

# Comprendre la logique de routage des appels sur Meeting Server

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Quelle est la logique de routage des appels de Cisco Meeting Server \(CMS\) ?](#)

[Étape 1. Table de correspondance des appels entrants](#)

[Étape 2. Table de transfert d'appels entrants](#)

[Réécrire le domaine](#)

[ID de l'appelant](#)

[Étape 3. Table des appels sortants](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

## Introduction

Ce document décrit la logique de routage des appels de Cisco Meeting Server (CMS) (anciennement produit Acano), qui est divisée en plusieurs tables de routage des appels. Ce document couvre les différentes étapes et les différents scénarios que les appels peuvent suivre à travers ces tables de routage d'appels.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Composant Pont d'appels Cisco Meeting Server.

### Components Used

Les informations de ce document sont basées sur Cisco Meeting Server version 2.3.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Quelle est la logique de routage des appels de Cisco Meeting Server (CMS) ?

Le routage des appels sur CMS implique quelques tables de routage des appels différentes. Avec le diagramme de flux qui peut être téléchargé , vous pouvez suivre la logique de routage des appels pour chaque appel qui arrive sur le CMS. Ceci est valide pour tous les types d'appels : Cisco Meeting App (CMA - client épais ou WebRTC), appels SIP (Standard Session Initiation Protocol) ou appels SIP Microsoft, sauf indication contraire.

**Note:** La seule exception concerne les appels initiés par CMS (soit directement par CMS pour les appels sortants planifiés TMS (TelePresence Management Suite), soit les appels sortants client CMA) dans lesquels la table de transfert d'appels est ignorée.

Il s'agit de l'ordre du processus de routage d'appel dans CMS :

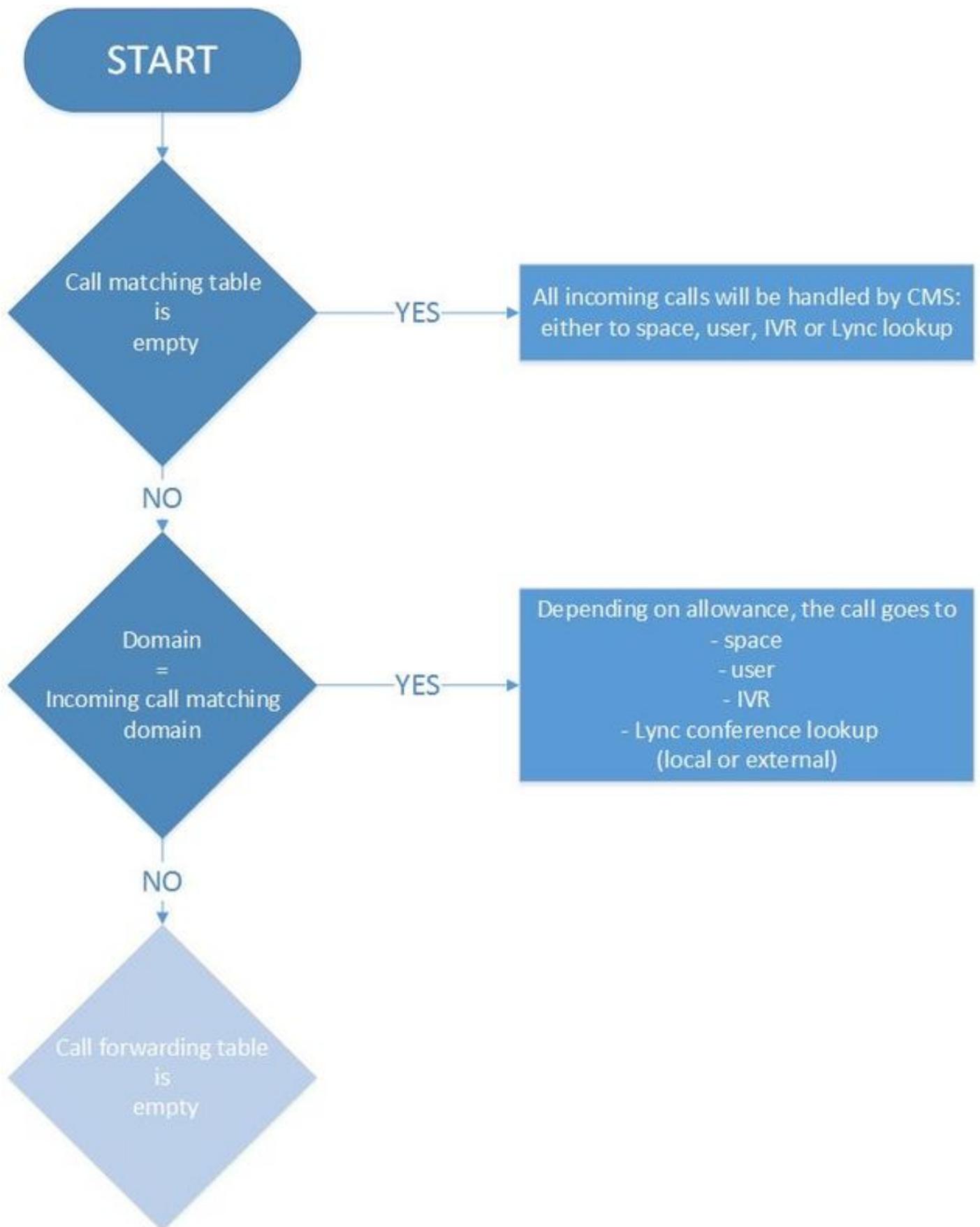
1. Table de correspondance des appels entrants
2. Table de transfert d'appels entrants
3. Table des appels sortants

Chaque tableau est expliqué plus en détail plus loin dans le document, qui inclut les images qui ne montrent que la partie pertinente du .

**Note:** CMS effectue uniquement le routage des appels en fonction du routage de domaine, basé donc sur le côté droit (RHS) de l'URI (Uniform Resource Identifier). Il n'existe aucune fonctionnalité de routage d'appels basée sur le côté gauche (LHS) de l'URI comme vous l'avez fait sur Cisco Unified Communications Manager (CUCM) avec routage DirectoryNumber (Route Patterns).

**Note:** Chaque table est une liste ordonnée définie par l'attribut priority. Plus la priorité est élevée, plus il tente d'être mis en correspondance en premier. Si elle ne correspond pas, elle passe à la règle suivante de la liste. En règle générale, donnez à des règles plus générales (comme un \* qui correspond à n'importe quel domaine) une priorité inférieure aux règles plus spécifiques. De cette façon, les règles spécifiques sont traitées en premier, et vous avez potentiellement le retour sur les règles plus générales.

## Étape 1. Table de correspondance des appels entrants



Il s'agit de la première étape du processus dans lequel CMS détermine si l'appel entrant est destiné à Cisco Meeting Server lui-même et doit être traité plus avant ou s'il s'agit d'un appel destiné à un système différent dans lequel CMS est l'agent qui interagit l'appel et gère à la fois le support et la signalisation (c.-à-d. La passerelle Skype appelle les terminaux SIP standard ou vice versa).

Il vérifie si la partie domaine de l'URI entrant correspond ou non à la table correspondante entrante. S'il correspond, il peut acheminer l'appel vers l'espace, l'utilisateur, l'IVR ou effectuer une recherche de conférence Lync (sur site ou hors site) conformément à votre configuration pour cette règle de plan de numérotation. La table ne permet pas les domaines génériques, elle nécessite une correspondance complète.

**Note:** Si aucun domaine de correspondance d'appels entrants n'est configuré, CMS accepte tous les URI entrants des appels SIP ou Lync qui atterrissent sur le pont d'appel. Pour les clients CMA (client WebRTC ou client épais) bien qu'il accepte l'appel, il n'est pas routé automatiquement vers l'espace approprié ou vers l'utilisateur. Il est donc important d'entrer dans le domaine correct lorsque vous utilisez le client CMA pour composer des numéros vers des espaces ou des utilisateurs dans ce cas.

Par exemple, un tableau de correspondance d'appels est affiché dans l'image (il affiche uniquement l'option **Espaces cibles** et **Utilisateurs cibles** pour plus de concision) :

### Incoming call handling

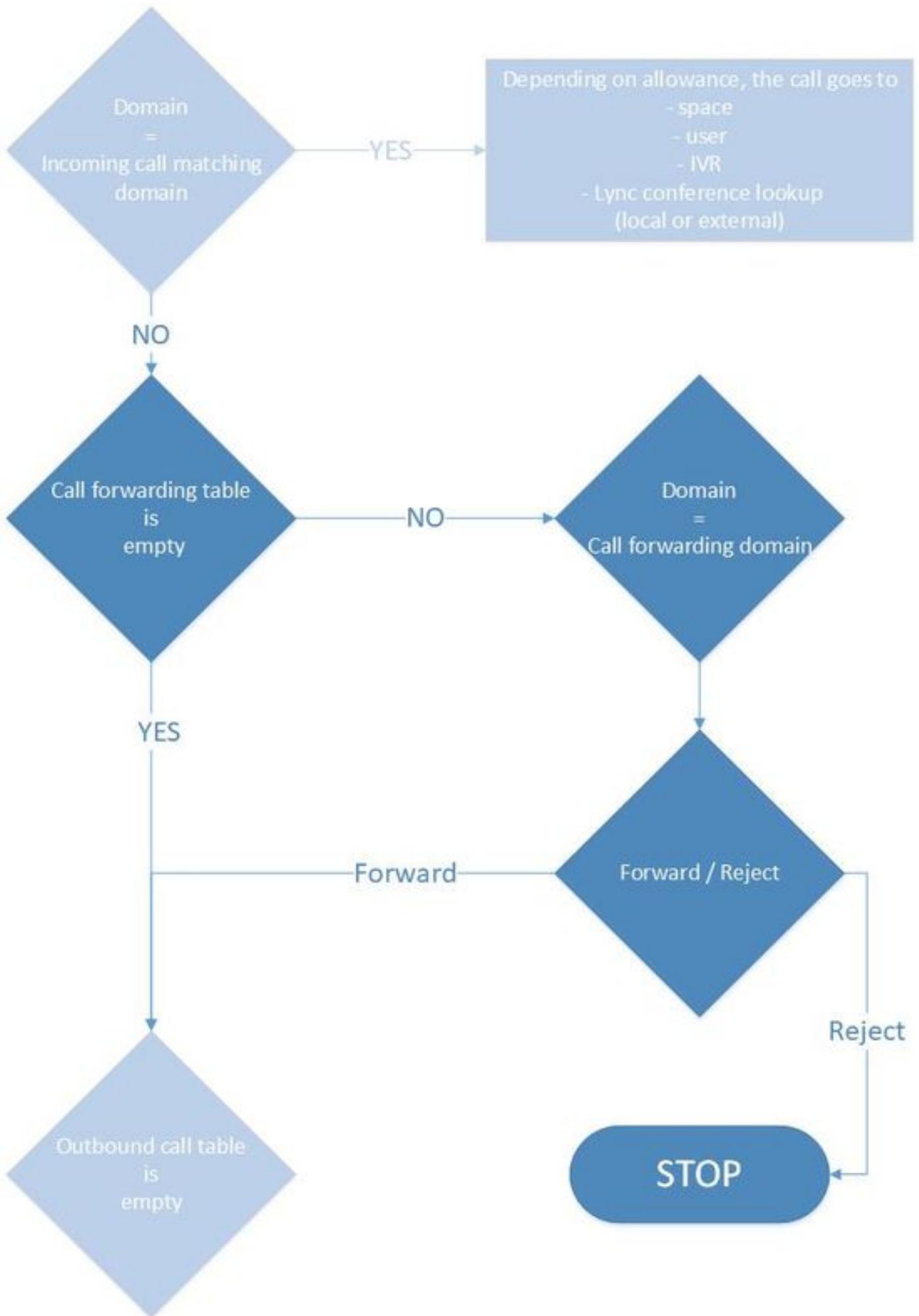
#### Call matching

<input type="checkbox"/>	Domain name	Priority	Targets spaces	Targets users
<input type="checkbox"/>	acano.steven.lab	2	yes	yes
<input type="checkbox"/>	10.48.54.160	1	yes	yes
<input type="checkbox"/>	acano1.acano.steven.lab	0	yes	yes
<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	yes <input type="text" value=""/>	yes <input type="text" value=""/>

1

Ici, le domaine est configuré en tant que acano.steven.lab que les clients composent normalement. Cependant, il autorise également des appels ad hoc ou des modèles de route SIP spécifiques de CUCM (ou des règles de recherche Expressway) qui ciblent uniquement un pont d'appel spécifique (dans le cas d'un cluster) par la première et la deuxième règle de secours dans la table qui correspondent à l'adresse IP du pont d'appel (10.48.54.160 dans ce cas) ou au nom de domaine complet callbridge (acano1.acano.steven.lab dans ce cas).

## Étape 2. Table de transfert d'appels entrants



Si l'appel n'a pas atteint l'une des règles de la table de correspondance des appels entrants ou si l'appel ne correspond pas (par exemple, URI d'espace non existant ou incorrect composé par l'utilisateur), il passe par la deuxième table appelée table de renvoi d'appels. Il s'agit également d'un domaine uniquement et vous permet de bloquer spécifiquement les appels vers certains domaines ou de n'autoriser spécifiquement que les appels vers certains domaines. Si vous voulez faire cela, il est important d'avoir des règles plus spécifiques avec une priorité plus élevée, de sorte qu'elles sont vérifiées en premier.

Cet exemple montre que les appels destinés à dummy.com sont rejetés, tandis que les appels destinés à tplab.local sont transférés :

Domain matching pattern	Priority	Forward	Caller ID	Rewrite domain	Forwarding domain	
<input type="checkbox"/> dummy.com	0	reject	use dial plan	no		[edit]
<input checked="" type="checkbox"/> tplab.local	0	forward	use dial plan	no		[edit]
<input type="text"/>	0	reject	use dial plan	no		[Add New] [Reset]

Lorsque vous laissez la table de renvoi d'appels vide, cela entraîne un état dans lequel CMS n'agit pas comme passerelle entre les participants Skype et SIP, par exemple, car il n'y a aucune règle de renvoi d'appels. Dans l'hypothèse où le domaine de l'appel entrant ne correspond pas à la table de correspondance des appels entrants ou au domaine mais qu'il n'y a pas de correspondance sur les espaces, les utilisateurs ou les IVR (ou les réunions Skype), l'appel n'est pas transféré en ce qui concerne la table d'appels sortants.

**Note:** Cela se produit cependant avec les clients CMA (clients épais et WebRTC) car ils peuvent passer des appels sortants (\*Web App dans la version 3.0 ne peut pas passer d'appels sortants, mais plutôt des appels effectués par l'espace CMS de Callbridge). De même, les appels sortants sur CMS fonctionnent aussi bien lorsqu'ils sont effectués via l'API par exemple (dans le cas de conférences planifiées TMS). En général, les appels qui sont initiés à partir de CMS lui-même (soit directement, soit via CMA) ne doivent pas suivre la logique de transfert d'appels.

Dans le journal des événements, vous pouvez voir le message **de transfert** mis en surbrillance comme par exemple lorsque CMS agit comme passerelle pour les appels SIP et Skype. Juste avant, vous pouvez voir l'appel **entrant** et l'appel **sortant** après.

```
2018-10-04 06:36:24.612 Info call 788: incoming SIP call from "sip:1060@10.48.36.215" to
local URI "sip:stejanss@any.com"
2018-10-04 06:36:24.624 Info forwarding call to 'sip:stejanss@any.com' to
'stejanss@any.com'
2018-10-04 06:36:24.625 Info call 789: outgoing SIP call to "stejanss@any.com"
```

Si la table de transfert ne contient aucune règle ou règle de rejet, le journal des événements n'affiche pas explicitement cette règle. Il vous informe simplement que l'appel SIP ne correspond pas (espace, utilisateur, IVR ou réunion Lync) et que la règle de transfert (ou qu'elle est définie pour être rejetée) vous manque pour passer à la section des règles sortantes.

```
2018-10-04 06:47:12.482 Info call 790: incoming SIP call from "sip:1060@10.48.36.215" to
local URI "sip:stejanss@any.com"
2018-10-04 06:47:12.495 Info call 790: ending; local teardown, destination URI not matched
- not connected after 0:00
```

Pour les appels clients CMA ou les appels sortants de CMS qui sont initiés par le biais de réunions planifiées TMS, il n'y a **aucun appel entrant** vu dans le journal des événements. L'appel

est immédiatement dirigé vers la table de plan de numérotation sortante et n'est pas traité par la table de transfert d'appels.

Dans la table de renvoi d'appels, il existe deux autres options de configuration : Réécrivez le domaine et l'ID de l'appelant.

## Réécrire le domaine

Cette option vous permet de réécrire le domaine de l'appel entrant sur un autre et de modifier la partie domaine de l'URI de requête SIP ainsi que l'en-tête To du message SIP.

Domain matching pattern	Priority	Forward	Caller ID	Rewrite domain	Forwarding domain
<input type="checkbox"/> any.com	2	forward	use dial plan	yes	newany.com
<input type="checkbox"/> dummy.com	0	reject	use dial plan	no	
<input type="checkbox"/> tplab.local	0	forward	use dial plan	no	
	0	reject	use dial plan	no	

Par exemple, avec la configuration sur cette image, le journal des événements (avec la trace SIP activée) est affiché ici pour un appel entrant avec domaine **any.com** mais sans correspondance dans la table de correspondance des appels entrants (espaces, utilisateurs, IVR ou conférences Skype) :

```
2018-10-04 07:02:24.818 Info SIP trace: connection 0: incoming SIP TCP data from
10.48.36.215:56457 to 10.48.80.71:5060, size 1000:
2018-10-04 07:02:24.818 Info SIP trace: INVITE sip:stejanss@any.com SIP/2.0
2018-10-04 07:02:24.818 Info SIP trace: Via: SIP/2.0/TCP
10.48.36.215:5060;branch=z9hG4bK53e4c4ce29394
2018-10-04 07:02:24.818 Info SIP trace: From: "EX60 Steven"
<sip:1060@steven.lab>;tag=742103~ee545a46-516a-4de6-87d7-7b1f5a5b848a-26001856
2018-10-04 07:02:24.818 Info SIP trace: To: <sip:stejanss@any.com>
..
2018-10-04 07:02:24.822 Info call 797: incoming SIP call from "sip:1060@10.48.36.215" to
local URI "sip:stejanss@any.com"
2018-10-04 07:02:24.834 Info forwarding call to 'sip:stejanss@any.com' to
'stejanss@newany.com'
2018-10-04 07:02:24.835 Info call 798: outgoing SIP call to "stejanss@newany.com"
..
2018-10-04 07:02:24.838 Info SIP trace: connection 19: outgoing SIP TCP data to
10.48.36.215:5060 from 10.48.80.71:57854, size 3286:
2018-10-04 07:02:24.838 Info SIP trace: INVITE sip:stejanss@newany.com SIP/2.0
2018-10-04 07:02:24.838 Info SIP trace: Via: SIP/2.0/TCP
10.48.80.71:5060;branch=z9hG4bKefc98b81a2961b37aee24f03c2142d8e
2018-10-04 07:02:24.839 Info SIP trace: Call-ID: 18644f28-e998-4032-a7df-75325e9d11b0
2018-10-04 07:02:24.839 Info SIP trace: CSeq: 659590315 INVITE
2018-10-04 07:02:24.839 Info SIP trace: Max-Forwards: 70
2018-10-04 07:02:24.839 Info SIP trace: Contact: <sip:1060@10.48.80.71;transport=tcp>
2018-10-04 07:02:24.839 Info SIP trace: To: <sip:stejanss@newany.com>
2018-10-04 07:02:24.839 Info SIP trace: From: "EX60 Steven"
<sip:1060@steven.lab>;tag=2aa2a49bba231a1b
```

Dans cette ligne d'appel de transfert, elle indique la modification qui s'est produite. Si le suivi SIP n'est pas activé, il indique toujours la modification de any.com à newany.com.

L'utilisation la plus courante de cette réécriture du domaine est associée à une [intégration Lync](#) sur site [avec un cluster CMS](#) où il est recommandé de définir l'en-tête Contact et l'en-tête From dans les règles sortantes de Lync/Skype sur les noms de domaine complets spécifiques au pont

d'appel. En raison de ces règles de routage :

- Skype envoie de nouvelles **transactions** dans une boîte de dialogue (par exemple un ACK après un INVITE - 200 OK) à l'en-tête **Contact** spécifié dans le 200 OK reçu du CMS. Pour les connexions entrantes de Skype à CMS, Skype envoie d'abord un message SIP NEGOTIATE contenant un en-tête ms-fe dans l'en-tête To qui spécifie comment l'en-tête Contact doit être rempli dans les réponses 200 OK de l'INVITE (car il utilise le même canal TCP)
- Skype envoie de nouvelles **boîtes de dialogue** (comme le partage de contenu, car il s'agit d'un appel distinct, ou d'un rappel en cas d'appel manqué) à l'en-tête **De** l'invitation initiale

Lorsqu'il réécrit le domaine, il est pertinent pour le rappel des appels Lync. L'en-tête From de l'invitation manquée pointe vers le pont d'appel spécifique d'où provient l'appel. Lync envoie ensuite une nouvelle requête (INVITE) avec l'URI de requête SIP qui correspond au FQDN du pont d'appel. Il est ensuite traduit dans le domaine SIP par le biais de ces règles de réécriture. Une fois l'appel transféré, il utilise les règles de sortie vers CUCM ou Expressway-C où le point de terminaison SIP est enregistré.

## ID de l'appelant

Deux options peuvent être définies sur les règles de transfert. Soit il est configuré pour **passer par** et ensuite aucune modification n'est apportée à l'en-tête De des INVITES sortantes, soit il est configuré pour **utiliser le plan de numérotation** qui permet au système de modifier l'en-tête De selon les règles de sortie. Ce paramètre est différent du fait que vous ayez ou non une réécriture du domaine qui concerne uniquement l'URI de la demande SIP ainsi que l'en-tête To de l'invitation sortante.

Par exemple, le même appel que précédemment a été passé mais il existe maintenant une règle de plan de numérotation sortante sur newany.com (comme après la réécriture sur la table de renvoi d'appels entrants) configurée en tant qu'appel de type Lync (Ms-Conversation-ID comme en-tête SIP supplémentaire par exemple). Il convient de renseigner le domaine Local From (et le domaine de contact local) pour indiquer le nom de domaine complet du pont d'appel, comme indiqué précédemment pour les appels Lync. Ceci reflète ensuite la modification de l'en-tête **From** et **Contact** de l'invitation SIP sortante. Comme le montre l'image, ils sont renseignés avec la même valeur et peuvent être sélectionnés individuellement selon vos besoins.

## Outbound calls

Filter	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority
<input type="checkbox"/>	steven.lab	10.48.36.46		<use local contact domain>	Standard SIP	Stop	5
<input type="checkbox"/>	newany.com	10.48.36.46	callbridgefqdn.any.com	callbridgefqdn.any.com	Lync	Stop	4

```
2018-10-12 09:09:24.488 Info SIP trace: connection 28: incoming SIP TCP data from
10.48.36.215:44460 to 10.48.80.71:5060, size 1000:
2018-10-12 09:09:24.489 Info SIP trace: INVITE sip:stejanss@any.com SIP/2.0
2018-10-12 09:09:24.489 Info SIP trace: Via: SIP/2.0/TCP
10.48.36.215:5060;branch=z9hG4bKf4a230ec178e
2018-10-12 09:09:24.489 Info SIP trace: From: "EX60 Steven"
<sip:1060@steven.lab>;tag=118288~ee545a46-516a-4de6-87d7-7b1f5a5b848a-32900729
2018-10-12 09:09:24.489 Info SIP trace: To: <sip:stejanss@any.com>
2018-10-12 09:09:24.489 Info SIP trace: Call-ID: 81e67f80-bc0164c4-f2c6-
d724300a@10.48.36.215
```

```

2018-10-12 09:09:24.494 Info call 803: incoming SIP call from "sip:1060@10.48.36.215" to
local URI "sip:stejanss@any.com"
2018-10-12 09:09:24.506 Info forwarding call to 'sip:stejanss@any.com' to
'stejanss@newany.com'
2018-10-12 09:09:24.507 Info call 804: outgoing SIP call to "stejanss@newany.com" (Lync)

2018-10-12 09:09:24.507 Info SIP trace: connection 33: allocated for outgoing connection
to 10.48.36.46:5060
2018-10-12 09:09:24.508 Info SIP trace: connection 33: outgoing connection successful,
10.48.80.71:39782 to 10.48.36.46:5060
2018-10-12 09:09:24.510 Info SIP trace: connection 33: outgoing SIP TCP data to
10.48.36.46:5060 from 10.48.80.71:39782, size 2971:
2018-10-12 09:09:24.510 Info SIP trace: INVITE sip:stejanss@newany.com SIP/2.0
2018-10-12 09:09:24.510 Info SIP trace: Via: SIP/2.0/TCP
10.48.80.71:5060;branch=z9hG4bK15bdde97ab641b586f162187cfdd98b5
2018-10-12 09:09:24.510 Info SIP trace: Call-ID: c366ddaf-e602-4fa5-b1d6-2e16ec08534a
2018-10-12 09:09:24.510 Info SIP trace: CSeq: 1498747095 INVITE
2018-10-12 09:09:24.510 Info SIP trace: Max-Forwards: 70
2018-10-12 09:09:24.510 Info SIP trace: Contact:
<sip:1060@callbridgefqdn.any.com;transport=tcp>
2018-10-12 09:09:24.510 Info SIP trace: Ms-Conversation-ID: 3P5Hu8grR1GGDF1BSMZAmw==
2018-10-12 09:09:24.510 Info SIP trace: To: <sip:stejanss@newany.com>
2018-10-12 09:09:24.510 Info SIP trace: From: "EX60 Steven"
<sip:1060@callbridgefqdn.any.com>;tag=fb4ae780677e9d9b

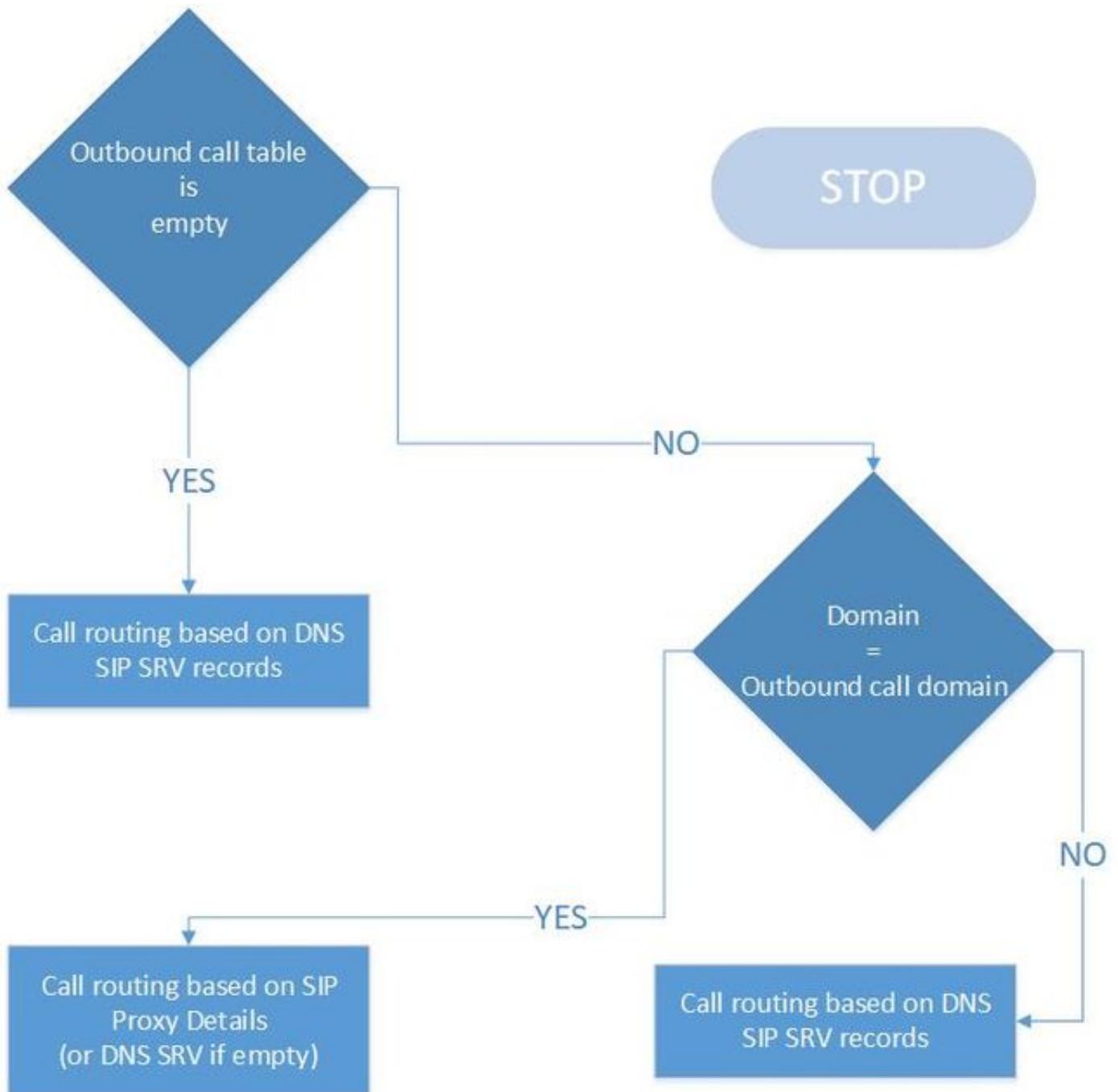
```

Dans le cas où la règle de transfert serait simplement définie au **passage**, alors il n'y aurait aucune modification sur l'en-tête De comme vu aussi à partir de l'exemple précédent (auquel cas le passage a été défini sur la règle de transfert). L'en-tête Contact est toujours adapté lorsque CMS démarre un callLeg et doit donc ajouter un en-tête Contact à lui-même.

Différentes combinaisons d'**ID d'appelant** et de **domaine de contact local** et de **domaine local** peuvent être utilisées. L'en-tête From de l'invitation SIP sortante est construit comme indiqué sur la table où l'appel entrant entre dans le CMS avec un en-tête From de `usera@from.com`.

Forwarding rule Caller ID	Outbound call rule Local contact domain	Outbound call rule Local from domain	Resulting from header
Pass through	NA	NA	usera@from.com
Use dial plan	NA	<u>newfrom.com</u>	usera@newfrom.com
Use dial plan	cms1.test.cms.com	<blank>	usera@cms1.test.cms.com
Use dial plan	<blank>	<blank>	usera@<ip_cms>

### Étape 3. Table des appels sortants



Il s'agit de la dernière table de la logique de routage des appels qui fait de l'appel vers un autre serveur :

- L'appel entrant n'est pas traité localement (sur le domaine correspondant à l'appel entrant).
- Il s'agit d'un appel sortant d'un espace CMS (via CMA ou via API dans le cas de téléconférences planifiées TMS, par exemple, ou d'un appel sortant de Cisco Meeting Manager (CMM)) ou d'un client CMA.

Sur l'image, vous pouvez voir que la logique est relativement facile. S'il n'y a aucune entrée dans la table, elle autorise toujours les appels sortants mais suppose que le serveur CMS est capable de résoudre les enregistrements SRV SIP (`_sips._tcp / _sip._tcp / _sip._udp`) pour ce domaine particulier comme indiqué sur l'URI de demande SIP. Si la table n'est pas vide, mais qu'il n'y a pas de correspondance pour le domaine composé, la même logique de recherche DNS est exécutée. S'il y a une correspondance sur le domaine, alors il suit la logique de cette règle particulière. À cet égard, si vous voulez bloquer les appels sortants de CMA ou tels qu'ils sont passés via TMS ou CMM, vous pouvez le faire de deux manières. Vous ne disposez d'aucun enregistrement SRV DNS (ou n'est pas résoluble par CMS) ou routez ces appels vers votre contrôle d'appel (CUCM)

ou Expressway par exemple) et bloquez les appels là-bas.

L'image présente un exemple de table d'appels sortants :

#### Outbound calls

Filter	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption
<input type="checkbox"/>	steven.lab	<none; call directly>	contact.test.com	test.com	Standard SIP	Stop	5	Unencrypted
<input type="checkbox"/>	newany.com	10.48.36.46	callbridgefqdn.any.com	callbridgefqdn.any.com	Lync	Stop	4	Unencrypted
<input type="checkbox"/>	any.com	10.48.36.46		<use local contact domain>	Standard SIP	Stop	3	Unencrypted
<input type="checkbox"/>	test.cms.com	10.48.36.46		<use local contact domain>	Standard SIP	Stop	2	Unencrypted
<input type="checkbox"/>	vcs.steven.lab	10.48.36.46		<use local contact domain>	Standard SIP	Stop	1	Unencrypted
<input type="checkbox"/>	<match all domains>	10.48.36.215		<use local contact domain>	Standard SIP	Stop	0	Unencrypted
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Standard SIP	Stop	0	Auto

Avec une règle générale **<match all domain>** à la fin et la première règle au domaine de steven.lab sans **proxy SIP à utiliser** rempli (il s'appuie donc sur les enregistrements SRV DNS pour cela).

Notez qu'il s'agit d'une liste ordonnée avec une valeur de **priorité** supérieure couverte en premier. Si vous associez une règle au **comportement** défini sur Arrêter, l'appel ne passe pas par le reste de la table après cette correspondance et l'appel a échoué si le proxy SIP n'a pas pu acheminer l'appel par exemple. Lorsque ce paramètre est défini sur Continuer, vous pouvez autoriser une reprise sur une route différente ou un noeud différent dans le cluster. Par exemple, vous pouvez spécifier un proxy SIP différent pour chaque règle sur le même domaine.

Les paramètres du **domaine de contact local** et du **domaine local de** sont couverts dans la section précédente du tableau de transfert d'appels entrants. Le **type de liaison** vous permet de spécifier le type d'appel à effectuer, qui peut être SIP standard, Lync ou Avaya qui dépend du système de réception.

Le champ **Encryption** détermine si la signalisation de l'appel doit être non chiffrée ou chiffrée. Toutefois, notez que cela n'implique aucun chiffrement de support tel que défini dans la configuration **de chiffrement de support SIP** telle qu'elle figure dans le menu **Configuration > Call Settings**. Dans cette configuration, vous avez également la possibilité de sélectionner Auto qui tente de passer l'appel en premier avec une signalisation chiffrée avec un éventuel retour vers une signalisation non chiffrée. Si vous savez d'emblée que l'autre côté est chiffré ou non, il est fortement recommandé de le définir en conséquence afin d'éviter tout retard de configuration d'appel dû au processus de secours.

Un exemple de sortie du fichier journal d'un appel à steven.lab (après la réécriture du domaine sur la table de transfert d'appel entrant), avec la trace DNS et la trace SIP définies en détail, nous montre les enregistrements SRV interrogés et le mécanisme de secours au cas où le chiffrement serait défini sur Auto.

```

2018-10-12 11:25:16.168 Info call 821: incoming SIP call from "sip:1060@steven.lab" to
local URI "sip:stejanss@any.com"
2018-10-12 11:25:16.179 Info forwarding call to 'sip:stejanss@any.com' to
'stejanss@steven.lab'
2018-10-12 11:25:16.180 Info call 822: outgoing SIP call to "stejanss@steven.lab"

2018-10-12 11:25:16.180 Info DNS trace: resolving "steven.lab" (SRV "_sips._tcp",
dnsType:1) for call 822

```

```

2018-10-12 11:25:16.181 Info      DNS trace: resolution of "steven.lab" (SRV "_sips._tcp") for
call 822 returned result, addresses: 1
2018-10-12 11:25:16.181 Info      DNS trace: resolution of "steven.lab" (SRV "_sips._tcp") for
call 822 succeeded; results: 1
2018-10-12 11:25:16.181 Info      DNS trace: resolution of "steven.lab" (SRV "_sips._tcp") for
call 822 using 10.48.36.215:5061
2018-10-12 11:25:16.181 Info      SIP trace: connection 45: allocated for outgoing encrypted
connection to 10.48.36.215:5061
2018-10-12 11:25:16.201 Info      handshake error 336151576 on outgoing connection 45 to
10.48.36.215:5061 from 10.48.80.71:54864
2018-10-12 11:25:16.201 Info      SIP trace: connection 45: shutting down...

2018-10-12 11:25:16.201 Info      call 822: falling back to unencrypted control connection...

2018-10-12 11:25:16.201 Info      DNS trace: resolving "steven.lab" (SRV "_sip._tcp",
dnsType:1) for call 822
2018-10-12 11:25:16.202 Info      DNS trace: resolution of "steven.lab" (SRV "_sip._tcp") for
call 822 returned result, addresses: 1
2018-10-12 11:25:16.202 Info      DNS trace: resolution of "steven.lab" (SRV "_sip._tcp") for
call 822 succeeded; results: 1
2018-10-12 11:25:16.202 Info      DNS trace: resolution of "steven.lab" (SRV "_sip._tcp") for
call 822 using 10.48.36.215:5060
2018-10-12 11:25:16.202 Info      SIP trace: connection 46: allocated for outgoing connection
to 10.48.36.215:5060
2018-10-12 11:25:16.203 Info      SIP trace: connection 46: outgoing connection successful,
10.48.80.71:59776 to 10.48.36.215:5060
2018-10-12 11:25:16.205 Info      SIP trace: connection 46: outgoing SIP TCP data to
10.48.36.215:5060 from 10.48.80.71:59776, size 3290:
2018-10-12 11:25:16.205 Info      SIP trace: INVITE sip:stejanss@steven.lab SIP/2.0

```

**Note:** Dans le cas d'un environnement en cluster avec plusieurs ponts d'appel, vous pouvez configurer des règles de plan de numérotation sortantes par pont d'appel lorsque vous le configurez via l'API et spécifiez sur l'objet API un ID de pont d'appel (ou ID de groupe d'appels). Supposez par exemple que vous voulez que tous les appels sortent d'un pont d'appel particulier pour un domaine particulier (par exemple, lorsque vous composez un numéro sur us.example.com, vous voulez qu'il sorte de vos serveurs basés aux États-Unis). Vérifiez ensuite que vous disposez d'une configuration API pour outboundDialPlanRules de sorte que l'autre pont d'appel que le pont basé aux États-Unis puisse acheminer l'appel vers le pont d'appel américain (dans le cas de cet exemple).

OutboundDialPlanRule (pour US callbridge)

- domaine = us.exemple.com
- sipProxy = <vide lors de l'utilisation de DNS SRV / IP ou FQDN si défini manuellement>
- scope = callbridge
- callbridge = <UScallbridge-ID>

OutboundDialPlanRules (pour tous les ponts d'appels non américains qui doivent permettre de passer cet appel) (besoin d'un par pont d'appel)

- domaine = us.exemple.com
- sipProxy = <IP-or-FQDN-of-US-Callbridge>
- scope = callbridge
- callbridge = <non-US-callbridge-ID>

## Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

## Dépannage

Aucune information de dépannage spécifique n'est actuellement disponible pour cette configuration.

## Informations connexes

- [Support et documentation techniques - Cisco Systems](#)
  - [Outil d'analyse des solutions de collaboration](#)
  - [Documentation CMS](#)
- 

NOTE: Pour obtenir des exemples de configuration, consultez les guides suivants :

- [Configuration et intégration du guide unique combiné CMS](#)
- [Guide de configuration de Cisco Meeting Server et CUCM](#)