

Risoluzione dei problemi relativi alla directory aziendale "Host non trovato"

Sommario

[Introduzione](#)

[Premesse](#)

[Informazioni importanti](#)

[Scenario di lavoro](#)

[L'URL del servizio telefonico è impostato su Application:Cisco/CorporateDirectory e il telefono utilizza HTTP](#)

[Risoluzione dei problemi](#)

[Altri scenari quando si verifica il problema "Host non trovato"](#)

Introduzione

Questo documento descrive come risolvere i problemi di "Host non trovato" nella funzionalità Directory aziendale dei telefoni IP.

Premesse

Informazioni importanti relative al presente documento:

- La directory aziendale è un servizio telefonico IP predefinito fornito da Cisco che si installa automaticamente con Cisco Unified Communications Manager (CUCM).
- Le informazioni sull'abbonamento telefonico ai vari servizi telefonici sono memorizzate nel database nelle tabelle telecasterservice, telecasterserviceparameter, telecastersubscribedparameter, telecastersubscribedservice.
- Al telefono, quando si seleziona l'opzione Directory aziendale, il telefono invia una richiesta HTTP o HTTPS a uno dei server CUCM e viene restituito come oggetto XML come risposta HTTP(S). Se si utilizza HTTPS, anche questo dipende dal telefono che si connette al servizio TVS per verificare il certificato per HTTPS. Sui telefoni che supportano i midlet, questa impostazione può essere implementata nel midlet telefonico e può essere influenzata dall'impostazione di [provisioning dei servizi](#).

Informazioni importanti

- Chiarire se il problema si verifica quando si accede alle directory o alla directory aziendale.
- In che modo è impostato il campo URL servizio nel servizio directory aziendale?
 - Se l'URL è impostato su Application:Cisco/CorporateDirectory, in base alla versione firmware del telefono, il telefono effettua una richiesta HTTP o HTTPS.
 - Per impostazione predefinita, i telefoni che utilizzano il firmware versione 9.3.3 e successive effettuano una richiesta HTTPS.
- Quando l'URL del servizio è impostato su Application:Cisco/CorporateDirectory, il telefono invia la richiesta HTTP(S) al server che si trova per primo nel gruppo CallManager (CM).
- Identificare la topologia di rete tra il telefono e il server a cui viene inviata la richiesta HTTP(S).
- Prestare attenzione ai firewall, agli ottimizzatori WAN e così via nel percorso che può causare il calo/blocco del traffico HTTP(S).
- Se HTTPS è in uso, verificare la connettività tra il telefono e il server TVS e che TVS funzioni.

Scenario di lavoro

In questo scenario, l'URL del servizio telefonico è impostato su Application:Cisco/CorporateDirectory e il telefono utilizza HTTPS.

In questo esempio viene mostrato il file di configurazione del telefono con l'URL corretto.

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

Dai registri della console telefonica è possibile verificare questi passaggi.

1. Il telefono usa 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. Il certificato Web Tomcat presentato al telefono dal server di elenchi in linea non è disponibile sul telefono. Pertanto, il telefono tenta di autenticare il certificato tramite il servizio di verifica dell'attendibilità (TVS, Trust Verification Service).

```
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. Il telefono cerca prima nella cache TVS e, se non viene trovato, contatta il server 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. Poiché anche la connessione al televisore è sicura, viene completata l'autenticazione del certificato e questo messaggio viene stampato se la connessione ha esito positivo.

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

5. Il telefono ora invia una richiesta per autenticare il certificato.

```
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 risposta "0" del TVS indica che l'autenticazione è riuscita.

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

7. Verrà visualizzato questo messaggio e verrà visualizzata la risposta.

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

Il processo di autenticazione dei certificati è simile a quello descritto in [Servizio di verifica dell'attendibilità dei contatti telefonici per i certificati sconosciuti](#).

Dalle acquisizioni dei pacchetti (PCAP) raccolte al terminale del telefono, è possibile verificare la comunicazione con la TV usando questo filtro - tcp.port==2445.

Nei registri TVS simultanei:

1. Esaminare le tracce relative al tremolio della mano TLS (Transport Layer Security).
2. Esaminare quindi il dump esadecimale in ingresso.

```
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. Il televisore recupera i dettagli dell'emittente.

```
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=Bllore;ST=KN;C=IN and Length: 43
04:04:15.272 |<--debug
```

4. Il televisore verifica il certificato.

```
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=Bllore;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. Il televisore invia la risposta al telefono.

```
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 del servizio telefonico è impostato su Application: Cisco/CorporateDirectory e il telefono utilizza HTTP

Nota: anziché utilizzare una versione precedente del firmware del telefono, l'URL del servizio e del servizio sicuro è stato hardcoded sull'URL HTTP. Tuttavia, la stessa sequenza di eventi è presente nel firmware del telefono che utilizza HTTP per impostazione predefinita.

L'URL del file di configurazione del telefono è corretto.

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

Dai registri della console telefonica è possibile verificare questi passaggi.

```
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
```

Dalle acquisizioni del pacchetto vengono visualizzate una richiesta HTTP GET e una RISPOSTA riuscita. Questo è il PCAP di CUCM:

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=SEP0021CC699172 HTTP/1.1
89	2015-01-23 09:04:10.368677000	10.106.111.99	64.103.236.206	HTTP/XML	1173	HTTP/1.1 200 OK

Risoluzione dei problemi

Prima di procedere alla risoluzione del problema, raccogliere i dettagli relativi al problema elencato in precedenza:

Log da raccogliere, se necessario

- Acquisizione simultanea dei pacchetti dal telefono IP e dal server CUCM (il primo server del gruppo CM a cui inviare la richiesta HTTP(S)).
- Registri della console telefonica IP.
- Registri TVS Cisco (informazioni dettagliate).

Quando si impostano i registri TVS in modo dettagliato, è necessario riavviare il servizio per rendere effettive le modifiche al livello di traccia. Per informazioni sul miglioramento, vedere l'ID bug Cisco [CSCuq22327](#) per notificare che è necessario riavviare il servizio quando vengono modificati i livelli di log.

Per isolare il problema, completare i seguenti passaggi:

Passaggio 1.

Creare un servizio di test con i seguenti dettagli:

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

Ora abbonati a uno dei telefoni interessati:

- a. Andare alla pagina di configurazione del dispositivo.
- b. Scegliere **Subscribe/Unsubscribe Services** in Collegamenti correlati.
- c. **Sottoscrivere** il servizio di test creato.
- d. **Salva**, applica la configurazione e ripristina il telefono.
 - i. Ciò che è stato fatto, a prescindere dalla versione FW del telefono, che determina se utilizzare l'URL HTTP o HTTPS, è forzarlo a utilizzare l'URL HTTP.
 - ii. Accedi al servizio Elenco utenti non autorizzati tramite telefono.
 - iii. Se l'operazione non riesce, raccogliere i registri menzionati in precedenza e confrontarli con lo scenario di lavoro indicato nella sezione Scenario di lavoro e identificare la posizione della deviazione.
 - iv. Se funziona, allora avete almeno confermato che dal punto di vista del servizio CUCM IP Phone non ci sono problemi.
 - v. In questa fase, il problema è più probabile con i telefoni che usano l'URL HTTPS.
 - vi. Scegliere un telefono che non funziona e procedere al passaggio successivo.

Quando la modifica viene apportata, è necessario decidere se è possibile lasciare la configurazione con la richiesta/risposta della directory aziendale che funziona su HTTP anziché su HTTPS. La comunicazione HTTPS non funziona a causa di uno dei motivi illustrati di seguito.

Passaggio 2.

Raccogliere i registri menzionati in precedenza e confrontarli con lo scenario di lavoro indicato nella sezione Scenario di lavoro e individuare la deviazione.

Potrebbe trattarsi di uno dei problemi seguenti:

- a. Il telefono non è in grado di contattare il server TVS.
 - i. Nel PCAPS, verificare la comunicazione sulla porta 2445.
 - ii. Verificare che nessuna delle periferiche di rete nel percorso blocchi questa porta.
- b. Il telefono contatta il server TVS, ma l'handshake TLS non riesce.

Queste righe possono essere stampate nei registri della console telefonica:

```
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>
```

Per ulteriori informazioni, vedere l'ID bug Cisco [CSCua65618](#).

- c. Il telefono contatta i server TVS e l'handshake TLS ha esito positivo, ma il TVS non è in grado di verificare il firmatario del certificato richiesto dal telefono per l'autenticazione.

Di seguito sono elencati i frammenti dei registri TVS:

Il telefono contatta il televisore.

```
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
```

Il TVS ottiene il nome dell'emittente.

```
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 certificato viene cercato, ma non trovato.

```
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. Il traffico HTTPS è bloccato/interrotto in un punto qualsiasi della rete.

Ottenere PCAP simultanei dal telefono e dal server CUCM per verificare la comunicazione.

Altri scenari quando si verifica il problema "Host non trovato"

1. Il server CUCM è definito dal nome host insieme ai problemi nella risoluzione dei nomi.
2. L'elenco dei server TVS è vuoto nel telefono quando scarica il file xmldefault.cnf.xml. (Nella versione 8.6.2, il file di configurazione predefinito non contiene la voce TVS a causa dell'ID bug Cisco [CSCti64589](#).)
3. Il telefono non riesce a usare la voce TVS nel file di configurazione perché ha scaricato il file xmldefault.cnf.xml. Vedere l'ID bug Cisco [CSCuq3297](#) - Telefono per analizzare le informazioni sulle TV dal file di configurazione predefinito.
4. La directory aziendale non funziona dopo un aggiornamento CUCM perché il firmware del telefono viene aggiornato a una versione successiva che alla fine modifica il comportamento dell'uso di HTTPS per impostazione predefinita.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).