres scénarios dans lesquels le problème « Hôte introuvable » se produit

1. Le serveur CUCM est défini par le nom d'hôte et les problèmes de résolution de noms.
2. La liste des serveurs TVS est vide sur le téléphone lorsqu'il télécharge le fichier

xmldefault.cnf.xml. (Dans la version 8.6.2, le fichier de configuration par défaut ne contient pas l'entrée TVS en raison du bogue Cisco ayant l'ID CSCti64589.)

3. Le téléphone ne peut pas utiliser l'entrée TVS dans le fichier de configuration, car il a téléchargé le fichier xmldefault.cnf.xml. Reportez-vous à l'ID de bogue Cisco CSCuq3297 - Phone pour analyser les informations TVS du fichier de configuration par défaut.
4. Le répertoire d'entreprise ne fonctionne pas après une mise à niveau de CUCM car le microprogramme du téléphone est mis à niveau vers une version ultérieure, ce qui modifie le comportement de l'utilisation de HTTPS par défaut.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.