# Konfigurieren von Cisco Meeting Server und Skype for Business

## Inhalt



## Einleitung

In diesem Dokument wird beschrieben, wie Sie als Ergänzung der offiziellen Leitfäden Cisco Meeting Server (CMS) CallBridge Cluster mit Skype for Business konfigurieren. Dieses Dokument enthält ein Beispiel für eine einzelne CallBridge und ein weiteres Beispiel für einen drei CallBridge-Cluster. Es können jedoch nach Bedarf weitere CallBridges hinzugefügt werden. Es werden auch zwei CallBridge-Cluster unterstützt.

Verfasst von Rogelio Galindo und herausgegeben von Viridiana Fuentes, Cisco TAC Engineers.

# Voraussetzungen

## Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

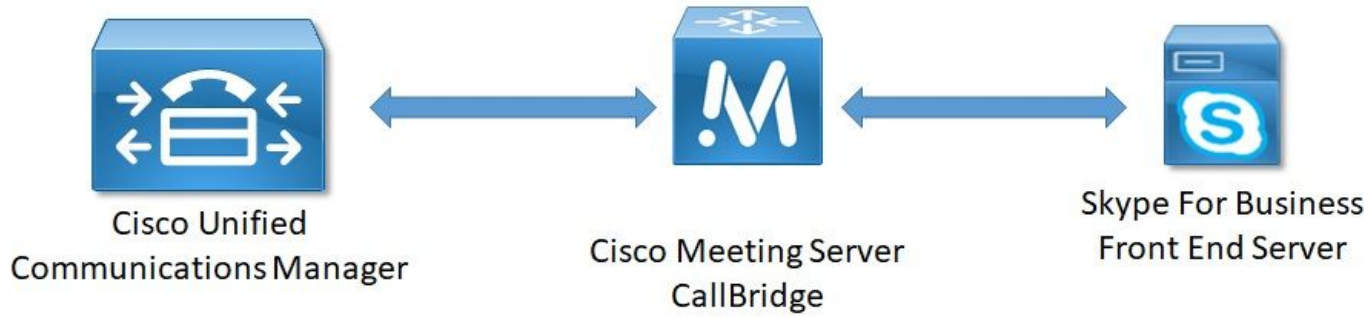
- Cisco Meeting Server (CMS)
- Domain Name Server (DNS)
- Skype for Business
- API (Application Programming Interface)

> **Hinweis**:Die Konfigurationsanleitung finden Sie hier: 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

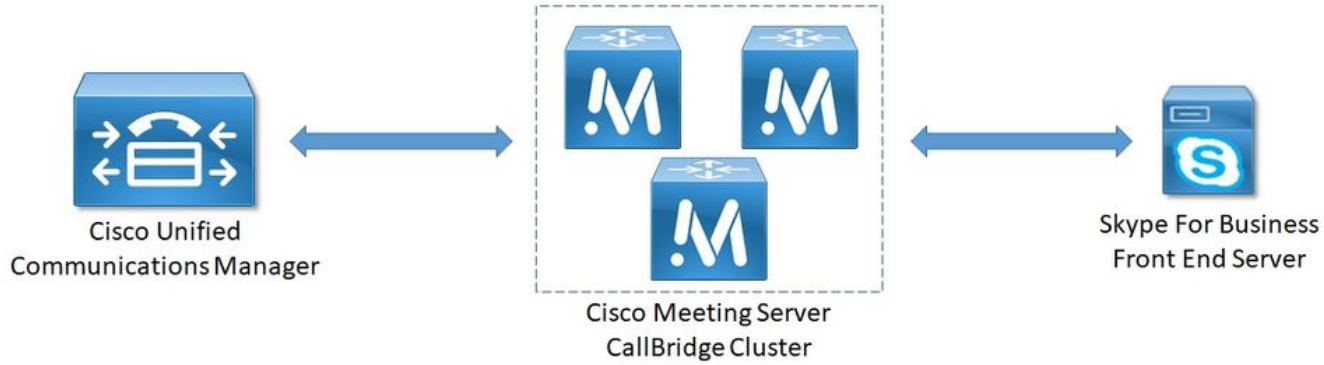
## Verwendete Komponenten

- 3 CMS-Server mit einem CallBridge-Cluster, Softwareversion 2.2.2.
- Skype for Business 2015
- Active Directory (AD) Windows Server 2012
- Secure Shell (SSH)-Client
- Secure File Transfer Protocol (SFTP)-Client wie WinSCP oder ähnliche
- API-Programm wie Postman oder Ähnliches
- Remotedesktop-Sitzung für Active Directory-, DNS- und Skype-Server

## Netzwerktopologie - Single CallBridge




## Netzwerktopologie - Clustered Call Bridges




## Voraussetzungen für das Callbridge-Zertifikat - Single CallBridge

Tabelle 1a enthält ein Beispiel für das CallBridge-Zertifikat für eine einzelne CallBridge-Umgebung.

Tabelle 1a

| CallBridge-Zertifikate | Beschreibung |
|---|---|
| **Eine Anrufbrücke** | |
| CN:cms.uc.local | CallBridge FQDN |

## Anforderungen an das Callbridge-Zertifikat - Clustered CallBridges

Tabelle 1b enthält ein Beispiel für die CallBridge-Zertifikate für eine geclusterte CallBridge-Umgebung. Ein einzelnes Zertifikat kann über die CallBridges in einem Cluster gemeinsam genutzt werden.

Tabelle 1b

| Callbridge-Zertifikate | Beschreibung |
|---|---|
| **Server 1: cms1.uc.local** | |
| CN:cms.uc.local | CallBridge-Cluster FQDN Dieser Datensatz muss an alle CallBridge-Cluster-Peers aufgelöst werden. |
| SAN: cms.uc.local | CallBridge-Cluster FQDN Dieser Datensatz muss an alle CallBridge-Cluster-Peers aufgelöst werden. |
| SAN: cms1.uc.local | CallBridge 1 FQDN |
| SAN: cms2.uc.local | CallBridge 2 FQDN |
| SAN: cms3.uc.local | CallBridge 3 FQDN |
| **Server 2: cms2.uc.local** | |
| CN:cms.uc.local | CallBridge-Cluster FQDN Dieser Datensatz muss an alle CallBridge-Cluster-Peers aufgelöst werden. |
| SAN: cms.uc.local | CallBridge-Cluster FQDN Dieser Datensatz muss an alle CallBridge-Cluster-Peers aufgelöst werden. |
| SAN: cms1.uc.local | CallBridge 1 FQDN |
| SAN: cms2.uc.local | CallBridge 2 FQDN |
| SAN: cms3.uc.local | CallBridge 3 FQDN |
| **Server 3: cms3.uc.local** | |
| CN:cms.uc.local | CallBridge-Cluster FQDN Dieser Datensatz muss an alle CallBridge-Cluster-Peers aufgelöst werden. |
| SAN: cms.uc.local | CallBridge-Cluster FQDN Dieser Datensatz muss an alle CallBridge-Cluster-Peers aufgelöst werden. |
| SAN: cms1.uc.local | CallBridge 1 FQDN |
| SAN: cms2.uc.local | CallBridge 2 FQDN |
| SAN: cms3.uc.local | CallBridge 3 FQDN |

Mit der CMS-CLI kann der Inhalt eines Zertifikats angezeigt werden:

```
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>
```

Bitte beachten Sie die Felder Betreff und X509v3 Subject Alternative Name. Diese werden zu einem späteren Zeitpunkt, wenn wir unsere Vertrauensbeziehungen in der Microsoft-Umgebung aufbauen, extrem wichtig sein.

```
        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
```

> **Anmerkung:** Den Leitfaden zur Zertifikatkonfiguration finden Sie hier: 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

## DNS-Datensatzanforderungen - Single CallBridge

Tabelle 2a zeigt ein Beispiel für die Konfiguration des DNS-Servers. Sie enthält eine Erklärung der Bedeutung der einzelnen Felder.

Tabelle 2a

| Ein Datensatz | IP-Beispiel | Beschreibung |
|---|---|---|
| cms.uc.local | 10.10.10.1 | CallBridge |
| fe.skype.local | 10.10.10.5 | Skype Front End Fully Qualified Domain Name (FQDN) |

## DNS-Datensatzanforderungen - Clustered Call Bridges

Tabelle 2b zeigt ein Beispiel für die Konfiguration des DNS-Servers. Sie enthält eine Erklärung der Bedeutung der einzelnen Felder.

Tabelle 2b

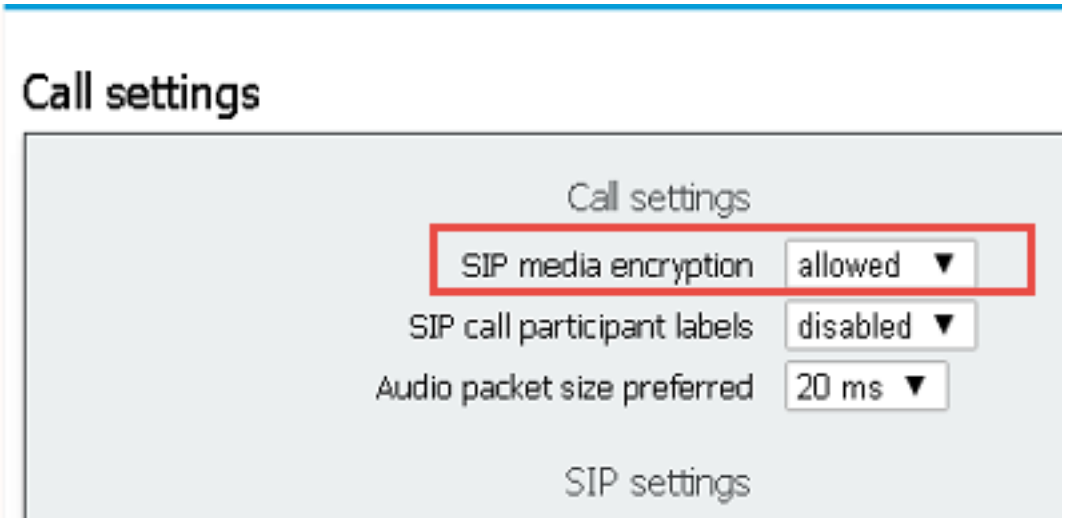
| Ein Datensatz | IP-Beispiel | Beschreibung |
|---|---|---|

| | | |
|---|---|---|
| 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<br>10.10.10.2<br>10.10.10.3 | Ein Datensatz, der zu allen CallBridges im Cluster aufgelöst wird. Dies wird als CallBridge-Cluster Fully Qualified Domain Name (FQDN) bezeichnet. |
| fe.skype.local | 10.10.10.5 | Skype Front End Fully Qualified Domain Name (FQDN) |

# Konfiguration

## SIP-Medienverschlüsselung

Navigieren Sie zu **Konfiguration > Anrufeinstellungen.** Die SIP-Medienverschlüsselung muss auf "Zulassen" gesetzt werden.




## Eingehende Regeln

Tabelle 3 beschreibt, was jedes Feld in der Konfiguration für eingehende Anrufe - Anrufzuordnung bedeutet.

Tabelle 3

| Feld für den Nummernplan für eingehende Anrufe | Beschreibung |
|---|---|
| Domänenname | Wenn ein Anruf mit dieser Domäne eingeht, suchen Sie mithilfe des Benutzerteils URI nach Übereinstimmungen in den aktivierten Zielen. |
| Priorität | Dadurch wird die Reihenfolge festgelegt, in der die Regeln berücksichtigt werden. Höhere Zahlen werden zuerst überprüft. Untere Zahlen werden zuletzt markiert. |
| Zielbereiche | Bei "Ja": Wenn der Benutzerteil des URI mit einem Leerzeichen übereinstimmt, da Anruf mit diesem Leerzeichen verbindet. |
| Zielkunden | Bei "Ja": Wenn der Benutzerteil des URI mit einem CMA-Benutzer übereinstimmt, versucht der Anruf, diesen Benutzer aufzurufen. |
| IVR-Ziele | Bei "Ja": Wenn der Benutzerteil des URI mit einer konfigurierten IVR übereinstimm wird der Anruf mit dieser IVR verbunden. |
| Ziele Lync | Bei "Ja": Wenn der Benutzerteil des URIs mit einer PSTN-Wählnummer eines Sky Business Meeting übereinstimmt, stellen Sie eine Verbindung zu diesem Meeting a Dual Home Call her. |
| Ziele Lync Simplejoin | Bei "Ja": Konvertieren Sie den Benutzerteil des URIs in ein HTTPS-Ziel, und versu Sie, ein Office365-Meeting zu finden, das unter dieser URL gehostet wird. |

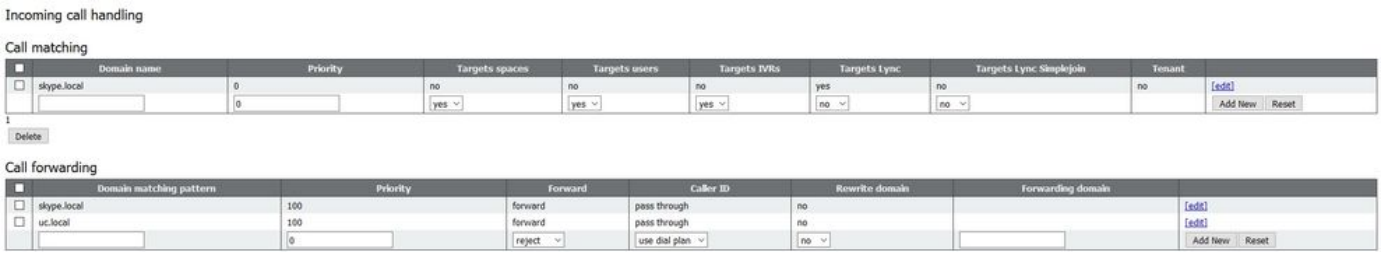
| | |
|---|---|
| Tenant | Dadurch wird festgelegt, für welche Tenants diese Regel gilt. |

Tabelle 4 beschreibt, was jedes Feld in der Konfiguration für eingehende Anrufe - Rufumleitung bedeutet.

Tabelle 4

| Feld für den Nummernplan zur Weiterleitung eingehender Anrufe | Beschreibung |
|---|---|
| Domänenzuordnungsmuster | Wenn ein Anruf bei dieser Domäne eingeht, leiten oder ablehnen Sie die Domäne wie konfiguriert weiter. |
| Priorität | Dadurch wird die Reihenfolge festgelegt, in der die Regeln berücksichtigt werden. Höhere Zahlen werden zuerst überprüft. Untere Zahlen werden zuletzt markiert. |
| Weiterleiten | Wenn die Weiterleitung festgelegt ist, wird der Anruf von den Regeln für ausgehende Anrufe behandelt. Wenn der Anruf auf Ablehnung eingestellt wird, wird er abgelehnt und nicht weitergeleitet. |
| Anrufer-ID | Wenn festgelegt, durch den from-Bereich der Domäne zu übergeben wird erhalten. Wenn der Wählplan auf Verwendung des Wählplans festgelegt ist, wird der aus-Teil wie in der Regel für ausgehende Anrufe konfiguriert neu geschrieben. Anmerkung: Passthrough kann nicht für Regeln verwendet werden, die einer Lync-/Skype-Domäne entsprechen, wenn sich die CallBridge in einem Cluster befindet. Dies würde die Präsentation bei Gateway-Anrufen unterbrechen. |
| Domäne umschreiben | Wenn diese Option aktiviert ist, ändern Sie die angerufene Domäne in den im Feld Weiterleitungsdomäne konfigurierten Wert. |
| Weiterleitungsdomäne | Wenn die Domäne rewrite aktiviert ist, ändert sich der Wert dieses Felds. |

## Konfigurationsbeispiel für eingehende Regeln - Single CallBridge




In dieser Umgebung sind die Dinge bemerkenswert einfach. Da keine geclusterten CallBridges verwendet werden, können wir für jede Domäne festlegen, dass die Weiterleitung als ihre Anrufer-ID verwendet wird. Dies kann in einer geclusterten Umgebung nicht durchgeführt werden, da die gemeinsame Nutzung von Präsentationen dadurch nicht möglich ist.

Zusätzlich gibt es eine Anrufabgleichregel für die Domäne Skype.local, wobei "Targets Lync" auf true festgelegt ist. Das bedeutet, wenn wir ein Lync-/Skype-Meeting über die PSTN-Wählnummer anrufen, sollten wir in der Lage sein, eine Verbindung als Dual-Home-Anruf herzustellen.

## Konfigurationsbeispiel für eingehende Regeln - Clustered Call Bridges

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 |

In dieser Umgebung wird ein CallBridge-Cluster verwendet, das aus drei CallBridges besteht. Aus diesem Grund benötigen wir eine Anrufweiterleitungsregel für jede CallBridge, die für das Umschreiben der Domäne auf uc.local konfiguriert ist. Das liegt daran, dass Benutzer von Lync/Skype, die Benutzer aus der UC-Umgebung zurückrufen, tatsächlich Anrufe in die Domäne cms1.uc.local, cms2.uc.local oder cms3.uc.local tätigen. Leider ist dies eine Einschränkung der Konfiguration, die erforderlich ist, damit Inhalte in einer geclusterten CallBridge-Umgebung funktionieren. Wir müssen diesen zurück in uc.local konvertieren, bevor wir den Anruf an den uc.local sip-Proxy weiterleiten.

Zusätzlich gibt es eine Anrufabgleichregel für die Domäne Skype.local, wobei "Targets Lync" auf true festgelegt ist. Das bedeutet, wenn wir ein Lync-/Skype-Meeting über die PSTN-Wählnummer anrufen, sollten wir in der Lage sein, eine Verbindung als Dual-Home-Anruf herzustellen.

## Ausgehende Regeln

Tabelle 5 beschreibt die Bedeutung jedes Felds in der Konfiguration ausgehender Anrufe.

Tabelle 5

| Feld für ausgehenden Wählplan | Beschreibung |
|---|---|
| Domäne | Für Anrufe aus dieser Domäne verwenden Sie diese Outbound-Regel |
| Verwendung des SIP-Proxys | Der SIP-Proxy sendet Anrufe an diese Domäne. |
| Lokale Kontaktdomäne | Bestimmt, welcher Wert in den Kontakt-Header eingefügt wird. Für die Lync-/Skype-Integration muss dieser Wert auf den FQDN der CallBridge festgelegt werden.<br>Anmerkung: Für ausgehende Regeln, die einen SIP-Proxy von Lync/Skype verwenden, MUSS dieses Feld konfiguriert werden. Bei ausgehenden Regeln, die einen SIP-Proxy verwenden, der nicht Lync/Skype ist, MUSS dieses Feld NICHT konfiguriert werden. |
| Lokal aus Domäne | Bestimmt, welcher Wert in den from-Header eingefügt wird. Dies ist die auf dem SIP-Proxy angezeigte Anrufer-ID-Adresse. Wenn dieses Feld leer gelassen wird, wird die konfigurierte "Domäne für lokalen Kontakt" verwendet. Lync/Skype verwendet dies als Ziel-URI für Callbacks und die gemeinsame Nutzung von Präsentationen.<br>Anmerkung: Dieser Wert wird nicht verwendet, wenn es sich bei dem Anruf um einen Gateway-Anruf handelt und die "Anrufer-ID" auf "Passthrough" (Durchwahl) eingestellt ist. |
| Trunk-Typ | Hierdurch wird festgelegt, welche SIP-Variation in der Kommunikation mit dem SIP-Proxy verwendet wird. |
| Verhalten | Dadurch wird festgelegt, ob wir weiterhin Regeln mit niedrigerer Priorität überprüfen ode die Suche im Falle einer Übereinstimmung beenden, bei der der Anruf nicht abgeschlossen werden konnte. |
| Priorität | Dadurch wird die Reihenfolge festgelegt, in der die Regeln berücksichtigt werden. Höhere Zahlen werden zuerst überprüft. Untere Zahlen werden zuletzt markiert. |
| Verschlüsselung | Dadurch wird festgelegt, ob verschlüsseltes oder unverschlüsseltes SIP verwendet wird. |
| Tenant | Dadurch wird festgelegt, für welche Tenants diese Regel gilt. |
| Bereich Anrufbrücke | Bestimmt, für welche CallBridges diese ausgehende Wählregel berücksichtigt wird. Bei geclusterten CallBridges muss dies erfolgen, um sicherzustellen, dass von jeder CallBridge die richtige Kontaktdomäne gesendet wird.<br>Anmerkung: Dieser Wert kann nur mithilfe der API wie unten erläutert festgelegt werden |

## Konfigurationsbeispiel für ausgehende Anrufe - eine 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 |

Erneut wie wir sehen, ist die einzelne CallBridge-Umgebung deutlich einfacher als die Cluster-Umgebung. Beachten Sie, dass wir eine Kontaktdomäne angeben. Dies liegt daran, dass wenn wir den vollqualifizierten Domänennamen unserer CallBridge nicht angeben, da die lokale Kontaktdomäne Lync/Skype Anrufe aus Sicherheitsgründen zurückweist. Da unsere Regeln für die Weiterleitung eingehender Anrufe so festgelegt sind, dass sie durchlaufen werden, werden wir die aus-Domäne in diesem Beispiel nicht umschreiben.

## Konfigurationsbeispiel für ausgehende Anrufe - Clustered Call Bridges

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 |

In dieser Umgebung wird ein CallBridge-Cluster verwendet, das aus drei CallBridges besteht. Aus diesem Grund benötigen wir eine Outbound-Regel für jede CallBridge mit unterschiedlichen lokalen Kontaktdomänen, lokal von Domänen und Bereichen. Es wird nur eine ausgehende Regel benötigt, um die Anrufe von allen CallBridges an den Cisco Unified Communications Manager weiterzuleiten. Um den Umfang festzulegen, muss die API verwendet werden.

# Modifizieren des Bereichs mit der API - Nur Clustered CallBridges

Nach dem Erstellen einer Regel für ausgehende Anrufe wird der Bereich für diese Regel auf <all> festgelegt. Das bedeutet, dass für alle CallBridges in einem Cluster eine Regel für ausgehenden Datenverkehr verwendet wird. Für ausgehende Regeln, die auf Lync/Skype hinweisen, müssen je nach verwendetem CallBridge ein anderer Kontakt und Header verwendet werden. Dazu müssen wir für jede CallBridge, bei der die Felder kontakt/from mit dieser CallBridge übereinstimmen, eine andere Outbound-Regel erstellen. Mithilfe der API müssen wir den Umfang dieser ausgehenden Wählregeln festlegen, sodass sie nur auf der CallBridge verarbeitet werden, die dieser Regel entspricht.

## Abrufen einer Liste aller CallBridges im Cluster

Navigieren Sie in einem Browser zur Seite /callbridges der CMS-API. Es werden alle CallBridges in Ihrem Cluster angezeigt.


Jetzt habe ich die IDs für alle meine CallBridges. Ihre IDs sind in Ihrer Umgebung unterschiedlich. Ich kann sehen, dass ich, wenn ich CallBridge cms1.uc.local referenzieren möchte, die ID von e4ab61ea-b5b4-4fac-ad4a-9979badea4e4 verwenden sollte.

## Abrufen einer Liste aller ausgehenden Wählregeln

Als Nächstes muss ich meine ausgehenden Regeln durchsuchen und mir deren IDs zuordnen. Navigieren Sie in einem Browser zur Seite /outbound

dialplanrules in der 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>
```

Jetzt habe ich die IDs für alle meine Regeln, aber ich kann nicht sagen, welches ist. Die erste Regel ist uns egal, da sie UC.local betrifft und wir dafür keinen Spielraum festlegen müssen. Wir müssen wissen, welche Regel für die verbleibenden ausgehenden Regeln für Skype.local gilt. Ab diesem Zeitpunkt ordne ich die IDs den CallBridges zu.

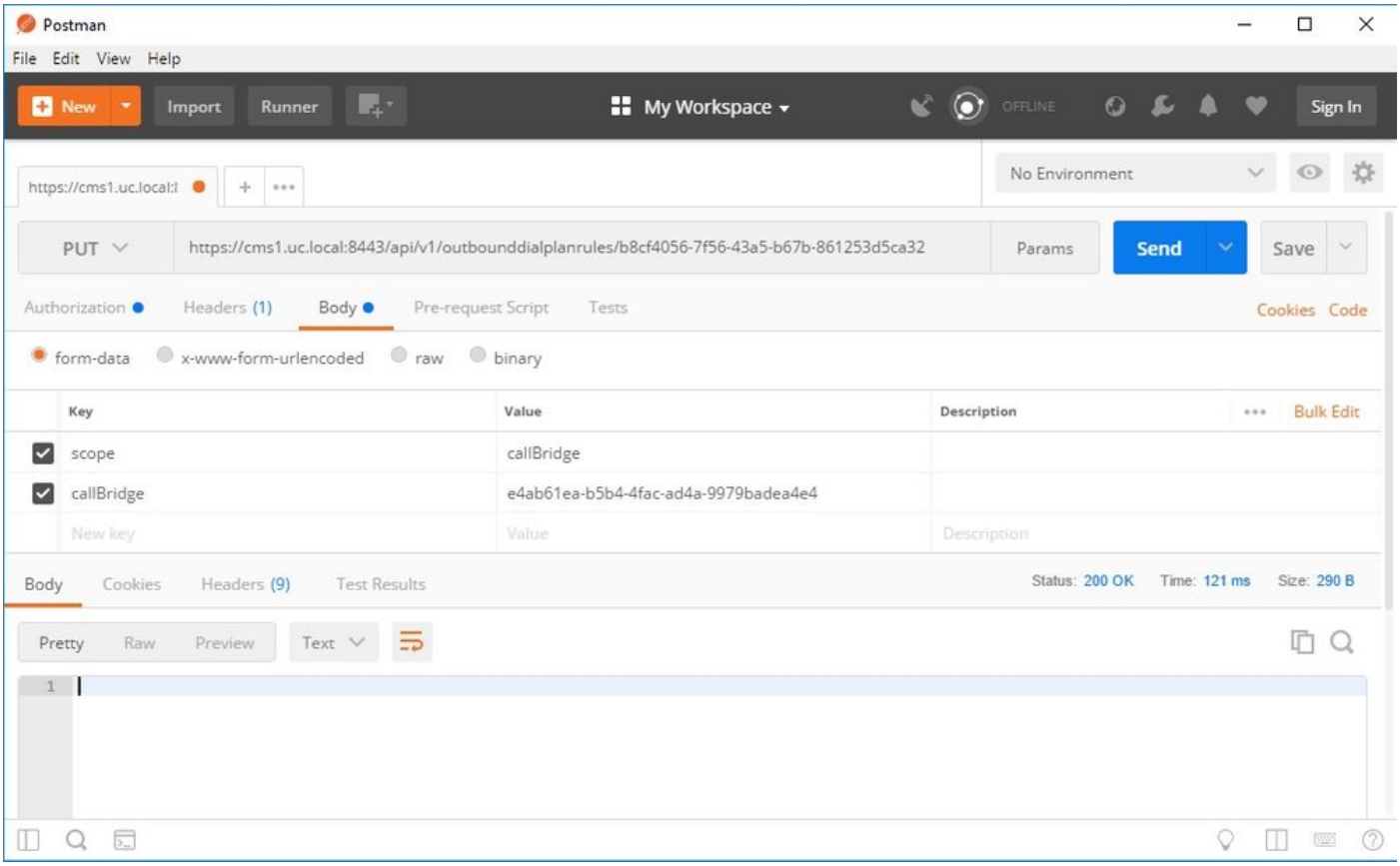
Ich werde in meinem Browser zu /outbound dialplanrules/b8cf4056-7f56-43a5-b67b-861253d5ca32 navigieren. Wenn Sie den hier aufgeführten Kontakt-Header lesen, kann ich Ihnen sagen, dass diese Regel für CMS1.UC.local gilt. Daher müssen wir den Umfang dieser Regel auf CMS1.UC.local festlegen.

## Senden Sie den CallBridge-Scope in

Mithilfe meines bevorzugten API-Tools sende ich einen PUT an die API unter /outbound dialplanrules/b8cf4056-7f56-43a5-b67b-861253d5ca32 mit dem folgenden Text:

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

In diesem Screenshot verwende ich PostMan, um diese Anfrage zu senden.




Wenn dieser HTTP-PUT erfolgreich war, sollte die Seite mit den Wählregeln für ausgehende Anrufe in WebAdmin nun einen Gültigkeitsbereich enthalten, der angewendet wurde. Wenn der Webadmin der CallBridge anzeigt, dass der auf ihn angewendete Bereich <local> angezeigt wird. Wenn der Webadmin einer anderen CallBridge verwendet wird, um die Regeln für ausgehende Anrufe anzuzeigen, sollte der CallBridge-FQDN im Bereichsfeld angezeigt werden. Ein Gültigkeitsbereich von <all> bedeutet, dass die Regel auf allen CallBridges verwendet wird. Ein Gültigkeitsbereich von <none> bedeutet, dass ein Bereich aktiviert wurde, jedoch keine CallBridges mit dem Gültigkeitsbereich übereinstimmen.

Nachdem der Bereich für eine CallBridge festgelegt wurde, muss er für jede zusätzliche CallBridge konfiguriert werden. Nach Abschluss dieser Konfiguration sollte jede ausgehende Regel für Ihre Skype-Domäne einen Gültigkeitsbereich haben.

## CMS-Dienstkonten

Auf der allgemeinen Konfigurationsseite von WebAdmin befindet sich ein Abschnitt mit Lync Edge-Einstellungen. Um TURN-Dienste zu nutzen oder über die PSTN-Einwahlnummer an Dual-Home-Meetings teilzunehmen, muss dies konfiguriert werden.

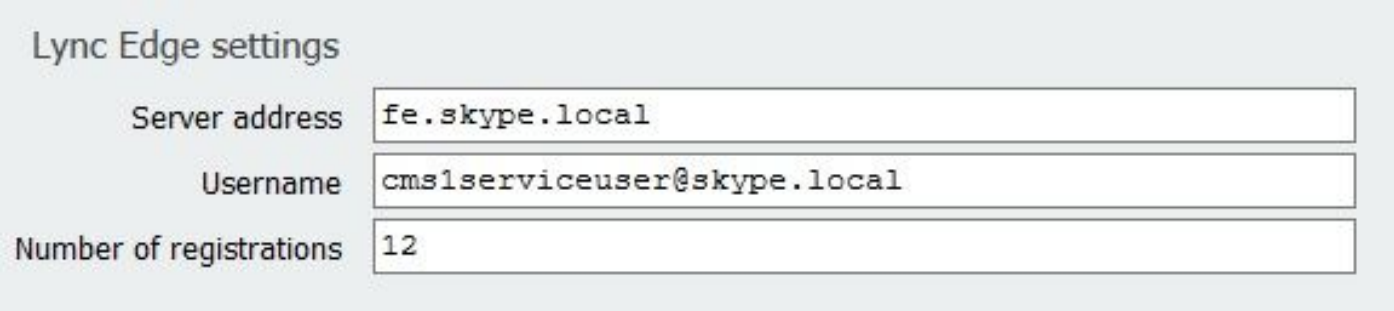
Tabelle 6 beschreibt, was jedes Feld in der Lync Edge-Konfiguration bedeutet.

Tabelle 6

| Feld "Lync Edge settings" | Beschreibung |
|---|---|
| Serveradresse | Vollqualifizierter Domänenname (FQDN) Ihres Front-End-Pools |
| Benutzername | Der Benutzername des Dienstkontos, das Sie für CMS verwenden möchten. |
| Anzahl der Registrierungen | Wie viele verschiedene Benutzerkonten möchten Sie registrieren? Wenn hier kein Wert konfiguriert ist, wird nur der oben angegebene Benutzername registriert. Wenn hier eine Zahl angewendet wird, werden die Zahlen 1-X als Suffixe auf den Benutzerteil des URIs angewendet, wobei X für die in diesem Feld konfigurierte Zahl steht. |

## Beispielkonfiguration eines CMS-Dienstkontos

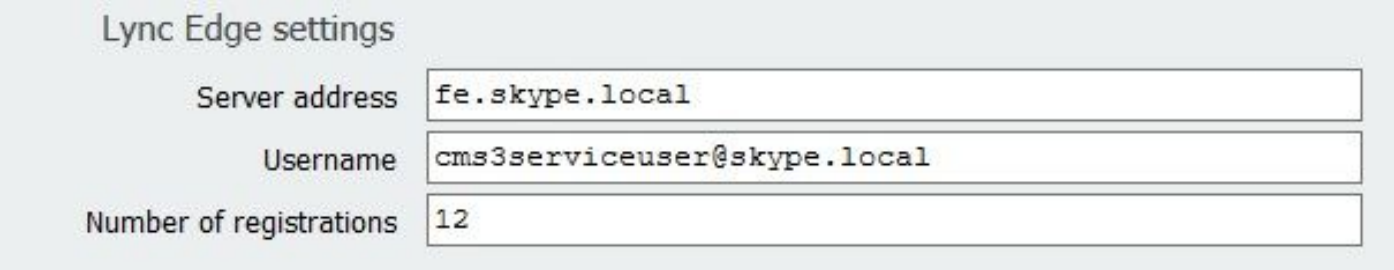
Konfiguration auf CMS1:




Diese Konfiguration registriert cms1serviceuser1@skype.local, cms1serviceuser2@skype.local, cms1serviceuser3@skype.local, ... cms1serviceuser11@skype.local und cms1serviceuser12@skype.local auf fe.skype.local. Da ich in diesem Beispiel in einer Cluster-Umgebung bin, müsste ich auch Dienstkonten für meine anderen CallBridges erstellen und separat konfigurieren. Beachten Sie, dass die Benutzernamen in diesem Beispiel unterschiedlich sind. Auf CMS1 werden den Benutzernamen cms1 vorangestellt. Auf CMS2 werden die Benutzernamen mit dem Präfix cms2 versehen. Auf CMS3 lautet das Präfix cms3. Alle diese Konten wurden in der Skype for Business-Umgebung erstellt und aktiviert. Da unser vertrauenswürdiger Anwendungspool mit "Als authentifiziert behandeln" konfiguriert ist, müssen wir keine Kennwörter zur Registrierung angeben.

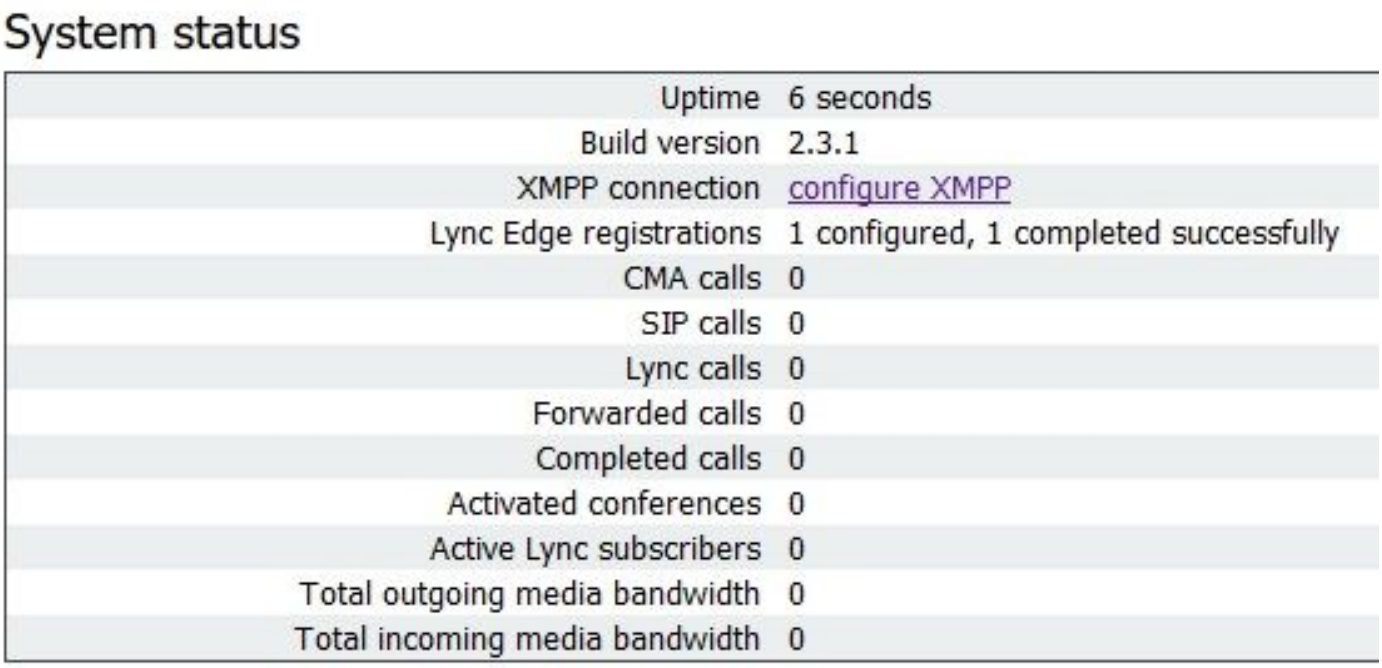
Konfiguration auf CMS2:


Konfiguration auf CMS3:




# Überprüfen von CMS-Dienstkonten

Auf der Statusseite des CMS WebAdmin wird angezeigt, ob die Lync-/Skype-Benutzer erfolgreich registriert wurden. Im folgenden Beispiel konfigurieren wir nur eine Registrierung und sie wurde erfolgreich abgeschlossen. Wenn Sie bemerken, dass der Status lange Zeit die laufenden Registrierungen anzeigt, sammeln Sie SIP- und DNS-Protokolle, um zu ermitteln, warum der Fehler auftritt.




## Lync/Skype-Konfiguration

Wenden Sie die folgenden Befehle in der Management-Shell von Lync/Skype an. Wenden Sie die Befehle auf dem Front End-Server an.

> **Anmerkung:** Die vorgeschlagenen Befehle dienen als Anleitung. Falls Sie Zweifel an der Konfiguration auf dem Skype-Server haben, müssen Sie sich an Ihr Lync/Skype-Administrator- und/oder Support-Team wenden.

## Eine Anrufbrücke

Zunächst müssen wir Skype auffordern, unserer CallBridge zu vertrauen. Hierzu fügen wir einen vertrauenswürdigen Anwendungspool hinzu. In der Microsoft-Terminologie bedeutet "Pool" nur "Cluster". In diesem Szenario ist unser Cluster nur ein Cluster aus einer CallBridge. Die Identität unseres Clusters MUSS mit dem gebräuchlichen Namen des Zertifikats übereinstimmen, das in unserer CallBridge verwendet wird. Microsoft verwendet dies als Sicherheitsprüfung. Die Identität in einem SAN reicht nicht aus. Wenn der gemeinsame Name nicht mit Microsoft übereinstimmt, wird die TCP-Verbindung beendet. Bei Verwendung dieses Befehls sollte die Identität der CallBridge FQDN sein. Der Registrar sollte der FQDN des Front-End-Pools sein, der diese Verbindungen bedient. Die Site sollte die Lync/Skype Site Identifier sein. Wenn Sie sich nicht sicher sind, welche Werte für die Registrierung oder die Website verwendet werden sollen, wenden Sie sich bitte an Ihren Lync-/Skype-Administrator.

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

Als Nächstes muss die Microsoft-Umgebung so konfiguriert werden, dass eingehende Kommunikation von unserem CallBridge (Trusted Application Pool) auf Port 5061 ermöglicht wird.

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

Die Microsoft-Umgebung ist derzeit so konfiguriert, dass sie Anrufe entgegennimmt, jedoch keine Rückrufe tätigen und keine Präsentation für Gateway-Anrufe senden kann. Um dies zu korrigieren, muss eine statische Route hinzugefügt werden. Im Einzel-CallBridge-Szenario benötigen wir nur eine Route, um alle Anrufe an unsere UC.local-Domäne zuzulassen. In den folgenden Befehlen ist Destination der FQDN der CallBridge, an den wir SIP-Anfragen senden möchten. Das MatchURI-Feld ist der Domänenteil des URI, der verwendet werden soll. Bitte beachten Sie, dass in einer Lync-/Skype-Umgebung nur eine statische Route pro MatchURI erstellt werden kann.

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

Schließlich müssen wir Skype auffordern, alle Änderungen, die wir gerade vorgenommen haben, umzusetzen.

```
Enable-CsTopology
```

## Clustered Call Bridges

Zunächst müssen wir Skype auffordern, unserem CallBridge-Cluster zu vertrauen. Hierzu fügen wir einen vertrauenswürdigen Anwendungspool hinzu. In der Microsoft-Terminologie bedeutet "Pool" nur "Cluster". Die Identität unseres Clusters MUSS mit dem gebräuchlichen Namen der Zertifikate übereinstimmen, die in unseren CallBridge(s) verwendet werden. Microsoft verwendet dies als Sicherheitsprüfung. Die Identität in einem SAN reicht nicht aus. Wenn der gemeinsame Name nicht mit Microsoft übereinstimmt, wird die TCP-Verbindung beendet. Bei Verwendung dieses Befehls sollte die Identität der CallBridge FQDN sein. ComputerFqdn sollte der FQDN der ersten CallBridge in Ihrem Cluster sein. Durch Angeben eines ComputerFqdn geben Sie der Lync-/Skype-Umgebung an, dass es sich nicht um ein Cluster mit nur einem Server handelt. Der Registrar sollte der FQDN des Front-End-Pools sein, der diese Verbindungen bedient. Die Site sollte die Lync/Skype Site Identifier sein. Wenn Sie sich nicht sicher sind, welche Werte für die Registrierung oder die Website verwendet werden sollen, wenden Sie sich bitte an Ihren Lync-/Skype-Administrator.

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

In dieser Umgebung müssen zwei CallBridges als Trusted Application Computers hinzugefügt werden. Die erste CallBridge wurde bereits hinzugefügt, als der oben angegebene vertrauenswürdige Anwendungspool erstellt wurde. Wenn wir diese Computer hinzufügen, müssen wir sie mit dem soeben erstellten Pool verknüpfen. Dies sagt Skype, dass wir weitere Computer in unserem Cluster haben, denen man vertrauen muss. Alle hier aufgeführten Computer-Identitäten müssen als SANs in unseren CallBridge-Zertifikaten aufgeführt sein. Diese Identitäten müssen auch mit den Kontaktheadern der ausgehenden Wählregeln in den CallBridges übereinstimmen. Wenn sie nicht übereinstimmen, reißt Microsoft die TCP-Verbindung ab.

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

Als Nächstes muss die Microsoft-Umgebung so konfiguriert werden, dass eingehende Kommunikation von unserem CallBridge-Cluster (Trusted Application Pool) auf Port 5061 zugelassen wird.

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

Die Microsoft-Umgebung ist derzeit so konfiguriert, dass sie Anrufe entgegennimmt, jedoch keine Rückrufe tätigen und keine Präsentation für Gateway-Anrufe senden kann. Um dies zu korrigieren, müssen statische Routen hinzugefügt werden. Zuerst müssen wir eine statische Route hinzufügen, um alle Anrufe an unsere UC.local-Domäne zuzulassen. In den folgenden Befehlen ist Destination der FQDN der CallBridge, an den wir SIP-Anfragen senden möchten. Das MatchURI-Feld ist der Domänenteil des URI, der verwendet werden soll. Bitte beachten Sie, dass in einer Lync-/Skype-Umgebung nur eine statische Route pro MatchURI erstellt werden kann. Da das Ziel der FQDN unseres CallBridge-Clusters ist und es einen DNS-A-Datensatz für jedes Mitglied des Clusters hat, kann Lync/Skype Datenverkehr an alle unsere CallBridges senden. Fällt also eine Verbindung aus, können Anfragen für unsere Domäne automatisch an eine andere CallBridge im Cluster weitergeleitet werden.

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

Als Nächstes müssen wir eine zusätzliche statische Route für jede CallBridge im Cluster erstellen. Dies ist eine Voraussetzung für die erfolgreiche Rückruffunktion und Präsentation.

```
$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}
```

Schließlich müssen wir Skype auffordern, alle Änderungen, die wir gerade vorgenommen haben, umzusetzen.

```
Enable-CsTopology
```

# Fehlerbehebung

## Erfassen von Protokollen aus dem CMS

Der erste Schritt bei der Diagnose eines Problems besteht darin, den Ort des Problems zu bestimmen. Dazu müssen die Protokolle vom Cisco Meeting Server analysiert werden. Zunächst müssen sie jedoch erfasst werden. Hier sind meine persönlichen Empfehlungen für Protokolle zu sammeln.

Aktivieren Sie zuerst das SIP- und DNS-Debugging für alle CallBridges über die WebAdmin-Schnittstelle. Navigieren Sie dazu zum WebAdmin und dann zu Logs > Detailed Tracing. Aktivieren Sie von hier aus die SIP- und DNS-Protokollierung für die nächsten 30 Minuten. Dies sollte mehr als die Zeit sein, das Problem zu erkennen und zu diagnostizieren. Beachten Sie, dass dies für alle CallBridges einzeln durchgeführt werden muss, da die Protokollaktivierung nicht für alle Cluster freigegeben wird.

Aktivieren Sie anschließend die Paketerfassung für alle CallBridges. Um diese Verbindung über SSH mit jeder CallBridge herzustellen und den Befehl pcap <interface> auszuführen, wobei <interface> für den Schnittstellendatenverkehr verwendet werden soll. In den meisten Fällen handelt es sich dabei um Schnittstelle a. Der Befehl "pcap a" startet also eine Paketerfassung auf Schnittstelle a für die CallBridge, mit der wir verbunden sind.

Wenn die Paketerfassung auf allen Schnittstellen ausgeführt wird, besteht der nächste Schritt darin, das Problem zu erzeugen. Gehen Sie voran, versuchen Sie einen Anruf, oder tun Sie, was immer der Fehler war. Nach Abschluss dieses Vorgangs werden alle Paketerfassungen beendet. Dies kann durch die Eingabe von Strg-C in allen SSH-Fenstern erfolgen. Nach Abschluss der Paketerfassung wird der Name der erstellten Datei auf den Bildschirm geschrieben. Behalten Sie diesen Dateinamen im Auge, da wir ihn im nächsten Schritt herunterladen müssen.

Schließlich müssen die Protokolle von den CallBridges erfasst werden. Um diese Verbindung über SFTP mit jeder CallBridge herzustellen. Laden Sie die Datei "logbündel.tar.gz" und die generierte Paketerfassungsdatei herunter. Diese Datei ist nur in CMS2.2+ verfügbar. In CMS Version 2.3+ wird die vollständige Konfiguration Ihres CMS enthalten sein. Wenn Sie die Version 2.2 ausführen, werden die Inbound/Outbound-Regeln nicht berücksichtigt. Daher empfiehlt es sich, Screenshots dieser Seiten sowie die Lync Edge-Einstellungen als Referenz zu erstellen. Speichern Sie die Protokolle/Screenshots, die in separaten Ordnern gesammelt wurden, die einen Namen haben, der der CallBridge entspricht, aus der die Protokolle gezogen wurden. Dadurch wird sichergestellt, dass die Protokolle nicht durcheinander geraten.

## Anzeigen der Lync-/Skype-Konfiguration

Diese Befehle sind bei der Fehlerbehebung der Lync-/Skype-Konfiguration äußerst hilfreich. In diesem Dokument werden Befehle zum Erstellen und Anzeigen von Konfigurationen angegeben, zum Entfernen von Konfigurationen werden jedoch keine Befehle angegeben. Das liegt daran, dass das Entfernen der Konfiguration gefährlich sein kann, wenn sie nicht von Administratoren durchgeführt wird, die mit der Lync-/Skype-Umgebung vertraut sind. Wenn Sie die Konfiguration entfernen müssen, wenden Sie sich hierzu an Ihren Lync-/Skype-Administrator.

| Command | Beschreibung |
| --- | --- |
| Get-CsTrustedApplicationPool | Dieser Befehl listet Cluster (Pools) auf, denen Lync/Skype vertrauen. Die Identität dieses Pools MUSS mit dem gebräuchlichen Namen des bzw. der CallBridge-Zertifikate übereinstimmen. Sogar in einer einzelnen CallBridge-Umgebung muss hier ein CallBridge-Cluster (Pool) von einem angegeben werden. |
| Get-CsTrustedApplicationComputer | Dieser Befehl listet Server auf, denen Lync/Skype vertrauen und die diese Server in Pools verbinden. Alle Computer hier MÜSSEN im von den CallBridges gesendeten Zertifikat identifiziert werden. In einer einzelnen CallBridge-Umgebung ist dies in der Regel der übliche Name. In einer Cluster-Umgebung MÜSSEN diese Computer als SAN-Einträge (Subject Alternative Name) aufgeführt werden. Zusätzlich MÜSSEN alle Computer hier durch lokale Kontaktdomäneneinträge in den ausgehenden CallBridge-Wählregeln identifiziert werden. |
| Get-CsTrustedApplication | Dieser Befehl listet auf, mit welchen Diensten vertrauenswürdige Anwendungspools kommunizieren dürfen. Für die CMS-Kommunikation mit Lync/Skype wird der TCP-Port 5061 für TLS-verschlüsseltes SIP verwendet. |
| Get-CsStaticRoutingKonfiguration \| Select-Objekt-ExpandProperty-Route | Dieser Befehl listet die statischen Routen auf, die Lync/Skype für die Weiterleitung von Anfragen verwendet. Das MatchURI-Feld ist die Zieldomäne der SIP-Nachricht. Das Feld "TLS Fqdn" im XML sollte den Zielserver für diesen Datenverkehr anzeigen. |

### Beispielausgabe der Befehle Lync/Skype Get

Unten sehen Sie die Ausgabe der oben genannten Befehle von Lync/Skype Get, die im drei in diesem Dokument behandelten CallBridge-Cluster-Szenario ausgegeben werden.

```
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>
```

# TAC kontaktieren

Wenn bei dieser Implementierung Fehler auftreten, wenden Sie sich bitte an das Cisco TAC. Fügen Sie beim Öffnen der Serviceanfrage einen Link zu diesem Dokument ein. Es hilft den TAC-Technikern, Ihre Konfiguration zu verstehen. Darüber hinaus wäre es äußerst hilfreich, wenn die Cisco Meeting Server-Protokolle wie oben beschrieben an den Fall angehängt werden und die Ausgabe aller Get-Befehle vom Front End von Lync/Skype in die Fallnotizen eingegeben wird. Wenn Sie diese Informationen nicht angeben, ist es sicher, dass es sich um eines der ersten Dinge handelt, die die TAC-Techniker erfragen. Bitte holen Sie sie daher zuerst ab, bevor Sie ein Ticket erstellen.