

Configurazione di Cisco Meeting Server e Skype for Business

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Topologia di rete - Single CallBridge](#)

[Topologia di rete - CallBridge in cluster](#)

[Requisiti del certificato Callbridge - Single CallBridge](#)

[Requisiti dei certificati Callbridge - CallBridge cluster](#)

[Requisiti record DNS - Single CallBridge](#)

[Requisiti record DNS - CallBridge cluster](#)

[Configurazione](#)

[Crittografia dei supporti SIP](#)

[Regole connessioni in entrata](#)

[Esempio di configurazione delle regole in entrata - Single CallBridge](#)

[Esempio di configurazione delle regole in entrata - CallBridge in cluster](#)

[Regole in uscita](#)

[Esempio di configurazione delle chiamate in uscita - Single CallBridge](#)

[Esempio di configurazione delle chiamate in uscita - CallBridge in cluster](#)

[Modifica dell'ambito utilizzando l'API - solo CallBridge cluster](#)

[OTTIENI un elenco di tutti i CallBridge nel cluster](#)

[OTTENERE un elenco di tutte le regole di composizione in uscita](#)

[Inserire l'ambito di CallBridge](#)

[Account del servizio CMS](#)

[Esempio di configurazione dell'account del servizio CMS](#)

[Verifica degli account del servizio CMS](#)

[Configurazione Lync/Skype](#)

[Single CallBridge](#)

[CallBridge cluster](#)

[Risoluzione dei problemi](#)

[Raccolta dei log dal CMS](#)

[Visualizzazione della configurazione di Lync/Skype](#)

[Output di esempio dei comandi Lync/Skype Get](#)

[Connessione a TAC](#)

Introduzione

In questo documento viene descritto come configurare il cluster CallBridge di Cisco Meeting Server (CMS) con Skype for Business come complemento alle guide ufficiali. In questo documento viene illustrato un esempio di un singolo elemento CallBridge e un altro esempio di un cluster CallBridge di tre elementi, ma è possibile aggiungere ulteriori elementi CallBridge, se necessario. È inoltre supportato un cluster CallBridge.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Meeting Server (CMS)
- DNS (Domain Name Server)
- Skype For Business
- API (Application Programming Interface)

Nota: la guida alla configurazione è disponibile qui:

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

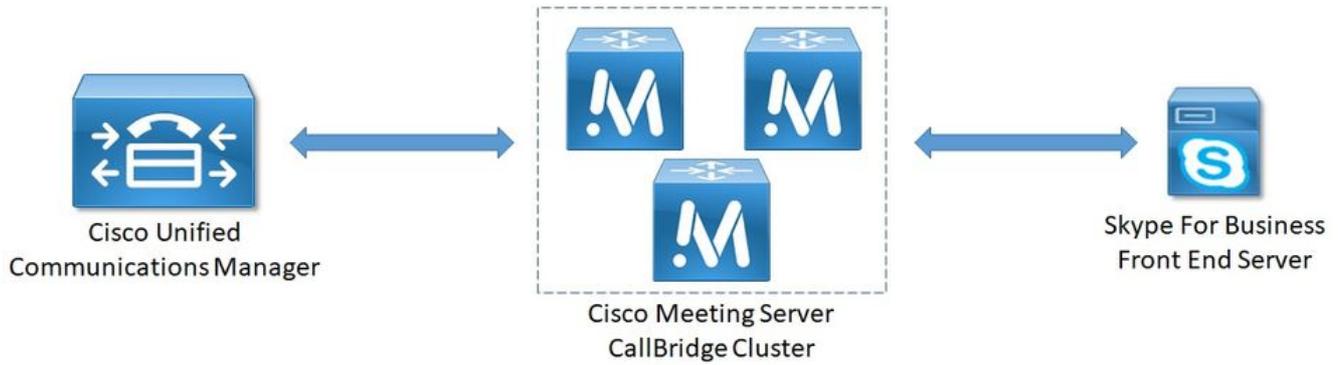
Componenti usati

- 3 server CMS che eseguono un cluster CallBridge, versione software 2.2.2.
- Skype for Business 2015
- Active Directory (AD) Windows Server 2012
- Client Secure Shell (SSH)
- Client SFTP (Secure File Transfer Protocol), ad esempio WinSCP o simili
- Programma API, ad esempio Postman o simili
- Sessione Desktop remoto per Active Directory, DNS e server Skype

Topologia di rete - Single CallBridge



Topologia di rete - CallBridge in cluster



Requisiti del certificato Callbridge - Single CallBridge

La tabella 1a fornisce un esempio del certificato CallBridge per un singolo ambiente CallBridge.

Tabella 1a

Certificati CallBridge Descrizione

Single CallBridge

CN:cms.uc.local FQDN di CallBridge

Requisiti dei certificati Callbridge - CallBridge cluster

La tabella 1b fornisce un esempio dei certificati CallBridge per un ambiente CallBridge in cluster. È possibile condividere un singolo certificato tra i CallBridge di un cluster.

Tabella 1b

Certificati Callbridge Descrizione

Server 1: cms1.uc.local

CN:cms.uc.local FQDN cluster CallBridge. Questo record deve essere risolto in tutti i peer del cluster CallBridge.

SAN:cms.uc.local FQDN cluster CallBridge. Questo record deve essere risolto in tutti i peer del cluster CallBridge.

SAN:cms1.uc.local FQDN di CallBridge 1.

SAN:cms2.uc.local FQDN di CallBridge 2.

SAN:cms3.uc.local FQDN di CallBridge 3.

Server 2: cms2.uc.local

CN:cms.uc.local FQDN cluster CallBridge. Questo record deve essere risolto in tutti i peer del cluster CallBridge.

SAN:cms.uc.local FQDN cluster CallBridge. Questo record deve essere risolto in tutti i peer del cluster CallBridge.

SAN:cms1.uc.local FQDN di CallBridge 1.

SAN:cms2.uc.local FQDN di CallBridge 2.

SAN:cms3.uc.local FQDN di CallBridge 3.

Server 3: cms3.uc.local

CN:cms.uc.local FQDN cluster CallBridge. Questo record deve essere risolto in tutti i peer del cluster CallBridge.

SAN:cms.uc.local FQDN cluster CallBridge. Questo record deve essere risolto in tutti i peer del cluster CallBridge.

SAN:cms1.uc.local FQDN di CallBridge 1.

SAN:cms2.uc.local FQDN di CallBridge 2.

SAN:cms3.uc.local FQDN di CallBridge 3.

CMS CLI può essere utilizzato per visualizzare il contenuto di un certificato:

```
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>

Prendere nota dei campi Oggetto e Nome alternativo soggetto X509v3. Queste funzionalità saranno estremamente importanti in un secondo momento, quando creeremo relazioni di fiducia nell'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

Nota: La guida alla configurazione dei certificati è disponibile qui:
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

Requisiti record DNS - Single CallBridge

La tabella 2a fornisce un esempio di come configurare il server DNS. Fornisce una spiegazione del significato di ogni campo.

Tabella 2a

Un record	Esempio	IP	Descrizione
cms.uc.local	10.10.10.1	10.10.10.1	CallBridge
fe.skype.local	10.10.10.5	10.10.10.5	Nome di dominio completo (FQDN) front-end Skype

Requisiti record DNS - CallBridge cluster

Nella tabella 2b viene illustrato un esempio di configurazione del server DNS. Fornisce una spiegazione del significato di ogni campo.

Tabella 2b

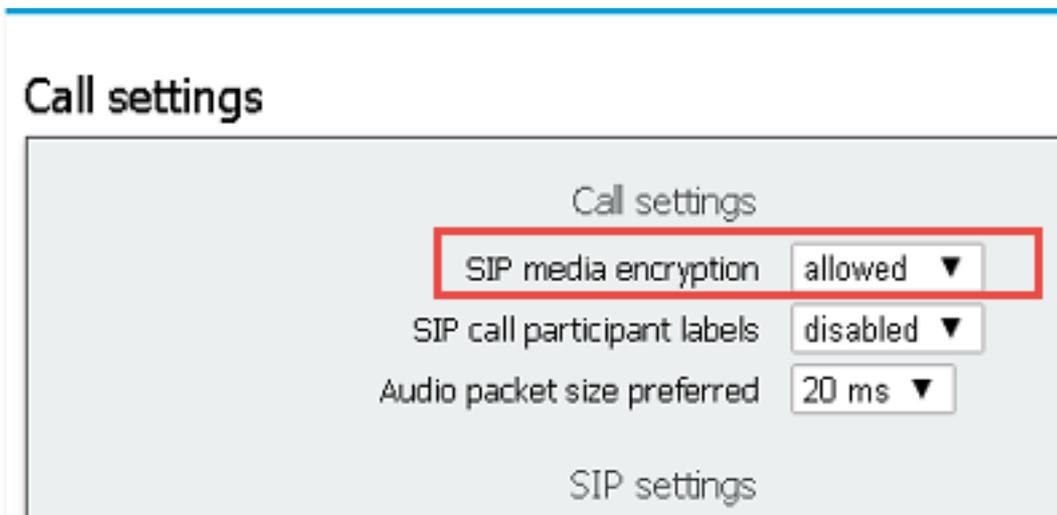
Un record	Esempio	IP	Descrizione
-----------	---------	----	-------------

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 Record A che viene risolto in tutti gli oggetti CallBridge del cluster. Tale nome ve
 10.10.10.2 indicato come nome di dominio completo (FQDN) del cluster CallBridge
 10.10.10.3
 fe.skype.local 10.10.10.5 Nome di dominio completo (FQDN) front-end Skype

Configurazione

Crittografia dei supporti SIP

Passare a **Configuration > Call Settings (Configurazione > Impostazioni chiamata)**. La crittografia dei supporti SIP deve essere impostata su allowed.



Regole connessioni in entrata

La tabella 3 descrive il significato di ogni campo nella configurazione Chiamate in arrivo - Corrispondenza chiamate.

Tabella 3

Campo Dial Plan corrispondente chiamata in arrivo	Descrizione
Nome dominio	Se viene ricevuta una chiamata con questo dominio, utilizzare la parte utente dell'URI per cercare le corrispondenze nelle destinazioni abilitate.
Priority	Determina l'ordine in cui le regole verranno considerate. I numeri più alti verranno controllati per primi. I numeri più bassi verranno controllati per ultimi.
Destinazioni Spazi	Se impostato su yes: se la parte utente dell'URI corrisponde a uno spazio, la chiamata si conatterà a tale spazio.
Utenti target	Se impostato su yes: se la parte utente dell'URI corrisponde a un utente CMA, la chiamata tenterà di chiamare tale utente.
IVR destinazioni	Se impostato su yes: se la parte utente dell'URI corrisponde a un IVR configurato, la chiamata si conatterà a tale IVR.
Targets Lync	Se impostato su yes: Se la parte utente dell'URI corrisponde a un numero di accesso PSTN di una riunione Skype for Business connettersi a tale riunione come chiamata con due persone.
Targets Lync Simplejoin	Se impostato su yes: Converte la parte utente dell'URI in una destinazione HTTP e prova a trovare una riunione di Office365 ospitata in tale URL.

Tenant

Determina per quali tenant verrà considerata questa regola.

La tabella 4 descrive il significato di ogni campo nella configurazione Chiamate in arrivo - Inoltro di chiamata.

Tabella 4

Campo Dial Plan
inoltro di chiamata
in arrivo

Descrizione

Modello di
corrispondenza
dominio

Se viene ricevuta una chiamata con questo dominio, inoltrare o rifiutare il dominio con il valore configurato.

Priority

Determina l'ordine in cui le regole verranno considerate. I numeri più alti verranno controllati per primi. I numeri più bassi verranno controllati per ultimi.

Avanti

Se impostato per l'inoltro, la chiamata verrà gestita dalle regole in uscita. Se impostato per Rifiuta, la chiamata verrà rifiutata e non inoltrata.

ID chiamante

Se impostato per passare attraverso la parte da del dominio verrà mantenuto. Se impostato per l'utilizzo del dial plan, la parte da verrà riscritta come configurato nella regola in uscita.

Riscrivi dominio

Nota: Impossibile utilizzare l'accesso automatico per le regole che corrispondono a un dominio Lync/Skype se CallBridge si trova in un cluster. La presentazione sulle chiamate del gateway verrà interrotta.

Dominio di inoltro

Se questa opzione è abilitata, sostituire il dominio chiamato con il valore configurato nel campo dominio di inoltro.

Se la riscrittura del dominio è abilitata, il dominio chiamato verrà impostato sul valore configurato in questo campo.

Esempio di configurazione delle regole in entrata - Single CallBridge

Incoming call handling

Call matching

Domain name	Priority	Targets spaces	Targets users	Targets IVRs	Targets Lync	Targets Lync Singlejoin	Tenant
skype.local	0	no	no	no	yes	no	no
	0	yes	yes	yes	no	no	

Delete

Call forwarding

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

In questo ambiente le cose sono straordinariamente semplici. Poiché non vengono utilizzati CallBridge cluster, è possibile impostare ogni dominio in modo che utilizzi pass through come ID chiamante. Non è possibile eseguire questa operazione in un ambiente cluster perché interromperà la condivisione della presentazione.

Esiste inoltre una regola di corrispondenza chiamate per il dominio Skype.local con "Targets Lync" impostato su true. Ciò significa che se chiamiamo una riunione Lync/Skype tramite il numero di telefono PSTN, dovremmo essere in grado di collegarci come una chiamata Dual Home.

Esempio di configurazione delle regole in entrata - CallBridge in cluster

Incoming call handling

Call matching

Domain name	Priority	Targets spaces	Targets users	Targets IVRs	Targets Lync	Targets Lync Singlejoin	Tenant
skype.local	0	no	no	no	yes	no	no
	0	yes	yes	yes	no	no	

Delete

Call forwarding

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

In questo ambiente viene utilizzato un cluster CallBridge costituito da tre CallBridge. Per questo motivo è necessaria una regola di inoltro di chiamata per ogni

CallBridge configurato per riscrivere il dominio in uc.local. Questo perché quando gli utenti di Lync/Skype richiamano gli utenti dall'ambiente UC, effettueranno effettivamente chiamate al dominio cms1.uc.local, cms2.uc.local o cms3.uc.local. Si tratta di una limitazione della configurazione necessaria per consentire il funzionamento del contenuto in un ambiente CallBridge in cluster. È necessario riconvertirlo in uc.local prima di inoltrare la chiamata al proxy uc.local sip.

Esiste inoltre una regola di corrispondenza chiamate per il dominio Skype.local con "Targets Lync" impostato su true. Ciò significa che se chiamiamo una riunione Lync/Skype tramite il numero di telefono PSTN, dovremmo essere in grado di collegarci come una chiamata Dual Home.

Regole in uscita

La tabella 5 descrive il significato di ogni campo nella configurazione delle chiamate in uscita.

Tabella 5

Campo Dial Plan in uscita	Descrizione
Dominio Proxy SIP da utilizzare	Per le chiamate in uscita verso questo dominio utilizza questa regola in uscita Il proxy SIP a cui inviare le chiamate per questo dominio
Dominio contatto locale	Determina il valore che verrà inserito nell'intestazione del contatto. Per l'integrazione Lync/Skype questo valore deve essere impostato sul nome di dominio completo (FQDN) CallBridge. Nota: Questo campo DEVE essere configurato per tutte le regole in uscita che utilizzano un proxy SIP di Lync/Skype. Per le regole in uscita che utilizzano un proxy SIP diverso da Lync/Skype, questo campo NON DEVE essere configurato.
Locale da dominio	Determina il valore che verrà inserito nell'intestazione da. Questo sarà l'indirizzo dell'ID chiamante visualizzato sul proxy SIP. Se lasciato vuoto, questo campo utilizzerà il "Dominio contatto locale" configurato. Lync/Skype utilizzerà questo come URI di destinazione per i callback e la condivisione delle presentazioni. Nota: Questo valore non viene utilizzato se la chiamata è una chiamata del gateway e per la regola di composizione in ingresso utilizzata l'ID chiamante è impostato su passthrough.
Tipo trunk	Determina la variazione del SIP da utilizzare nelle comunicazioni con il proxy SIP.
Comportamento	Determina se continueremo a controllare le regole di priorità inferiore o interromperemo la ricerca nel caso di una corrispondenza in cui non siamo stati in grado di completare la chiamata.
Priority	Determina l'ordine in cui le regole verranno considerate. I numeri più alti verranno controllati per primi. I numeri più bassi verranno controllati per ultimi.
Crittografia	Determina se verrà utilizzato il SIP crittografato o non crittografato.
Tenant	Determina per quali tenant verrà considerata questa regola.
Ambito bridge di chiamate	Determina per quali CallBridge verrà considerata la regola di composizione in uscita. Ne CallBridge in cluster questo è necessario per garantire l'invio del dominio di contatto corretto da ogni CallBridge. Nota: Questo valore può essere impostato solo utilizzando l'API come spiegato di seguito.

Esempio di configurazione delle chiamate in uscita - Single CallBridge

Outbound calls

<input type="checkbox"/>	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption	Tenant
<input type="checkbox"/>	uc.local	ucm.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

Ancora l'ambiente CallBridge singolo è notevolmente più semplice rispetto all'ambiente cluster. Una cosa che vale la pena notare qui sopra è che abbiamo un dominio di contatto specificato. Questo perché se non si specifica il nome di dominio completo del CallBridge come dominio di contatto locale Lync/Skype rifiuterà le chiamate per motivi di sicurezza. Poiché le regole di inoltro in ingresso sono impostate per l'utilizzo di pass-through, in questo esempio non verrà riscritto il dominio da.

Esempio di configurazione delle chiamate in uscita - CallBridge in 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

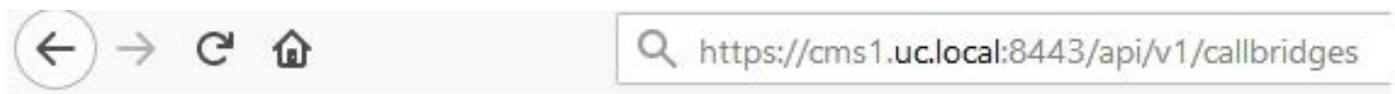
In questo ambiente viene utilizzato un cluster CallBridge costituito da tre CallBridge. Per questo motivo è necessaria una regola in uscita per ogni CallBridge, ognuna con diversi domini di contatto locali, locali da domini e ambiti. È necessaria una sola regola in uscita per instradare le chiamate da tutti i CallBridge a Cisco Unified Communications Manager. Per impostare l'ambito è necessario utilizzare l'API.

Modifica dell'ambito utilizzando l'API - solo CallBridge cluster

Dopo aver creato una regola di chiamata in uscita, l'ambito verrà impostato su <all> per tale regola. Ciò significa che la regola in uscita verrà utilizzata in tutti gli oggetti CallBridge di un cluster. Per le regole in uscita che puntano a Lync/Skype, è necessario utilizzare un contatto e intestazioni diversi a seconda di CallBridge in cui ci troviamo. A tale scopo, è necessario creare una regola in uscita diversa per ogni CallBridge in cui i campi del contatto o del mittente corrispondono a tale CallBridge. Utilizzando l'API è necessario impostare l'ambito di queste regole di composizione in uscita in modo che vengano elaborate solo sul CallBridge corrispondente a tale regola.

OTTIENI un elenco di tutti i CallBridge nel cluster

In un browser passare alla pagina /callbridges dell'API CMS. Verranno visualizzati tutti i CallBridge del 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>
```

Ora ho i documenti per tutti i miei CallBridge. Gli ID saranno diversi nel tuo ambiente. Posso vedere che se voglio fare riferimento a CallBridge cms1.uc.local devo usare l'ID di e4ab61ea-b5b4-4fac-ad4a-9979badea4e4.

OTTENERE un elenco di tutte le regole di composizione in uscita

Successivamente, è necessario cercare le regole in uscita e ottenere i relativi ID. In un browser passare alla pagina /outbounddialplanrules nell'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>
```

Ora ho i documenti per tutte le mie regole, ma non so dire quale sia. La prima regola non ci interessa, poiché si tratta della UC.local, per cui non abbiamo bisogno di definire un ambito. Dobbiamo sapere quale è la regola per le restanti regole in uscita su Skype.local. Quindi, partendo uno alla volta, abbinerò gli ID ai CallBridge.

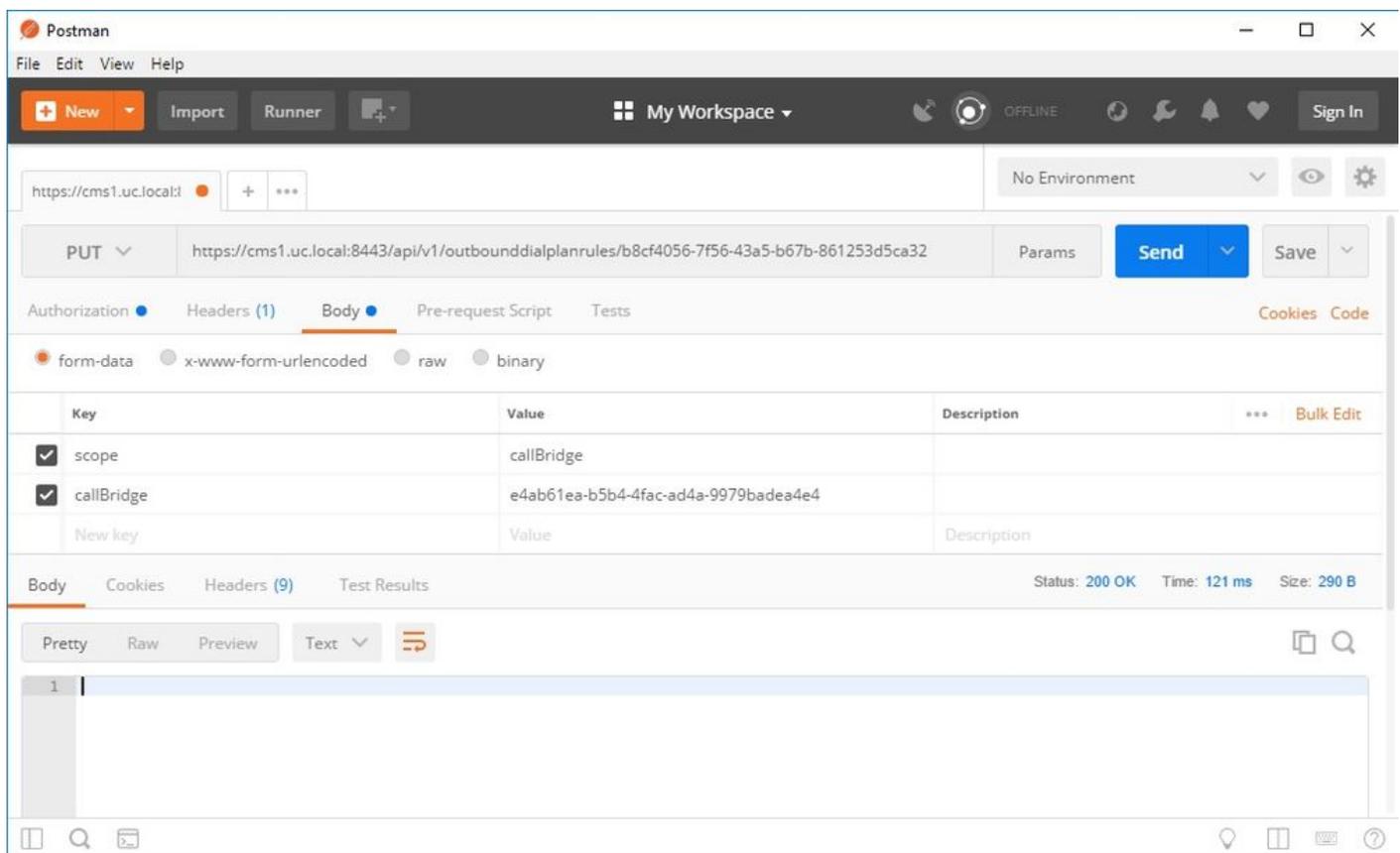
Passerò a /outbounddialplanrules/b8cf4056-7f56-43a5-b67b-861253d5ca32 nel mio browser. Lettura dell'intestazione del contatto elencata. È possibile che questa regola sia per CMS1.UC.local. È quindi necessario impostare l'ambito di questa regola su CMS1.UC.local.

Inserire l'ambito di CallBridge

Utilizzando lo strumento API preferito, invierò un PUT all'api su /outbounddialplanrules/b8cf4056-7f56-43a5-b67b-861253d5ca32 con il seguente corpo:

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

In questa schermata sto utilizzando PostMan per inviare questa richiesta.



Se l'operazione HTTP PUT ha esito positivo, la pagina delle regole di composizione in uscita in WebAdmin dovrebbe riflettere l'applicazione di un ambito. Se l'ambito è stato applicato a CallBridge e visualizzato da Webadmin, dovrebbe essere visualizzato <local>. Se l'amministratore Web di un altro CallBridge viene utilizzato per visualizzare le regole di composizione in uscita, deve visualizzare l'FQDN di CallBridge nel campo ambito. L'ambito <all> indica che la regola verrà utilizzata in tutti gli oggetti CallBridge. Un ambito di <none> indica che è stato abilitato un ambito, ma nessun CallBridges corrisponde all'ambito.

Dopo aver impostato l'ambito per un CallBridge, è necessario configurarlo per ogni CallBridge aggiuntivo. Dopo il completamento di questa configurazione, ogni regola in uscita per il tuo dominio Skype deve avere un ambito.

Account del servizio CMS

Nella pagina di configurazione generale di WebAdmin è presente una sezione delle impostazioni di Lync Edge. Per utilizzare i servizi TURN o partecipare a riunioni Dual Home tramite il numero PSTN Dialin, è necessario configurarlo.

Nella tabella 6 viene descritto il significato di ogni campo della configurazione delle impostazioni di Lync Edge.

Tabella 6

campo delle impostazioni di Lync Edge	Descrizione
Indirizzo server	Nome di dominio completo (FQDN) del pool Front End
Username	Nome utente dell'account del servizio da utilizzare per CMS
Numero di registrazioni	Numero di account utente da registrare. Se un valore non è configurato qui, verrà registrato il nome utente indicato sopra. Se viene applicato un numero, i numeri da 1 a X verranno apposti come suffissi alla parte utente dell'URI, dove X è il numero configurato in questo campo.

Esempio di configurazione dell'account del servizio CMS

Configurazione su 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"/>

Questa configurazione consente di registrare cms1serviceuser1@skype.local, cms1serviceuser2@skype.local, cms1serviceuser3@skype.local, ... cms1serviceuser11@skype.local e cms1serviceuser12@skype.local in fe.skype.local. Poiché in questo esempio si è in un ambiente cluster, è necessario creare anche account di servizio per gli altri CallBridge e configurarli separatamente. I nomi utente in questo esempio sono diversi. Su CMS1 i nomi utente sono preceduti dal prefisso cms1. Su CMS2 i nomi utente sono preceduti dal prefisso cms2. Su CMS3 il prefisso è cms3. Tutti questi account sono stati creati e abilitati nell'ambiente Skype for Business. Poiché il pool di applicazioni attendibili è configurato con l'opzione "Considera autenticato", non è necessario fornire password per la registrazione.

Configurazione su 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"/>

Configurazione su 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"/>

Verifica degli account del servizio CMS

La pagina di stato di CMS WebAdmin mostrerà se gli utenti Lync/Skype sono stati registrati correttamente. Nell'esempio seguente viene configurata una sola registrazione che è stata completata correttamente. Se lo stato indica registrazioni in corso da molto tempo, raccogliere i registri SIP e DNS per determinare

la causa dell'errore.

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

Configurazione Lync/Skype

Applicare i comandi seguenti in Lync/Skype Management Shell. Applicare i comandi nel server Front End.

Nota: I comandi suggeriti servono da guida. In caso di dubbi sulla configurazione del server Skype, è necessario contattare l'amministratore di Lync/Skype e/o il team di supporto.

Single CallBridge

Primo, dobbiamo dire a Skype di fidarsi del nostro CallBridge. A tale scopo, viene aggiunto un pool di applicazioni attendibili. Nella terminologia Microsoft "Pool" significa semplicemente "Cluster". In questo scenario il cluster è solo un cluster di un CallBridge. L'identità del cluster DEVE corrispondere al nome comune del certificato in uso in CallBridge. Microsoft utilizza questo valore come controllo di protezione. Non è sufficiente disporre dell'identità in una SAN. Se il nome comune non corrisponde, Microsoft interromperà la connessione TCP. Quando si utilizza questo comando, l'identità deve essere il nome di dominio completo di CallBridge. La funzione di registrazione deve essere il nome di dominio completo del pool Front End che gestisce queste connessioni. Il sito deve essere l'identificatore del sito Lync/Skype. Se non si è certi dei valori da utilizzare per la funzione di registrazione o il sito, contattare l'amministratore di Lync/Skype.

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

È quindi necessario configurare l'ambiente Microsoft in modo da consentire le comunicazioni in entrata dal CallBridge (Trusted Application Pool) sulla porta 5061.

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

L'ambiente Microsoft è attualmente configurato per accettare chiamate, ma non è in grado di effettuare chiamate di ritorno e di inviare presentazioni per le chiamate del gateway. Per risolvere il problema, è necessario aggiungere una route statica. Nello scenario con CallBridge singolo è sufficiente un unico percorso per consentire tutte le chiamate al dominio locale UC. Nei comandi seguenti Destination è l'FQDN del CallBridge a cui si desidera inviare le richieste SIP. Il campo MatchURI è la parte dell'URI relativa al dominio da utilizzare. In un ambiente Lync/Skype è possibile creare una sola route statica per MatchURI.

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

Infine, dobbiamo dire a Skype di implementare tutte le modifiche che abbiamo appena fatto.

```
Enable-CsTopology
```

CallBridge cluster

Innanzitutto, dobbiamo dire a Skype di fidarsi del nostro cluster CallBridge. A tale scopo, viene aggiunto un pool di applicazioni attendibili. Nella terminologia Microsoft "Pool" significa semplicemente "Cluster". L'identità del cluster DEVE corrispondere al nome comune dei certificati in uso sui propri CallBridge. Microsoft utilizza questo valore come controllo di protezione. Non è sufficiente disporre dell'identità in una SAN. Se il nome comune non corrisponde, Microsoft interromperà la connessione TCP. Quando si utilizza questo comando, l'identità deve essere il nome di dominio completo di CallBridge. ComputerFqdn deve essere il nome di dominio completo del primo CallBridge nel cluster. Specificando un ComputerFqdn si indica all'ambiente Lync/Skype che questo non è un cluster con un solo server. La funzione di registrazione deve essere il nome di dominio completo del pool Front End che gestisce queste connessioni. Il sito deve essere l'identificatore del sito Lync/Skype. Se non si è certi dei valori da utilizzare per la funzione di registrazione o il sito, contattare l'amministratore di Lync/Skype.

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

In questo ambiente è necessario aggiungere due CallBridge come computer di applicazioni attendibili. Il primo CallBridge è già stato aggiunto quando è stato creato il pool di applicazioni attendibili sopra indicato. Quando aggiungiamo questi computer dobbiamo associarli al pool che abbiamo appena creato. Ciò indica a Skype che nel cluster sono presenti altri computer che devono essere considerati attendibili. Tutte le identità dei computer devono essere elencate come SAN nei certificati CallBridge. Tali identità devono inoltre corrispondere alle intestazioni dei contatti nelle regole di composizione in uscita nei CallBridge. Se non corrispondono, Microsoft interromperà la connessione TCP.

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

È quindi necessario configurare l'ambiente Microsoft per consentire le comunicazioni in entrata dal cluster CallBridge (Trusted Application Pool) sulla porta 5061.

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

L'ambiente Microsoft è attualmente configurato per accettare chiamate, ma non è in grado di effettuare chiamate di ritorno e di inviare presentazioni per le chiamate del gateway. Per risolvere il problema, è necessario aggiungere route statiche. Innanzitutto è necessario aggiungere una route statica per consentire tutte le chiamate al dominio locale UC. Nei comandi seguenti Destination è l'FQDN del CallBridge a cui si desidera inviare le richieste SIP. Il campo MatchURI è la parte dell'URI relativa al dominio da utilizzare. In un ambiente Lync/Skype è possibile creare una sola route statica per MatchURI. Poiché la destinazione è il nome di dominio completo (FQDN) del cluster CallBridge e dispone di un record A DNS per ogni membro del cluster, Lync/Skype può inviare traffico a tutti i CallBridge. In questo modo, se uno si blocca, può instradare automaticamente le richieste del dominio verso un altro CallBridge nel cluster.

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

È quindi necessario creare una route statica aggiuntiva per ogni CallBridge nel cluster. Questo è un requisito per il callback e la presentazione per funzionare.

```
$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}
```

Infine, dobbiamo dire a Skype di implementare tutte le modifiche che abbiamo appena fatto.

```
Enable-CsTopology
```

Risoluzione dei problemi

Raccolta dei log dal CMS

Il primo passo per diagnosticare un problema è determinare la posizione del problema. A tale scopo, è necessario analizzare i registri da Cisco Meeting Server, ma prima è necessario raccogliergli. Ecco i miei consigli personali sui log da raccogliere.

Innanzitutto, abilitare il debug SIP e DNS per tutti i CallBridge tramite l'interfaccia WebAdmin. A tale scopo, passare a WebAdmin e quindi a Log > Analisi dettagliata. Da qui abilitare la registrazione SIP e DNS per i prossimi trenta minuti. Questo dovrebbe essere più che sufficiente per rilevare e diagnosticare il problema. Tenere presente che questa operazione deve essere eseguita singolarmente per tutti gli oggetti CallBridge, poiché l'abilitazione del log non è condivisa in un cluster.

In secondo luogo, abilitare le acquisizioni dei pacchetti su tutti i CallBridge. A tale scopo, connettersi a ciascun CallBridge tramite SSH ed eseguire il comando `pcap <interface>`, dove <interface> è il valore dell'interfaccia da usare per il traffico. Nella maggior parte dei casi si tratta dell'interfaccia a. Il

comando "pcap a" avvia l'acquisizione di un pacchetto sull'interfaccia a per il CallBridge a cui siamo connessi.

Quando l'acquisizione del pacchetto è in esecuzione su tutte le interfacce, il passaggio successivo è quello di generare il problema. Provate a fare una chiamata o fate quello che non riusciva. Al termine, terminare tutte le acquisizioni dei pacchetti. A tale scopo, è possibile immettere Ctrl-C in tutte le finestre SSH. Una volta completata l'acquisizione del pacchetto, il nome del file generato viene scritto sullo schermo. Tenere traccia di questo nome file poiché sarà necessario scaricarlo nel passaggio successivo.

Infine è necessario raccogliere i registri dai CallBridges. Per eseguire questa connessione tramite SFTP a ogni CallBridge. Scaricare il file logbundle.tar.gz e il file di acquisizione dei pacchetti generato. Questo file è disponibile solo in CMS2.2+. In CMS versioni 2.3+ includerà la configurazione completa del CMS. Se è in esecuzione la versione 2.2, non includerà le regole in entrata/in uscita, quindi è consigliabile eseguire screenshot di tali pagine e delle impostazioni di Lync Edge come riferimento. Assicurarsi di archiviare i log/screenshot raccolti in cartelle separate il cui nome corrisponda a quello di CallBridge da cui sono stati estratti i log. In questo modo sarà possibile verificare che i registri non vengano alterati.

Visualizzazione della configurazione di Lync/Skype

Questi comandi sono estremamente utili per la risoluzione dei problemi di configurazione di Lync/Skype. In questo documento vengono forniti comandi per creare e visualizzare la configurazione, ma non per rimuovere la configurazione. Ciò è dovuto al fatto che la rimozione della configurazione può essere pericolosa a meno che non venga eseguita da amministratori con una completa comprensione dell'ambiente Lync/Skype. Se è necessario rimuovere la configurazione, rivolgersi all'amministratore di Lync/Skype.

Comando	Descrizione
Get-CsTrustedApplicationPool	Con questo comando vengono elencati i cluster (pool) considerati attendibili da Lync/Skype. L'identità di questo pool DEVE corrispondere al nome comune dei certificati CallBridge. Anche in un singolo ambiente CallBridge è necessario specificare qui un cluster (pool) CallBridge di uno.
Get-CsTrustedApplicationComputer	Con questo comando vengono elencati i server trusted di Lync/Skype e il pool a cui sono associati questi server. Tutti i computer qui DEVONO essere identificati nel certificato inviato dai CallBridge. In un singolo ambiente CallBridge questo è in genere il nome comune. In un ambiente cluster questi computer DEVONO essere elencati come voci SAN (Subject Alternative Name). Inoltre, tutti i computer qui DEVONO essere identificati dalle voci del dominio del contatto locale nelle regole di composizione in uscita di CallBridge.
Get-CsTrustedApplication	Con questo comando vengono elencati i servizi con cui i pool di applicazioni attendibili possono comunicare. Per la comunicazione CMS con Lync/Skype useremo la porta TCP 5061 per il SIP crittografato TLS.
Get-CsStaticRoutingConfiguration Select-Object -Route ExpandProperty	Con questo comando vengono elencate le route statiche utilizzate da Lync/Skype per l'inoltro delle richieste. Il campo MatchURI è il dominio di destinazione del messaggio SIP. Il campo "Fqdn TLS" nel file XML deve indicare il server di destinazione per questo traffico.

Output di esempio dei comandi Lync/Skype Get

Di seguito è riportato l'output dei comandi Lync/Skype Get sopra riportati generati nei tre scenari di cluster CallBridge descritti in questo 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: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>
```

Connessione a TAC

In caso di errori con questa implementazione, contattare Cisco TAC. Quando si apre la richiesta di assistenza, includere un collegamento a questo documento, che consentirà ai tecnici TAC di comprendere la configurazione. Inoltre, sarebbe estremamente utile se i log di Cisco Meeting Server fossero associati alla richiesta come descritto sopra e l'output di tutti i comandi Get del Front End Lync/Skype fosse inserito nelle note della richiesta. Se non si includono queste informazioni, è sicuramente una delle prime richieste dei tecnici TAC, quindi è necessario raccoglierle prima di aprire la richiesta.