Borde de la Colaboración la mayoría de los problemas frecuentes

Contenido

Introducción

El borde de la Colaboración/el móvil y el Acceso Remoto (MRA) es una solución del despliegue para la capacidad privada virtual del Jabber de la red-menos (VPN). Esta solución permite que los usuarios finales conecten con los recursos internos de la empresa desde cualquier lugar del mundo. Esta guía se ha escrito para dar a los ingenieros que resuelven problemas la solución límite de la Colaboración la capacidad para identificar rápidamente y resolver a los clientes de los problemas más comunes haga frente durante la frase del despliegue.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administrador de las Comunicaciones unificadas de Cisco (CUCM)
- Base de la autopista de Cisco
- Borde de la autopista de Cisco
- Cisco IM y presencia (IM&P)
- Jabber de Cisco para Windows
- Cisco Jabber para Mac
- Cisco Jabber para Android
- Jabber de Cisco para el IOS
- Certificados de la Seguridad
- Domain Name System (DNS)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión X8.1.1 del servidor del comunicación mediante video (VCS) o más adelante
- Control VCS y autopista/base y borde de la autopista
- Versión 9.1(2)SU1 o más adelante e IM CUCM y versión 9.1(1) o posterior P
- Versión 9.7 o posterior del Jabber de Cisco

Problemas del login

Jabber incapaz al registro con MRA

Este síntoma se puede causar por una amplia gama de problemas, algunos cuyo se delinean

aquí.

1. Expediente de servicio perimetral de la Colaboración (SRV) no creado y/o puerto 8443 inalcanzable

Para que un cliente del Jabber pueda iniciar sesión con éxito con MRA, un expediente específico del borde SRV de la Colaboración debe ser creado y accesible externamente. Cuando comienzan a un cliente del Jabber inicialmente, hace las interrogaciones DNS SRV:

1. **_cisco-uds**: Este expediente SRV se utiliza para determinar si un servidor CUCM está disponible.

2. **_cuplogin**: Este expediente SRV se utiliza para determinar si un servidor IM&P está disponible.

3. **_collab-edge**: Este expediente SRV se utiliza para determinar si MRA está disponible.

Si comienzan y no recibe una respuesta SRV para los **_cisco-uds** y el **_cuplogin** y recibe al cliente del Jabber una respuesta para el **_collab-edge**, después utiliza esta respuesta para intentar entrar en contacto la autopista-e enumerada en la respuesta SRV.

El expediente del **_collab-edge** SRV debe señalar al nombre de dominio completo (FQDN) de la autopista-e con el puerto **8443**. Si el **_collab-edge** SRV no se crea, o no está externamente disponible, o si es disponible, pero el puerto 8443 no es accesible, después el cliente del Jabber no puede iniciar sesión.

2. Certificado inaceptable o ningún disponible en la autopista VCS

Después de que el cliente del Jabber haya recibido una respuesta para el **_collab-edge**, entonces entra en contacto la autopista con Transport Layer Security (TLS) sobre el puerto 8443 para intentar extraer el certificado de la autopista para configurar TLS para la comunicación entre el cliente del Jabber y la autopista.

Si la autopista no tiene un certificado firmado válido que contenga el FQDN o el dominio de la autopista, después éste falla y el cliente del Jabber no puede iniciar sesión.

Si ocurre este problema, el cliente debe utilizar la herramienta del pedido de firma de certificado (CSR) en la autopista, que incluye automáticamente el FQDN de la autopista como nombre alternativo sujeto (SAN).

> Nota: MRA requiere la comunicación segura entre la autopista-C y la autopista-e, y entre la autopista-e y los puntos finales del externo.

Requisitos del certificado de servidor de la autopista-C:

- **Los alias del nodo de la charla** configurados en los servidores IM&P. Se requiere esto si usted realiza la federación extensible de la Mensajería y del protocolo de la presencia (XMPP). La autopista-C debe incluir automáticamente éstos en el CSR a condición de que un servidor

IM&P se ha descubierto ya en la autopista-C.

- Los nombres en el formato FQDN de todos los **perfiles de seguridad del teléfono** en CUCM configurado para TLS y usado en los dispositivos configurados para MRA. Esto permite la comunicación segura entre el CUCM y la autopista-C para los dispositivos que utilizan esos perfiles de seguridad del teléfono.

Requisitos del certificado de servidor de la autopista-e:

1. Todos los dominios configurados para las Comunicaciones unificadas. Esto incluye el dominio de la autopista-e y del C, el dominio de la dirección de correo electrónico configurado para el Jabber, y cualquier dominio de la presencia.

2. **Los alias del nodo de la charla** configurados en los servidores IM&P. Se requiere esto si usted realiza la federación XMPP.

El Guía de despliegue MRA describe este problema minuciosamente en las páginas 17-18.

3. Ningunos servidores UD encontrados en configuración del borde

Después de que el cliente del Jabber establezca con éxito una conexión segura con la autopista-e, pide su configuración del borde (**get_edge_config**). Esta configuración del borde contiene los expedientes SRV para el **_cuplogin** y los **_cisco-uds**. Si estos expedientes SRV no se vuelven en la configuración del borde, después el cliente del Jabber no puede proceder con el login.

Para reparar esto, aseegurese que los **_cisco-uds** y los expedientes del **_cuplogin** SRV son creados internamente y resolvable por la autopista-C.

Más información sobre los expedientes DNS SRV se puede encontrar en la página 10 del Guía de despliegue MRA para X8.5.

Esto es también un síntoma común si usted está en un dominio dual. Si usted se ejecuta en un dominio dual y encuentra no están volviendo al cliente del Jabber ningún servicio de datos del usuario (UD), usted debe asegurarse que su configuración siga la sección DNS de la nota de configuración: Móvil y Acceso Remoto con Expressway/VCS en un despliegue del multi-dominio.

4. Los registros de la autopista-C muestran este error: XCP_JABBERD Detail= " incapaz de conectar para recibir “el %IP%”, conexión del puerto 7400:(111) rechazada”

Si la autopista-e Network Interface Controller (NIC) se configura incorrectamente, ésta puede hacer el servidor extensible de la plataforma de las comunicaciones (XCP) no ser actualizado. Si la autopista-e cumple estos criterios, después usted encontrará probablemente este problema:

1. Utiliza un solo NIC.
2. La clave avanzada de la opción de interconexión de redes está instalada.
3. La opción de interfaces de la red dual del uso se fija a **sí**.

Para corregir este problema, cambie la opción de interfaces de la red dual del uso a **no.**

La razón que esto es un problema es porque la autopista-e está atenta la sesión XCP sobre la interfaz de la red incorrecta, que causa fallar/descanso de la conexión. La autopista-e escucha en

el puerto TCP 7400 la sesión XCP. Usted puede verificar esto si usted utiliza el **comando netstat del** VCS como raíz.

5. El nombre de host/el Domain Name del servidor VCE-E no hace juego qué se configura en el _collab-edge SRV

Si el nombre de host/el Domain Name del servidor de la autopista-e no hace juego qué fue recibida en la respuesta del **_collab-edge** SRV, el cliente del Jabber no puede comunicar con la autopista-e. El cliente del Jabber utiliza el xmppEdgeServer/el elemento del direccionamiento en la respuesta del **get_edge_config** para establecer la conexión XMPP a la autopista-e.

Éste es un ejemplo de lo que parece el xmppEdgeServer/el direccionamiento en la respuesta del **get_edge_config de la** autopista-e al cliente del Jabber:

```
<xmppEdgeServer>
<server>
<address>examplelab-vcse1.example.com</address>
<tlsPort>5222</tlsPort>
</server>
</xmppEdgeServer>
```

Para evitar esto, aseegurese que el expediente del **_collab-edge** SRV hace juego el nombre de host/el Domain Name de la autopista-e. La mejora CSCuo83458 se ha clasifiado para esto.

6. Incapaz de registrar en ciertos servidores IM&P - los registros de la autopista visualizan un error

Los registros de la autopista visualizan uno de estos errores:

```
"No realm found for host cups-example.domain.com, check connect auth configuration" Module="cm-
1.expressway-edge-example-com" Level="INFO " CodeLocation=
"SASLManager.cpp:198" Detail="Failed to query auth component for SASL mechanisms"
```

De la autopista-C, vaya a la **configuración > a las Comunicaciones unificadas > a los servidores IM&P**. Seleccione la casilla de verificación al lado de cada servidor IM&P y el tecleo **restaura los servidores**.

> Nota: Si esto no repara el problema, el router XCP en el servidor IM&P también debe ser recomenzado.

7. Incapaz de iniciar sesión debido a un WebEx existente conecte la suscripción

Farfulle para los registros de Windows muestran esto:

```
2014-11-22 19:55:39,122 INFO  [0x00002808] [very\WebexCasLookupDirectorImpl.cpp(134)]
[service-discovery] [WebexCasLookupDirectorImpl::makeCasLookupWhenNetworkIs
Available] - makeCasLookupForDomain result is 'Code: IS_WEBEX_CUSTOMER; Server:
http://loginp.webexconnect.com;
Url: http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com';;;.2014-11-22
19:55:39,122 INFO [0x00002808] [overy\WebexCasLookupDirectorImpl.cpp(67)]
[service-discovery] [WebexCasLookupDirectorImpl::determineIsWebexCustomer] -
Discovered Webex Result from server. Returning server result.2014-11-22 19:55:39,122
```

```
DEBUG [0x00002808] [ery\WebexCasLookupUrlConfigImpl.cpp(102)]
[service-discovery] [WebexCasLookupUrlConfigImpl::setLastCasUrl] - setting last_cas_
lookup_url : http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com2014-11-22
19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStoreManager.cpp(286)]
[ConfigStoreManager] [ConfigStoreManager::storeValue] - key : [last_cas_lookup_url]
value : [http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com]2014-11-22
19:55:39,123 DEBUG [0x00002808] [common\processing\TaskDispatcher.cpp(29)]
[TaskDispatcher] [Processing::TaskDispatcher::enqueue] - Enqueue ConfigStore::persist
Values - Queue Size: 02014-11-22 19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStore
Manager.cpp(140)]
[ConfigStoreManager] [ConfigStoreManager::getValue] - key : [last_cas_lookup_url]
skipLocal : [0] value: [http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com]
success: [true] configStoreName: [LocalFileConfigStore]
```

Los intentos de inicio de sesión se dirigen al WebEx conectan.

Para una resolución permanente, usted debe entrar en contacto el WebEx para hacer el sitio desarmar.

Solución alternativa:

A corto plazo, usted puede utilizar una de estas dos opciones para excluirlo de las operaciones de búsqueda.

- Agregue este parámetro al jabber-config.xml. Entonces cargue el archivo jabber-config.xml al servidor TFTP en CUCM. Requiere que el cliente abra una sesión internamente primero.

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
<Policies>
<ServiceDiscoveryExcludedServices>WEBEX<
/ServiceDiscoveryExcludedServices>
</Policies>
</config>
```

- De una perspectiva de la aplicación, ejecute esto: **msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=CUP EXCLUDED_SERVICES=WEBEX**

  Nota: La segunda opción no trabaja para los dispositivos móviles.

Problemas del registro

El softphone no puede registrarse, el método SIP/2.0 405 no permitido

Un registro de diagnóstico de la autopista-C muestra un mensaje **no permitido del método SIP/2.0 405** en respuesta al pedido de inscripción enviado por el cliente del Jabber. Ésta es probablemente a causa a un trunk del protocolo de iniciación de la sesión existente (SORBO) entre la autopista-C y CUCM usando el puerto 5060/5061.

```
SIP/2.0 405 Method Not Allowed
Via: SIP/2.0/TCP 10.10.40.108:5060;egress-zone=CollabZone;branch=z9hG4bK81e7f5f1c1
ab5450c0b406c91fcbdf181249.81ba6621f0f43eb4f9c0dc0db83fb291;proxy-call-id=da9e25aa-
80de-4523-b9bc-be31ee1328ce;rport,SIP/2.0/TLS 10.10.200.68:7001;egress-zone=Traversal
Zone;branch=z9hG4bK55fc42260aa6a2e3741919177aa84141920.a504aa862a5e99ae796914e85d35
```

```
27fe;proxy-call-id=6e43b657-d409-489c-9064-3787fc4919b8;received=10.10.200.68;rport=
7001;ingress-zone=TraversalZone,SIP/2.0/TLS
192.168.1.162:50784;branch=z9hG4bK3a04bdf3;received=172.18.105.10;rport=50784;
ingress-zone=CollaborationEdgeZone
From: <sip:5151@collabzone>;tag=cb5c78b12b4401ec236e1642-1077593a
To: <sip:5151@collabzone>;tag=981335114
Date: Mon, 19 Jan 2015 21:47:08 GMT
Call-ID: cb5c78b1-2b4401d7-26010f99-0fa7194d@192.168.1.162
Server: Cisco-CUCM10.5
CSeq: 1105 REGISTER
Warning: 399 collabzone "SIP trunk disallows REGISTER"
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
Content-Length: 0
```

Para corregir este problema, cambie el puerto del SORBO en el perfil de seguridad del trunk del SORBO que se aplica al trunk existente del SORBO configurado en CUCM y a la zona vecina de la autopista-C para CUCM a un diverso puerto tal como 5065. Esto se explica más lejos en el Guía de despliegue MRA en la página 39.

Resumen de la configuración

CUCM:

1. Cree un nuevo perfil de seguridad del trunk del SORBO con un puerto de escucha con excepción de 5060 (5065).
2. Cree un trunk del SORBO asociado al perfil de seguridad y al destino del trunk del SORBO fijados a la dirección IP de la autopista-C, el puerto 5060.

Autopista-C:

1. Cree una zona vecina a CUCM con un puerto de destino con excepción de 5060 (5065) para hacer juego la configuración CUCM.
2. En las **configuraciones > los protocolos > el SORBO de la** autopista-C, aseegurese la autopista-C todavía escucha en 5060 el SORBO.

El softphone no puede registrarse, Reason= " dominio desconocido”

Un registro de diagnóstico del sorbo **desconocido rechazado " registro”** " TCP” AOR= " del " XXX.XXX.XXX.XXX” el Src-port="51601" Protocol= de Src-ip= del " SORBO” de Service= **dominio” de** Event= **Reason= del " de las** demostraciones de la autopista-C: XXX.XXX.XXX.XXX”.

Para corregir este problema, marque estas puntas:

- ¿El cliente del Jabber utiliza un **perfil de seguridad del dispositivo seguro** en CUCM cuando la intención no es utilizar un perfil de seguridad del dispositivo NON-seguro?
- ¿Si los clientes del Jabber utilizan un perfil de seguridad del dispositivo asegurado, está el nombre del perfil de seguridad en el formato FQDN y ese nombre FQDN se configura en el certificado Autopista-c como SAN?
- Si los clientes del Jabber utilizan un perfil de seguridad del dispositivo asegurado, navegue a los **parámetros del > Security (Seguridad) del System (Sistema) > Enterprise Parameters (Parámetros Enterprise) > al modo seguro** y al control del **cluster** que fijan al modo seguro del

cluster a 1 para verificar que se ha asegurado el cluster CUCM. Si el valor es **0**, el administrador debe pasar con el procedimiento documentado asegurar el cluster.

El softphone no puede registrarse, razón expiró la “que cuenta descendiente ociosa”

Cuando usted revisa los registros de la autopista-e durante el timeframe que el cliente del Jabber envía en un mensaje del REGISTRO, usted puede ser que encuentre una **cuenta descendiente ociosa expiró** error como se indica en el fragmento de código aquí.

```
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"
Module="network.tcp" Level="DEBUG": Src-ip="JabberPubIP" Src-port="4211"
Dst-ip="VCS-E_IP" Dst-port="5061" Detail="TCP Connecting"
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"
Module="network.tcp" Level="DEBUG": Src-ip="JabberPubIP" Src-port="4211" Dst-ip=
"VCS-E_IP" Dst-port="5061" Detail="TCP Connection Established"2015-02-02T19:46:49+01:00
collabedge tvcs: UTCTime="2015-02-02 18:46:49,606"
Module="network.tcp" Level="DEBUG": Src-ip="92.90.21.82" Src-port="4211" Dst-ip=
"VCS-E_IP" Dst-port="5061" Detail="TCP Connection Closed" Reason="Idle
countdown expired"
```

Este snippet indica que el Firewall tiene puerto 5061 abierto; sin embargo, no hay tráfico de la capa de la aplicación que se pasa encima en una cantidad suficiente de hora así que la conexión TCP se cierra.

Si usted encuentra esta situación, hay un nivel alto de probabilidad que el Firewall delante de la autopista-e tiene funciones del examen/del gateway de capa de aplicación del SORBO (ALG) giradas. Para remediate este problema, usted debe diable estas funciones. Si usted es inseguro de cómo hacer esto, usted debe referirse a la Documentación del Producto de su proveedor de escudos de protección.

Para más información sobre el SORBO Inspection/ALG, usted puede referirse al apéndice 4 del control y del Guía de despliegue básico de la autopista (página 55) VCS.

Jabber y clientes EX incapaces al registro a la autopista-e cuando aprovisionado con un LSC

Para corregir este problema, **cargue el certificado CAPF.pem a la** lista de la confianza del Certificate Authority de la autopista-e.

Problemas de los media

Ningunos media cuando usted llama con MRA

En un solo despliegue NIC con el NAT configurado, estos parámetros están faltando o no configurado correctamente:

- La autopista-C no se señala al IP Address público de la autopista-e, que no prohibe a Firewall a la horquilla la señalización.

- Si señala al FQDN de la autopista-e para TLS, verifique el FQDN debe resolver al IP Address público de la autopista-e.

- Éstos no se configuran en la autopista-e:

```
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"
Module="network.tcp" Level="DEBUG": Src-ip="JabberPubIP" Src-port="4211"
Dst-ip="VCS-E_IP" Dst-port="5061" Detail="TCP Connecting"
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"
Module="network.tcp" Level="DEBUG": Src-ip="JabberPubIP" Src-port="4211" Dst-ip=
"VCS-E_IP" Dst-port="5061" Detail="TCP Connection Established"2015-02-02T19:46:49+01:00
collabedge tvcs: UTCTime="2015-02-02 18:46:49,606"
Module="network.tcp" Level="DEBUG": Src-ip="92.90.21.82" Src-port="4211" Dst-ip=
"VCS-E_IP" Dst-port="5061" Detail="TCP Connection Closed" Reason="Idle
countdown expired"
```

Más información sobre esto se puede encontrar en la página 63 del control VCS y del Guía de despliegue de la autopista.

Ninguna señal de llamada cuando llamada sobre MRA al PSTN

Este problema es debido a una limitación en las autopistas antes de la versión x8.5. El Id. de bug Cisco CSCua72781 describe cómo la autopista-C no remite los media tempranos en el progreso de 183 sesiones o 180 que suenan a través de la zona del traversal. Si usted funciona con las versiones x8.1.x o x8.2.x, usted puede actualizar a la versión x8.5 o alternativamente realizar la solución alternativa enumerada aquí.

Es posible utilizar una solución alternativa en el Cisco Unified Border Element (CUBO) si usted hace un perfil del SORBO que dé vuelta a los 183 en 180 y lo aplica en el dial-peer entrante. Por ejemplo:

```
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"
Module="network.tcp" Level="DEBUG": Src-ip="JabberPubIP" Src-port="4211"
Dst-ip="VCS-E_IP" Dst-port="5061" Detail="TCP Connecting"
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"
Module="network.tcp" Level="DEBUG": Src-ip="JabberPubIP" Src-port="4211" Dst-ip=
"VCS-E_IP" Dst-port="5061" Detail="TCP Connection Established"2015-02-02T19:46:49+01:00
collabedge tvcs: UTCTime="2015-02-02 18:46:49,606"
Module="network.tcp" Level="DEBUG": Src-ip="92.90.21.82" Src-port="4211" Dst-ip=
"VCS-E_IP" Dst-port="5061" Detail="TCP Connection Closed" Reason="Idle
countdown expired"
```

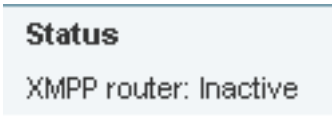
Inhabilitarían luego 180 media tempranos en el perfil del SORBO del **CUCM > CUBO** o el CUBO sí mismo dentro del modo de configuración sorbo-UA.

```
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"
Module="network.tcp" Level="DEBUG": Src-ip="JabberPubIP" Src-port="4211"
Dst-ip="VCS-E_IP" Dst-port="5061" Detail="TCP Connecting"
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"
Module="network.tcp" Level="DEBUG": Src-ip="JabberPubIP" Src-port="4211" Dst-ip=
"VCS-E_IP" Dst-port="5061" Detail="TCP Connection Established"2015-02-02T19:46:49+01:00
collabedge tvcs: UTCTime="2015-02-02 18:46:49,606"
Module="network.tcp" Level="DEBUG": Src-ip="92.90.21.82" Src-port="4211" Dst-ip=
"VCS-E_IP" Dst-port="5061" Detail="TCP Connection Closed" Reason="Idle
countdown expired"
```

Problemas Autopista-céntricos

La autopista-C pudo visualizar a un “router XMPP: ” Error inactivo

Usted puede ser que encuentre este error después de que usted complete la configuración:



Este error puede suceder por varias diversas razones descritas aquí:

- El CM unificado mantiene no se habilita en Expressway-C/E.

  Para reparar este problema, complete estos pasos:

  Navegue a la **configuración > a las zonas > a las zonas > a la zona del Traversal**.Seleccione **sí** para los servicios unificados de Communcations bajo sección del SORBO.Haga clic en Save (Guardar).

- El LAN2 es activo pero parado en la autopista-e.

  Para reparar este problema, complete estos pasos:

  Navegue al **sistema > al IP de la** autopista-e.Seleccione **no** para el parámetro dual de las interfaces de la red del uso.

- Un dominio del SORBO no se ha definido en la autopista-C.

  Para reparar este problema, complete estos pasos:

  Navegue a la **configuración > a los dominios > nuevo**.Agregue su dominio y dé vuelta a los **registros del SORBO y al aprovisionamiento en el CM unificado** e **IM y a los servicios de la presencia en el CM unificado a encendido**.Cree un dominio.

- No giran la autopista-C **IM y a los servicios de la presencia en el CM unificado**.

  Para reparar este problema, complete estos pasos:

  Navegue a la **configuración > al dominio > seleccionan su dominio**.Fije el **IM y los servicios de la presencia en el CM unificado a encendido.**Haga clic en Save (Guardar).

- La zona del Traversal entre la autopista-C y la autopista-e no es segura.

  Para reparar este problema, complete estos pasos:

  Asegúrese de que el Traversal esté fijado **para forzar cifrado.**Asegúrese de que fijen a la dirección de peer en la autopista-C al nombre de host de la autopista-e y no de la dirección IP de modo que haga juego el certificado.

Problemas CUCM e IM&P

Error ASCII que evita que CUCM sea agregado

Cuando usted agrega CUCM a la autopista-C, usted encuentra un error ASCII que evite que CUCM sea agregado.

Cuando la autopista-C agrega CUCM a su base de datos, se ejecuta con una serie de interrogaciones AXL que se relacionen para conseguir y para enumerar las funciones. Los ejemplos de éstos incluyen el **getCallManager**, el **listCallManager**, el **listProcessNode**, el **listProcessNodeService**, y el **getCCMVersion**. Después de que se funcione con el proceso del **getCallManager**, es tenido éxito por un conjunto de **ExecuteSQLQuery** para extraer toda la Administrador-confianza de la llamada CUCM o las Tomcat-confianzas.

Una vez que CUCM recibe la interrogación y la ejecuta en él, CUCM entonces informa todos sus Certificados. Si uno de los Certificados contiene un carácter NON-ASCII, la autopista genera un error en la interfaz Web similar al **codificador-decodificador ASCII no puede decodificar el byte 0xc3 en la posición 42487: ordinal no en range(128).**

Este problema se sigue con el Id. de bug Cisco CSCuo54489 y se resuelve en la versión x8.2.

Errores salientes de TLS en 5061 de la autopista-C a CUCM en las implementaciones seguras

Este problema ocurre cuando usted utilizan los certificados autofirmados en CUCM y Tomcat.pem/CallManager.pem tienen el mismo tema. El problema se aborda con el Id. de bug Cisco CSCun30200. La solución alternativa para corregir el problema es borrar el tomcat.pem y la neutralización TLS verifica de la configuración CUCM en la autopista-C.

Servidor IM&P no agregado y errores encontrados

Cuando usted agrega un servidor IM&P, la autopista-C señala que “este servidor no no puede un servidor de IM y de la presencia” o “comunicar con el error de HTTP el "HTTPError:500"' de la interrogación .AXL, que da lugar al servidor IM&P que no es agregado.

Como parte de la adición de un servidor IM&P, la autopista-C utiliza una interrogación AXL para buscar los Certificados IM&P en un directorio explícito. Debido desertar CSCul05131, los Certificados no están en ese almacén; por lo tanto, usted encuentra el error falso.

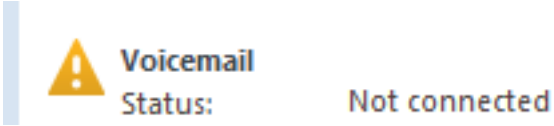
Error del servidor XCP encontrado

En la autopista-C, conforme al **estatus > a las Comunicaciones unificadas**, las visualizaciones de un error del servidor XCP que lee “accesible inactivo solamente la conexión no está para arriba. Contraseña del control”.

La solución es reiniciar ambas autopistas.

Problemas diversos

El estatus del voicemail en el cliente del Jabber muestra “no conectado



Para hacer que el estatus del voicemail del cliente del Jabber con éxito conecta, usted debe configurar la dirección IP o el nombre de host del Cisco Unity Connection dentro de la lista blanca del servidor HTTP en la autopista-C.

Para completar esto de la autopista-C, realice el procedimiento relevante:

Procedimiento para las versiones x8.1 y x8.2

1. **La configuración del** tecleo **> las Comunicaciones unificadas > el servidor HTTP de la configuración > de la configuración permiten la lista**.
2. El tecleo **nuevo > ingresa IP/Hostname > crea la entrada**.
3. El logout del cliente del Jabber, y entonces registra detrás adentro.

Procedimiento para la versión x8.5

1. **Configuración del** tecleo **> Comunicaciones unificadas > servidores del Unity Connection**.
2. El tecleo **nuevo > ingresa IP/Hostname, direccionamiento de las credenciales de la cuenta de usuario > Add**.
3. El logout del cliente del Jabber, y entonces registra detrás adentro.

Las fotos del contacto no aparecen en los clientes del Jabber a través de las autopistas

El móvil y la solución de acceso remoto utiltizes solamente los UD para la resolución de la foto del contacto. Esto requiere que usted tenga un servidor Web disponible salvar las fotos. La configuración sí mismo es doble.

1. El jabber-config.xml se debe modificar para dirigir a los clientes al servidor Web para la resolución de la foto del contacto. La configuración aquí debe alcanzar esto.

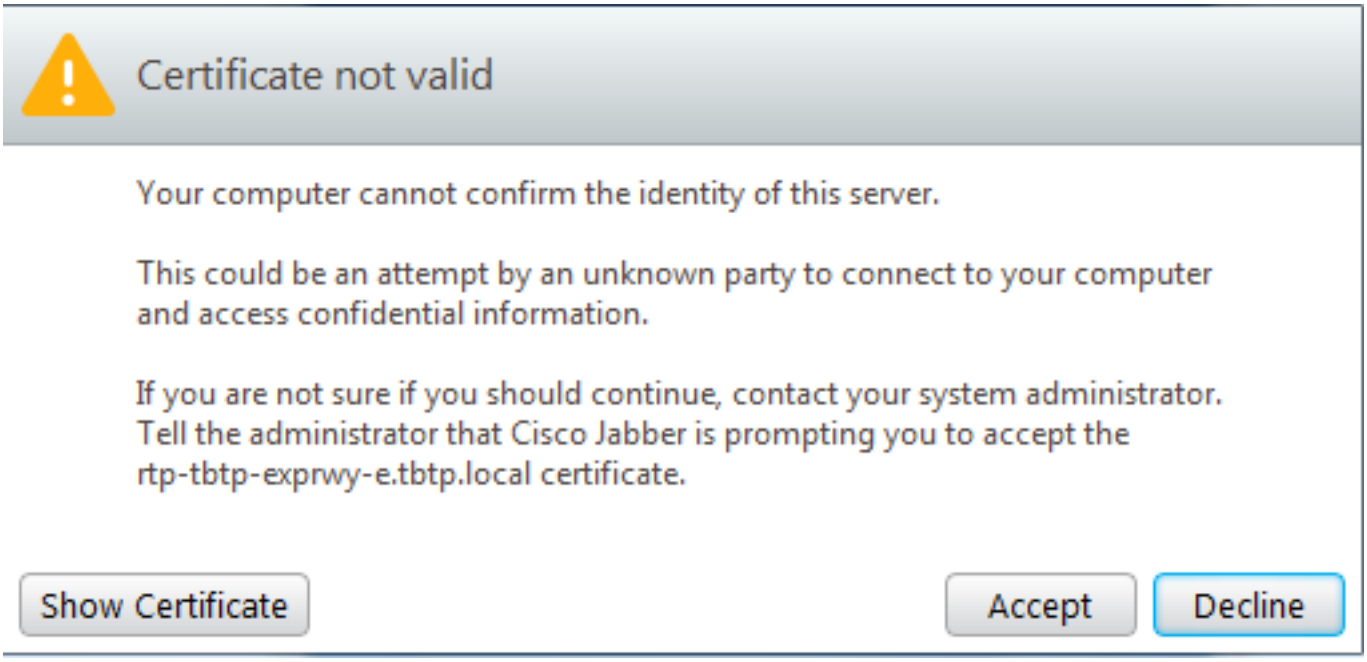
```
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"
Module="network.tcp" Level="DEBUG": Src-ip="JabberPubIP" Src-port="4211"
Dst-ip="VCS-E_IP" Dst-port="5061" Detail="TCP Connecting"
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"
Module="network.tcp" Level="DEBUG": Src-ip="JabberPubIP" Src-port="4211" Dst-ip=
"VCS-E_IP" Dst-port="5061" Detail="TCP Connection Established"2015-02-02T19:46:49+01:00
collabedge tvcs: UTCTime="2015-02-02 18:46:49,606"
Module="network.tcp" Level="DEBUG": Src-ip="92.90.21.82" Src-port="4211" Dst-ip=
"VCS-E_IP" Dst-port="5061" Detail="TCP Connection Closed" Reason="Idle
countdown expired"
```

2. La autopista-C debe tener el servidor Web enumerado dentro del servidor HTTP para permitir la lista.

La configuración del tecleo **> las Comunicaciones unificadas > el servidor HTTP de la configuración > de la configuración permiten la lista**.El tecleo **nuevo > ingresa IP/Hostname > crea la entrada**.El logout del cliente del Jabber, y entonces registra detrás adentro.

Nota: Para más información sobre los UD entre en contacto la resolución de la foto, refieren a la documentación de la foto del contacto del Jabber.

Se indica a los clientes del Jabber que validen el certificado de la autopista-e durante el login



Para parar al cliente del Jabber de ser indicado para validar el certificado de la autopista, usted debe resolver el criteteria dos enumerado abajo:

- El dispositivo/la máquina que funciona con al cliente del Jabber debe tener el firmante del certificado de la autopista-e enumerado dentro de su almacén de la confianza del certificado.

  Nota: Esto se logra fácilmente si usted utiliza un Certificate Authority público porque los dispositivos móviles contienen un almacén grande de la confianza del certificado.

- El dominio externo usado para el expediente del collab-borde debe estar presente dentro del SAN del certificado de la autopista-e.

  Nota: El cliente del Jabber busca el SAN para este dominio cuando lo recibe. Si no está presente, le indica a que lo valide.

Información Relacionada

- Móvil y Acceso Remoto de las Comunicaciones unificadas vía Cisco VCS
- Guía de despliegue de la creación y del uso del certificado del Cisco TelePresence VCS
- Uso del puerto IP del servidor del comunicación mediante video del Cisco TelePresence

(Cisco VCS) para el Traversal del Firewall
- Despliegue y guía de instalación para el Jabber de Cisco
- Soporte Técnico y Documentación - Cisco Systems