Configurer Cisco Meeting Server et Skype Entreprise

Contenu

Introduction

Ce document décrit comment configurer le cluster CallBridge de Cisco Meeting Server (CMS) avec Skype Entreprise en complément des guides officiels. Ce document fournit un exemple d'un seul pont d'appel et un autre exemple d'un cluster de trois ponts d'appel, mais des ponts d'appel supplémentaires peuvent être ajoutés si nécessaire. Deux clusters CallBridge sont également pris en charge.

Contribué par Rogelio Galindo et édité par Viridiana Fuentes, Ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

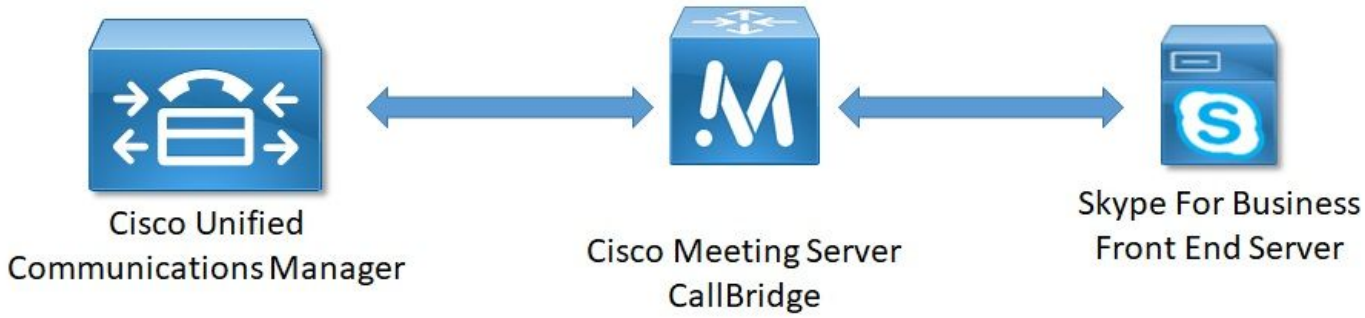
- Cisco Meeting Server (CMS)
- Serveur de noms de domaine (DNS)
- Skype Entreprise
- API (Application Programming Interface)

> **Remarque** : le guide de configuration est disponible ici : 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

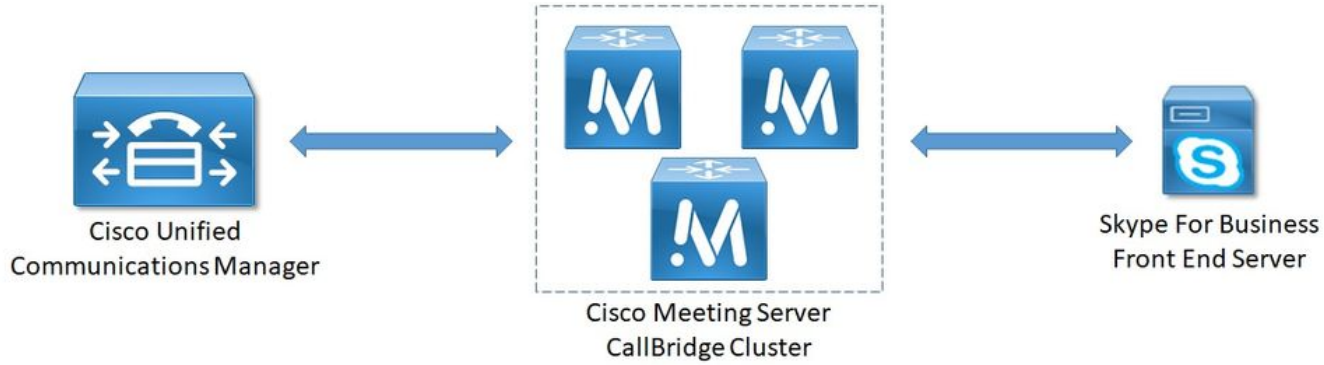
Components Used

- 3 serveurs CMS exécutant un cluster CallBridge, version logicielle 2.2.2.
- Skype Entreprise 2015
- Windows Server 2012 Active Directory (AD)
- Client Secure Shell (SSH)
- Client SFTP (Secure File Transfer Protocol) tel que WinSCP ou similaire
- Programme API tel que Postman ou similaire
- Session Bureau à distance pour Active Directory, DNS et serveur Skype

Topologie réseau - Pont d'appel unique



Topologie réseau - Ponts d'appels en cluster



Exigences relatives au certificat Callbridge - Single CallBridge

Le tableau 1a fournit un exemple de certificat CallBridge pour un environnement CallBridge unique.

Tableau 1a

Certificats CallBridge	Description
Pont d'appel unique	
CN : cms.uc.local	FQDN CallBridge

Exigences de certificat Callbridge - Pontages d'appels en cluster

Le tableau 1b fournit un exemple de certificats CallBridge pour un environnement CallBridge en cluster. Un certificat unique peut être partagé sur les ponts d'appels d'un cluster.

Tableau 1b

Certificats Callbridge	Description
Serveur 1 : cms1.uc.local	
CN : cms.uc.local	Nom de domaine complet du cluster CallBridge. Cet enregistrement doit être résolu pour tous les homologues de cluster CallBridge.
SAN : cms.uc.local	Nom de domaine complet du cluster CallBridge. Cet enregistrement doit être résolu pour tous les homologues de cluster CallBridge.
SAN : cms1.uc.local	Nom de domaine complet CallBridge 1.
SAN : cms2.uc.local	Nom de domaine complet CallBridge 2.
SAN : cms3.uc.local	Nom de domaine complet CallBridge 3.
Serveur 2 : cms2.uc.local	
CN : cms.uc.local	Nom de domaine complet du cluster CallBridge. Cet enregistrement doit être résolu pour tous les homologues de cluster CallBridge.
SAN : cms.uc.local	Nom de domaine complet du cluster CallBridge. Cet enregistrement doit être résolu pour tous les homologues de cluster CallBridge.
SAN : cms1.uc.local	Nom de domaine complet CallBridge 1.
SAN : cms2.uc.local	Nom de domaine complet CallBridge 2.
SAN : cms3.uc.local	Nom de domaine complet CallBridge 3.
Serveur 3 : cms3.uc.local	
CN : cms.uc.local	Nom de domaine complet du cluster CallBridge. Cet enregistrement doit être résolu pour tous les homologues de cluster CallBridge.
SAN : cms.uc.local	Nom de domaine complet du cluster CallBridge. Cet enregistrement doit être résolu pour tous les homologues de cluster CallBridge.
SAN : cms1.uc.local	Nom de domaine complet CallBridge 1.

SAN : cms2.uc.local Nom de domaine complet CallBridge 2.
SAN : cms3.uc.local Nom de domaine complet CallBridge 3.

L'interface CLI CMS peut être utilisée pour afficher le contenu d'un certificat :

```
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>
```

Veuillez prendre note des champs Subject et X509v3 Subject Alternative Name. Celles-ci seront extrêmement importantes plus tard lorsque nous établirons nos relations de confiance dans l'environnement 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**: Le guide de configuration des certificats se trouve ici : 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

Exigences d'enregistrement DNS - Pont d'appel unique

Le tableau 2a fournit un exemple de configuration du serveur DNS. Il fournit une explication de ce que chaque champ signifie.

Tableau 2a

Un enregistrement	Exemple IP	Description
cms.uc.local	10.10.10.1	Pont d'appel
fe.skype.local	10.10.10.5	Nom de domaine complet (FQDN) du frontal Skype

Exigences d'enregistrement DNS - Pontages d'appels en cluster

Le tableau 2b fournit un exemple de configuration du serveur DNS. Il fournit une explication de ce que chaque champ signifie.

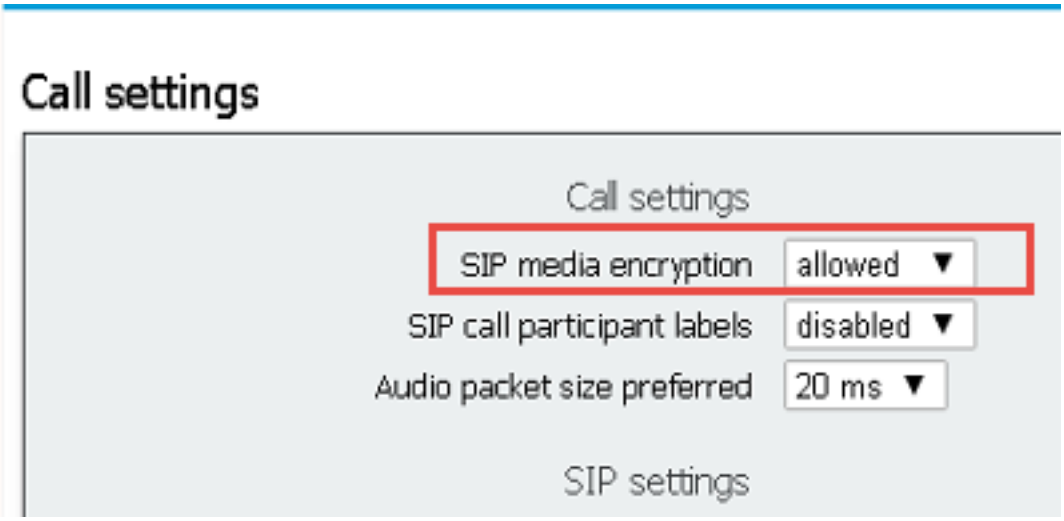
Tableau 2b

Un enregistrement	Exemple IP	Description
cms1.uc.local	10.10.10.1	CallBridge 1
cms2.uc.local	10.10.10.2	CallBridge 2
cms3.uc.local	10.10.10.3	CallBridge 3
cms.uc.local	10.10.10.1 10.10.10.2 10.10.10.3	Un enregistrement A qui se résout à tous les ponts d'appels du cluster. Ce nor sera appelé nom de domaine complet du cluster CallBridge (FQDN)
fe.skype.local	10.10.10.5	Nom de domaine complet (FQDN) du frontal Skype

Configuration

Chiffrement de support SIP

Accédez à **Configuration > Call Settings.** Le cryptage de support SIP doit être défini sur autorisé.



Règles entrantes

Le tableau 3 décrit la signification de chaque champ de la configuration Appels entrants - Correspondance d'appels.

Tableau 3

Champ Plan de numérotation correspondant à l'appel entrant	Description
le nom de domaine	Si un appel est reçu avec ce domaine, utilisez la partie utilisateur de l'URI pour rechercher des correspondances dans les cibles activées.
Priorité	Cela détermine l'ordre dans lequel les règles seront prises en compte. Les nomb plus élevés seront d'abord vérifiés. Les numéros inférieurs seront vérifiés en der
Espaces cibles	Si la valeur est yes : si la partie utilisateur de l'URI correspond à un espace, l'ap connecte à cet espace.
Utilisateurs cibles	Si la valeur est yes : si la partie utilisateur de l'URI correspond à un utilisateur Cl l'appel tente d'appeler cet utilisateur.
Cible IVR	Si la valeur est yes : si la partie utilisateur de l'URI correspond à un IVR configur l'appel se connecte à cet IVR.
Cible Lync	Si la valeur est yes : Si la partie utilisateur de l'URI correspond à un numéro de numérotation RTPC d'une téléconférence Skype Entreprise se connecte à cette

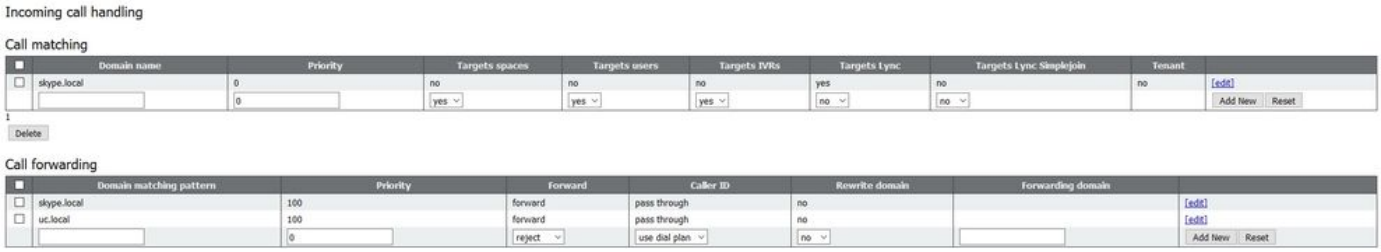
	téléconférence en tant qu'appel à résidence double.
Cible Lync Simplejoin	Si la valeur est yes : Convertissez la partie utilisateur de l'URI en cible HTTPS e essayez de trouver une réunion Office365 hébergée à cette URL.
Locataire	Cela détermine les locataires pour lesquels cette règle sera prise en compte.

Le tableau 4 décrit la signification de chaque champ de la configuration Appels entrants - Renvoi d'appels.

Tableau 4

Champ Plan de numérotation de transfert d'appel entrant	Description
Modèle de correspondance de domaine	Si un appel est reçu avec ce domaine, transférez ou rejetez le domaine tel que configuré.
Priorité	Cela détermine l'ordre dans lequel les règles seront prises en compte. Les nombre plus élevés seront d'abord vérifiés. Les numéros inférieurs seront vérifiés en dernie
Transférer	Si cette option est définie pour transférer l'appel, il sera traité par les règles de trafi sortant. Si défini sur rejeter l'appel, il sera rejeté et non transféré.
ID de l'appelant	Si cette option est définie pour passer par la partie du domaine de départ, elle sera conservée. Si cette option est définie pour utiliser le plan de numérotation, la partie sera réécrite comme configurée dans la règle de sortie. Note: L'intercommunication ne peut pas être utilisée pour les règles qui correspond un domaine Lync/Skype si CallBridge se trouve dans un cluster. Cela interromprait présentation des appels de passerelle.
Réécrire le domaine	Si cette option est activée, remplacez le domaine appelé par la valeur configurée d le champ de domaine de transfert.
Domaine de transfert	Si le domaine de réécriture est activé, le domaine appelé passe à la valeur de ce champ.

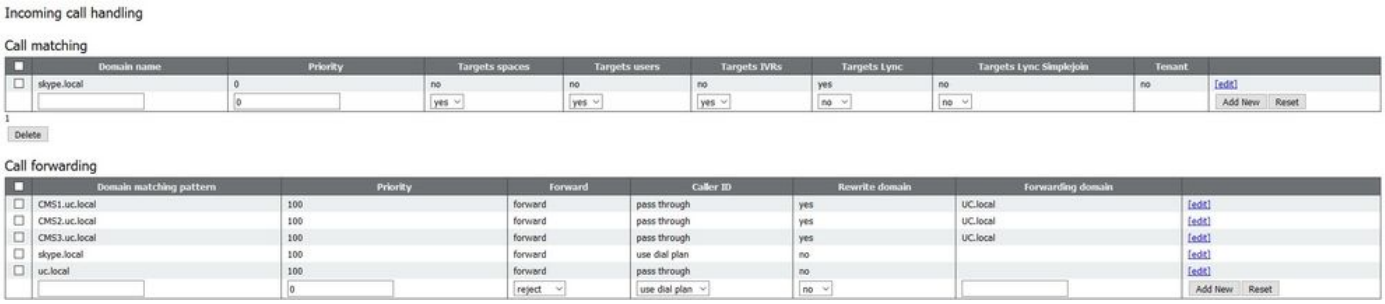
Exemple de configuration de règles entrantes - Single CallBridge



Dans cet environnement, les choses sont remarquablement simples. Puisque nous n'utilisons pas les ponts d'appels en cluster, nous pouvons configurer chaque domaine pour qu'il utilise le transfert comme ID d'appelant. Cela ne peut pas être fait dans un environnement en cluster, car cela rompra le partage des présentations.

En outre, il existe une règle de correspondance d'appels pour le domaine Skype.local avec la valeur true pour « Targets Lync ». Cela signifie que si nous appelons une téléconférence Lync/Skype par le numéro de numérotation RTPC, nous devrions pouvoir nous connecter en tant qu'appel à double domicile.

Exemple de configuration de règles entrantes - Pontages d'appels en cluster



Dans cet environnement, nous utilisons un cluster CallBridge qui se compose de trois ponts d'appel. Pour cette raison, nous avons besoin d'une règle de transfert d'appel pour chaque CallBridge configuré pour réécrire le domaine sur uc.local. En effet, lorsque les utilisateurs Lync/Skype rappellent des utilisateurs de l'environnement UC, ils passent des appels vers le domaine cms1.uc.local, cms2.uc.local ou cms3.uc.local. Malheureusement, il s'agit d'une limitation de la configuration requise pour que le contenu fonctionne dans un environnement CallBridge en cluster. Nous devons reconvertir cet appel en uc.local avant de le renvoyer au proxy sip uc.local.

En outre, il existe une règle de correspondance d'appels pour le domaine Skype.local avec la valeur true pour « Targets Lync ». Cela signifie que si nous appelons une téléconférence Lync/Skype par le numéro de numérotation RTPC, nous devrions pouvoir nous connecter en tant qu'appel à double domicile.

Règles sortantes

Le tableau 5 décrit ce que chaque champ de la configuration des appels sortants signifie.

Tableau 5

Champ Plan de numérotation sortant	Description
Domaine	Pour les appels sortants vers ce domaine, utilisez cette règle sortante
Proxy SIP à utiliser	Le proxy SIP auquel envoyer les appels pour ce domaine
Domaine de contact local	Cela détermine la valeur qui sera placée dans l'en-tête du contact. Pour l'intégration Lync/Skype, cette valeur doit être définie sur le nom de domaine complet du pont d'appel. Note: Pour toute règle sortante utilisant un proxy SIP de Lync/Skype, ce champ DOIT être configuré. Pour toute règle sortante utilisant un proxy SIP qui n'est pas Lync/Skype, ce champ NE DOIT PAS être configuré.
Local à partir du domaine	Cela détermine la valeur qui sera placée dans l'en-tête de départ. Il s'agit de l'adresse ID de l'appelant vue sur le proxy SIP. Si ce champ n'est pas renseigné, il utilisera le domaine de contact local configuré. Lync/Skype utilisera cet URI comme URI de destination pour les rappels et le partage de présentations. Note: Cette valeur n'est pas utilisée si l'appel est un appel de passerelle et que la règle de numérotation entrante utilisée a l'ID de l'appelant défini sur passthrough.
Type de liaison	Cela détermine quelle variante du SIP sera utilisée dans la communication avec le proxy SIP.
Comportement	Cela détermine si nous allons continuer ou non à vérifier les règles de priorité inférieure ou arrêter la recherche en cas de correspondance où nous n'avons pas pu terminer l'appel.
Priorité	Cela détermine l'ordre dans lequel les règles seront prises en compte. Les nombres plus élevés seront d'abord vérifiés. Les numéros inférieurs seront vérifiés en dernier.
Chiffrement	Cela détermine si nous utiliserons le protocole SIP chiffré ou non.
Locataire	Cela détermine les locataires pour lesquels cette règle sera prise en compte.
Étendue du pont d'appel	Ceci détermine les ponts d'appel pour lesquels cette règle de numérotation sortante sera prise en compte. Dans CallBridges en cluster, cela est nécessaire pour s'assurer que le domaine de contact correct est envoyé à partir de chaque CallBridge. Note: Cette valeur ne peut être définie qu'en utilisant l'API comme expliqué ci-dessous.

Exemple de configuration d'appels sortants - Single CallBridge

Outbound calls

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

Encore une fois nous constatons que l'environnement CallBridge unique est considérablement plus simple que l'environnement en cluster. Une chose à noter ci-dessus est que nous avons un domaine de contact spécifié. En effet, si nous ne spécifions pas le nom de domaine complet de notre CallBridge comme domaine de contact local Lync/Skype rejettera les appels pour des raisons de sécurité. Étant donné que nos règles de transfert entrantes sont configurées pour utiliser le transfert, nous ne réécrirons pas le domaine de départ dans cet exemple.

Exemple de configuration d'appels sortants - Ponts d'appels en cluster

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

Dans cet environnement, nous utilisons un cluster CallBridge qui se compose de trois ponts d'appel. C'est pourquoi nous avons besoin d'une règle de sortie pour chaque CallBridge avec des domaines de contact locaux différents, locaux de domaines et étendues. Une seule règle de trafic sortant est nécessaire pour acheminer les appels de tous les ponts d'appel vers Cisco Unified Communications Manager. Pour définir la portée, nous devons utiliser l'API.

Modification de l'étendue à l'aide de l'API - Pontages d'appels en cluster uniquement

Après avoir créé une règle d'appel sortant, la portée sera définie sur <all> pour cette règle. Cela signifie que la règle de trafic sortant sera utilisée sur tous les ponts d'appels d'un cluster. Pour les règles sortantes qui pointent vers Lync/Skype, nous devons utiliser des contacts et des en-têtes différents en fonction du pont d'appel sur lequel nous nous trouvons. Pour ce faire, nous devons créer une règle de sortie différente pour chaque CallBridge où les champs contact/de correspondent à ce CallBridge. À l'aide de l'API, nous devons définir l'étendue de ces règles de numérotation sortante de sorte qu'elles ne soient traitées que sur le pont d'appel correspondant à cette règle.

OBTENIR la liste de tous les ponts d'appel du cluster

Dans un navigateur, accédez à la page /callbridge de l'API CMS. Cette option affiche tous les ponts d'appel de votre cluster.

J'ai maintenant les ID de tous mes ponts d'appels. Vos ID seront différents dans votre environnement. Je peux voir que si je veux référencer CallBridge cms1.uc.local, je dois utiliser l'ID de e4ab61ea-b5b4-4fac-ad4a-9979badea4e4.

OBTENIR une liste de toutes les règles de numérotation sortante

Ensuite, je dois rechercher mes règles sortantes et obtenir leurs ID. Dans un navigateur, accédez à la page /outbound dialplanrules de l'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>
```

Maintenant j'ai les ID pour toutes mes règles, mais je ne peux pas dire laquelle est. La première règle ne nous intéresse pas, car celle-ci est destinée à UC.local et nous n'avons pas besoin d'en définir la portée. Nous devons savoir quelle règle correspond aux règles sortantes restantes sur Skype.local. En commençant un par un, je ferai correspondre les ID aux ponts d'appels.

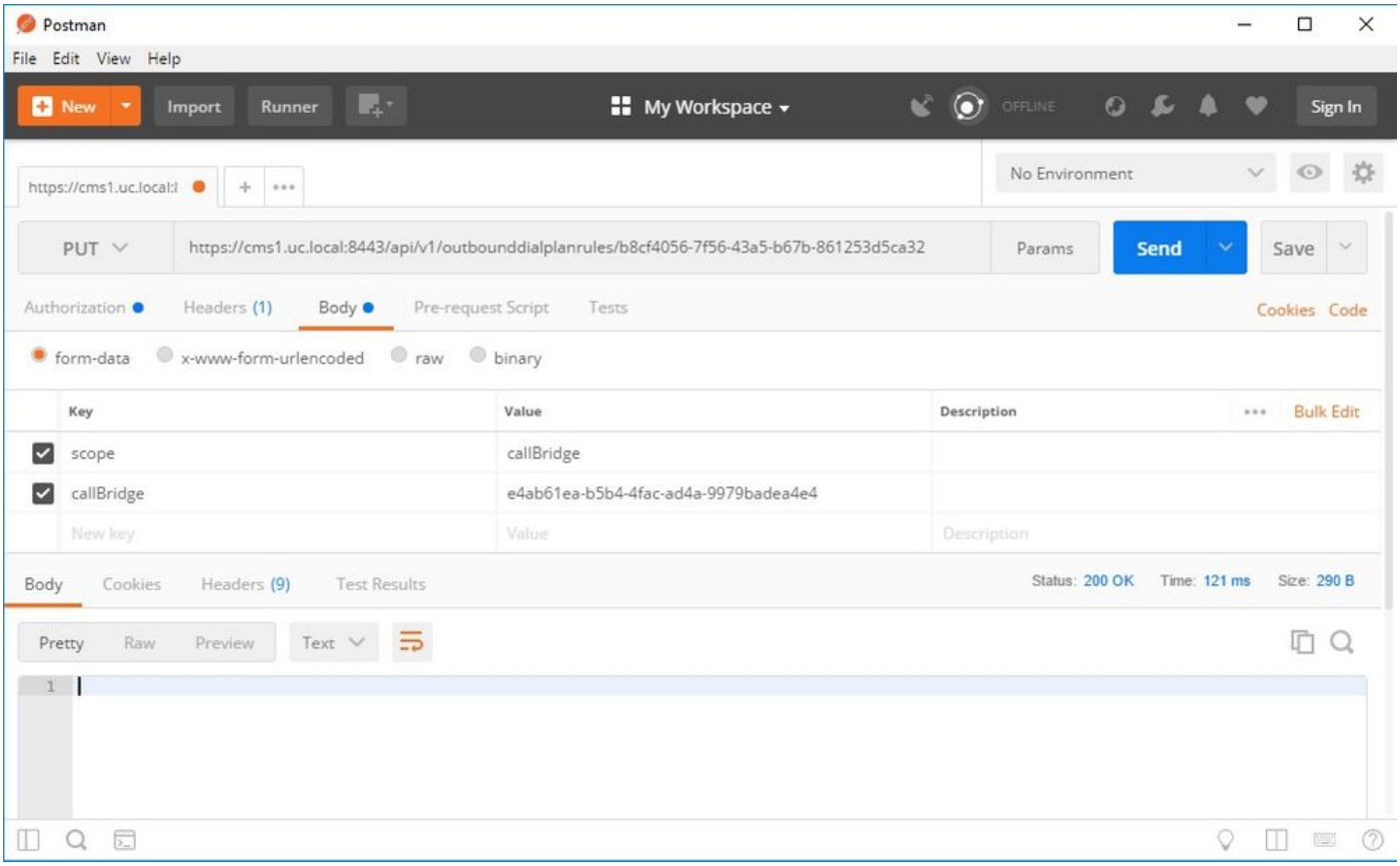
Je naviguerai vers /outbound dialplanrules/b8cf4056-7f56-43a5-b67b-861253d5ca32 dans mon navigateur. La lecture de l'en-tête de contact indiqué ici je peux dire que cette règle est pour CMS1.UC.local. Nous devons donc définir la portée de cette règle sur CMS1.UC.local.

Placer l'étendue CallBridge dans

À l'aide de mon outil d'API préféré, j'enverrai un PUT à l'api sur /outbound dialplanrules/b8cf4056-7f56-43a5-b67b-861253d5ca32 avec le corps suivant :

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

Dans cette capture d'écran, j'utilise PostMan pour envoyer cette demande.



Si cette PUT HTTP a réussi, la page des règles de numérotation sortante dans WebAdmin doit maintenant refléter une étendue qui a été appliquée. Si l'affichage de la Webadmin du pont d'appel indique que la portée lui a été appliquée, il doit afficher <local>. Si le Webadmin d'un autre CallBridge est utilisé pour afficher les règles de numérotation sortante, il doit afficher le nom de domaine complet CallBridge dans le champ de portée. Une étendue de <all> signifie que la règle sera utilisée sur tous les ponts d'appels. Une étendue de <none> signifie qu'une étendue a été activée, mais qu'aucun pont d'appel ne correspond à la portée.

Après avoir défini la portée d'un CallBridge, il doit être configuré pour chaque CallBridge supplémentaire. Une fois cette configuration terminée, chaque règle de trafic sortant de votre domaine Skype doit avoir une portée.

Comptes de service CMS

Dans la page de configuration générale de WebAdmin, vous trouverez une section Paramètres Lync Edge. Pour utiliser les services TURN ou rejoindre des téléconférences à double domicile via le numéro de numérotation RTPC, vous devez configurer cette option.

Le tableau 6 décrit ce que chaque champ de la configuration des paramètres Lync Edge signifie.

Tableau 6

Champ Paramètres Lync Edge	Description
Adresse du serveur	Nom de domaine complet (FQDN) de votre pool frontal
Nom d'utilisateur	Nom d'utilisateur du compte de service que vous voulez utiliser pour CMS
Nombre d'inscriptions	Combien de comptes d'utilisateurs différents souhaitez-vous enregistrer ? Si une valeur n'est pas configurée ici, seul le nom d'utilisateur indiqué ci-dessus sera enregistré. Si un nombre est appliqué ici, les numéros 1-X seront appliqués en tant que suffixes à la partie utilisateur de l'URI où X est le numéro configuré dans ce champ.

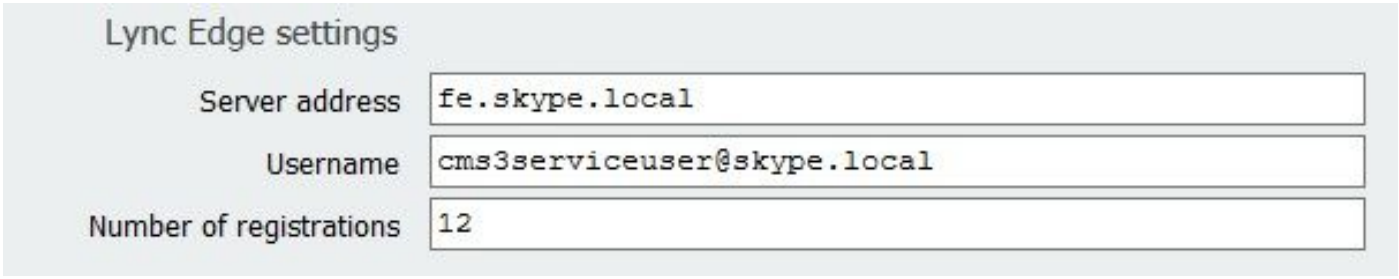
Exemple de configuration de compte de service CMS

Configuration sur CMS1 :

Cette configuration enregistrerait cms1serviceuser1@skype.local, cms1serviceuser2@skype.local, cms1serviceuser3@skype.local, ... cms1serviceuser11@skype.local et cms1serviceuser12@skype.local à fe.skype.local. Puisque dans cet exemple, je suis dans un environnement en cluster, je dois également créer des comptes de service pour mes autres ponts d'appel et les configurer séparément. Veuillez noter que les noms d'utilisateur dans cet exemple sont différents. Sur CMS1, les noms d'utilisateur sont prédéfinis par cms1. Sur CMS2, les noms d'utilisateur sont préfixes avec cms2. Sur CMS3, le préfixe est cms3. Tous ces comptes ont été créés et activés dans l'environnement Skype Entreprise. Puisque notre pool d'applications de confiance est configuré avec « Traiter comme authentifié », nous n'avons pas besoin de fournir des mots de passe pour l'enregistrement.

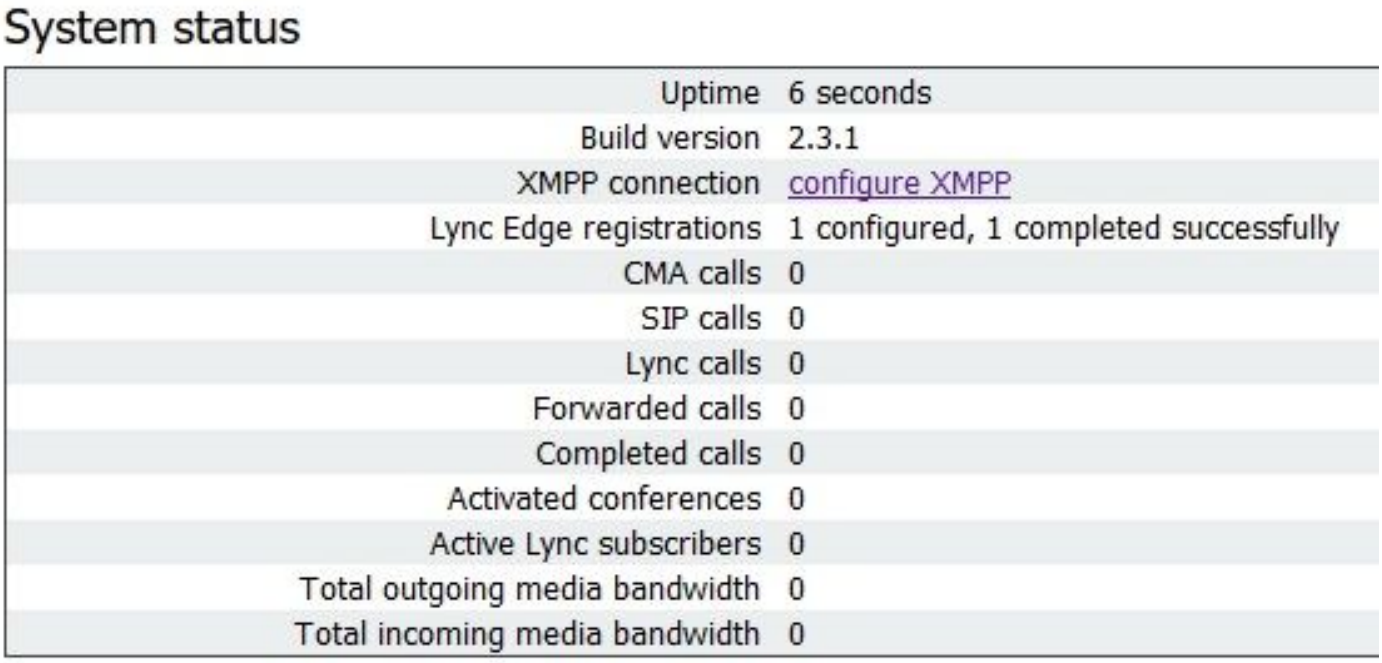
Configuration sur CMS2 :

Configuration sur CMS3 :



Vérification des comptes de service CMS

La page d'état de CMS WebAdmin s'affiche si les utilisateurs Lync/Skype se sont enregistrés avec succès. Dans l'exemple ci-dessous, nous ne configurons qu'un enregistrement et celui-ci s'est terminé avec succès. Si vous remarquez que l'état affiche les enregistrements en cours pendant longtemps, collectez les journaux SIP et DNS pour déterminer pourquoi l'échec se produit.



Configuration Lync/Skype

Appliquez les commandes ci-dessous dans le shell de gestion Lync/Skype. Appliquez les commandes sur le serveur frontal.

> **Note**: Les commandes suggérées sont à titre indicatif. Si vous avez des doutes sur la configuration du serveur Skype, vous devez contacter votre administrateur Lync/Skype et/ou votre équipe d'assistance.

Pont d'appel unique

Tout d'abord, nous devons demander à Skype de faire confiance à notre CallBridge. Pour ce faire, nous ajoutons un pool d'applications de confiance. Dans la terminologie Microsoft, « Pool » signifie simplement « Cluster ». Dans ce scénario, notre cluster n'est qu'un cluster d'un CallBridge. L'identité de notre cluster DOIT correspondre au nom commun du certificat utilisé sur notre CallBridge. Microsoft l'utilise comme contrôle de sécurité. Avoir l'identité dans un SAN ne suffit pas. Si le nom commun ne correspond pas à Microsoft, la connexion TCP sera interrompue. Lors de l'utilisation de cette commande, l'identité doit être le nom de domaine complet CallBridge. Le Registrar doit être le nom de domaine complet du pool frontal assurant la maintenance de ces connexions. Le site doit être l'identificateur de site Lync/Skype. Si vous n'êtes pas sûr des valeurs qui doivent être utilisées pour le bureau d'enregistrement ou le site, contactez votre administrateur Lync/Skype.

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

Ensuite, l'environnement Microsoft doit être configuré pour autoriser les communications entrantes à partir de notre CallBridge (pool d'applications de confiance) sur le port 5061.

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

L'environnement Microsoft est actuellement configuré pour accepter les appels, mais il ne peut pas renvoyer d'appels et ne peut pas envoyer de présentation pour les appels de passerelle. Pour corriger cela, nous devons ajouter une route statique. Dans le scénario CallBridge unique, nous avons seulement besoin d'une route unique pour autoriser tous les appels vers notre domaine UC.local. Dans les commandes ci-dessous, Destination est le nom de domaine complet du pont d'appel auquel nous voulons envoyer des requêtes SIP. Le champ MatchURI est la partie domaine de l'URI qui doit être utilisée. Veuillez noter que dans un environnement Lync/Skype, une seule route statique peut être créée par MatchURI.

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

Enfin, nous devons demander à Skype de mettre en oeuvre toutes les modifications que nous venons d'apporter.

```
Enable-CsTopology
```

Ponts d'appels en cluster

Tout d'abord, nous devons demander à Skype de faire confiance à notre cluster CallBridge. Pour ce faire, nous ajoutons un pool d'applications de confiance. Dans la terminologie Microsoft, « Pool » signifie simplement « Cluster ». L'identité de notre cluster DOIT correspondre au nom commun du ou des certificats utilisés sur nos ponts d'appel. Microsoft l'utilise comme contrôle de sécurité. Avoir l'identité dans un SAN ne suffit pas. Si le nom commun ne correspond pas à Microsoft, la connexion TCP sera interrompue. Lors de l'utilisation de cette commande, l'identité doit être le nom de domaine complet CallBridge. ComputerFqdn doit être le nom de domaine complet du premier CallBridge de votre cluster. En spécifiant un ComputerFqdn, vous indiquez à l'environnement Lync/Skype qu'il ne s'agit pas d'un cluster avec un seul serveur. Le Registrar doit être le nom de domaine complet du pool frontal assurant la maintenance de ces connexions. Le site doit être l'identificateur de site Lync/Skype. Si vous n'êtes pas sûr des valeurs qui doivent être utilisées pour le bureau d'enregistrement ou le site, contactez votre administrateur Lync/Skype.

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

Dans cet environnement, nous devons ajouter deux CallBridges en tant qu'ordinateurs d'application fiables. Le premier CallBridge a déjà été ajouté lors de la création du pool d'applications approuvées ci-dessus. Lorsque nous ajoutons ces ordinateurs, nous devons les associer au pool que nous venons de créer. Cela indique à Skype que nous avons des ordinateurs supplémentaires dans notre cluster qui doivent être approuvés. Toutes les identités d'ordinateur ici doivent être répertoriées en tant que SAN dans nos certificats CallBridge. Ces identités doivent également correspondre aux en-têtes de contact dans les règles de numérotation sortante dans les ponts d'appels. Si elles ne correspondent pas à Microsoft, la connexion TCP sera interrompue.

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

Ensuite, l'environnement Microsoft doit être configuré pour autoriser les communications entrantes à partir de notre cluster CallBridge (pool d'applications de confiance) sur le port 5061.

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

L'environnement Microsoft est actuellement configuré pour accepter les appels, mais il ne peut pas renvoyer d'appels et ne peut pas envoyer de présentation pour les appels de passerelle. Pour corriger cela, nous devons ajouter des routes statiques. Tout d'abord, nous devons ajouter une route statique pour autoriser tous les appels vers notre domaine UC.local. Dans les commandes ci-dessous, Destination est le nom de domaine complet du pont d'appel auquel nous voulons envoyer des requêtes SIP. Le champ MatchURI est la partie domaine de l'URI qui doit être utilisée. Veuillez noter que dans un environnement Lync/Skype, une seule route statique peut être créée par MatchURI. Puisque la destination est le nom de domaine complet de notre cluster CallBridge et qu'elle a un enregistrement DNS A pour chaque membre du cluster Lync/Skype peut envoyer du trafic à tous nos ponts d'appels. Ainsi, si l'un tombe en panne, il peut automatiquement router les demandes de notre domaine vers un autre CallBridge dans le cluster.

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

Ensuite, nous devons créer une route statique supplémentaire pour chaque CallBridge dans le cluster. Il s'agit d'une condition requise pour que le rappel et la présentation fonctionnent.

```
$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}
```

Enfin, nous devons demander à Skype de mettre en oeuvre toutes les modifications que nous venons d'apporter.

```
Enable-CsTopology
```

Dépannage

Collecte des journaux à partir de CMS

La première étape du diagnostic d'un problème consiste à déterminer où se trouve le problème. Pour ce faire, nous devons analyser les journaux de Cisco Meeting Server, mais nous devons d'abord les collecter. Voici mes recommandations personnelles sur les journaux à collecter.

Tout d'abord, activez le débogage SIP et DNS pour tous les ponts d'appel via l'interface WebAdmin. Pour ce faire, accédez à WebAdmin, puis à Logs > Details Tracing. À partir de là, activez la journalisation SIP et DNS pendant les trente prochaines minutes. Cela devrait être plus que suffisant pour détecter et diagnostiquer le problème. Gardez à l'esprit que cela doit être fait individuellement pour tous les ponts d'appel, car l'activation du journal n'est pas partagée sur un cluster.

Ensuite, activez les captures de paquets sur tous les ponts d'appel. Pour ce faire, connectez-vous via SSH à chaque CallBridge et exécutez la commande pcap <interface> où <interface> est le trafic d'interface à utiliser. Dans la plupart des cas, il s'agit de l'interface a. Ainsi, la commande « pcap a » lancerait une capture de paquets sur l'interface a pour le pont d'appel auquel nous sommes connectés.

Une fois la capture de paquets exécutée sur toutes les interfaces, l'étape suivante consiste à générer le problème. Allez-y et essayez d'appeler ou faites ce qui a échoué. Une fois cette opération terminée, arrêtez toutes les captures de paquets. Pour cela, vous pouvez entrer Ctrl-C dans toutes les fenêtres SSH. Une fois la capture de paquets terminée, le nom du fichier généré est affiché à l'écran. Suivez ce nom de fichier car nous devrons le télécharger à l'étape suivante.

Enfin, nous devons collecter les journaux des ponts d'appel. Pour ce faire, connectez-vous via SFTP à chaque CallBridge. Téléchargez le fichier logbundle.tar.gz et le fichier de capture de paquets généré. Ce fichier est uniquement disponible dans CMS2.2+. Dans CMS versions 2.3+, il inclut la configuration complète de votre CMS. Si vous exécutez la version 2.2, elle n'inclura pas vos règles entrantes/sortantes, il serait donc bon de prendre des captures d'écran de ces pages ainsi que les paramètres Lync Edge pour référence. Veillez à stocker les journaux/captures d'écran collectés dans des dossiers distincts dont le nom correspond au pont d'appel à partir duquel les journaux ont été extraits. Cela permettra de s'assurer que les journaux ne sont pas mélangés.

Affichage de la configuration Lync/Skype

Ces commandes sont extrêmement utiles lors du dépannage de la configuration Lync/Skype. Dans ce document, les commandes sont données pour créer et afficher la configuration, mais aucune commande n'est donnée pour supprimer la configuration. En effet, la suppression de la configuration peut être dangereuse, sauf si elle est effectuée par des administrateurs ayant une compréhension complète de l'environnement Lync/Skype. Si vous devez supprimer la configuration, contactez votre administrateur Lync/Skype.

Commande	Description
Get-CsTrustedApplicationPool	Cette commande répertorie les clusters (pools) approuvés par Lync/Skype. L'identité de ce pool DOIT correspondre au nom commun du ou des certificats CallBridge. Même dans un environnement CallBridge unique, un cluster (pool) CallBridge d'un seul doit être spécifié ici.
Get-CsTrustedApplicationComputer	Cette commande répertorie les serveurs approuvés par Lync/Skype et le pool auquel ces serveurs sont associés. Tous les ordinateurs ici DOIVENT être identifiés dans le certificat envoyé par les ponts d'appel. Dans un environnement CallBridge unique, il s'agit généralement du nom commun. Dans un environnement en cluster, ces ordinateurs DOIVENT être répertoriés en tant qu'entrées de nom alternatif de sujet (SAN). En outre, tous les ordinateurs ici DOIVENT être identifiés par des entrées de domaine de contact local sur les règles de numérotation sortante CallBridge.
Get-CsTrustedApplication	Cette commande répertorie les services avec lesquels les pools d'applications approuvés sont autorisés à communiquer. Pour les communications CMS avec Lync/Skype, nous utiliserons le port TCP 5061 pour SIP chiffré TLS.
Get-CsStaticRoutingConfiguration | Select-Object -ExpandProperty Route	Cette commande répertorie les routes statiques utilisées par Lync/Skype pour le transfert des requêtes. Le champ MatchURI est le domaine de destination du message SIP. Le champ « TLS Fqdn » dans le fichier XML doit indiquer le serveur de destination pour ce trafic.

Exemple de sortie de commandes Lync/Skype Get

Vous trouverez ci-dessous les résultats des commandes Lync/Skype Get ci-dessus émises dans le scénario de cluster des trois ponts d'appel traité dans ce document

```
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>
```

Contacter le TAC

Si vous rencontrez des erreurs avec cette mise en oeuvre, contactez le TAC Cisco. Lors de l'ouverture de la demande de service, veuillez inclure un lien vers ce document. Il aidera les ingénieurs du centre d'assistance technique à comprendre votre configuration. En outre, il serait extrêmement utile que les journaux de Cisco Meeting Server soient joints au dossier comme décrit ci-dessus et que les résultats de toutes les commandes Get du serveur frontal Lync/Skype soient entrés dans les notes de dossier. Si vous n'incluez pas ces informations, il est certain que ce sera l'une des premières choses que les ingénieurs du centre d'assistance technique vous demandent. Alors allez-y et collectez-les avant d'ouvrir votre dossier.