Resolver problemas más comunes de Collaboration Edge

Contenido

Introducción

En este documento se describe cómo solucionar los problemas más comunes de Collaboration Edge a los que se enfrenta durante la fase de implementación.

Antecedentes

Mobile & Remote Access (MRA) es una solución de implementación para la capacidad Jabber sin red privada virtual (VPN). Esta solución permite a los usuarios finales conectarse a recursos internos de la empresa desde cualquier lugar del mundo. Esta guía se ha redactado para ofrecer a los ingenieros que solucionan problemas de la solución Collaboration Edge la capacidad de identificar y resolver rápidamente los problemas más habituales a los que se enfrenta durante la frase de implementación.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Communications Manager (CUCM)
- Núcleo de Cisco Expressway
- Perímetro de Cisco Expressway
- IM y presencia de Cisco (IM&P)
- Cisco Jabber para Windows
- Cisco Jabber para MAC
- Cisco Jabber para Android
- Cisco Jabber para IOS®
- Certificados de seguridad
- Sistema de nombres de dominio (DNS)

Componentes Utilizados

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

- Expressway versión X8.1.1 o posterior
- CUCM versión 9.1(2)SU1 o posterior y IM&P versión 9.1(1) o posterior
- Cisco Jabber versión 9.7 o posterior

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problemas de inicio de sesión

Jabber no puede iniciar sesión mediante MRA

Este síntoma puede ser causado por una amplia gama de problemas, algunos de los cuales se describen aquí.

1. Registro de servicios perimetrales de colaboración (SRV) no creado o puerto 8443 inaccesible

Para que un cliente Jabber pueda iniciar sesión correctamente con MRA, se debe crear un registro SRV específico de Collaboration Edge y se debe poder acceder a él externamente. Cuando se inicia inicialmente un cliente Jabber, realiza consultas DNS SRV:

1. _cisco-uds: este registro SRV se utiliza para determinar si un servidor CUCM está disponible.

2. _cuplogin: este registro SRV se utiliza para determinar si un servidor IM&P está disponible.

3. _collab-edge: este registro SRV se utiliza para determinar si MRA está disponible.

Si el cliente Jabber se inicia y no recibe una respuesta SRV para _cisco-uds y _cuplogin y no recibe una respuesta para _collab-edge, entonces utiliza esta respuesta para intentar comunicarse con Expressway-E que aparece en la respuesta SRV.

El registro SRV _collab-edge apunta al nombre de dominio completamente calificado (FQDN) de Expressway-E con el puerto 8443. Si el SRV _collab-edge no se crea, o no está disponible externamente, o si está disponible, pero el puerto 8443 no es accesible, entonces el cliente Jabber no puede iniciar sesión.

Puede confirmar si el registro SRV _collab-edge se puede resolver y si el puerto TCP 8443 se puede alcanzar con el verificador SRV en Collaboration Solutions Analyzer (CSA).

Si el puerto 8443 no es accesible, es posible que se deba a que un dispositivo de seguridad (firewall) bloquee el puerto o a una configuración incorrecta de la puerta de enlace predeterminada (GW) o de las rutas estáticas en Exp-E.

2. Certificado inaceptable o no disponible en VCS Expressway

Una vez que el cliente Jabber ha recibido una respuesta para _collab-edge, se pone en contacto con Expressway con seguridad de la capa de transporte (TLS) a través del puerto 8443 para intentar recuperar el certificado de Expressway para configurar TLS para la comunicación entre el cliente Jabber y Expressway.

Si Expressway no tiene un certificado firmado válido que contenga el FQDN o el dominio de Expressway, esto falla y el cliente Jabber no puede iniciar sesión.

Si se produce este problema, use la herramienta de solicitud de firma de certificado (CSR) en Expressway, que incluye automáticamente el FQDN de Expressway como nombre alternativo de sujeto (SAN).

Nota: MRA requiere comunicación segura entre Expressway-C y Expressway-E, y entre Expressway-E y los terminales externos.

La siguiente tabla con los requisitos de certificado de Expressway por función se puede encontrar en la Guía de implementación de MRA:

Table 1. CSR Alternative Name Element and Unified Communications Features

Add These Items as Subject Alternative Names	When Generating a CSR for These Purposes			
	Mobile and Remote Sccess	Jabber guest	XMPP Federation	Business to Business Calls
Unified CM registrations domains (despite their name, these have more in common with service discovery domains than with Unified CM Unified CM SIP registration domains)	Required on Expressway-E only	–	–	–
XMPP federation domains	–	–	Required on Expressway-E only	–
IM and Presence Service chat node aliases (federated group chat)	–	–	Required	–
Unified CM phone security profile names	Required on Expressway-C only	–	–	–
(Clustered systems only) Expressway cluster name	Required on Expressway-C only	Required on Expressway-C only	Required on Expressway-C only	

3. No se encontraron servidores UDS en la configuración perimetral

Una vez que el cliente Jabber establece correctamente una conexión segura con Expressway-E, solicita su configuración de extremo (get_edge_config). Esta configuración de borde contiene los registros SRV para _cuplogin y _cisco-uds. Si los registros SRV _cisco-uds no se devuelven en la configuración de borde, el cliente Jabber no puede continuar con el inicio de sesión.

Para solucionar esto, asegúrese de que los registros _cisco-uds SRV se crean internamente y que Expressway-C puede resolverlos.

Puede encontrar más información sobre los registros DNS SRV en la Guía de implementación de MRA para X8.11.

Este también es un síntoma común si se encuentra en un dominio dual. Si se ejecuta en un dominio dual y encuentra que el cliente Jabber no devuelve ningún servicio de datos de usuario (UDS), debe confirmar que los registros SRV _cisco-uds se crean en el DNS interno con el dominio externo.

Nota: después de la versión X12.5 de Expressway, ya no es necesario agregar un registro SRV _cisco-UDS al DNS interno. Para obtener más información sobre esta mejora, consulte la Guía de implementación de Mobile and Remote Access Through Cisco Expressway (X12.5).

---

4. Los registros de Expressway-C muestran este error: XCP_JABBERD Detail=No se puede

conectar al host '%IP%', puerto 7400:(111) Conexión rechazada

Si el controlador de interfaz de red (NIC) de Expressway-E no está configurado correctamente, puede que el servidor de la plataforma de comunicaciones extensible (XCP) no se actualice. Si Expressway-E cumple estos criterios, probablemente tenga este problema:

1. Utiliza una única NIC.
2. Se ha instalado Advanced Networking Option Key.
3. La opción Use Dual Network Interfaces está establecida en Yes.

Para corregir este problema, cambie la opción Use Dual Network Interfaces a No.

La razón por la que esto es un problema es que Expressway-E escucha la sesión XCP en la interfaz de red incorrecta, lo que hace que la conexión falle o se agote el tiempo de espera. Expressway-E escucha en el puerto TCP 7400 la sesión XCP. Puede verificar esto si utiliza el comando netstat del VCS como root.

5. El nombre de host/nombre de dominio del servidor de Expressway-E no coincide con lo configurado en el SRV _collab-edge

Si el nombre de host/dominio del servidor de Expressway-E en la configuración de la página DNS no coincide con lo que se recibió en la respuesta SRV _collab-edge, el cliente Jabber no puede comunicarse con Expressway-E. El cliente Jabber utiliza el elemento xmppEdgeServer/Address de la respuesta get_edge_config para establecer la conexión XMPP a Expressway-E.

Este es un ejemplo de cómo se ve el xmppEdgeServer/Address en la respuesta get_edge_config de Expressway-E al cliente Jabber:

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

Para evitar esto, asegúrese de que el registro SRV _collab-edge coincida con el nombre de host/dominio de Expressway-E. El ID de bug de Cisco CSCuo83458 se ha archivado para esto y se ha agregado soporte parcial en el ID de bug de Cisco CSCuo82526.

6. No se puede iniciar sesión debido a una suscripción actual a WebEx Connect

Los registros de Jabber para Windows muestran lo siguiente:

```
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://URL server;
Url: http://example URL server';;;.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://example URL server2014-11-22
19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStoreManager.cpp(286)]
[ConfigStoreManager] [ConfigStoreManager::storeValue] - key : [last_cas_lookup_url]
value : [http://example URL server/cas/FederatedSSO?org=example URL]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://website URL/cas/FederatedSSO?org=example URL]
success: [true] configStoreName: [LocalFileConfigStore]
```

Los intentos de inicio de sesión se dirigen a WebEx Connect.

Para obtener una resolución permanente, debe ponerse en contacto con WebEx para que se clausure el sitio.

Solución Aternativa

A corto plazo, puede utilizar una de estas opciones para excluirla de la búsqueda.

- Agregue este parámetro al archivo jabber-config.xml. A continuación, cargue el archivo jabber-config.xml en el servidor TFTP de CUCM. Requiere que el cliente inicie sesión internamente primero.

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

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

Nota: la segunda opción no funciona para dispositivos móviles.

- Cree una URL en la que se pueda hacer clic y que excluya el servicio WEBEX: ciscojabber://provision?ServiceDiscoveryExcludedServices=WEBEX

Puede encontrar más detalles sobre la detección de servicios de UC y cómo excluir algunos servicios en Implementación in situ para Cisco Jabber 12.8.

7. El servidor de Expressway-C muestra el mensaje de error: "Configurado pero con errores. Servidor de aprovisionamiento: esperando información del servidor transversal."

Si navega hasta Estado > Unified Communications y ve el mensaje de error "Configurado pero con errores. Servidor de aprovisionamiento: esperando información de servidor transversal." Para los registros de Unified CM y el servicio IM&P, los servidores DNS internos configurados en Expressway-C tienen dos registros A de DNS para Expressway-E. La razón detrás de varios registros A de DNS para Expressway-E podría ser que el usuario afectado se movió de una sola NIC con NAT estática habilitada en Expressway-E a NIC dual con NAT estática habilitada, o viceversa, y olvidó eliminar el registro A de DNS adecuado en los servidores DNS internos. Por lo tanto, cuando utiliza la utilidad de búsqueda de DNS en Expressway-C y resuelve el FQDN de Expressway-E, observa dos registros A de DNS.

Solución

Si la NIC de Expressway-E está configurada para una sola NIC con NAT estática:

1. Elimine el registro A de DNS para la dirección IP interna de Expressway-E en los servidores DNS configurados en Expressway-C.
2. Vaciar la memoria caché de DNS en Expressway-C y el equipo del usuario a través de CMD (ipconfig /flushdns).
3. Reinicie el servidor de Expressway-C.

Si la NIC de Expressway-E está configurada para NIC dual con NAT estática habilitada:

1. Elimine el registro A de DNS de la dirección IP externa de Expressway-E en los servidores DNS configurados en Expressway-C.
2. Vaciar la memoria caché de DNS en Expressway-C y el equipo del usuario mediante CMD (ipconfig /flushdns).
3. Reinicie el servidor de Expressway-C.,

8. Microsoft DirectAccess instalado

Si utiliza Microsoft DirectAccess en el mismo equipo que el cliente Jabber, cuando intente iniciar sesión de forma remota, esto puede interrumpir MRA. DirectAccess obliga a las consultas DNS a tunelizarse en la red interna como si el equipo usara una VPN.

Nota: Microsoft DirectAccess no es compatible con Jabber sobre MRA. Cualquier solución de problemas es lo mejor. La configuración de DirectAccess es responsabilidad del administrador de la red.

En ocasiones, puede bloquear correctamente todos los registros DNS de la tabla de directivas de resolución de nombres de Microsoft DirectAccess. DirectAccess no procesa estos registros (Jabber debe poder resolverlos mediante DNS público con MRA):

- registro SRV para _cisco-uds
- registro SRV para _cuplogin
- Registro SRV para _collab-edge
- Un registro para todos los Expressway Es

9. Fallos de búsquedas de DNS inverso de Expressway

A partir de la versión X8.8, Expressway/VCS requiere que se creen entradas de DNS directo e inverso para ExpE, ExpC y todos los nodos de CUCM.

Para conocer los requisitos completos, consulte Prerrequisitos y dependencias de software en las Notas de la versión x8.8 y Registros DNS para acceso móvil y remoto.

Si no hay registros DNS internos, existe un posible error en los registros de Expressway que hacen referencia a reverseDNSLookup:

2016-07-30T13:58:11.102-06:00 hostname XCP_JABBERD[20026]: UTCTime="2016-07-30 19:58:11,102" ThreadID="139882696623872" Module="Jabber" Level="WARN " CodeLocation="cvsservice.cpp:409" Detail="caught exception: exception in reverseDNSLookup: reverse DNS lookup failed for address=x.x.x.x"

Expressway-C solo recibe un FQDN al consultar el registro PTR para la IP de Expressway-E. Si recibe un FQDN incorrecto de DNS, muestra esta línea en los registros y falla:

2020-04-03T17:48:43.685-04:00 hostname XCP_JABBERD[10043]: UTCTime="2020-04-03 21:48:43,685" ThreadID="140028119959296" Module="Jabber" Level="WARN " CodeLocation="cvsservice.cpp:601" Detail="Certificate verification failed for host=xx.xx.xx.xx, additional info: Invalid Hostname"

Problemas de registro

Softphone no se puede registrar, método SIP/2.0 405 no permitido

Un registro de diagnóstico de Expressway-C muestra un mensaje SIP/2.0 405 Method Not Allowed en respuesta a la solicitud de registro enviada por el cliente Jabber. Probablemente, esto se debe a un enlace troncal de protocolo de inicio de sesión (SIP) actual entre Expressway-C y CUCM con el puerto 5060/5061.

<#root>

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 SIP en el perfil de seguridad del troncal SIP que se aplica al troncal SIP actual configurado en CUCM y la zona vecina de Expressway-C para CUCM a un puerto diferente como 5065. Esto se explica con más detalle en este vídeo. Este es un resumen de la configuración:

CUCM

1. Cree un nuevo perfil de seguridad de troncal SIP con un puerto de escucha distinto de 5060 (5065).
2. Cree un troncal SIP asociado al perfil de seguridad del troncal SIP y al destino configurado en la dirección IP de Expressway-C, puerto 5060.

Expressway-C

1. Cree una zona vecina a CUCM con un puerto de destino distinto de 5060 (5065) para que coincida con la configuración de CUCM.
2. En Expressway-C Settings > Protocols > SIP, asegúrese de que Expressway-C aún escucha en 5060 para SIP.

Softphone no se puede registrar, Motivo="Dominio desconocido"

Un registro de diagnóstico de Expressway-C muestra Event="**Registration Rejected" Reason="Unknown domain**" Service="SIP" Src-ip="XXX.XXX.XXX" Src-port="51601" Protocol="TCP" AOR="sip:XXX.XXX.XXX.XXX".

Para corregir este problema, verifique estos puntos:

- ¿Utiliza el cliente Jabber un perfil de seguridad de dispositivo seguro en CUCM cuando se pretende no utilizar un perfil de seguridad de dispositivo no seguro?

- Si los clientes Jabber utilizan un perfil de seguridad de dispositivo seguro, ¿el nombre del perfil de seguridad está en formato FQDN y el nombre FQDN está configurado en el certificado de Expressway-C como SAN?

- Si los clientes de Jabber utilizan un perfil de seguridad de dispositivo seguro, navegue hasta System > Enterprise Parameters > Security Parameters > Cluster Security Mode y verifique que el modo de seguridad de clúster esté configurado en 1 para verificar que el clúster de CUCM ha sido protegido. Si el valor es 0, el administrador debe seguir el procedimiento

documentado para proteger el clúster.

Softphone no se puede registrar, motivo "Cuenta atrás para inactividad vencida"

Cuando revise los registros de Expressway-E durante el período de tiempo que el cliente Jabber envía en un mensaje REGISTER, busque el error "Idle Countdown expired" como se indica en el fragmento de código aquí.

<#root>

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-port="4211" Dst-ip=
"

VCS-E_IP

" Dst-port="

5061

" Detail="

TCP Connection Closed

" Reason="

```
Idle
countdown expired

"
```

Este fragmento de código indica que el firewall tiene el puerto 5061 abierto; sin embargo, no hay tráfico de capa de aplicación que se pase en un tiempo suficiente para que se cierre la conexión TCP.

Si se encuentra con esta situación, existe un alto grado de probabilidad de que el firewall que se encuentra frente a Expressway-E tenga activada la funcionalidad SIP Inspection/Application Layer Gateway (ALG). Para solucionar este problema, debe desactivar esta funcionalidad. Si no está seguro de cómo hacerlo, consulte la documentación del producto del proveedor del firewall.

Para obtener más información sobre SIP Inspection/ALG, puede consultar el Apéndice 4 de la Guía de implementación de configuración de Cisco Expressway-E y Expressway-C-Basic.

MRA falla debido a un proxy del teléfono configurado en el firmware

Un registro de diagnóstico de Expressway-E muestra un error de negociación de TLS en el puerto 5061; sin embargo, el intercambio de señales SSL se realizó correctamente en el puerto 8443.

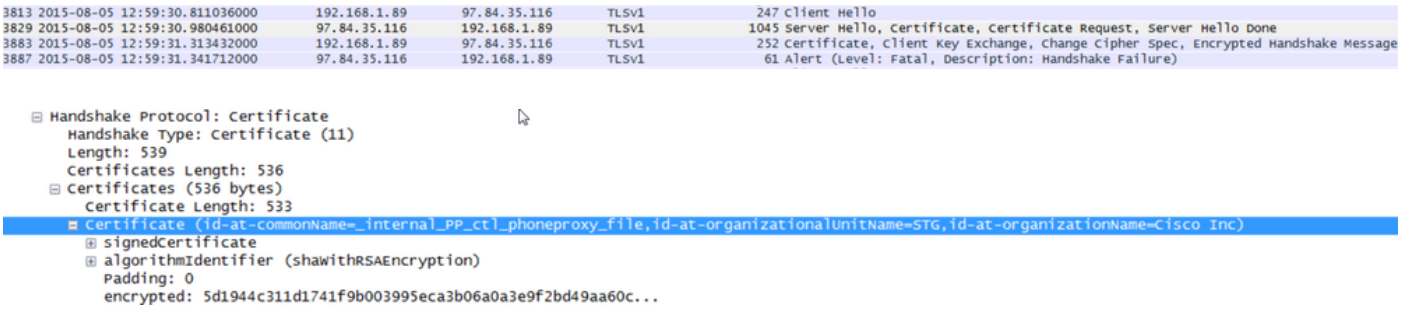
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,533" Module="network.tcp" Level="DEBUG": Src-port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connecting"
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,534" Module="network.tcp" Level="DEBUG": Src-port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connection Established"
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,535" Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(67)" Method="::TTSSLErrorOutput" Thread="0x7fae4ddb1700": TTSSL_continueHandshake: Failed to establish SSL connection
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,535" Module="network.tcp" Level="DEBUG": Src-port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connection Closed" Reason="Got EOF on socket"
2015-08-04T10:14:23-05:00 expe tvcs: Event="Inbound TLS Negotiation Error" Service="SIP" Src-port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="No SSL error available, probably remote disconnect" Protocol="TLS" Level="1" UTCTime="2015-08-04 15:14:23,535"

Registros de Jabber:

-- 2015-08-04 10:48:04.775 ERROR [ad95000] - [csf.cert.][checkIdentifiers] Verification of identity: 'URL address' failed.
-- 2015-08-04 10:48:04.777 INFO [ad95000] - [csf.cert][handlePlatformVerificationResultSynchronously] Verification result : FAILURE reason : [CN_NO_MATCH UNKNOWN]
-- 2015-08-04 10:48:05.284 WARNING [ad95000] - [csf.ecc.handyiron][ssl_state_callback] SSL alert read:fatal:handshake failure
type=eSIP, isRelevant=true, server=URL server name:5061, connectionState=eFailed, isEncrypted=true, failureReason=eTLSFailure, SSLErrorCode=336151568
type=eSIP, isRelevant=true, server=192.168.102.253:5060, connectionState=eFailed, isEncrypted=false, failureReason=eFailedToConnect, serverType=ePrimary, role=eNone
-- 2015-08-04 10:48:05.287 ERROR [ad95000] - [csf.ecc.handyiron][secSSLIsConnected] SSL_do_handshake() returned : SSL_ERROR_SSL.

La captura de paquetes de Jabber muestra una negociación SSL con la IP de Expressway E; sin

embargo, el certificado enviado no proviene de este servidor:



El firmware tiene configurado el proxy de teléfono.

Solución:

Confirme que el firmware ejecute Phone Proxy. Para verificar eso, ingrese el **show run policy-map** comando y le mostrará algo similar a:

```
class sec_sip
inspect sip phone-proxy ASA-phone-proxy
```

Deshabilite el proxy de teléfono para que los servicios del teléfono se conecten correctamente.

Problemas relacionados con la llamada

Sin medios cuando llama a través de MRA

Estas son algunas de las configuraciones ausentes e incorrectas que pueden causar este problema en las implementaciones de NIC única y doble:

- La NAT estática no se configura en Expressway-E en System > Network Interfaces > IP. La NAT en la capa de red todavía debe realizarse en el firewall, pero esta configuración traduce la IP en la capa de aplicación.
- Los puertos TCP/UDP no están abiertos en el firewall. Para obtener una lista de puertos, consulte la Guía de configuración de uso de puertos IP de Cisco Expressway.

No se recomienda una sola NIC con implementaciones NAT estáticas. A continuación, se incluyen algunas consideraciones para evitar problemas con los medios:

- En la zona transversal de UC, Expressway-C debe señalar a la dirección IP pública configurada en Expressway-E.
- Los medios deben "horquilla" o reflejarse en el firewall externo. Puede encontrar un ejemplo de configuración con un firewall Cisco ASA en Configure NAT Reflection On The ASA For The VCS Expressway TelePresence Devices.

Puede encontrar más información sobre esto en el Apéndice 4 de la Guía de implementación de

la configuración básica de Cisco Expressway-E y Expressway-C.

No hay recepción de llamada cuando la llamada pasa por MRA a PSTN

Este problema se debe a una limitación de Expressways anterior a la versión X8.5. El Id. de error de Cisco CSCua72781 describe cómo Expressway-C no reenvía medios tempranos en 183 Session Progress o 180 Ringing a través de la zona transversal. Si ejecuta las versiones X8.1.x o X8.2.x, puede actualizar a la versión X8.5 o, alternativamente, realizar la solución alternativa enumerada aquí.

Es posible utilizar una solución alternativa en Cisco Unified Border Element (CUBE) si crea un perfil SIP que convierte el 183 en un 180 y lo aplica en el dial-peer entrante. Por ejemplo:

```
voice class sip-profiles 11
response 183 sip-header SIP-StatusLine modify "SIP/2.0 183 Session Progress"
"SIP/2.0 180 Ringing"
```

Posteriormente, desactivarían 180 Early Media en el perfil SIP de CUCM > CUBE o en el propio CUBE dentro del modo de configuración sip-ua.

```
disable-early-media 180
```

Problemas de CUCM e IM&P

Error de ASCII que impide la adición de CUCM

Al agregar CUCM a Expressway-C, se produce un error ASCII que impide la adición de CUCM.

Cuando Expressway-C agrega CUCM a su base de datos, se ejecuta a través de una serie de consultas AXL relacionadas con las funciones get y list. Algunos ejemplos son getCallManager, listCallManager, listProcessNode, listProcessNodeService y getCCMVersion. Después de ejecutar el proceso getCallManager, un conjunto ExecuteSQLQuery lo ejecuta correctamente para recuperar todas las relaciones de confianza de CUCM Call Manager o tomcat.

Una vez que CUCM recibe la consulta y se ejecuta en ella, CUCM devuelve todos sus certificados. Si uno de los certificados contiene un carácter que no es ASCII, Expressway genera un error en la interfaz web similar a "ascii codec cannot decode byte 0xc3 in position 42487: ordinal not in range(128)".

Este problema se rastrea con el ID de bug Cisco CSCuo54489 y se resuelve en la versión X8.2.

Errores de TLS salientes en 5061 de Expressway-C a CUCM en implementaciones

seguras

Este problema ocurre cuando utiliza certificados autofirmados en CUCM y Tomcat.pem/CallManager.pem tienen el mismo asunto. El problema se resuelve con el ID de bug de Cisco CSCun30200. La solución alternativa para corregir el problema es eliminar tomcat.pem y deshabilitar la verificación de TLS de la configuración de CUCM en Expressway-C.

No se agregó el servidor IM&P y se encontraron errores

Al agregar un servidor de IM&P, Expressway-C informa de que "este servidor no es un servidor de IM&P" o de que "no se puede comunicar con el error HTTP de consulta .AXL "HTTPError:500"', lo que hace que no se agregue el servidor de IM&P.

Como parte de la adición de un servidor IM&P, Expressway-C utiliza una consulta AXL para buscar los certificados IM&P en un directorio explícito. Debido al Id. de bug Cisco CSCul05131, los certificados no están en ese almacén; por lo tanto, se encuentra el error falso.

Problemas varios

El estado del correo de voz en el cliente Jabber muestra "No conectado"

Para que el estado del correo de voz del cliente Jabber se conecte correctamente, debe configurar la dirección IP o el nombre de host de Cisco Unity Connection en la lista de permitidos HTTP en Expressway-C.

Para completar esto desde Expressway-C, realice el procedimiento pertinente:

Procedimiento para las versiones X8.1 y X8.2

1. Haga clic en Configuration > Unified Communications > Configuration > Configure HTTP server allow list.
2. Haga clic en New > Enter IP/Hostname > Create entry.
3. Cierre la sesión del cliente Jabber y vuelva a iniciarla.

Procedimiento para la versión X8.5

1. Haga clic en Configuration > Unified Communications > Unity Connection Servers.
2. Haga clic en New > Enter IP/Hostname, User account credentials > Add Address.
3. Cierre la sesión del cliente Jabber y vuelva a iniciarla.

Las fotografías de los contactos no aparecen en los clientes de Jabber a través de Expressways

La solución Mobile & Remote Access sólo utiliza UDS para la resolución de fotos de contacto. Para ello, es necesario disponer de un servidor web para almacenar las fotografías. La configuración en sí es doble.

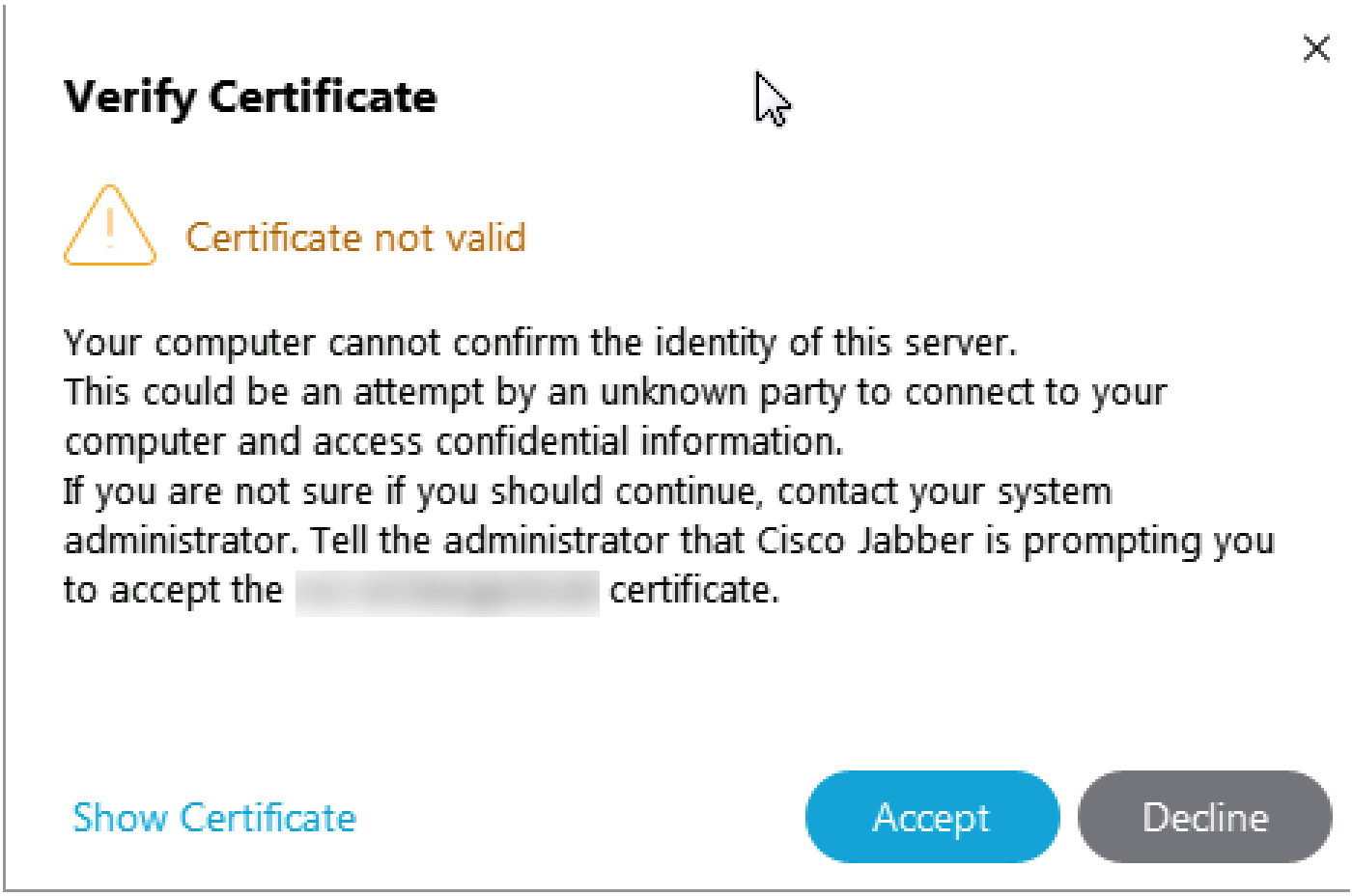
1. El archivo jabber-config.xml debe modificarse para dirigir a los clientes al servidor web para la resolución de fotografías de contacto. La configuración aquí lo logra.

```
<Directory>
<DirectoryServerType>UDS</DirectoryServerType>
<PhotoUriWithToken>http://%IP/Hostname%/photo%%uid%%.jpg<
/PhotoUriWithToken>
<UdsServer>%IP%</UdsServer>
<MinimumCharacterQuery>3</MinimumCharacterQuery>
</Directory>
```

2. 1. Haga clic en Configuration > Unified Communications > Configuration > Configure HTTP server allow list.
   2. Haga clic en New > Enter IP/Hostname > Create entry.
   3. Cierre la sesión del cliente Jabber y, a continuación, vuelva a iniciarla.Expressway-C debe tener el servidor web en la lista de permitidos del servidor HTTP.

Nota: para obtener más información sobre la resolución de la foto de contacto de UDS, consulte la documentación de la foto de contacto de Jabber.

Se solicita a los clientes de Jabber que acepten el certificado de Expressway-E durante el inicio de sesión



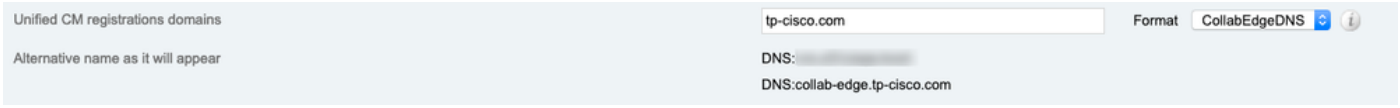
Este mensaje de error puede estar relacionado con el certificado de Expressway Edge no firmado por una CA pública en la que confía el dispositivo cliente o que el dominio está ausente como SAN en el certificado del servidor.

Para detener el cliente Jabber de la solicitud de aceptación del certificado de Expressway, debe cumplir con los dos criterios que se enumeran a continuación:

- El dispositivo o equipo que ejecuta el cliente Jabber debe tener el firmante del certificado de Expressway-E en su almacén de confianza de certificados.

> Nota: Esto se logra fácilmente si utiliza una autoridad de certificación pública porque los dispositivos móviles contienen un gran almacén de certificados de confianza.

- El dominio de registro de Unified CM utilizado para el registro collab-edge debe estar presente en la SAN del certificado de Expressway-E. La herramienta CSR del servidor de Expressway le ofrece la opción de agregar el dominio de registro de Unified CM como una SAN; se carga previamente si el dominio está configurado para MRA. Si la CA que firma el certificado no acepta un dominio como SAN, también puede utilizar la opción "CollabEdgeDNS", que agrega el prefijo "collab-edge" al dominio:



Información Relacionada

- Guía de acceso móvil y remoto en Expressways
- Guía de creación y uso de certificados de Cisco Expressway
- Uso de puertos IP de Cisco TelePresence Video Communication Server (Cisco VCS) para firewall transversal
- Guía de implementación e instalación de Cisco Jabber
- Soporte Técnico y Documentación - Cisco Systems

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).