Corporate Directory (Directorio corporativo) problemas no encontrados del “host”

ID del Documento: 118699

Actualizado: De enero el 26 de 2015

Contribuido por Gagarin Sathiyanarayanan, ingeniero de Cisco TAC.

Descarga PDF
Imprimir
Comentarios

Productos Relacionados

- Cisco Unified Communications Manager (CallManager)

Contenido

Introducción

Este documento describe cómo resolver problemas los problemas no encontrados del “host” en Corporate Directory (Directorio corporativo). La información importante relevante a este documento es:

- Corporate Directory (Directorio corporativo) es Cisco-proporcionó al servicio telefónico del IP predeterminado que instala automáticamente con el administrador de las Comunicaciones unificadas de Cisco (CUCM).
- La tabla de “TelecasterService” salva los parámetros para todos los servicios telefónicos que sean aprovisionado en el sistema.
- En el teléfono cuando usted selecciona la opción “Corporate Directory (Directorio

corporativo)", el teléfono envía una petición HTTP o HTTPS a uno de los servidores CUCM y se vuelve un objeto XML como HTTP de respuesta.

Información importante

- Aclare si ocurre el problema cuando usted accede los "directorios" o "Corporate Directory (Directorio corporativo)".
- ¿Cuál es el campo definido del "servicio URL" bajo Corporate Directory (Directorio corporativo) a servicio? Si el URL se fija a la "aplicación: Cisco/CorporateDirectory" entonces, sobre la base de la versión de firmware del teléfono, el teléfono hace una petición HTTP o HTTPS.Los teléfonos que utilizan la versión de firmware 9.3.3 y posterior por abandono hacen una petición HTTPS.
- Cuando el servicio URL se fija a la "aplicación: Cisco/CorporateDirectory", el teléfono envía el pedido de HTTP al servidor que es primer en él es grupo del CallManager (CM).
- Identifique la topología de red entre el teléfono y el servidor a los cuales se envía el pedido de HTTP.
- Preste la atención a los Firewall, los optimizadores PÁLIDOS, y así sucesivamente en la trayectoria que puede caer/tráfico HTTP del cesto.

Escenario de trabajo

En este escenario, fijan al servicio telefónico URL a la "aplicación: Cisco/CorporateDirectory" y las aplicaciones HTTPS del teléfono.

Este ejemplo muestra el archivo de configuración del teléfono con el URL correcto.

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

De los registros de la consola del teléfono usted podrá verificar estos pasos.

1. El teléfono utiliza el 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::getCdUrl:
   [thread=appmgr MQThread]
   [class=cip.app.ar] Using HTTPS URL`
2. El certificado de la red de Tomcat presentado al teléfono del servidor de los directorios no estará disponible en el teléfono. Por lo tanto el teléfono intenta autenticar el certificado vía el servicio de la verificación de la confianza (TV).`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, will attempt via TVS`
3. Las miradas del teléfono en el theTVS ocultan primero y si no encontraron que entra en contacto el servidor TV.`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. Puesto que la conexión al theTVS es también segura, se completa una autenticación

certificada y se imprime este mensaje si es acertado.`8096 NOT 11:04:15.173585  SECD: -Successfully obtained a TLS connection to the TVS server`

5. El teléfono ahora envía una petición de 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 el "0" de los TV significa que la autenticación era acertada. `8172 NOT 11:04:15.220060  SECD: -Authentication Response received, status : 0`
7. Se visualiza este mensaje y entonces usted verá 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 certificada es similar a qué se discute en el servicio de la verificación de la confianza de los contactos del teléfono para el certificado desconocido.De las capturas de paquetes (PCAPs) recogidas en el extremo del teléfono, usted debe poder verificar la comunicación TV con el uso de este filtro - el "tcp.port==2445".

En los registros simultáneos TV:

1. Las trazas del estudio con respecto a la mano de Transport Layer Security (TLS) sacuden.
2. Después, revise el vaciado Hex 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. Los TV extraen 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. Los TV verifican 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. Los TV envían 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
```

Fijan al servicio telefónico URL a la “aplicación: Cisco/CorporateDirectory” y las aplicaciones HTTP del teléfono

> Nota: En vez del uso de una versión de firmware anterior del teléfono, el servicio y el servicio seguro URL fueron puestos en hard-code al HTTP URL. Sin embargo, la misma Secuencia de eventos se considera en el firmware del teléfono que hace uso del HTTP por abandono.

El archivo de configuración del teléfono tiene el URL correcto.

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

De los registros de la consola del teléfono usted podrá verificar 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
```

De las capturas de paquetes usted verá una petición get HTTP y una RESPUESTA acertada. Éste es el PCAP de CUCM:

Troubleshooting

Antes de que usted resuelva problemas, recolecte los detalles del problema enumerado anterior:

Registros a recoger, si procede

- Capturas de paquetes simultáneas del teléfono del IP y del servidor CUCM (el servidor que es primer en él es el grupo CM al donde el pedido de HTTP sería enviado).
- Registros de la consola del teléfono del IP.
- Registros de Cisco TV (detallados).Cuando usted fija los registros TV a detallado, el servicio necesita ser recomenzado para que los cambios del nivel de traza ocurran. Vea el Id. de bug Cisco CSCuq22327 para la mejora para notificar que un reinicio del servicio está requerido cuando se cambian los niveles del registro.

Complete estos pasos para aislar el problema:

Paso 1

Cree un servicio de la 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, inscriba este servicio a uno de los teléfonos afectados:

1. Vaya a la página de la configuración del dispositivo.
2. Selecto **inscriba/desinscriba los servicios** conforme a los links relacionados.
3. Inscriba el servicio de la prueba que usted creó.
4. Salve, aplique la configuración, y reajuste el teléfono. Qué usted ha hecho está, con independencia de la versión FW del teléfono que determina si utilizar el HTTP o el HTTPS URL, lo fuerza para utilizar HTTP URL.Acceda “Corporate Directory (Directorio corporativo)” el servicio en el teléfono.Si no trabaja, después recoger los registros mencionados

anteriormente y compararlos con el escenario de trabajo mencionado bajo de “escenario trabajo” e identificar donde está la desviación.Si trabaja, después usted por lo menos ha confirmado que de la perspectiva del servicio telefónico IP CUCM no hay problemas.En esta etapa el problema podría lo más probablemente posible estar con los teléfonos que utilizan el HTTPS URL.Ahora, escoja un teléfono que no funcione y proceda al siguiente paso.

Cuando trabaja con este cambio, usted necesita decidir si es ACEPTABLE dejar la configuración con Corporate Directory (Directorio corporativo) la petición/la respuesta que trabaja sobre el HTTP en vez del HTTPS. La comunicación HTTPS no trabaja debido a una de las razones discutió después.

Paso 2

Recoja los registros mencionados previamente y compárelos con el escenario de trabajo mencionado bajo de “escenario trabajo” e identifique donde está la desviación.

Podría ser uno de estos problemas:

1. El teléfono no puede entrar en contacto el servidor TV. En el PCAPS, verifique la comunicación sobre el puerto 2445.Asegúrese de que ningunos de los dispositivos de red en el bloque de la trayectoria este puerto.
2. El teléfono entra en contacto el servidor TV, pero la entrada en contacto TLS falla.Estas líneas serán impresas 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>
```
Vea el Id. de bug Cisco CSCua65618 para más información.

3. El teléfono entra en contacto los servidores TV y la entrada en contacto TLS es acertada, pero los TV no pueden verificar al firmante del certificado que el teléfono pedido autenticar.El snippets de los registros TV se enumera aquí:El teléfono entra en contacto los 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
```
Los TV consiguen 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
```
Mira para arriba el certificado, pero no puede encontrarlo.
```
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
```

4. El tráfico HTTPS se bloquea/se cae en alguna parte en la red.Consiga PCAPs simultáneo del teléfono y del servidor CUCM para verificar la comunicación.

Otros escenarios cuando ocurre el problema no encontrado del “host”

1. El servidor CUCM es definido por el nombre de host junto con los problemas en la resolución de nombre.
2. La lista de servidores TV está vacía en el teléfono cuando descarga el archivo xmldefault.cnf.xml. (En la versión 8.6.2 el archivo de configuración predeterminada no tendrá la entrada TV en él debido al Id. de bug Cisco CSCti64589.)
3. El teléfono no puede utilizar la entrada TV en el archivo de configuración porque descargó el archivo xmldefault.cnf.xml. Vea el Id. de bug Cisco CSCuq33297 - Phoneto analiza la información TV del archivo de configuración predeterminada.
4. Corporate Directory (Directorio corporativo) no trabaja después de una actualización CUCM porque las actualizaciones del firmware del teléfono a una versión posterior que cambie eventual el comportamiento del uso del HTTPS por abandono.

Discusiones relacionadas de la comunidad del soporte de Cisco

La comunidad del soporte de Cisco es un foro para que usted haga y conteste a las preguntas, las sugerencias de la parte, y colabora con sus pares.

Actualizado: De enero el 26 de 2015
ID del Documento: 118699