

Solucionar problemas más comunes para las llamadas interempresariales mediante Expressway

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problemas comunes](#)

[1. Error "// SIP/SIPTcp/wait_SdlReadRsp: Se omite el mensaje de gran tamaño. Solo se permiten hasta 5000 bytes. Se restablece la conexión".](#)

[2. Los flujos de medios se detienen si otro servidor de llamadas transfiere la llamada.](#)

[3. El dominio de nivel superior no está configurado en CUCM.](#)

[4. El certificado CUCM debe tener el atributo de autenticación de cliente aplicado.](#)

[5. Problemas de interacción.](#)

[6. No se envió el mensaje ACK que se recibió de CUCM a VCS-E/Expressway-E.](#)

[7. CUCM interrumpe la sesión TCP para llamadas entrantes](#)

[8. VCS no puede resolver los FQDN correctamente o no puede consultar los registros de SRV.](#)

[Información Relacionada](#)

Introducción

Este documento describe los problemas más comunes en la implementación interempresarial (B2B). Cómo solucionar problemas de llamadas B2B con Expressways.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Expressway-C (Exp-C)
- Expressway-E
- Cisco Unified Call Manager (CUCM)
- Servidor-C de comunicación por video (VCS-C) de TelePresence

Componentes Utilizados

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

- Expressway C y E X8.1.1 o posterior
- Unified Communications Manager (CUCM) 10.0 o posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problemas comunes

1. Error "/ / SIP/SIPTcp/wait_SdlReadRsp: Se omite el mensaje de gran tamaño. Solo se permiten hasta 5000 bytes. Se restablece la conexión".

Las llamadas de los TelePresence endpoints registradas en VCS, entrantes a CUCM en un protocolo SIP (Session Initiation Protocol) troncal, provocan el error "/ / SIP/SIPTcp/wait_SdlReadRsp: Se omite el mensaje de gran tamaño. Solo se permiten hasta 5000 bytes. Se restablece la conexión".

La configuración de enrutamiento de llamada en Expressway-C/VCS-C es correcta; se envía la llamada a CUCM. Se envía un mensaje de invitación de SIP a CUCM, pero en los registros de SDL hay no hay mensajes SIP. Este error puede verse en los registros de SDL:

```
"|ApplInfo |SIPTcp: se omite un mensaje grande de xxx.xxx.xxx.xxx:[27469]. Solo se permiten hasta 5000 bytes. Se restablece la conexión".
```

En CUCM 8.6 y versiones anteriores el valor predeterminado del tamaño máximo de mensaje SIP entrante era de 5000; a partir de la versión CUCM 9.X, esto se cambió a 11000. Sin embargo, la actualización de la versión 8 o anterior a la versión 9 o 10 mantendrá el valor predeterminado de la versión anterior del software (5000).

Solución


Este problema está relacionado con el error [CSCts00642](#)

Aumente el parámetro de servicio avanzado de CUCM **Tamaño máximo de mensajes SIP entrantes del valor predeterminado de 5000 a un tamaño adecuado para estos tipos de llamadas.** 11000 parece ser un buen valor para la mayoría de las posibles situaciones con los clientes.

En la **página de administración de CUCM**, vaya a los parámetros de servicio y **seleccione su servidor de CUCM y el servicio CallManager:**

Save Set to Default Advanced

- Status

 Status: Ready

- Select Server and Service

Server*

Service*

All parameters apply only to the current server except parameters that are in the cluster-wide group(s).

Seleccione la opción **Avanzadas** y busque **Tamaño máximo de mensaje SIP entrante**:

SIP Max Incoming Message Size *	<input type="text" value="11000"/>	11000
SIP Max Incoming Message Headers *	<input type="text" value="100"/>	100

2. Los flujos de medios se detienen si otro servidor de llamadas transfiere la llamada.

Esto puede suceder en las llamadas de acceso remoto y móvil (MRA) y de B2B.

Puede no provocar ningún sonido unidireccional o un zumbido (mismo sonido que al tratar de reproducir una captura con audio cifrado) después de transferir la llamada. Esto sucede porque en la configuración de llamadas se ha seleccionado un conjunto de cifrado que no es compatible con el terminal al que se transfiere.

Puede comparar la negociación de SIP antes y después de transferir la llamada. En la primera negociación de los registros de VCS o CUCM se pueden ver las líneas cifradas en el mensaje 200 OK de VCS:

```
m=audio 54582 RTP/SAVP 9 96 97 0 8 18 101
a=rtpmap:9 G722/8000
a=rtpmap:96 G7221/16000
a=fmtp:96 bitrate=32000
a=rtpmap:97 G7221/16000
a=fmtp:97 bitrate=24000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:ckXijkT3CcVY+xlOf3ozX/TjHPz05OzEdY49rAHA|2^48
a=sendrecv
a=rtcp:54583 IN IP4 10.1.1.201.7
m=video 54658 RTP/SAVP 96 97
b=TIAS:4000000
a=rtpmap:96 H264/90000
a=fmtp:96 profile-level-id=42e01e;max-fs=1621;packetization-mode=1;max-rcmd-nalu-size=32000;level-asymmetry-allowed=1
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42e01e;max-fs=1621;packetization-mode=0;level-asymmetry-allowed=1
```

```
a=rtcp-fb:* nack pli
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:S8BJvGB/216F7XP8izXxId443Xd9f27oUI/4gxSt|2^48
```

Las líneas cifradas se aceptan en la primera llamada, pero en la segunda llamada verá que el mensaje ACK elimina las líneas cifradas:

```
m=audio 24826 RTP/AVP 0
c=IN IP4 10.1.231.30
a=ptime:20
a=rtpmap:0 PCMU/8000
m=video 0 RTP/AVP 126
c=IN IP4 10.1.98.80
b=TIAS:448000
a=label:11
a=rtpmap:126 H264/90000
a=fmtp:126 profile-level-id=42E01F;packetization-mode=1;max-fs=3601;max-rcmd-nalu-size=32000;level-asymmetry-allowed=1
a=content:main
```

VCS intenta usar las líneas cifradas negociadas al principio, incluso si el terminal al que se transfiere la llamada no admite el cifrado.

Solución

Este problema está relacionado con el error [CSCuv11790](#)

Actualice VCS/Expressway a la versión x8.6.1 para solucionar este problema.

3. El dominio de nivel superior no está configurado en CUCM.

Si no se configura el parámetro de la empresa de dominio de nivel superior, CUCM enruta las llamadas entrantes a su propio dominio y se usan los patrones de enrutamiento SIP. Esto podría provocar un bucle, porque lo más probable es que la llamada se envíe de vuelta a Exp-C, o también puede fallar debido al error "404: no encontrado".

Solución

En la página de administración de CUCM, vaya a **Sistema > Parámetros de la empresa para cambiar esta configuración**

Clusterwide Domain Configuration	
Organization Top Level Domain	<input type="text"/>
Cluster Fully Qualified Domain Name	<input type="text"/>

4. El certificado CUCM debe tener el atributo de autenticación de cliente aplicado.

Cuando se establece una conexión segura entre Exp-C y CUCM (comprobación de TLS activada), el intercambio de señales SSL se inicia por un servidor de llamadas determinado que depende de la dirección de la llamada. Esto significa que ambos servidores deben tener autenticación de cliente y servidor en sus certificados. Este error se ve en los registros de VCS/Expressway si el atributo no está presente:

```
Line 190: 2015-05-07T07:34:01-04:00 XXXXXXXXXXXXXXXXXXXX tvcs: UTCTime="2015-05-07 11:34:01,060"
Module="network.tcp" Level="DEBUG": Src-ip="10.50.47.16" Src-port="45215" Dst-ip="10.50.47.51"
Dst-port="5061" Detail="TCP Connecting"
Line 239: 2015-05-07T07:34:01-04:00 XXXXXXXXXXXXXXXXXXXX tvcs: UTCTime="2015-05-07 11:34:01,071"
Module="network.tcp" Level="DEBUG": Src-ip="10.50.47.16" Src-port="45215" Dst-ip="10.50.47.51"
Dst-port="5061" Detail="TCP Connection Established"
Line 249: 2015-05-07T07:34:01-04:00 XXXXXXXXXXXXXXXXXXXX tvcs: UTCTime="2015-05-07 11:34:01,081"
Module="network.tcp" Level="DEBUG": Src-ip="10.50.47.16" Src-port="45215" Dst-ip="10.50.47.51"
Dst-port="5061" Detail="TCP Connection Closed" Reason="no certificate returned"
```

Solución

Puede encontrar información sobre cómo configurar una plantilla con los atributos de cliente y el servidor web en la guía de certificado VCS

http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-7/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-7.pdf

5. Problemas de interacción.

La versión X8.6.x de VCS/Expressway tuvo algunos problemas con el proceso de interconexión.

Errores relacionados con el problema:

El defecto [CSCuw85626 se puede detectar si busca en los registros de diagnóstico de VCS/Expressway líneas m de video rechazadas:](#)

Este mensajes de error se muestra cuando se negocian las líneas de medios en la parte de TCS del flujo de H323.

índice de línea de medios: 1

rechazado: true, dirección: SDP_MEDIA_DIR_SENDRECV

type: video/SDP_MF_AU_VID

El defecto [CSCuw85715 es similar, pero en este caso, los registros de VCS/Expressway especifican que la causa es dataTypeNotSupported:](#)

```
2015-10-29T09:49:00+04:00 XXXXXXXXXXXXXXXXXXXX tvcs: UTCTime="2015-10-29 05:49:00,197"
Module="network.h323" Level="INFO": Action="Sent" Dst-ip="XXXXXXXXXXXXXXXXXXXX" Dst-port="49162"
Detail="Sending H.245 OpenLogicalChannelRejResponse "
2015-10-29T09:49:00+04:00 XXXXXXXXXXXXXXXXXXXX tvcs: UTCTime="2015-10-29 05:49:00,197"
Module="network.h323" Level="DEBUG": Dst-ip="XXXXXXXXXXXXXXXXXXXX" Dst-port="49162"
Sending H.245 PDU:
value MultimediaSystemControlMessage ::= response : openLogicalChannelReject :
{
forwardLogicalChannelNumber 3,
cause dataTypeNotSupported : NULL
}
```

Solución

Actualización a X8.7 o posterior.

6. No se envió el mensaje ACK que se recibió de CUCM a VCS-E/Expressway-E.

Esto suele aparecer cuando la zona transversal configurada no apunta a la dirección IP correcta de VCS Expressway/Expressway-E.

En las implementaciones de NIC simples (en Expressway/perímetro), la zona de cliente transversal del control/núcleo es debe apuntar a la dirección IP pública del servidor transversal.

En las implementaciones de NIC duales, el cliente transversal debe apuntar a la dirección IP interna (el NIC interno suele ser LAN1, pero puede ser LAN2) del servidor transversal. Tenga en cuenta que se trata de la dirección IP interna de la LAN interna.

Solución

Consulte el apéndice 4 de la [Configuración básica de Cisco VCS Expressway y VCS Control para obtener más información y consultar un diagrama de las distintas implementaciones de red.](#)

7. CUCM interrumpe la sesión TCP para llamadas entrantes

Cuando las llamadas se reenvían desde el núcleo de VCS Control/Expressway, CUCM puede rechazar esto e interrumpir la sesión de TCP.

Esto puede ocurrir cuando el puerto entre la zona vecina y el perfil de seguridad del troncal SIP no coincide o está configurado para ser 5060/5061.

MRA usa una comunicación en línea, mientras que las llamadas de B2B usan una comunicación troncal, CUCM tiene una limitación que no permite que las comunicaciones en línea y troncales pasen por el mismo puerto. Como MRA principalmente se configura automáticamente, las implementaciones de B2B deben usar un puerto diferente.


Solución

Para ello, el puerto de destino configurado en la zona vecina a CUCM (en VCS-C/Expressway-C) debe ser distinto que 5060/5061, normalmente se usa 5065, pero se pueden usar otros; el puerto configurado debe coincidir con el puerto configurado en el perfil de seguridad del troncal SIP asignado al troncal SIP de este servidor en CUCM.

En la **página de administración de CUCM**, vaya a Dispositivo > Troncal.

Perfil de seguridad del troncal SIP con puerto 5065.

Status

 Status: Ready

SIP Trunk Security Profile Information

Name*

Description

Device Security Mode

Incoming Transport Type*

Outgoing Transport Type

Enable Digest Authentication

Nonce Validity Time (mins)*

X.509 Subject Name

Incoming Port*

El puerto de destino de troncal SIP puede ser 5060/5061, como se muestra en la imagen.

SIP Information

Destination

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	<input type="text" value="14.80.86.72"/>	<input type="text"/>	<input type="text" value="5060"/>

El puerto SIP de la zona vecina a VCS/Expressway debe coincidir con el puerto configurado en el perfil de seguridad del troncal SIP, como se muestra en la imagen.

En la página **Administración de Expressway**, vaya a **Configuración > Protocolos > SIP**

SIP

Mode

Port *

Transport

Accept proxied registrations

Media encryption mode

ICE support

Preloaded SIP routes support

El VCS no tiene esta limitación o no corresponde a esta situación; esto significa que se puede configurar el troncal SIP mismo con 5060/5061.

8. VCS no puede resolver los FQDN correctamente o no puede consultar los registros de SRV.

Para las llamadas de B2B que se originaron en CUCM, puede producirse un problema debido a la forma en que CUCM maneja y enruta las llamadas.

Cuando CUCM reenvía las llamadas a los servidores VCS, CUCM tiende a agregar :5060 o :5061 (depende de la configuración) al final del URI marcado (es decir, test@lab.local >> test@lab.local:5060) cuando alcanza la expressway y alcanza una regla de búsqueda hacia la zona DNS, el VCS no consulta el registro SRV, sino que sólo consulta para A o AAAA. registros. Puede confirmar esto en los registros de diagnóstico de VCS/Expressway.

Solución

Para resolver este problema, cree una transformación que elimine el puerto al final (en cualquier servidor, no importa en cuál) antes de que llegue a la zona de DNS.

En la **página de administración de Expressway**, navegue a **Configuración > Plan de marcación > Transformación y configuración > Plan de marcación > Transformar**

Ejemplos de transformaciones:

Create transform

Configuration

Priority: 1

Description:

Pattern type: Regex

Pattern string: *(?!.*@%localdomains%)(.*):(5060|5061)

Pattern behavior: Replace

Replace string: \\1

State: Enabled

Create transform

Configuration

Priority: 1

Description:

Pattern type: Regex

Pattern string: *(.*):(5060|5061)

Pattern behavior: Replace

Replace string: \\1

State: Enabled

Si por alguna razón no se puede crear una transformación, también puede realizarse con reglas de búsqueda, aunque se recomienda hacerlo con transformaciones.

En la **página de administración de Expressway**, vaya a **Configuración > Plan de marcación > Transformación y configuración > Plan de marcación > Reglas de búsqueda**

Información Relacionada

- [Cisco VCS Expressway y VCS Control: configuración básica](#)