

Configurar o Cisco Meeting Server e o Skype for Business

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Topologia de rede - CallBridge único](#)

[Topologia de rede - CallBridges em cluster](#)

[Requisitos do certificado Callbridge - Single CallBridge](#)

[Requisitos do certificado Callbridge - CallBridges em cluster](#)

[Requisitos de registro DNS - CallBridge único](#)

[Requisitos de registro DNS - CallBridges em cluster](#)

[Configuração](#)

[Criptografia de mídia SIP](#)

[Regras de entrada](#)

[Exemplo de configuração de regras de entrada - Single CallBridge](#)

[Exemplo de configuração de regras de entrada - CallBridges em cluster](#)

[Regras de saída](#)

[Exemplo de configuração de chamadas de saída - Single CallBridge](#)

[Exemplo de configuração de chamadas de saída - CallBridges em cluster](#)

[Modificando o escopo utilizando a API - somente CallBridges em cluster](#)

[OBTENHA uma lista de todas as CallBridges no cluster](#)

[OBTENHA uma lista de todas as regras de discagem de saída](#)

[COLOQUE o escopo do CallBridge em](#)

[Contas de serviço do CMS](#)

[Exemplo de configuração de conta de serviço CMS](#)

[Verificando contas de serviço do CMS](#)

[Configuração do Lync/Skype](#)

[CallBridge único](#)

[CallBridges em cluster](#)

[Troubleshooting](#)

[Coleta de logs do CMS](#)

[Exibição da Configuração do Lync/Skype](#)

[Exemplo de saída dos comandos Lync/Skype Get](#)

[Entrando em contato com o TAC](#)

Introduction

Este documento descreve como configurar o Cisco Meeting Server (CMS) CallBridge Cluster com Skype for Business como um complemento dos guias oficiais. Este documento fornece um exemplo de um único CallBridge e outro exemplo de um cluster de três CallBridge, mas CallBridges adicionais podem ser adicionados conforme necessário. Também há suporte para dois clusters CallBridge.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Meeting Server (CMS)
- Servidor de Nomes de Domínio (DNS)
- Skype Para Empresas
- Interface de programação de aplicativos (API)

Nota: O guia de configuração pode ser encontrado aqui:

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

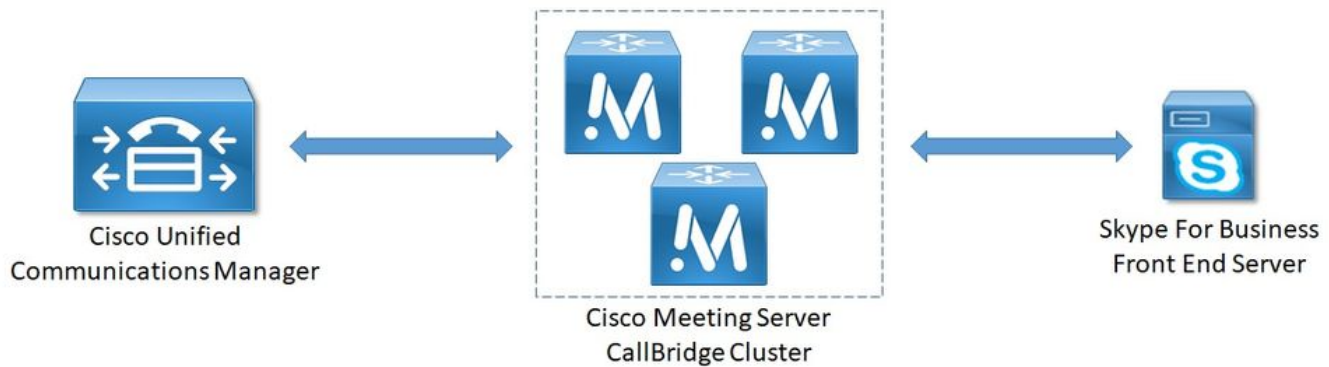
Componentes Utilizados

- 3 servidores CMS executando um cluster CallBridge, versão de software 2.2.2.
- Skype para Empresas 2015
- Windows Server 2012 do Ative Directory (AD)
- Cliente Secure Shell (SSH)
- Cliente Secure File Transfer Protocol (SFTP) como WinSCP ou similar
- Programa de API, como Postman ou similar
- sessão de Área de Trabalho Remota para servidor Ative Directory, DNS e Skype

Topologia de rede - CallBridge único



Topologia de rede - CallBridges em cluster



Requisitos do certificado Callbridge - Single CallBridge

A Tabela 1a fornece um exemplo do certificado CallBridge para um único ambiente CallBridge.

Quadro 1a

Certificados CallBridge Descrição

CallBridge único

CN:cms.uc.local FQDN do CallBridge

Requisitos do certificado Callbridge - CallBridges em cluster

A Tabela 1b fornece um exemplo dos certificados CallBridge para um ambiente CallBridge em cluster. Um único certificado pode ser compartilhado pelas CallBridges em um cluster.

Quadro 1b

Certificados Callbridge Descrição

Servidor 1:

cms1.uc.local

CN:cms.uc.local

FQDN do cluster do CallBridge. Esse registro deve ser resolvido para todos os peers de cluster do CallBridge.

SAN:cms.uc.local

FQDN do cluster do CallBridge. Esse registro deve ser resolvido para todos os peers de cluster do CallBridge.

SAN:cms1.uc.local

FQDN do CallBridge 1.

SAN:cms2.uc.local

FQDN do CallBridge 2.

SAN:cms3.uc.local

FQDN do CallBridge 3.

Servidor 2:

cms2.uc.local

CN:cms.uc.local

FQDN do cluster do CallBridge. Esse registro deve ser resolvido para todos os peers de cluster do CallBridge.

SAN:cms.uc.local

FQDN do cluster do CallBridge. Esse registro deve ser resolvido para todos os peers de cluster do CallBridge.

SAN:cms1.uc.local

FQDN do CallBridge 1.

SAN:cms2.uc.local

FQDN do CallBridge 2.

SAN:cms3.uc.local

FQDN do CallBridge 3.

Servidor 3:

cms3.uc.local

CN:cms.uc.local

FQDN do cluster do CallBridge. Esse registro deve ser resolvido para todos os peers de cluster do CallBridge.

SAN:cms.uc.local

FQDN do cluster do CallBridge. Esse registro deve ser resolvido para todos os peers de cluster do CallBridge.

SAN:cms1.uc.local

FQDN do CallBridge 1.

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

A CLI do CMS pode ser usada para exibir o conteúdo de um 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>

Anotar os campos Subject (Assunto) e X509v3 Subject Alternative Name (Nome alternativo do assunto X509v3). Estes serão extremamente importantes mais tarde quando criarmos as nossas relações de confiança no ambiente 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
```

Note: O guia de configuração do certificado pode ser encontrado aqui:

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 - CallBridge único

A Tabela 2a fornece um exemplo de como configurar o servidor DNS. Ele fornece uma explicação do que cada campo significa.

Quadro 2a

Um registro	Exemplo de IP	Descrição
cms.uc.local	10.10.10.1	Callbridge
fe.skype.local	10.10.10.5	Nome de domínio totalmente qualificado (FQDN) do front-end do Skype

Requisitos de registro DNS - CallBridges em cluster

A Tabela 2b fornece um exemplo de como configurar o servidor DNS. Ele fornece uma explicação do que cada campo significa.

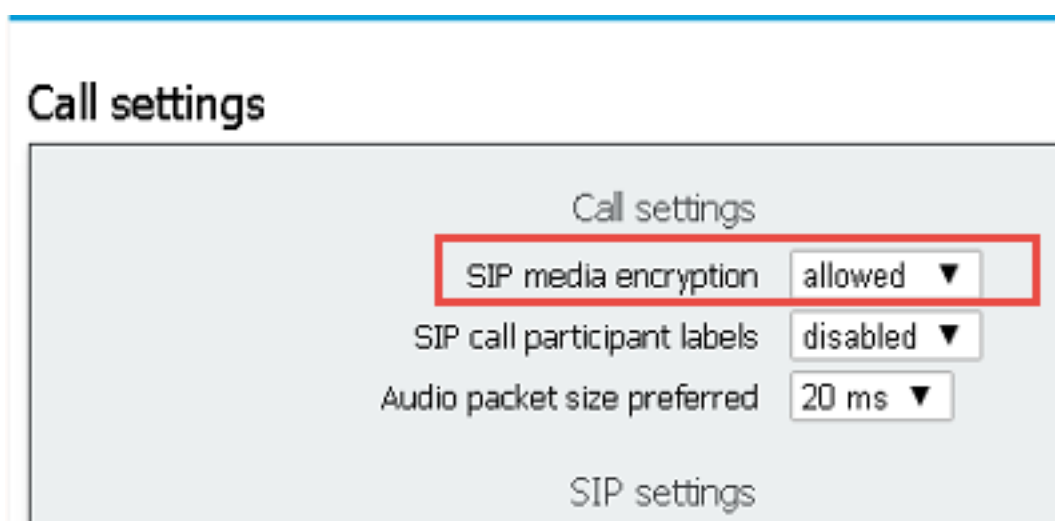
Quadro 2b

Um registro	Exemplo de IP	Descrição
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	Um registro A que é resolvido para todas as CallBridges no cluster. Isso será conhecido como Nome de domínio totalmente qualificado (FQDN) do cluster do
	10.10.10.2	CallBridge
	10.10.10.3	CallBridge
fe.skype.local	10.10.10.5	Nome de domínio totalmente qualificado (FQDN) do front-end do Skype

Configuração

Criptografia de mídia SIP

Navegue até **Configuração > Configurações da chamada**. A criptografia de mídia SIP deve ser definida como permitida.



Regras de entrada

A Tabela 3 descreve o que cada campo da configuração Chamadas recebidas - Correspondência de chamada significa.

Tabela 3

Campo Plano de discagem correspondente de chamada recebida	Descrição
Nome de domínio	Se uma chamada for recebida com esse domínio, use a parte do usuário do U para procurar correspondências nos destinos habilitados.
Prioridade	Isso determina a ordem em que as regras serão consideradas. Números mais altos serão verificados primeiro. Os números mais baixos serão verificados por último.
Espaços de Destino	Se definido como sim: se a parte do usuário do URI corresponder a um espaço de chamada será conectada a esse espaço.
Destina-se a usuários	Se definido como sim: se a parte do usuário da URI corresponder a um usuário CMA, a chamada tentará ligar para esse usuário.
Destinos IVR	Se definido como sim: se a parte do usuário do URI corresponder a um IVR configurado, a chamada será conectada a esse IVR.
Direciona Lync	Se definido como sim: Se a parte do usuário do URI corresponder a um número de discagem PSTN de uma reunião do Skype for Business, conecte-se a essa

Destina Lync Simplejoin
Locatário

reunião como uma chamada Dual Homed.
Se definido como sim: Converta a parte do usuário do URI em um destino HT e tente localizar uma reunião do Office365 hospedada nesse URL.
Isso determina para quais espaços esta regra será considerada.

A Tabela 4 descreve o que cada campo da configuração Chamadas recebidas - Encaminhamento de chamada significa.

Tabela 4

Campo Plano de discagem de encaminhamento de chamada recebida	Descrição
Padrão de correspondência de domínio	Se uma chamada for recebida com este domínio, encaminhe ou rejeite o domínio conforme configurado.
Prioridade	Isso determina a ordem em que as regras serão consideradas. Números mais altos serão verificados primeiro. Os números mais baixos serão verificados por último.
Encaminhar	Se definida para encaminhar a chamada será tratada pelas regras de saída. Se definida para rejeitar a chamada, ela será rejeitada e não encaminhada. Se estiver definido para passar pela parte de remetente do domínio será preservado. Se definido para usar o plano de discagem, a parte de de de se regravada conforme configurado na regra de saída.
ID do chamador	Note: A passagem não pode ser usada para regras que correspondam a um domínio do Lync/Skype se o CallBridge estiver em um cluster. Isso interrompe a apresentação em chamadas de gateway.
Reescrever domínio	Se habilitado, altere o domínio chamado para o valor configurado no campo domínio de encaminhamento.
Domínio de encaminhamento	Se o domínio de reescrita estiver ativado, o domínio chamado mudará para o valor deste campo.

Exemplo de configuração de regras de entrada - Single CallBridge

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	[edit]
	0	yes	yes	yes	no	no	[Add New] [Reset]

Delete

Call forwarding

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

Neste ambiente as coisas são extraordinariamente simples. Como não estamos usando CallBridges em cluster, podemos definir cada domínio para usar a passagem como ID de chamador. Isso não pode ser feito em um ambiente de cluster, pois isso quebrará o compartilhamento de apresentações.

Além disso, há uma regra de correspondência de chamadas para o domínio Skype.local com "Targets Lync" definido como true. Isso significa que, se chamarmos uma reunião do Lync/Skype pelo número de discagem PSTN, deveremos ser capazes de nos conectar como uma chamada Dual Home.

Exemplo de configuração de regras de entrada - CallBridges em cluster

Incoming call handling

Call matching

	Domain name	Priority	Targets spaces	Targets users	Targets IVRs	Targets Lync	Targets Lync Singlejoin	Tenant	
<input type="checkbox"/>	skype.local	0	no	no	no	yes	no	no	[edit]
	<input type="text"/>	<input type="text"/>	yes	yes	yes	no	no		Add New Reset

Call forwarding

	Domain matching pattern	Priority	Forward	Caller ID	Rewrite domain	Forwarding domain	
<input type="checkbox"/>	CMS1.uc.local	100	forward	pass through	yes	UC.local	[edit]
<input type="checkbox"/>	CMS2.uc.local	100	forward	pass through	yes	UC.local	[edit]
<input type="checkbox"/>	CMS3.uc.local	100	forward	pass through	yes	UC.local	[edit]
<input type="checkbox"/>	skype.local	100	forward	use dial plan	no		[edit]
<input type="checkbox"/>	uc.local	100	forward	pass through	no		[edit]
	<input type="text"/>	<input type="text"/>	reject	use dial plan	no	<input type="text"/>	Add New Reset

Neste ambiente, estamos usando um cluster CallBridge que consiste em três CallBridges. Por causa disso, precisamos de uma regra de encaminhamento de chamadas para cada CallBridge configurado para regravar o domínio para uc.local. Isso porque quando os usuários do Lync/Skype ligam de volta para os usuários do ambiente UC, eles realmente farão chamadas para o domínio de cms1.uc.local, cms2.uc.local ou cms3.uc.local. Infelizmente, essa é uma limitação da configuração necessária para que o conteúdo funcione em um ambiente CallBridge em cluster. Precisamos converter isso de volta em uc.local antes de encaminhar a chamada para o proxy do sip uc.local.

Além disso, há uma regra de correspondência de chamadas para o domínio Skype.local com "Targets Lync" definido como true. Isso significa que, se chamarmos uma reunião do Lync/Skype pelo número de discagem PSTN, deveremos ser capazes de nos conectar como uma chamada Dual Home.

Regras de saída

A Tabela 5 descreve o significado de cada campo na configuração de chamadas de saída.

Tabela 5

Campo Plano

de discagem de Descrição

saída

domínio

Para chamadas para este domínio, use esta regra de saída

proxy SIP a ser usado

O proxy SIP para o qual enviar chamadas para este domínio

Isso determina qual valor será colocado no cabeçalho do contato. Para a integração do Lync/Skype, esse valor deve ser definido como o FQDN do CallBridge.

Domínio de contato local

Note: Para quaisquer regras de saída usando um proxy SIP do Lync/Skype, esse campo DEVE ser configurado. Para quaisquer regras de saída usando um proxy SIP que não seja Lync/Skype, esse campo NÃO DEVE ser configurado.

Isso determina qual valor será colocado no cabeçalho de. Esse será o endereço de ID do chamador visto no proxy SIP. Se deixado em branco, este campo usará o "Domínio de contato local" configurado. O Lync/Skype usará esse como URI de destino para retornos de chamada e compartilhamento de apresentação.

Local do domínio

Note: Esse valor não será usado se a chamada for uma chamada de gateway e a regra de discagem de entrada usada tiver "ID do chamador" definido como passagem.

Tipo de tronco

Isso determina qual variação do SIP será usada na comunicação com o proxy SIP.

Isso determina se continuaremos ou não verificando regras de prioridade mais baixa ou pararemos de pesquisar no caso de uma correspondência em que não pudemos concluir a chamada.

Prioridade

Isso determina a ordem em que as regras serão consideradas. Números mais altos serão verificados primeiro. Os números mais baixos serão verificados por último.

Criptografia

Isso determina se usaremos SIP criptografado ou não.

Localatário

Isso determina para quais espaços esta regra será considerada.

Escopo da ponte de chamadas

Isso determina para que CallBridges essa regra de discagem de saída será considerada. Em CallBridges em cluster, isso é necessário para garantir que o domínio de contato correto seja enviado de cada CallBridge.

Note: Esse valor só pode ser definido utilizando a API conforme explicado abaixo.

Exemplo de configuração de chamadas de saída - Single CallBridge

Outbound calls

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

Novamente vemos que o ambiente CallBridge único é consideravelmente mais simples do que o ambiente em cluster. Uma coisa que vale a pena observar acima é que temos um domínio de contato especificado. Isso porque se não especificarmos o Nome de domínio totalmente qualificado do CallBridge como o domínio de contato local, o Lync/Skype rejeitará as chamadas por motivos de segurança. Como nossas regras de encaminhamento de entrada estão definidas para usar a passagem, não estaremos reescrevendo o domínio de origem neste exemplo.

Exemplo de configuração de chamadas de saída - CallBridges em cluster

Outbound calls

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

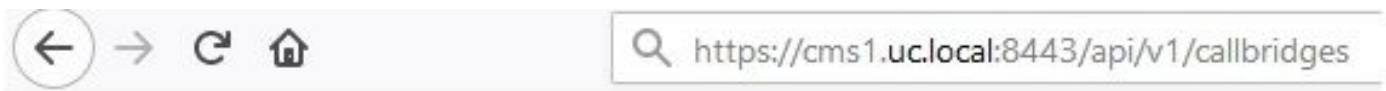
Neste ambiente, estamos usando um cluster CallBridge que consiste em três CallBridges. Por causa disso, precisamos de uma regra de saída para cada CallBridge com domínios de contato locais diferentes, locais de domínios e escopos. Somente uma regra de saída é necessária para rotear as chamadas de todas as CallBridges para o Cisco Unified Communications Manager. Para definir o escopo, precisamos utilizar a API.

Modificando o escopo utilizando a API - somente CallBridges em cluster

Depois de criar uma regra de chamada de saída, o escopo será definido como <all> para essa regra. Isso significa que a regra de saída será usada em todas as CallBridges em um cluster. Para regras de saída que apontam para o Lync/Skype, precisamos usar diferentes contatos e cabeçalhos, dependendo do CallBridge em que estamos. Para fazer isso, precisamos criar uma regra de saída diferente para cada CallBridge onde o contato/dos campos correspondem ao CallBridge. Usando a API, precisamos definir o escopo dessas regras de discagem de saída para que elas sejam processadas apenas no CallBridge que corresponde a essa regra.

OBTER uma lista de todas as CallBridges no cluster

Em um navegador, navegue até a página /callbridges da API do CMS. Isso mostrará todas as CallBridges em seu cluster.



```
– <callBridges total="3">
  – <callBridge id="53138c04-98ce-40f6-bf07-b01bef2b64d8">
    <name>cms2.uc.local</name>
  </callBridge>
  – <callBridge id="7260b2da-3dad-4edb-aa51-932a690e5b0d">
    <name>cms3.uc.local</name>
  </callBridge>
  – <callBridge id="e4ab61ea-b5b4-4fac-ad4a-9979badea4e4">
    <name>cms1.uc.local</name>
  </callBridge>
</callBridges>
```

Agora tenho as IDs de todas as minhas CallBridges. Suas IDs serão diferentes em seu ambiente. Posso ver que se eu quiser consultar a CallBridge cms1.uc.local, devo usar a ID do e4ab61ea-b5b4-4fac-ad4a-9979badea4e4.

OBTER uma lista de todas as regras de discagem de saída

Em seguida, preciso pesquisar minhas regras de saída e obter suas identificações. Em um navegador, navegue até a página /outbound dialplanrules na 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>
```

Agora eu tenho as identificações para todas as minhas regras, mas eu não posso dizer qual é qual. Não nos importamos com a primeira regra, já que esta é para UC.local e não precisamos definir um escopo para isso. Precisamos saber qual é a regra para as regras de saída restantes para o Skype.local. Assim, iniciando uma de cada vez, corresponderei as IDs às CallBridges.

No meu navegador, navegarei para /outbound dialplanrules/b8cf4056-7f56-43a5-b67b-861253d5ca32. Lendo o cabeçalho do contato listado aqui, posso dizer que esta regra é para CMS1.UC.local. Portanto, precisamos definir o escopo desta regra para CMS1.UC.local.

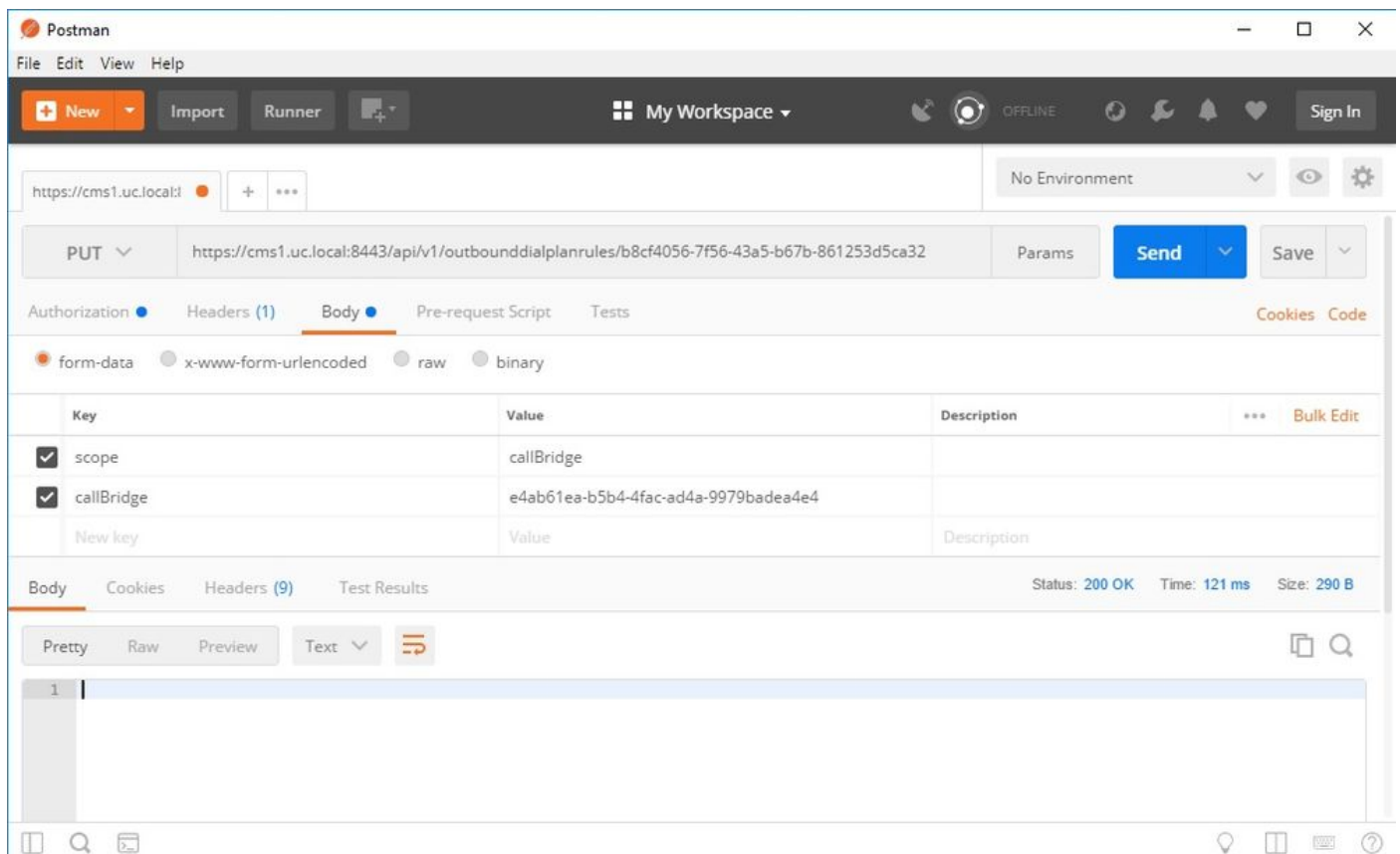
COLOQUE o escopo do CallBridge em

Usando minha ferramenta de API favorita, enviarei uma PUT para a api em /outbound dialplanrules/b8cf4056-7f56-43a5-b67b-861253d5ca32 com o seguinte corpo:

scope: callBridge

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

Nesta imagem, estou usando o PostMan para enviar esta solicitação.



Se esse PUT HTTP tiver sido bem-sucedido, a página de regras de discagem de saída no WebAdmin deve refletir que um escopo foi aplicado. Se

visualizado no Webadmin do CallBridge, o escopo foi aplicado a ele deve mostrar <local>. Se o Webadmin de outro CallBridge for usado para visualizar as regras de discagem de saída, ele deverá mostrar o FQDN do CallBridge no campo de escopo. Um escopo de <all> significa que a regra será usada em todas as CallBridges. Um escopo de <none> significa que um escopo foi ativado, mas nenhuma CallBridges corresponde ao escopo.

Depois de definir o escopo de um CallBridge, ele precisa ser configurado para cada CallBridge adicional. Depois que esta configuração tiver sido concluída, todas as regras de saída para o domínio do Skype devem ter um escopo.

Contas de serviço do CMS

Na página de configuração geral do WebAdmin, há uma seção de configurações do Lync Edge. Para utilizar os serviços TURN ou participar de reuniões Dual Home através do número de discagem PSTN, ele deve ser configurado.

A Tabela 6 descreve o significado de cada campo na configuração de configurações do Lync Edge.

Tabela 6

campo de configurações do Lync Edge	Descrição
Endereço do servidor	Nome de domínio totalmente qualificado (FQDN) de seu pool de front-end
Nome de usuário	O nome de usuário da conta de serviço que você deseja usar para o CMS
Número de registros	Quantas contas de usuário diferentes você deseja registrar. Se um valor não estiver configurado aqui, somente o nome de usuário listado acima será registrado. Se um número for aplicado aqui, os números de 1 a X serão aplicados como sufixos na parte do usuário do URI, onde X é o número configurado neste campo.

Exemplo de configuração de conta de serviço CMS

Configuração no CMS1:

Lync Edge settings	
Server address	<input type="text" value="fe.skype.local"/>
Username	<input type="text" value="cms1serviceuser@skype.local"/>
Number of registrations	<input type="text" value="12"/>

Esta configuração registraria cms1serviceuser1@skype.local, cms1serviceuser2@skype.local, cms1serviceuser3@skype.local, ... cms1serviceuser11@skype.local e cms1serviceuser12@skype.local para fe.skype.local. Como neste exemplo estou em um ambiente de cluster, também precisaria criar contas de serviço para meus outros CallBridges e configurá-las separadamente. Observe que os nomes de usuário neste exemplo são diferentes. No CMS1, os nomes de usuário são prefixados com cms1. No CMS2, os nomes de usuário são prefixados com cms2. No CMS3, o prefixo é cms3. Todas essas contas foram criadas e habilitadas no ambiente do Skype for Business. Como nosso pool de aplicativos confiáveis está configurado com a opção "Tratar como autenticado", não precisamos fornecer senhas para registro.

Configuração no CMS2:

Lync Edge settings	
Server address	<input type="text" value="fe.skype.local"/>
Username	<input type="text" value="cms2serviceuser@skype.local"/>
Number of registrations	<input type="text" value="12"/>

Configuração no CMS3:

Lync Edge settings	
Server address	<input type="text" value="fe.skype.local"/>
Username	<input type="text" value="cms3serviceuser@skype.local"/>
Number of registrations	<input type="text" value="12"/>

Verificando contas de serviço do CMS

A página de status do WebAdmin do CMS mostrará se os usuários do Lync/Skype foram registrados com êxito. No exemplo abaixo, estamos configurando apenas um registro e ele foi concluído com êxito. Se você observar que o status mostra registros em andamento por um longo tempo coletar registros SIP e DNS para determinar por que a falha está ocorrendo.

System status

Uptime	6 seconds
Build version	2.3.1
XMPP connection	configure XMPP
Lync Edge registrations	1 configured, 1 completed successfully
CMA calls	0
SIP calls	0
Lync calls	0
Forwarded calls	0
Completed calls	0
Activated conferences	0
Active Lync subscribers	0
Total outgoing media bandwidth	0
Total incoming media bandwidth	0

Configuração do Lync/Skype

Aplique os comandos abaixo no Shell de Gerenciamento do Lync/Skype. Aplique os comandos no servidor Front-End.

Note: Os comandos sugeridos são para orientação. Caso tenha dúvidas sobre a configuração no servidor Skype, você precisará entrar em contato com o administrador do Lync/Skype e/ou com a equipe de suporte.

CallBridge único

Primeiro, precisamos dizer ao Skype para confiar em nosso CallBridge. Para fazer isso, adicionamos um pool de aplicativos confiáveis. Na terminologia da Microsoft, "Pool" significa apenas "Cluster". Neste cenário, nosso cluster é apenas um cluster de uma CallBridge. A identidade do nosso cluster DEVE corresponder ao nome comum do certificado em uso em nosso CallBridge. A Microsoft usa isso como uma verificação de segurança. Ter a identidade em uma SAN não é suficiente. Se o nome comum não corresponder, a Microsoft destruirá a conexão TCP. Ao usar esse comando, a identidade deve ser o FQDN da CallBridge. O Registrador deve ser o FQDN do Pool Front-End que atende a essas conexões. O site deve ser o identificador do site Lync/Skype. Se você não tiver certeza dos valores que devem ser usados para o agente de registro ou o site, entre em contato com o administrador do Lync/Skype.

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

Em seguida, o Ambiente Microsoft deve ser configurado para permitir a comunicação de entrada do CallBridge (Trusted Application Pool) na porta 5061.

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

O ambiente da Microsoft está configurado para aceitar chamadas, mas não pode retornar chamadas e não pode enviar apresentação para chamadas de gateway. Para corrigir isso, precisamos adicionar uma rota estática. No cenário do CallBridge único, precisamos apenas de uma única rota para permitir todas as chamadas para nosso domínio UC.local. Nos comandos abaixo, Destino é o FQDN do CallBridge ao qual queremos enviar solicitações SIP. O campo MatchURI é a parte do domínio do URI que deve ser usada. Observe que em um ambiente Lync/Skype somente uma rota estática pode ser criada por MatchURI.

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

Finalmente, precisamos dizer ao Skype para implementar todas as mudanças que acabamos de fazer.

```
Enable-CsTopology
```

CallBridges em cluster

Primeiro, precisamos dizer ao Skype para confiar em nosso cluster CallBridge. Para fazer isso, adicionamos um pool de aplicativos confiáveis. Na terminologia da Microsoft, "Pool" significa apenas "Cluster". A identidade do cluster DEVE corresponder ao nome comum do(s) certificado(s) em uso em nossa CallBridge. A Microsoft usa isso como uma verificação de segurança. Ter a identidade em uma SAN não é suficiente. Se o nome comum não corresponder, a Microsoft destruirá a conexão TCP. Ao usar esse comando, a identidade deve ser o FQDN da CallBridge. ComputerFqdn deve ser o FQDN da primeira CallBridge em seu cluster. Ao especificar um ComputerFqdn, você está indicando para o ambiente Lync/Skype que este não é um cluster com apenas um único servidor nele. O Registrador deve ser o FQDN do Pool Front-End que atende a essas conexões. O site deve ser o identificador do site Lync/Skype. Se você não tiver certeza dos valores que devem ser usados para o agente de registro ou o site, entre em contato com o administrador do Lync/Skype.

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

Neste ambiente, precisamos adicionar duas CallBridges como computadores de aplicativos confiáveis. O primeiro CallBridge já foi adicionado quando criamos o Trusted Application Pool Acima. Quando adicionamos estes computadores, precisamos associá-los ao pool que acabamos de criar. Isso diz ao Skype que temos computadores adicionais em nosso cluster que precisam ser confiáveis. Todas as identidades de computador aqui precisam ser listadas como SANs em nossos certificados CallBridge. Essas identidades também devem corresponder aos cabeçalhos dos contatos nas regras de discagem de saída nas CallBridges. Se não corresponderem, a Microsoft destruirá a conexão TCP.

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

Em seguida, o Ambiente Microsoft deve ser configurado para permitir a comunicação de entrada do cluster CallBridge (Trusted Application Pool) na porta 5061.

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

O ambiente da Microsoft está configurado para aceitar chamadas, mas não pode retornar chamadas e não pode enviar apresentação para chamadas de gateway. Para corrigir isso, precisamos adicionar rotas estáticas. Primeiro, precisamos adicionar uma rota estática para permitir todas as chamadas para nosso domínio UC.local. Nos comandos abaixo, Destino é o FQDN do CallBridge ao qual queremos enviar solicitações SIP. O campo MatchURI é a parte do domínio do URI que deve ser usada. Observe que em um ambiente Lync/Skype somente uma rota estática pode ser criada por MatchURI. Como o destino é o FQDN do cluster CallBridge e tem um registro DNS A para cada membro do cluster, o Lync/Skype pode enviar tráfego para todas as CallBridges. Assim, se um for desativado, ele poderá rotear automaticamente as solicitações do nosso domínio para outro CallBridge no cluster.

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

Em seguida, precisamos criar uma rota estática adicional para cada CallBridge no cluster. Esse é um requisito para que o retorno de chamada e a apresentação funcionem.

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

Finalmente, precisamos dizer ao Skype para implementar todas as mudanças que acabamos de fazer.

```
Enable-CsTopology
```

Troubleshooting

Coleta de logs do CMS

A primeira etapa no diagnóstico de qualquer problema é determinar onde o problema está. Para fazer isso, precisamos analisar os registros do Cisco Meeting Server, mas primeiro precisamos coletá-los. Aqui estão minhas recomendações pessoais sobre registros a serem coletados.

Primeiro, habilite a depuração SIP e DNS para todas as CallBridges através da interface WebAdmin. Para fazer isso, navegue até WebAdmin e, em seguida, para Logs > Detailed Tracing. A partir daí, ative o registro SIP e DNS para os próximos trinta minutos. Isso deve ser mais do que tempo suficiente para detectar e diagnosticar o problema. Lembre-se de que isso precisa ser feito individualmente para todas as CallBridges, pois a ativação de log não é compartilhada em um cluster.

Em segundo lugar, habilitar capturas de pacotes em todas as CallBridges. Para fazer isso, conecte-se via SSH a cada CallBridge e execute o comando `pcap <interface>` em que `<interface>` é o tráfego de interface que deve ser usado. Na maioria dos casos, será a interface `a`. Assim, o comando `"pcap a"` iniciará uma captura de pacote na interface `a` para a CallBridge à qual estamos conectados.

Quando a captura de pacotes estiver sendo executada em todas as interfaces, a próxima etapa é produzir o problema. Vá em frente e tente uma chamada ou faça o que estava falhando. Depois que isso for concluído, encerre todas as capturas de pacote. Isso pode ser feito inserindo-se `Ctrl-C` em todas as janelas do SSH. Quando a captura de pacotes for concluída, o nome do arquivo gerado será gravado na tela. Acompanhe esse nome de arquivo, pois precisaremos baixá-lo na próxima etapa.

Por fim, precisamos coletar os registros das CallBridges. Para fazer isso, conecte-se via SFTP a cada CallBridge. Faça o download do arquivo `logbundle.tar.gz` e do arquivo de captura de pacote gerado. Esse arquivo está disponível somente no CMS2.2+. Nas versões 2.3+ do CMS, ele incluirá a configuração completa do CMS. Se você estiver executando a versão 2.2, ela não incluirá suas regras de entrada/saída, portanto, seria bom tirar capturas de tela dessas páginas, bem como as configurações do Lync Edge para referência. Certifique-se de armazenar os registros/capturas de tela coletados em pastas separadas que tenham um nome correspondente ao CallBridge de onde os registros foram extraídos. Isso ajudará a garantir que os registros não se misturem.

Exibição da Configuração do Lync/Skype

Esses comandos serão extremamente úteis na solução de problemas da configuração do Lync/Skype. Neste documento, os comandos são fornecidos para criar e exibir a configuração, mas nenhum comando é fornecido para remover a configuração. Isso ocorre porque a remoção da configuração pode ser perigosa, a menos que seja executada por administradores com um entendimento completo do ambiente Lync/Skype. Se precisar remover a configuração, trabalhe com o administrador do Lync/Skype para fazer isso.

Comando	Descrição
<code>Get-CsTrustedApplicationPool</code>	Este comando lista clusters (pools) confiáveis pelo Lync/Skype. A identidade desse pool DEVE corresponder ao nome comum do(s) certificado(s) CallBridge. Mesmo em um único ambiente CallBridge, um cluster (pool) CallBridge de um deve ser especificado aqui. Esse comando lista os servidores confiáveis pelo Lync/Skype e com qual pool esses servidores estão associados. Todos os computadores aqui DEVEM ser identificados no certificado enviado pelas CallBridges. Em um único ambiente CallBridge, esse é
<code>Get-CsTrustedApplicationComputer</code>	geralmente o nome comum. Em um ambiente em cluster, esses computadores DEVEM ser listados como entradas de Nome alternativo do assunto (SAN). Além disso, todos os computadores aqui DEVEM ser identificados por entradas de domínio de contato local nas regras de discagem de saída do CallBridge. Esse comando lista com quais serviços os pools de aplicativos confiáveis podem se comunicar. Para comunicação CMS com Lync/Skype, usaremos a porta TCP 5061 para SIP criptografado TLS.
<code>Get-CsTrustedApplication</code>	
<code>Get-CsStaticRoutingConfiguration Select-Object -ExpandProperty Route</code>	Este comando lista as rotas estáticas que o Lync/Skype usa para encaminhar solicitações. O campo <code>MatchURI</code> é o domínio de destino da mensagem SIP. O campo <code>"TLS Fqdn"</code> no XML deve mostrar o servidor de destino para esse tráfego.

Exemplo de saída dos comandos Lync/Skype Get

Abaixo está a saída dos comandos Lync/Skype Get acima emitidos no três cenário de cluster CallBridge abordado neste 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
ComputerGruu       : {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:dt8XJKciS1GhEeT62tyNogAA}
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>
```

Entrando em contato com o TAC

Se você encontrar erros com essa implementação, entre em contato com o Cisco TAC. Ao abrir a solicitação de serviço, inclua um link para este documento. Isso ajudará os engenheiros do TAC a entender sua configuração. Além disso, seria extremamente útil se os registros do Cisco Meeting Server fossem anexados ao caso conforme descrito acima e a saída de todos os comandos Get do Front-End do Lync/Skype fosse inserida nas notas do caso. Se você não incluir essas informações, é certo que é uma das primeiras coisas que os engenheiros do TAC solicitam. Por isso, vá em frente e colete-as antes de abrir seu caso.