Configuración de Cisco Meeting Server y Skype Empresarial

Contenido

Introducción

Este documento describe cómo configurar Cisco Meeting Server (CMS) CallBridge Cluster con Skype for Business como complemento de las guías oficiales. Este documento proporciona un ejemplo de un CallBridge único y otro ejemplo de un clúster de tres CallBridge, pero se pueden agregar CallBridges adicionales según sea necesario. También se admite un clúster de dos CallBridge.

Colaborado por Rogelio Galindo y editado por Viridiana Fuentes, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

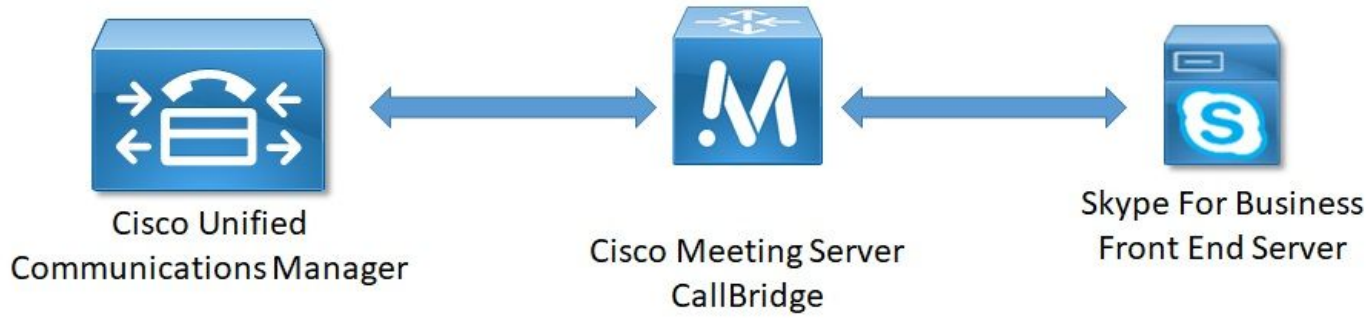
- Cisco Meeting Server (CMS)
- Servidor de nombres de dominio (DNS)
- Skype Empresarial
- Interfaz de programación de aplicaciones (API)

> **Nota**: La guía de configuración se puede encontrar aquí: https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Deployment_Guide/Version-2-2/Cisco-Meeting-Server-2-2-Scalable-and-Resilient-Deployments.pdf

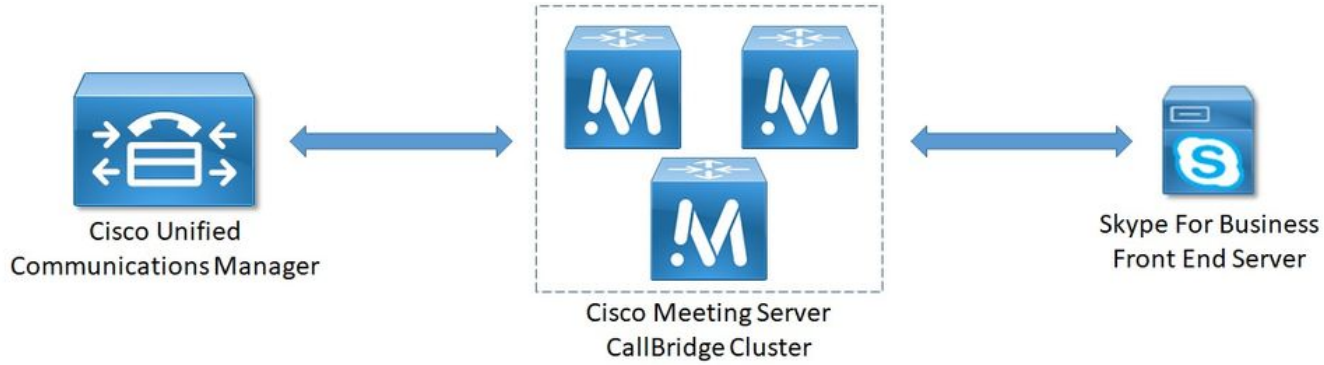
Componentes Utilizados

- 3 servidores CMS que ejecutan un clúster CallBridge, versión de software 2.2.2.
- Skype Empresarial 2015
- Active Directory (AD) Windows Server 2012
- Cliente Secure Shell (SSH)
- Cliente de protocolo seguro de transferencia de archivos (SFTP) como WinSCP o similar
- Programa API como Postman o similar
- Sesión de Escritorio remoto para Active Directory, DNS y servidor Skype

Topología de la red - Single CallBridge



Topología de red - CallBridges agrupados



Requisitos de certificado de Callbridge - Single CallBridge

La tabla 1a proporciona un ejemplo del certificado CallBridge para un único entorno CallBridge.

Cuadro 1a

Certificados CallBridge	Descripción
CallBridge único	
CN:cms.uc.local	FQDN de CallBridge

Requisitos de certificado de Callbridge - CallBridges agrupados

La tabla 1b proporciona un ejemplo de los certificados CallBridge para un entorno CallBridge agrupado. Se puede compartir un único certificado en CallBridges en un clúster.

Tabla 1b

Certificados Callbridge	Descripción
Servidor 1: cms1.uc.local	
CN:cms.uc.local	FQDN de clúster de CallBridge. Este registro debe resolverse a todos los peers del clúster de CallBridge.
SAN:cms.uc.local	FQDN de clúster de CallBridge. Este registro debe resolverse a todos los peers del clúster de CallBridge.
SAN:cms1.uc.local	FQDN de CallBridge 1.
SAN:cms2.uc.local	FQDN de CallBridge 2.
SAN:cms3.uc.local	FQDN de CallBridge 3.
Servidor 2: cms2.uc.local	
CN:cms.uc.local	FQDN de clúster de CallBridge. Este registro debe resolverse a todos los peers del clúster de CallBridge.
SAN:cms.uc.local	FQDN de clúster de CallBridge. Este registro debe resolverse a todos los peers del clúster de CallBridge.
SAN:cms1.uc.local	FQDN de CallBridge 1.
SAN:cms2.uc.local	FQDN de CallBridge 2.
SAN:cms3.uc.local	FQDN de CallBridge 3.
Servidor 3: cms3.uc.local	
CN:cms.uc.local	FQDN de clúster de CallBridge. Este registro debe resolverse a todos los peers del clúster de CallBridge.
SAN:cms.uc.local	FQDN de clúster de CallBridge. Este registro debe resolverse a todos los peers del clúster de CallBridge.
SAN:cms1.uc.local	FQDN de CallBridge 1.

SAN:cms2.uc.local FQDN de CallBridge 2.
SAN:cms3.uc.local FQDN de CallBridge 3.

La CLI de CMS se puede utilizar para ver el contenido de un certificado:

```
cms1> pki inspect cmsuccluster.cer
Checking ssh public keys...not found
Checking user configured certificates and keys...found
File contains a PEM encoded certificate
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            60:00:00:00:21:db:36:e8:b9:0d:96:44:41:00:00:00:00:00:21
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=local, DC=uc, CN=DC-CA
        Validity
            Not Before: Mar 16 19:00:53 2018 GMT
            Not After : Mar 16 19:10:53 2020 GMT
        Subject: C=US, ST=NC, L=RTP, O=Systems, OU=Cisco, CN=CMS.UC.local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b8:41:69:d9:1d:47:ef:b1:23:70:ae:69:da:e3:
                    ff:12:f8:97:2b:ee:1e:c0:6c:66:e4:95:3f:8a:74:
                    4d:ec:fc:1e:0d:38:56:1b:00:5c:ce:6d:d3:68:13:
                    e4:9d:b6:e7:7d:de:c4:a4:f3:00:02:11:e5:33:06:
                    b4:f6:64:29:c3:77:62:a9:dc:9d:ad:a2:e9:c1:0b:
                    72:f4:18:af:df:d3:e3:f4:4a:5d:66:e5:e8:4f:63:
                    09:15:5f:8e:ec:df:86:fb:35:47:99:db:18:d1:b7:
                    40:4e:b6:b3:b6:66:28:8e:89:15:8b:cc:0f:e6:5c:
                    e6:2d:de:83:6c:f8:e3:46:49:97:a6:a9:0e:6d:b1:
                    65:08:8e:aa:fc:f0:ae:2f:c1:c2:cd:b6:4f:a5:eb:
                    29:32:9a:48:8c:86:6d:1e:3a:c2:22:70:a3:56:e9:
                    17:01:ef:3a:ce:bb:9f:04:47:e5:24:e0:16:ba:c0:
                    85:df:92:4d:51:d2:95:bf:84:f7:9a:2e:c0:31:e9:
                    9f:91:4f:4a:ce:2c:27:17:f8:ae:3e:96:4e:3b:0a:
                    15:1a:66:cf:e9:12:96:e1:17:ee:65:3c:04:7a:c0:
                    a0:b3:09:fd:3e:16:08:c6:0b:36:51:57:cb:d8:09:
                    a3:40:d0:2c:ae:d6:06:e0:8c:06:de:b7:ce:24:83:
                    28:69
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:CMS.UC.local, DNS:CMS.UC.local, DNS:CMS1.UC.local, DNS:CMS2.UC.local,
DNS:CMS3.UC.local
            X509v3 Subject Key Identifier:
                FE:EF:64:D6:85:7A:62:C5:CA:7B:64:10:B7:F9:E7:18:1D:65:0B:70
            X509v3 Authority Key Identifier:
                keyid:B5:FC:2D:1E:7F:D9:3E:68:F4:B2:78:1F:F0:E8:B2:FC:80:7F:9C:E8

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:ldap:///CN=DC-
CA,CN=DC,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=uc,DC=local?certifica
teRevocationList?base?objectClass=cRLDistributionPoint

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=DC-
CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=uc,DC=local?cACertificate?b
```

```
ase?objectClass=certificationAuthority

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            1.3.6.1.4.1.311.21.7:
                0..&+.....7.....\..........A........N...O..d...
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            1.3.6.1.4.1.311.21.10:
                0.0
..+.......0
..+.......
    Signature Algorithm: sha256WithRSAEncryption
         83:31:16:15:74:41:98:e4:40:02:70:cc:6e:c0:53:15:8a:7a:
         8a:87:0a:aa:c8:99:ff:5b:23:e4:8b:ce:dd:c0:61:9c:06:b4:
         3d:22:91:b6:91:54:3a:99:8d:6e:db:18:27:ef:f7:5e:60:e6:
         48:a2:dd:d5:85:1d:85:55:79:e0:64:1a:55:22:9e:39:0c:27:
         53:a4:d8:3f:54:fd:bc:f9:d4:6e:e1:dd:91:49:05:3e:65:59:
         6e:d4:cd:f6:de:90:cb:3d:b3:15:03:4b:b8:9d:41:f1:78:f5:
         d9:42:33:62:b5:18:4f:47:54:c9:fa:58:4b:88:aa:0d:f6:26:
         9b:fb:8f:98:b4:82:96:97:24:fe:02:5b:03:04:67:c2:9e:63:
         3d:02:ae:ef:92:a7:be:ad:ca:7e:4e:d2:1e:54:e6:bf:75:3b:
         72:32:7c:d6:78:3f:5e:b9:e6:43:bd:1c:74:20:46:57:1b:81:
         c2:4b:b4:fc:9f:cc:c9:63:a8:2d:fd:dd:09:3f:24:d6:ac:f7:
         7c:bd:26:80:a5:b4:d1:a7:c8:fb:3d:d4:a7:93:70:d1:5c:77:
         06:9e:1c:f8:6a:81:a5:97:91:e9:21:e9:7a:df:a3:64:ab:ed:
         15:c7:be:89:5f:1e:53:a7:b5:01:55:ab:a2:cd:8f:67:8d:14:
         83:bc:29:a1
cms1>
```

Tenga en cuenta los campos Asunto y Nombre alternativo del asunto X509v3. Estas serán extremadamente importantes más adelante cuando construyamos nuestras relaciones de confianza en el entorno de Microsoft.

```
        Subject: C=US, ST=NC, L=RTP, O=Systems, OU=Cisco, CN=CMS.UC.local

            X509v3 Subject Alternative Name:
                DNS:CMS.UC.local, DNS:CMS.UC.local, DNS:CMS1.UC.local, DNS:CMS2.UC.local,
DNS:CMS3.UC.local
```

> **Nota:** La guía de configuración de certificados se puede encontrar aquí: https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Deployment_Guide/Version-2-2/Certificate-Guidelines-Single-Split_Server-Deployment-2-2.pdf

Requisitos de registro DNS - Single CallBridge

La tabla 2a proporciona un ejemplo de cómo configurar el servidor DNS. Proporciona una explicación de lo que significa cada campo.

Cuadro 2a

Un registro	Ejemplo de IP	Descripción
cms.uc.local	10.10.10.1	Callbridge
fe.skype.local	10.10.10.5	Nombre de dominio completamente calificado (FQDN) de la parte frontal de Skype

Requisitos de registro DNS - CallBridges agrupados

La tabla 2b proporciona un ejemplo de cómo configurar el servidor DNS. Proporciona una explicación de lo que significa cada campo.

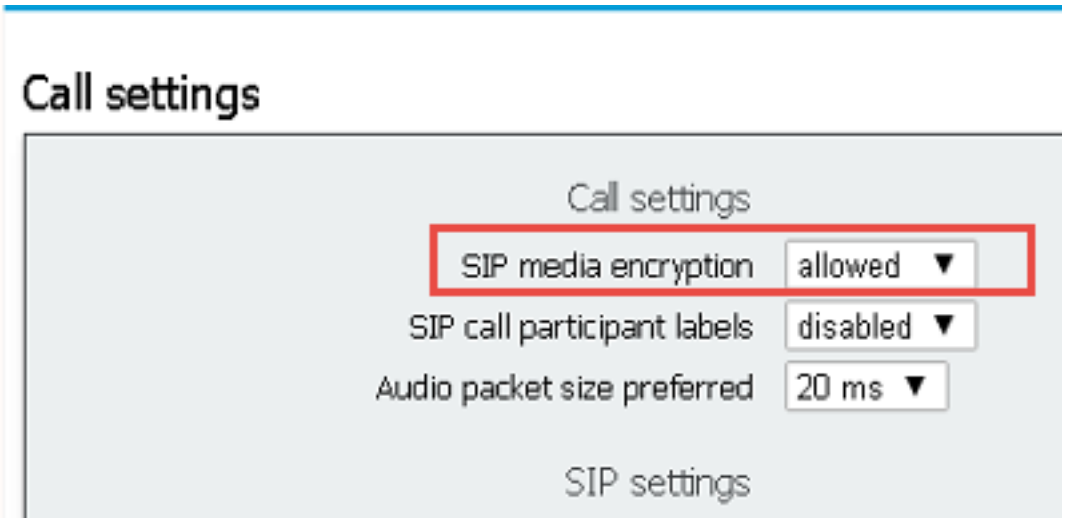
Cuadro 2b

Un registro	Ejemplo de IP	Descripción
cms1.uc.local	10.10.10.1	CallBridge 1
cms2.uc.local	10.10.10.2	CallBridge 2
cms3.uc.local	10.10.10.3	CallBridge 3
cms.uc.local	10.10.10.1 10.10.10.2 10.10.10.3	Un registro A que se resuelve en todos los CallBridges del clúster. Esto se denominará CallBridge Cluster Full Qualified Domain Name (FQDN)
fe.skype.local	10.10.10.5	Nombre de dominio completamente calificado (FQDN) de la parte frontal de Sky

Configuración

Cifrado de medios SIP

Vaya a **Configuración> Configuración de llamadas.** La encriptación de medios SIP se debe establecer en allowed (permitida).



Reglas entrantes

En la tabla 3 se describe el significado de cada campo de la configuración Llamadas entrantes: Coincidencia de llamadas.

Tabla 3

Campo de plan de marcación coincidente de llamada entrante	Descripción
Nombre de dominio	Si se recibe una llamada con este dominio, utilice la parte de usuario del URI p buscar coincidencias en los destinos habilitados.
Prioridad	Esto determina el orden en que se considerarán las reglas. Los números más se comprobarán primero. Los números más bajos se marcarán en último lugar
Espacios objetivo	Si se establece en yes: si la parte de usuario del URI coincide con un espacio, llamada se conectará a ese espacio.
Destina a los usuarios	Si se establece en yes: si la parte de usuario del URI coincide con un usuario CMA, la llamada intentará llamar a ese usuario.
IVR objetivo	Si se establece en yes: si la parte del usuario del URI coincide con un IVR configurado, la llamada se conectará a ese IVR.
Se dirige a Lync	Si se establece en yes: Si la parte de usuario del URI coincide con un número

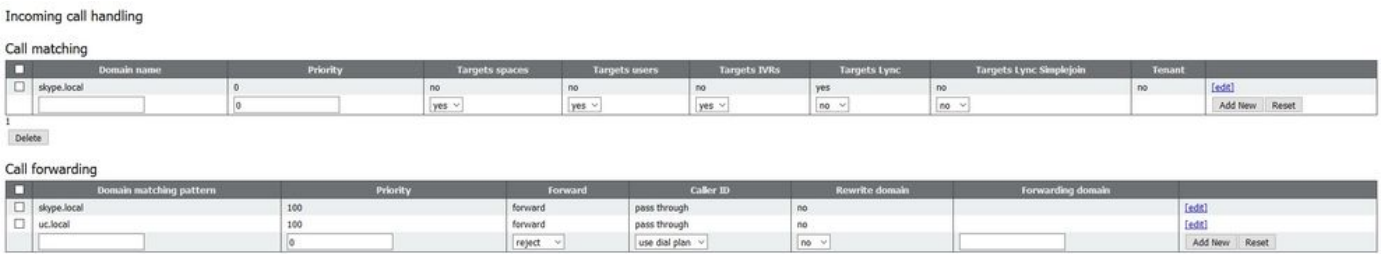
	marcación PSTN de una reunión de Skype Empresarial, conéctese a esa reun como una llamada de inicio doble.
Se dirige a Lync Simplejoin	Si se establece en yes: Convierta la parte de usuario del URI en un destino HT e intente encontrar una reunión de Office365 alojada en esa URL.
Arrendatario	Esto determina para qué arrendatarios se considerará esta regla.

En la tabla 4 se describe el significado de todos los campos de la configuración Llamadas entrantes: Reenvío de llamada.

Tabla 4

Campo de plan de marcación de reenvío de llamada entrante	Descripción
Patrón de coincidencia de dominios	Si se recibe una llamada con este dominio, reenvíe o rechace el dominio tal y c está configurado.
Prioridad	Esto determina el orden en que se considerarán las reglas. Los números más a se comprobarán primero. Los números más bajos se marcarán en último lugar.
Reenvío	Si se establece para reenviar la llamada, las reglas salientes se ocuparán de la misma. Si se establece para rechazar la llamada, se rechazará y no se reenviar Si se establece para pasar a través de la parte de origen del dominio se presion
ID de la persona que llama	Si se establece para utilizar el plan de marcación, la parte de la desde se reesc como se configuró en la regla de salida. Nota: El paso a través no se puede utilizar para reglas que coincidan con un do Lync/Skype si CallBridge está en un clúster. Esto interrumpiría la presentación llamadas de gateway.
Reescritura del dominio	Si está habilitado, cambie el dominio llamado al valor configurado en el campo dominio de reenvío.
Dominio de reenvío	Si se habilita el dominio de reescritura, el dominio llamado cambiará al valor de campo.

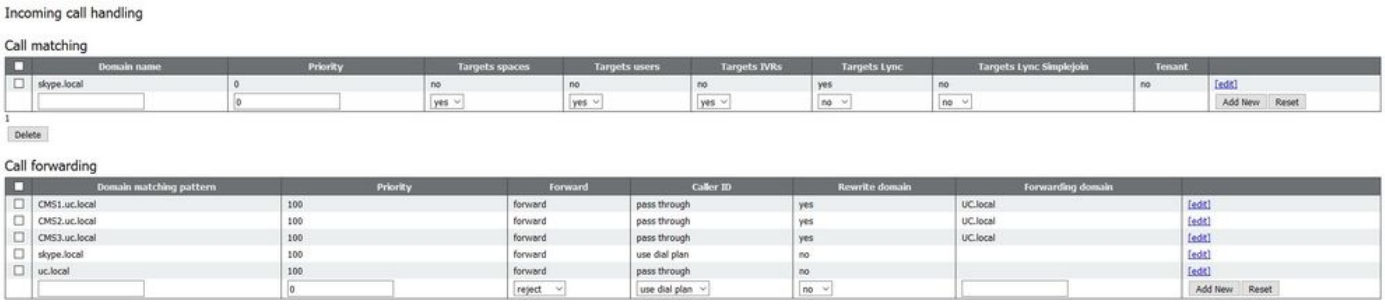
Ejemplo de configuración de reglas entrantes - Single CallBridge



En este entorno las cosas son notablemente simples. Dado que no utilizamos CallBridges agrupados, podemos configurar cada dominio para que utilice el paso como su ID de la persona que llama. Esto no se puede hacer en un entorno en clúster, ya que interrumpirá el uso compartido de presentaciones.

Además, hay una regla de coincidencia de llamadas para el dominio Skype.local con "Targets Lync" establecido en true. Esto significa que si llamamos a una reunión de Lync/Skype mediante el número de marcado de PSTN, deberíamos poder conectarnos como una llamada doméstica dual.

Ejemplo de configuración de reglas de entrada: CallBridges agrupados


Incoming call handling

Call matching

	Domain name	Priority	Targets spaces	Targets users	Targets IVRs	Targets Lync	Targets Lync Simplejoin	Tenant	
☐	skype.local	0	no	no	no	yes	no	no	[edit]
		0	yes	yes	yes	no	no		Add New Reset

1

Delete

Call forwarding

	Domain matching pattern	Priority	Forward	Caller ID	Rewrite domain	Forwarding domain	
☐	CMS1.uc.local	100	forward	pass through	yes	UC.local	[edit]
☐	CMS2.uc.local	100	forward	pass through	yes	UC.local	[edit]
☐	CMS3.uc.local	100	forward	pass through	yes	UC.local	[edit]
☐	skype.local	100	forward	use dial plan	no		[edit]
☐	uc.local	100	forward	pass through	no		[edit]
		0	reject	use dial plan	no		Add New Reset

En este entorno, estamos utilizando un clúster de CallBridge que consta de tres CallBridges. Debido a esto, necesitamos una regla de reenvío de llamadas para cada CallBridge configurado para reescribir el dominio en uc.local. Esto se debe a que cuando los usuarios de Lync/Skype devuelvan la llamada desde el entorno de UC, en realidad realizarán llamadas al dominio de cms1.uc.local, cms2.uc.local o cms3.uc.local. Desafortunadamente, se trata de una limitación de la configuración necesaria para que el contenido funcione en un entorno CallBridge agrupado. Necesitamos convertir esto de nuevo a uc.local antes de reenviar la llamada al proxy sip uc.local.

Además, hay una regla de coincidencia de llamadas para el dominio Skype.local con "Targets Lync" establecido en true. Esto significa que si llamamos a una reunión de Lync/Skype mediante el número de marcado de PSTN, deberíamos poder conectarnos como una llamada doméstica dual.

Reglas salientes

En la tabla 5 se describe el significado de cada campo de la configuración de llamadas salientes.

Tabla 5

Campo de plan de marcación saliente	Descripción
Dominio	Para llamadas a este dominio utilice esta regla de salida
Proxy SIP a utilizar	El proxy SIP al que se enviarán las llamadas para este dominio
Dominio de contacto local	Esto determina qué valor se colocará en el encabezado del contacto. Para la integración de Lync/Skype, este valor se debe establecer en el FQDN del CallBridge. Nota: Para cualquier regla saliente que utilice un proxy SIP de Lync/Skype, este campo DEBE configurarse. Para cualquier regla saliente que utilice un proxy SIP que no sea Lync/Skype, este campo NO DEBE configurarse.
Local del dominio	Esto determina qué valor se colocará en el encabezado from. Esta será la dirección de ID de la persona que llama que se ve en el proxy SIP. Si se deja en blanco, este campo utilizará el "dominio de contacto local" configurado. Lync/Skype lo utilizará como URI de destino para las devoluciones de llamadas y el uso compartido de presentaciones. Nota: Este valor no se utiliza si la llamada es una llamada de gateway y la regla de marcación entrante utilizada tiene la "ID de la persona que llama" establecida en passthrough.
Tipo de tronco	Esto determina qué variación de SIP se utilizará en la comunicación con el proxy SIP.
Comportamiento	Esto determina si continuaremos o no comprobando las reglas de prioridad baja o si dejaremos de buscar en caso de coincidencia cuando no pudimos completar la llamada.
Prioridad	Esto determina el orden en que se considerarán las reglas. Los números más altos se comprobarán primero. Los números más bajos se marcarán en último lugar.
Cifrado	Esto determina si utilizaremos SIP cifrado o no cifrado.
Arrendatario	Esto determina para qué arrendatarios se considerará esta regla.
Alcance del puente de llamada	Esto determina para qué CallBridges se considerará esta regla de marcado saliente. En CallBridges agrupados, esto es necesario para asegurarse de que se envía el dominio de contacto correcto desde cada CallBridge. Nota: Este valor sólo se puede establecer utilizando la API como se explica a continuación.

Ejemplo de configuración de llamadas salientes - Single CallBridge

Outbound calls

	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption	Tenant
☐	UC.local	cucm.uc.local		<use local contact domain>	Standard SIP	Stop	100	Encrypted	no
☐	skype.local	fe.skype.local	cms.uc.local	<use local contact domain>	Lync	Stop	100	Encrypted	no

De nuevo observamos que el entorno CallBridge único es considerablemente más sencillo que el entorno agrupado. Algo que vale la pena mencionar arriba es que tenemos un dominio de contacto especificado. Esto se debe a que si no especificamos el nombre de dominio completamente calificado de nuestro CallBridge, puesto que el dominio de contacto local Lync/Skype rechazará las llamadas por razones de seguridad. Dado que nuestras reglas de reenvío entrante están configuradas para utilizar el paso a través, en este ejemplo no reescribiremos el dominio de origen.

Ejemplo de configuración de llamadas salientes: CallBridges agrupados

Outbound calls

	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption	Tenant	Call Bridge Scope
☐	UC.local	cucm.uc.local		<use local contact domain>	Standard SIP	Stop	0	Encrypted	no	<all>
☐	skype.local	fe01.skype.local	CMS1.UC.local	<use local contact domain>	Lync	Stop	0	Encrypted	no	<local>
☐	skype.local	fe01.skype.local	CMS2.UC.local	<use local contact domain>	Lync	Stop	0	Encrypted	no	cms2.uc.local
☐	skype.local	fe01.skype.local	CMS3.UC.local	<use local contact domain>	Lync	Stop	0	Encrypted	no	cms3.uc.local

En este entorno, estamos utilizando un clúster de CallBridge que consta de tres CallBridges. Debido a esto, necesitamos una regla de salida para cada CallBridge cada una con diferentes dominios de contacto locales, locales de dominios y ámbitos. Solo se necesita una regla de salida para enrutar las llamadas de todos los CallBridges a Cisco Unified Communications Manager. Para establecer el alcance que necesitamos para utilizar la API.

Modificación del ámbito Utilizando la API - Solo CallBridges agrupados

Después de crear una regla de llamada saliente, el alcance se establecerá en <all> para esa regla. Esto significa que la regla saliente se utilizará en todos los CallBridges de un clúster. Para las reglas salientes que apuntan a Lync/Skype, necesitamos utilizar diferentes contactos y encabezados según en qué CallBridge nos encontramos. Para hacerlo, necesitamos crear una regla de salida diferente para cada CallBridge donde los campos de contacto/de coinciden con ese CallBridge. Mediante la API, debemos establecer el alcance de estas reglas de marcación saliente para que se procesen sólo en el CallBridge que coincida con esa regla.

Obtener una lista de todos los CallBridges del clúster

En un explorador, vaya a la página /callbridges de la API de CMS. Esto mostrará todos los CallBridges del clúster.

Ahora tengo los ID de todos mis CallBridges. Sus ID serán diferentes en su entorno. Puedo ver que si quiero hacer referencia a CallBridge cms1.uc.local debería usar el ID de e4ab61ea-b5b4-4face-ad4a-9979badea4e4.

Obtener una lista de todas las reglas de marcación saliente

A continuación, necesito buscar mis reglas salientes y obtener sus ID. En un explorador, vaya a la página /outbounddialplanrules de la API.

```
<outboundDialPlanRules total="4">
  <outboundDialPlanRule id="7c76b6c7-4c42-45b0-af47-796cb6737e4e">
    <domain>UC.local</domain>
    <priority>0</priority>
  </outboundDialPlanRule>
  <outboundDialPlanRule id="b8cf4056-7f56-43a5-b67b-861253d5ca32">
    <domain>skype.local</domain>
    <priority>0</priority>
  </outboundDialPlanRule>
  <outboundDialPlanRule id="4ae1d777-48b7-423b-a646-a329e1e822af">
    <domain>skype.local</domain>
    <priority>0</priority>
  </outboundDialPlanRule>
  <outboundDialPlanRule id="05f00293-50fd-4c17-9452-dec224b43430">
    <domain>skype.local</domain>
    <priority>0</priority>
  </outboundDialPlanRule>
</outboundDialPlanRules>
```

Ahora tengo las identificaciones de todas mis reglas, pero no puedo decir cuál es cuál. No nos importa la primera regla ya que es para UC.local y no necesitamos establecer un alcance para eso. Necesitamos saber qué regla es la que se aplica a las restantes reglas salientes de Skype.local. Así que, a partir de uno en uno, coincidiré los ID con los CallBridges.

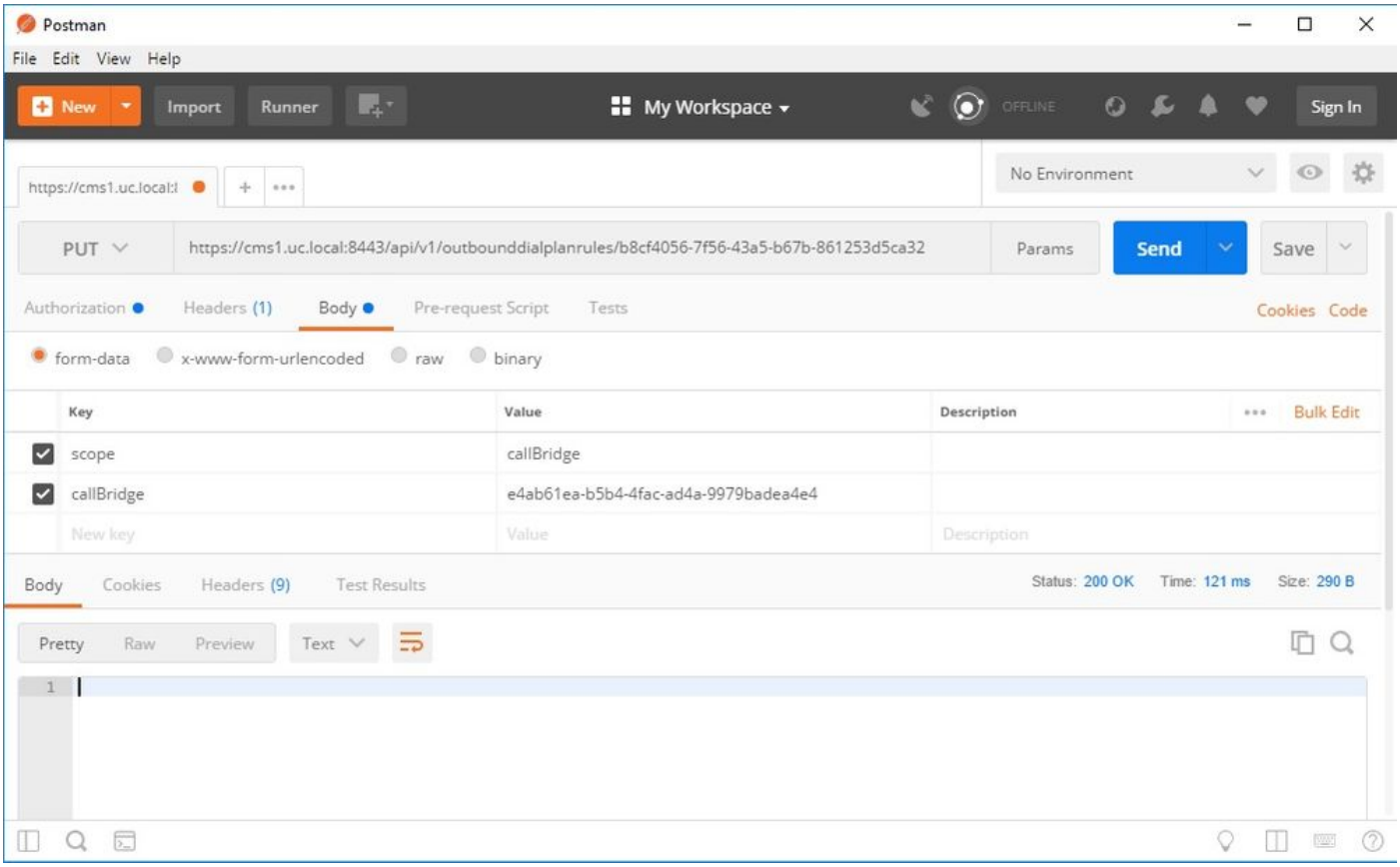
Navegaré a /outbounddialplanrules/b8cf4056-7f56-43a5-b67b-861253d5ca32 en mi navegador. Al leer el encabezado de contacto que se muestra allí, puedo decir que esta regla es para CMS1.UC.local. Por lo tanto, necesitamos establecer el alcance de esta regla en CMS1.UC.local.

PULSE el alcance de CallBridge en

Utilizando mi herramienta API favorita enviaré un PUT a la api en /outbounddialplanrules/b8cf4056-7f56-43a5-b67b-861253d5ca32 con el siguiente cuerpo:

```
scope: callBridge
callBridge: e4ab61ea-b5b4-4fac-ad4a-9979badea4e4
```

En esta captura de pantalla estoy usando PostMan para enviar esta solicitud.



Si este HTTP PUT se ha realizado correctamente, la página de reglas de marcación saliente de WebAdmin ahora debería reflejar un ámbito que se ha

aplicado. Si se ve desde el administrador web de CallBridge que el alcance se le aplicó, debe mostrar <local>. Si el administrador web de otro CallBridge se utiliza para ver las reglas de marcación saliente, debería mostrar el FQDN de CallBridge en el campo de alcance. Un alcance de <all> significa que la regla se utilizará en todos los CallBridges. Un alcance de <none> significa que se ha habilitado un alcance, pero ningún CallBridges coincide con el alcance.

Después de establecer el alcance de un CallBridge, debe configurarse para cada CallBridge adicional. Después de completar esta configuración, todas las reglas salientes para el dominio Skype deben tener un alcance.

Cuentas de servicio de CMS

En la página de configuración general de WebAdmin hay una sección de configuración de Lync Edge. Para utilizar los servicios TURN o unirse a las reuniones Dual Home a través del número de marcado PSTN, se debe configurar.

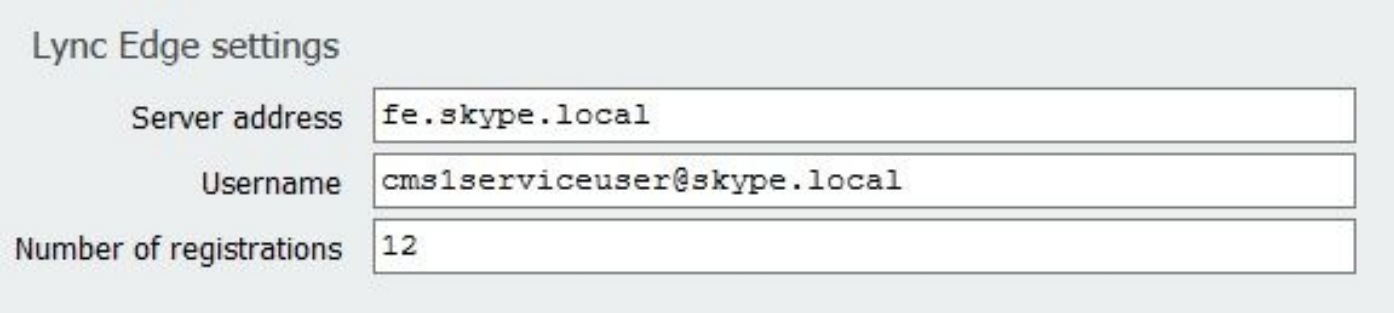
En la tabla 6 se describe el significado de todos los campos de la configuración de Lync Edge.

Tabla 6

campo Configuración de Lync Edge	Descripción
Dirección del servidor	Nombre de dominio completamente calificado (FQDN) de su grupo frontal
Nombre de usuario	El nombre de usuario de la cuenta de servicio que desea utilizar para CMS
Número de registros	¿Cuántas cuentas de usuario diferentes desea registrar? Si no se configura un valor aquí, sólo se registrará el nombre de usuario como se indica arriba. Si se aplica un número aquí, los números 1-X se aplicarán como sufijos a la parte de usuario del URI donde X es el número configurado en este campo.

Ejemplo de configuración de cuenta de servicio CMS

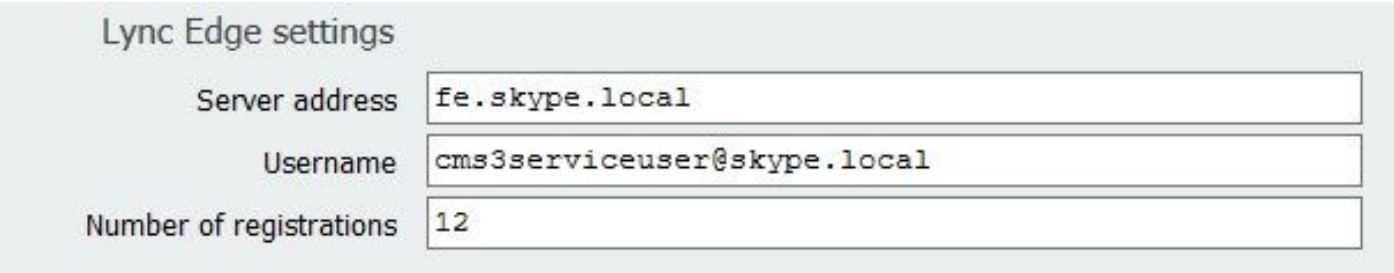
Configuración en CMS1:



Esta configuración registraría cms1serviceuser1@skype.local, cms1serviceuser2@skype.local, cms1serviceuser3@skype.local, ... cms1serviceuser11@skype.local y cms1serviceuser12@skype.local a fe.skype.local. Dado que en este ejemplo estoy en un entorno agrupado, también tendría que crear cuentas de servicio para mis otros CallBridges y configurarlas por separado. Tenga en cuenta que los nombres de usuario de este ejemplo son diferentes. En CMS1, los nombres de usuario tienen como prefijo cms1. En CMS2, los nombres de usuario tienen como prefijo cms2. En CMS3, el prefijo es cms3. Todas estas cuentas se realizaron y habilitaron en el entorno Skype for Business. Dado que nuestro grupo de aplicaciones de confianza está configurado con "Tratar como autenticado", no necesitamos proporcionar contraseñas para registrarse.

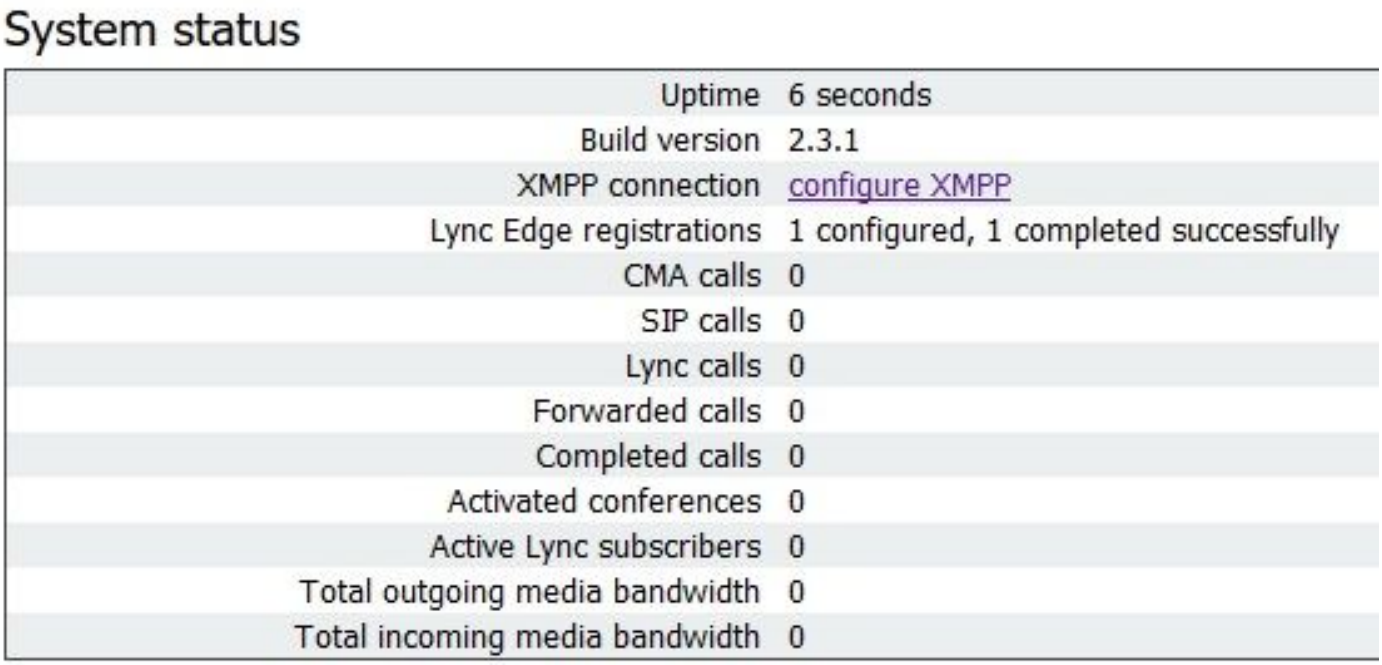
Configuración en CMS2:

Configuración en CMS3:



Verificación de las Cuentas de Servicio de CMS

La página de estado de CMS WebAdmin mostrará si los usuarios de Lync/Skype se han registrado correctamente. En el siguiente ejemplo, sólo configuramos un registro y se ha completado correctamente. Si observa que el estado muestra los registros en curso durante mucho tiempo, recopile los registros de SIP y DNS para determinar por qué se produce la falla.



Configuración de Lync/Skype

Aplique los siguientes comandos en el Shell de administración de Lync/Skype. Aplique los comandos en el servidor Front End.

> **Nota:** Los comandos sugeridos son para obtener orientación. En caso de que tenga dudas sobre la configuración del servidor Skype, deberá ponerse en contacto con el administrador de Lync/Skype o con el equipo de soporte.

CallBridge único

En primer lugar, tenemos que decirle a Skype que confíe en nuestro CallBridge. Para ello, agregamos un grupo de aplicaciones de confianza. En la terminología de Microsoft "Pool" solo significa "Cluster". En este escenario, nuestro clúster es sólo un clúster de un CallBridge. La identidad de nuestro clúster DEBE coincidir con el nombre común del certificado en uso en nuestro CallBridge. Microsoft utiliza esto como comprobación de seguridad. Tener la identidad en una SAN no es suficiente. Si el nombre común no coincide, Microsoft eliminará la conexión TCP. Al utilizar este comando, la identidad debe ser el FQDN de CallBridge. El Registrador debe ser el FQDN del grupo de servidores front-end que presta servicio a estas conexiones. El sitio debe ser el identificador del sitio de Lync/Skype. Si no está seguro de los valores que deben utilizarse para el registro o el sitio, póngase en contacto con el administrador de Lync/Skype.

```
New-CsTrustedApplicationPool -Identity CMS.UC.local -Registrar fe.skype.local -site 1 -RequiresReplication $false -
ThrottleAsServer $true -TreatAsAuthenticated $true
```

A continuación, el entorno de Microsoft debe configurarse para permitir la comunicación entrante desde nuestro CallBridge (grupo de aplicaciones de

confianza) en el puerto 5061.

```
New-CsTrustedApplication -ApplicationId AcanoApplication -TrustedApplicationPoolFqdn CMS.UC.local -Port 5061
```

El entorno de Microsoft está configurado actualmente para aceptar llamadas, pero no puede realizar llamadas de vuelta ni enviar presentaciones para llamadas de gateway. Para corregir esto, necesitamos agregar una ruta estática. En el escenario de CallBridge único, solo necesitamos una ruta única para permitir todas las llamadas a nuestro dominio local de UC. En los siguientes comandos, Destination es el FQDN del CallBridge al que queremos enviar solicitudes SIP. El campo MatchURI es la parte de dominio del URI que se debe utilizar. Tenga en cuenta que en un entorno Lync/Skype sólo se puede crear una ruta estática por MatchURI.

```
$x1=New-CsStaticRoute -TLSRoute -Destination "CMS.UC.local" -MatchUri "UC.local" -Port 5061 -UseDefaultCertificate $true Set-CsStaticRoutingConfiguration -Identity global -Route @{Add=$x1}
```

Por último, tenemos que decirle a Skype que implemente todos los cambios que acabamos de hacer.

```
Enable-CsTopology
```

CallBridges agrupados

En primer lugar, tenemos que decirle a Skype que confíe en nuestro clúster de CallBridge. Para ello, agregamos un grupo de aplicaciones de confianza. En la terminología de Microsoft "Pool" solo significa "Cluster". La identidad de nuestro clúster DEBE coincidir con el nombre común de los certificados en uso en nuestros CallBridge(s). Microsoft utiliza esto como comprobación de seguridad. Tener la identidad en una SAN no es suficiente. Si el nombre común no coincide, Microsoft eliminará la conexión TCP. Al utilizar este comando, la identidad debe ser el FQDN de CallBridge. ComputerFqdn debe ser el FQDN del primer CallBridge del clúster. Al especificar un ComputerFqdn, indica al entorno Lync/Skype que no se trata de un clúster con un solo servidor. El Registrador debe ser el FQDN del grupo de servidores front-end que presta servicio a estas conexiones. El sitio debe ser el identificador del sitio de Lync/Skype. Si no está seguro de los valores que deben utilizarse para el registro o el sitio, póngase en contacto con el administrador de Lync/Skype.

```
New-CsTrustedApplicationPool -Identity CMS.UC.local -ComputerFqdn CMS1.UC.local -Registrar fe.skype.local -site 1 -RequiresReplication $false -ThrottleAsServer $true -TreatAsAuthenticated $true
```

En este entorno, necesitamos agregar dos CallBridges como Equipos de aplicaciones de confianza. El primer CallBridge ya se agregó cuando creamos el grupo de aplicaciones de confianza anterior. Cuando agregamos estos ordenadores necesitamos asociarlos al conjunto que acabamos de crear. Esto indica a Skype que tenemos ordenadores adicionales en nuestro clúster de confianza. Todas las identidades de los equipos de aquí deben aparecer como SAN en nuestros certificados de CallBridge. Estas identidades también deben coincidir con los encabezados de contacto en las reglas de marcación saliente de CallBridges. Si no coinciden, Microsoft eliminará la conexión TCP.

```
New-CsTrustedApplicationComputer -Identity CMS2.UC.local -Pool CMS.UC.local New-CsTrustedApplicationComputer -Identity CMS3.UC.local -Pool CMS.UC.local
```

A continuación, se debe configurar el entorno de Microsoft para permitir la comunicación entrante desde nuestro clúster de CallBridge (grupo de aplicaciones de confianza) en el puerto 5061.

```
New-CsTrustedApplication -ApplicationId AcanoApplication -TrustedApplicationPoolFqdn CMS.UC.local -Port 5061
```

El entorno de Microsoft está configurado actualmente para aceptar llamadas, pero no puede realizar llamadas de vuelta ni enviar presentaciones para llamadas de gateway. Para corregir esto, necesitamos agregar rutas estáticas. En primer lugar, necesitamos agregar una ruta estática para permitir todas las llamadas a nuestro dominio local de UC. En los siguientes comandos, Destination es el FQDN del CallBridge al que queremos enviar solicitudes SIP. El campo MatchURI es la parte de dominio del URI que se debe utilizar. Tenga en cuenta que en un entorno Lync/Skype sólo se puede crear una ruta estática por MatchURI. Dado que el Destino es el FQDN de nuestro clúster de CallBridge y tiene un registro A DNS para cada miembro del clúster Lync/Skype puede enviar tráfico a todos nuestros CallBridges. Por lo tanto, si uno se desactiva, puede rutear automáticamente las solicitudes de nuestro dominio a otro CallBridge en el clúster.

```
$x1=New-CsStaticRoute -TLSRoute -Destination "CMS.UC.local" -MatchUri "UC.local" -Port 5061 -UseDefaultCertificate $true Set-CsStaticRoutingConfiguration -Identity global -Route @{Add=$x1}
```

A continuación, necesitamos crear una ruta estática adicional para cada CallBridge en el clúster. Se trata de un requisito para que la devolución de llamada y la presentación funcionen.

```
$x2=New-CsStaticRoute -TLSRoute -Destination "CMS1.UC.local" -MatchUri "CMS1.UC.local" -Port 5061 -UseDefaultCertificate $true Set-CsStaticRoutingConfiguration -Identity global -Route @{Add=$x2} $x3=New-CsStaticRoute -TLSRoute -Destination "CMS2.UC.local" -MatchUri "CMS2.UC.local" -Port 5061 -UseDefaultCertificate $true Set-CsStaticRoutingConfiguration -Identity global -Route @{Add=$x3} $x4=New-CsStaticRoute -TLSRoute -Destination "CMS3.UC.local" -MatchUri "CMS3.UC.local" -Port 5061 -UseDefaultCertificate $true Set-CsStaticRoutingConfiguration -Identity global -Route @{Add=$x4}
```

Por último, tenemos que decirle a Skype que implemente todos los cambios que acabamos de hacer.

Enable-CsTopology

Resolución de problemas

Recopilación de registros de CMS

El primer paso para diagnosticar cualquier problema es determinar dónde está el problema. Para ello, necesitamos analizar los registros de Cisco Meeting Server, pero primero debemos recopilarlos. Estas son mis recomendaciones personales sobre los registros que debo recopilar.

En primer lugar, habilite la depuración SIP y DNS para todos los CallBridges a través de la interfaz WebAdmin. Para ello, vaya a WebAdmin y, a continuación, a Logs > Detail Tracing. Desde aquí, active el registro de SIP y DNS durante los próximos treinta minutos. Este debería ser más que suficiente tiempo para detectar y diagnosticar el problema. Tenga en cuenta que esto debe hacerse de forma individual para todos los CallBridges, ya que la habilitación de registro no se comparte en un clúster.

En segundo lugar, habilite las capturas de paquetes en todos los CallBridges. Para realizar esta conexión mediante SSH a cada CallBridge y ejecutar el comando pcap <interface> donde <interface> es el tráfico de interfaz que debe utilizar. En la mayoría de los casos, será la interfaz a. Por lo tanto, el comando "pcap a" iniciaría una captura de paquetes en la interfaz a para el CallBridge al que estamos conectados.

Una vez que la captura de paquetes se está ejecutando en todas las interfaces, el siguiente paso es producir el problema. Siga adelante e intente una llamada o haga lo que sea que haya fallado. Después de que esto se complete, finalice todas las capturas de paquetes. Esto se puede hacer ingresando Ctrl-C en todas las ventanas SSH. Una vez completada la captura de paquetes, el nombre del archivo generado se escribirá en la pantalla. Realice un seguimiento de este nombre de archivo, ya que tendrá que descargarlo en el siguiente paso.

Por último, necesitamos recopilar los registros de CallBridges. Para realizar esta conexión mediante SFTP a cada CallBridge. Descargue el archivo logbundle.tar.gz y el archivo de captura de paquetes generado. Este archivo sólo está disponible en CMS2.2+. En las versiones 2.3+ de CMS, se incluirá la configuración completa de su CMS. Si está ejecutando la versión 2.2, no incluirá las reglas de entrada/salida, por lo que sería bueno realizar capturas de pantalla de esas páginas, así como de los parámetros de Lync Edge como referencia. Asegúrese de almacenar los registros/capturas de pantalla recopilados en carpetas separadas que tienen un nombre que coincida con el CallBridge del que se extrajeron los registros. Esto ayudará a asegurarse de que los registros no se mezclen.

Visualización de la configuración de Lync/Skype

Estos comandos resultarán extremadamente útiles a la hora de solucionar problemas de la configuración de Lync/Skype. En este documento se dan comandos para crear y ver la configuración, pero no se dan comandos para quitar la configuración. Esto se debe a que la eliminación de la configuración puede ser peligrosa a menos que los administradores lo realicen con un conocimiento completo del entorno de Lync/Skype. Si necesita eliminar la configuración, colabore con el administrador de Lync/Skype para hacerlo.

Comando	Descripción
Get-CsTrustedApplicationPool	Este comando enumera los clústeres (grupos) en los que Lync/Skype confía. La identidad de este conjunto DEBE coincidir con el nombre común de los certificados de CallBridge. Incluso en un único entorno CallBridge, se debe especificar aquí un clúster de CallBridge (conjunto) de uno.
Get-CsTrustedApplicationComputer	Este comando enumera los servidores con los que Lync/Skype confía y con los que se asocian estos servidores. Todos los ordenadores de aquí DEBEN identificarse en el certificado enviado por CallBridges. En un único entorno CallBridge, éste es normalmente el nombre común. En un entorno en clúster, estos ordenadores DEBEN aparecer como entradas de nombre alternativo del sujeto (SAN). Además, todos los ordenadores de aquí DEBEN ser identificados por las entradas de dominio de contacto locales en las reglas de marcación saliente de CallBridge.
Get-CsTrustedApplication	Este comando enumera con qué grupos de aplicaciones de confianza se pueden comunicar los servicios. Para la comunicación de CMS con Lync/Skype, utilizaremos el puerto TCP 5061 para el SIP cifrado de TLS.
Get-CsStaticRoutingConfiguration | Select-Object -ExpandirRuta de propiedades	Este comando enumera las rutas estáticas que Lync/Skype utiliza para reenviar solicitudes. El campo MatchURI es el dominio de destino del mensaje SIP. El campo "TLS Fqdn" en el XML debe

mostrar el servidor de destino para este tráfico.

Ejemplo de resultado de comandos Lync/Skype Get

A continuación se muestra el resultado de los comandos Lync/Skype Get anteriores ejecutados en el escenario del clúster de tres CallBridge que se describe en este documento

```
PS C:\Users\administrator.SKYPE> Get-CsTrustedApplicationPool


Identity             : TrustedApplicationPool:CMS.UC.local
Registrar            : Registrar:lyncpoolfe01.skype.local
FileStore            :
ThrottleAsServer     : True
TreatAsAuthenticated : True
OutboundOnly         : False
RequiresReplication  : False
AudioPortStart       :
AudioPortCount       : 0
AppSharingPortStart  :
AppSharingPortCount  : 0
VideoPortStart       :
VideoPortCount       : 0
Applications         : {urn:application:acanoapplication}
DependentServiceList : {}
ServiceId            : 1-ExternalServer-1
SiteId               : Site:RTP
PoolFqdn             : CMS.UC.local
Version              : 7
Role                 : TrustedApplicationPool



PS C:\Users\administrator.SKYPE> Get-CsTrustedApplicationComputer


Identity : CMS1.UC.local
Pool     : CMS.UC.local
Fqdn     : CMS1.UC.local

Identity : CMS2.UC.local
Pool     : CMS.UC.local
Fqdn     : CMS2.UC.local

Identity : CMS3.UC.local
Pool     : CMS.UC.local
Fqdn     : CMS3.UC.local



PS C:\Users\administrator.SKYPE> Get-CsTrustedApplication


Identity                   : CMS.UC.local/urn:application:acanoapplication
ComputerGruus              : {CMS1.UC.local
sip:CMS1.UC.local@skype.local;gruu;opaque=srvr:acanoapplication:GMqDXW_1rVCEMQi4qS6ZxwAA,
CMS2.UC.local

sip:CMS2.UC.local@skype.local;gruu;opaque=srvr:acanoapplication:_Z9CnV49LFufGDXjnFFi4gAA,
CMS3.UC.local
```

```
sip:CMS3.UC.local@skype.local;gruu;opaque=srvr:acanoapplication:dt8XJKciSlGhEeT62tyNogAA}
ServiceGruu                :
sip:CMS.UC.local@skype.local;gruu;opaque=srvr:acanoapplication:dQFM4E4YgV6J0rjuNgqxIgAA
Protocol                   : Mtls
ApplicationId              : urn:application:acanoapplication
TrustedApplicationPoolFqdn : CMS.UC.local
Port                       : 5061
LegacyApplicationName      : acanoapplication



PS C:\Users\administrator.SKYPE> Get-CsStaticRoutingConfiguration | Select-Object -
ExpandProperty Route


Transport              :
TransportChoice=Certificate=Microsoft.Rtc.Management.WritableConfig.Settings.SipProxy.UseDefault
Cert;Fqdn=CMS.UC.local;Port=5061
MatchUri               : UC.local
MatchOnlyPhoneUri      : False
Enabled                : True
ReplaceHostInRequestUri : False
Element                : <Route
xmlns="urn:schema:Microsoft.Rtc.Management.Settings.SipProxy.2008" MatchUri="UC.local"
MatchOnlyPhoneUri="false" Enabled="true" ReplaceHostInRequestUri="false">
                           <Transport Port="5061">
                             <TLS Fqdn="CMS.UC.local">
                               <UseDefaultCert />
                             </TLS>
                           </Transport>
                         </Route>

Transport              :
TransportChoice=Certificate=Microsoft.Rtc.Management.WritableConfig.Settings.SipProxy.UseDefault
Cert;Fqdn=CMS1.UC.local;Port=5061
MatchUri               : CMS1.UC.local
MatchOnlyPhoneUri      : False
Enabled                : True
ReplaceHostInRequestUri : False
Element                : <Route
xmlns="urn:schema:Microsoft.Rtc.Management.Settings.SipProxy.2008" MatchUri="CMS1.UC.local"
MatchOnlyPhoneUri="false" Enabled="true" ReplaceHostInRequestUri="false">
                           <Transport Port="5061">
                             <TLS Fqdn="CMS1.UC.local">
                               <UseDefaultCert />
                             </TLS>
                           </Transport>
                         </Route>

Transport              :
TransportChoice=Certificate=Microsoft.Rtc.Management.WritableConfig.Settings.SipProxy.UseDefault
Cert;Fqdn=CMS2.UC.local;Port=5061
MatchUri               : CMS2.UC.local
MatchOnlyPhoneUri      : False
Enabled                : True
ReplaceHostInRequestUri : False
Element                : <Route
xmlns="urn:schema:Microsoft.Rtc.Management.Settings.SipProxy.2008" MatchUri="CMS2.UC.local"
MatchOnlyPhoneUri="false" Enabled="true" ReplaceHostInRequestUri="false">
                           <Transport Port="5061">
                             <TLS Fqdn="CMS2.UC.local">
                               <UseDefaultCert />
                             </TLS>
                           </Transport>
```

```
                          </Route>

Transport               :
TransportChoice=Certificate=Microsoft.Rtc.Management.WritableConfig.Settings.SipProxy.UseDefault
Cert;Fqdn=CMS3.UC.local;Port=5061
MatchUri                : CMS3.UC.local
MatchOnlyPhoneUri       : False
Enabled                 : True
ReplaceHostInRequestUri : False
Element                 : <Route
xmlns="urn:schema:Microsoft.Rtc.Management.Settings.SipProxy.2008" MatchUri="CMS3.UC.local"
MatchOnlyPhoneUri="false" Enabled="true" ReplaceHostInRequestUri="false">
                            <Transport Port="5061">
                              <TLS Fqdn="CMS3.UC.local">
                                <UseDefaultCert />
                              </TLS>
                            </Transport>
                          </Route>



PS C:\Users\administrator.SKYPE>
```

Contacto con el TAC

Si detecta errores en esta implementación, póngase en contacto con el TAC de Cisco. Al abrir la solicitud de servicio, incluya un enlace a este documento. Ayudará a los ingenieros del TAC a comprender su configuración. Además, sería extremadamente útil que los registros de Cisco Meeting Server se adjunten al caso como se describe anteriormente y que se introduzca el resultado de todos los comandos Get de Lync/Skype Front End en las notas del caso. Si no incluye esta información, es seguro que será una de las primeras cosas que los ingenieros del TAC piden, así que por favor, continúe y recopile antes de abrir su caso.