Solucionar problemas de directorio corporativo "Host no encontrado"

Contenido

Introducción

Este documento describe cómo resolver problemas de "Host no encontrado" en la función Corporate Directory de los teléfonos IP.

Antecedentes

La información importante relacionada con este documento es:

- El directorio corporativo es un servicio de teléfono IP predeterminado proporcionado por Cisco que se instala automáticamente con Cisco Unified Communications Manager (CUCM).
- La información sobre la suscripción telefónica a los distintos servicios telefónicos se almacena en la base de datos de las tablas telecasterservice, telecasterserviceparameter, telecastersubscribedparameter y telecastersubscribedservice.
- En el teléfono, al seleccionar la opción Directorio corporativo, el teléfono envía una solicitud HTTP o HTTPS a uno de los servidores de CUCM y se devuelve como un objeto XML como una respuesta HTTP(S). Si es HTTPS, esto también depende de que el teléfono se conecte al servicio TVS para verificar el certificado para HTTPS. En los teléfonos que admiten midlets, esto se puede implementar en el midlet del teléfono y se verá afectado por la configuración de aprovisionamiento de servicios.

Información importante

- Aclare si el problema se produce al acceder a Directorios o Directorio corporativo.
- ¿Cuál es el valor del campo URL de servicio establecido en el servicio de directorio corporativo?
  - Si la URL se establece en Application:Cisco/CorporateDirectory y, a continuación, en función de la versión de firmware del teléfono, éste realiza una solicitud HTTP o HTTPS.
  - Los teléfonos que utilizan la versión 9.3.3 y posteriores del firmware realizan una solicitud HTTPS de forma predeterminada.
- Cuando la URL del servicio se establece en Application:Cisco/CorporateDirectory, el teléfono envía la solicitud HTTP(S) al servidor que es el primero de su grupo CallManager (CM).
- Identifique la topología de red entre el teléfono y el servidor al que se envía la solicitud HTTP(S).
- Preste atención a los firewalls, los optimizadores de WAN, etc. en la ruta que puede interrumpir o interrumpir el tráfico HTTP(S).
- Si HTTPS está en uso, asegúrese de que haya conectividad entre el teléfono y el servidor de TVS y de que TVS funciona.

Escenario de trabajo

En esta situación, la URL del servicio telefónico se establece en Application:Cisco/CorporateDirectory y el teléfono utiliza HTTPS.

En este ejemplo se muestra el archivo de configuración del teléfono con la dirección URL correcta.

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

En los registros de la consola del teléfono, puede comprobar estos pasos.

1. El teléfono utiliza la 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. El certificado web Tomcat presentado al teléfono desde el servidor Directories no está disponible en el teléfono. Por lo tanto, el teléfono intenta autenticar el certificado a través del Servicio de verificación de confianza (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. El teléfono busca primero en la caché de TVS y, si no lo encuentra, se pone en contacto con el servidor de 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. Dado que la conexión al TVS también es segura, se completa una autenticación de certificado y este mensaje se imprime si es exitosa.

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

5. El teléfono ahora envía una solicitud para autenticar el certificado.

   ```
   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 respuesta "0" del TVS significa que la autenticación fue exitosa.

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

7. Se muestra este mensaje y, a continuación, se muestra la respuesta.

```
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>
```

El proceso de autenticación de certificados es similar a lo que se describe en Servicio de verificación de confianza de contactos del teléfono para certificado desconocido.

A partir de las capturas de paquetes (PCAP) recopiladas en el extremo del teléfono, puede verificar la comunicación de TVS mediante este filtro: tcp.port==2445.

En los registros de TV simultáneos:

1. Revise los seguimientos relacionados con el intercambio de señales de seguridad de la capa de transporte (TLS).
2. A continuación, revise el volcado hexadecimal entrante.

```
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. El TVS recupera los detalles del emisor.

```
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. El TVS verifica el certificado.

```
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. El TVS envía la respuesta al teléfono.

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

La URL del servicio telefónico se establece en Aplicación:Cisco/CorporateDirectory y el teléfono utiliza HTTP

> **Nota**: en lugar de utilizar una versión anterior del firmware del teléfono, el servicio y la URL de servicio seguro se codificaron de forma rígida en la URL HTTP. Sin embargo, la misma secuencia de eventos se ve en el firmware del teléfono que hace uso de HTTP de forma predeterminada.

El archivo de configuración del teléfono tiene la URL correcta.

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

En los registros de la consola del teléfono, puede comprobar estos pasos.

```
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
```

A partir de las capturas de paquetes, verá una solicitud GET HTTP y una RESPUESTA correcta. Este es el PCAP de CUCM:

Troubleshoot

Antes de resolver el problema, recopile los detalles del problema que se mencionó anteriormente:

Registros para recopilar, si es necesario

- Capturas simultáneas de paquetes desde el teléfono IP y desde el servidor de CUCM (el servidor que es el primero en su grupo CM al que se enviaría la solicitud HTTP(S)).
- Registros de la consola del teléfono IP.
- Registros de Cisco TVS (detallados).

  Cuando establece los registros de TVS en detallados, es necesario reiniciar el servicio para que se realicen los cambios de nivel de seguimiento. Consulte Cisco bug ID CSCuq22327 para obtener información sobre la mejora para notificar que se requiere un reinicio del servicio cuando se cambian los niveles de registro.

Complete estos pasos para aislar el problema:

Paso 1.

Cree un servicio de prueba con estos detalles:

```
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
```

Ahora, suscriba este servicio a uno de los teléfonos afectados:

a. Vaya a la página de configuración del dispositivo.
b. Elija **Subscribe/Unsubscribe Services** en Enlaces Relacionados.
c. **Suscríbase** al servicio de prueba que ha creado.
d. **Guarde**, aplique la configuración y reinicie el teléfono.
    i. Lo que ha hecho, independientemente de la versión de FW del teléfono, que determina si debe utilizar la URL HTTP o HTTPS, es obligarlo a utilizar la URL HTTP.
    ii. Acceda al servicio Directorio corporativo desde el teléfono.
    iii. Si no funciona, recopile los registros mencionados anteriormente, compárelos con el escenario de trabajo mencionado en la sección Escenario de trabajo e identifique dónde se encuentra la desviación.
    iv. Si funciona, al menos ha confirmado que desde la perspectiva del servicio de telefonía IP de CUCM no hay problemas.
    v. En esta etapa, el problema es más probable con los teléfonos que utilizan la URL HTTPS.
    vi. A continuación, seleccione un teléfono que no funcione y vaya al paso siguiente.

Cuando funciona con este cambio, debe decidir si está bien dejar la configuración con la solicitud/respuesta del directorio corporativo que funciona a través de HTTP en lugar de HTTPS. La comunicación HTTPS no funciona debido a uno de los motivos que se explican a continuación.

Paso 2.

Recopile los registros mencionados anteriormente y compárelos con el escenario de trabajo mencionado en la sección Escenario de trabajo e identifique dónde se encuentra la desviación.

Podría ser uno de estos problemas:

a. El teléfono no puede ponerse en contacto con el servidor de TVS.
    i. En PCAPS, verifique la comunicación en el puerto 2445.
    ii. Asegúrese de que ninguno de los dispositivos de red de la ruta bloquee este puerto.
b. El teléfono entra en contacto con el servidor de TVS, pero el intercambio de señales TLS falla.

   Estas líneas se pueden imprimir en los registros de la consola del teléfono:

```
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>
```

Consulte Cisco bug ID CSCua65618 para obtener más información.

c. El teléfono entra en contacto con los servidores TVS y el intercambio de señales TLS se realiza correctamente, pero el TVS no puede comprobar el firmante del certificado que el teléfono solicitó autenticar.

Los fragmentos de los registros de TVS se enumeran aquí:

El teléfono entra en contacto con el televisor.

```
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
```

El TVS obtiene el nombre del emisor.

```
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
```

Busca el certificado, pero no lo encuentra.

```
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. El tráfico HTTPS se bloquea o descarta en algún lugar de la red.

   Obtenga PCAPs simultáneas del teléfono y el servidor de CUCM para verificar la comunicación.

Otros Escenarios Cuando Ocurre el Problema "Host No Encontrado"

1. El servidor de CUCM está definido por el nombre de host junto con problemas en la resolución de nombres.
2. La lista de servidores TVS está vacía en el teléfono cuando descarga el archivo xmldefault.cnf.xml. (En la versión 8.6.2, el archivo de configuración predeterminado no tiene la entrada TVS debido al Id. de error de Cisco CSCti64589.)
3. El teléfono no puede utilizar la entrada TVS del archivo de configuración porque descargó el archivo xmldefault.cnf.xml. Consulte Cisco bug ID CSCuq33297 - Phone para analizar la información de TVS desde el archivo de configuración predeterminado.
4. El directorio corporativo no funciona después de una actualización de CUCM porque el firmware del teléfono se actualiza a una versión posterior, lo que finalmente cambia el comportamiento del uso de HTTPS de forma predeterminada.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).