

# Ajouter des participants à une conférence ou un espace existant dans le déploiement de cluster CMS avec l'équilibrage de charge activé

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Méthodes pour ajouter un participant à une conférence CMS existante](#)

[Configurer](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit comment ajouter des participants à une conférence CMS existante dans le déploiement de CMS en cluster avec l'équilibrage de charge activé.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Équilibrage de charge CMS (Cisco Meeting Server)
- Conférence CUCM ad hoc (Cisco Unified Communications Manager)

Ce document suppose que l'équilibrage de charge est déjà configuré pour vos ponts d'appels en cluster (CB) et que vous travaillez pour des appels directs vers ces serveurs CMS (appelant directement vers un espace CMS existant). Cela signifie que ces conditions sont déjà configurées :

- Tous les serveurs CMS qui doivent être utilisés pour les conférences ad hoc sont ajoutés à CUCM > Ressources multimédias > Pont de conférence et sont enregistrés
- Une liste de groupes de ressources multimédias (MRGL) contenant un groupe de ressources multimédias (MRG) est créée, elle ne comporte que les serveurs CMS et elle est le premier groupe de la liste MRGL
- Une liste de routage contenant un groupe de routage est créée et elle contient les serveurs CMS, et l'algorithme de distribution sélectionné est Circular

## Composants utilisés


Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CMS 2.9.1
- CUCM 12.5.1

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.

## Méthodes pour ajouter un participant à une conférence CMS existante

---

 Remarque : il existe trois méthodes principales pour ajouter un participant à une conférence CMS existante : ajouter un participant via l'API, ajouter un participant via le contrôle actif et ajouter un participant sans contrôle actif.

---

### 1. Ajouter un participant via l'API

Pour utiliser cette méthode, LoadbalanceOutgoingCalls sur le groupe Callbridge doit être activé.

Pour ajouter le participant à l'aide de cette méthode, une demande API POST doit être effectuée auprès de `/calls/<active-call-id>/participants/`. La demande POST doit inclure l'ID de participant du participant qui est ajouté à la conférence en tant que valeur du paramètre `remoteParty`, qui fait partie de cette demande POST.

Cette requête POST demande au CMS d'effectuer un appel sortant vers le participant qui est ajouté. Si LoadbalanceOutgoingCalls sur le groupe Callbridge est activé et si CMS a atteint sa limite de charge, il trouve un serveur CMS libre dans le cluster pour effectuer un appel sortant au participant ajouté, et un appel distribué est créé entre les deux serveurs. Il s'agit de la même méthode utilisée par CMM pour ajouter des participants à une conférence CMS.

### 2. Ajouter un participant via le contrôle actif

Pour utiliser l'ajout de participants Active Control, Active Control doit d'abord être négocié entre le serveur CMS et l'utilisateur qui ajoute le participant.

Vous devez activer le contrôle actif sur le profil de liaison SIP qui est configuré sur la liaison SIP connectant CUCM à CMS, pour le faire, activez le paramètre Allow IX application media, et notez que le profil SIP standard pour la téléconférence TelePresence Conferencing l'a activé par défaut. En outre, LoadbalanceOutgoingCalls sur le groupe Callbridge doit être activé.

Lorsqu'un participant est ajouté via le contrôle actif à une conférence CMS existante, CMS1 reçoit l'instruction de l'utilisateur (via un message de contrôle actif) d'effectuer un appel sortant vers le nouveau participant. Si la valeur de limite de charge configurée sur CMS1 est atteinte et que l'utilisateur tente d'ajouter un nouveau participant avec contrôle actif, CMS1 affiche ce message

d'erreur (jusqu'à la version 2.9.1 de CMS) :

```
add participant "<participant-uri>" request failed: call bridge unavailable
```

Cela s'applique aux deux cas d'utilisation : lorsque le participant est ajouté à une conférence ad hoc et lorsqu'il est ajouté à un espace CMS existant via le contrôle actif.

Il s'agit d'un comportement défectueux et il est suivi sous le défaut : [CSCvu72374](#)

### 3. Ajouter un participant sans contrôle actif

Lorsqu'un participant est ajouté sans utiliser le contrôle actif (par conséquent, Allow IX application media not enabled on the SIP Profile), CUCM effectue un appel entre l'utilisateur qui initie l'action et le nouveau participant. Ensuite, lorsque l'utilisateur est prêt à rejoindre le nouveau participant à la conférence, CUCM effectue un appel sortant vers la conférence ad hoc exécutée sur CMS1. Si la limite de charge est atteinte sur CMS1, le participant ne peut pas être ajouté et CMS1 affiche ce message d'erreur (55 est un exemple de numéro d'appel) :

```
call 55: ending; local teardown, system participant limit reached - not connected after 0:00
```


Ce message d'erreur est un message d'erreur normal qui doit être imprimé par un serveur CMS lorsqu'il reçoit un appel entrant et après avoir atteint sa limite de charge maximale. Il appartient ensuite au serveur de contrôle d'appel (CUCM ou VCS) de continuer à acheminer l'appel vers d'autres membres du cluster. Cependant, dans le cas d'une conférence ad hoc, cela ne fonctionne pas et ce n'est pas possible puisque CUCM n'a pas de liste de routage pour les conférences adhoc.

## Configurer

Ce document fournit les étapes de configuration requises pour utiliser la 3ème façon d'ajouter un participant à une conférence existante (Ajouter un participant sans contrôle actif).

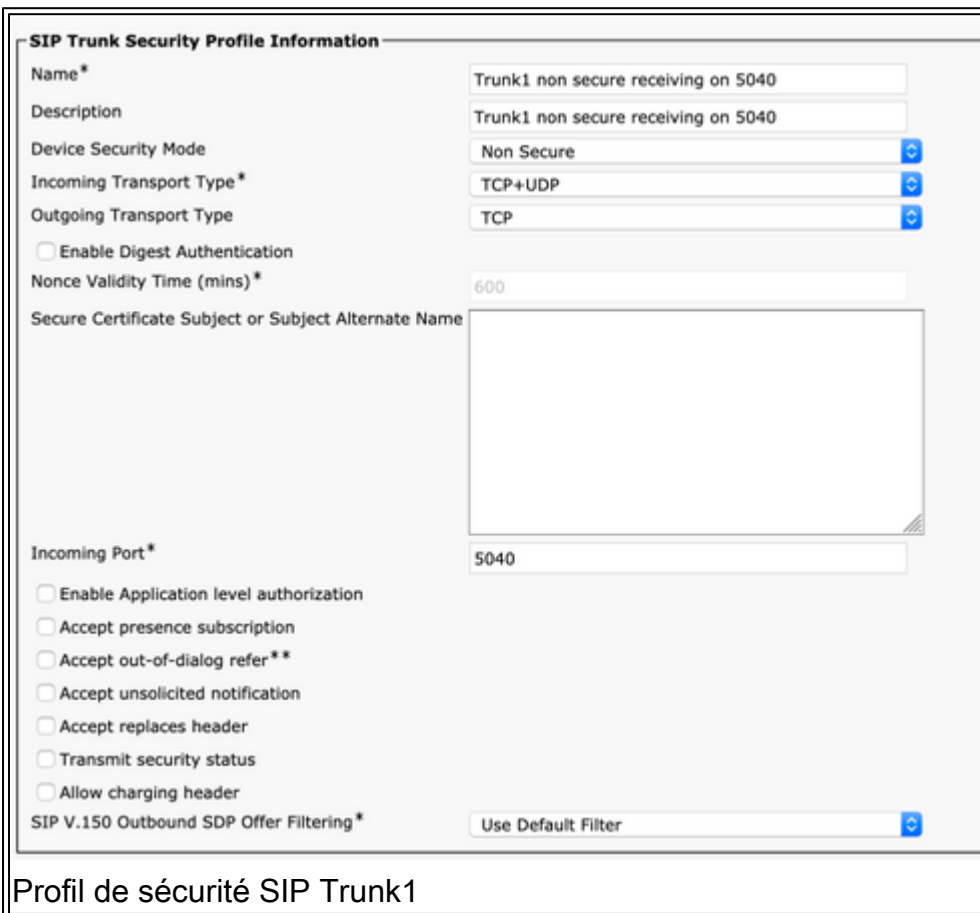
Le comportement traité dans les étapes de configuration de ce document est le suivant :

1. L'utilisateur crée une conférence ad hoc, le serveur CMS1 l'héberge
2. Une fois la conférence ad hoc établie, CMS1 atteint progressivement sa limite de charge configurée (configurée sur l'API `at/system/configuration/cluster`)
3. L'utilisateur tente d'ajouter un nouveau participant à la conférence ad hoc en cours, mais il ne se connecte pas à la conférence

 Remarque : cette procédure de configuration permet à un utilisateur d'ajouter des participants à une conférence ad hoc CMS existante même si le serveur CMS hébergeant la conférence a atteint sa limite de charge, et elle peut être utilisée jusqu'à ce que le défaut de contrôle actif soit corrigé. Le contrôle actif est désactivé dans cette conférence ad hoc.

## Étape 1. Créer un nouveau profil de sécurité de ligne principale SIP pour la ligne principale 1

- Accédez à Système > Sécurité > Profil de sécurité de la ligne principale SIP
- Sélectionnez Add New (ajouter nouveau)
- Définissez le nom sur Trunk1 non secure receive sur 5040
- Définir le mode de sécurité du périphérique sur Non sécurisé
- Définissez le port entrant sur 5040
- Sélectionnez Save (enregistrer)



**SIP Trunk Security Profile Information**

Name\* Trunk1 non secure receiving on 5040

Description Trunk1 non secure receiving on 5040

Device Security Mode Non Secure

Incoming Transport Type\* TCP+UDP

Outgoing Transport Type TCP

Enable Digest Authentication

Nonce Validity Time (mins)\* 600

Secure Certificate Subject or Subject Alternate Name

Incoming Port\* 5040

Enable Application level authorization

Accept presence subscription

Accept out-of-dialog refer\*\*

Accept unsolicited notification

Accept replaces header

Transmit security status

Allow charging header

SIP V.150 Outbound SDP Offer Filtering\* Use Default Filter

Profil de sécurité SIP Trunk1

## Étape 2. Créer un nouveau profil de sécurité de ligne principale SIP pour la ligne principale 2

- Accédez à Système > Sécurité > Profil de sécurité de la ligne principale SIP
- Sélectionnez Add New (ajouter nouveau)
- Définissez le nom sur Trunk2 non secure receive sur 5041
- Définir le mode de sécurité du périphérique sur Non sécurisé
- Définissez le port entrant sur 5041
- Sélectionnez Save (enregistrer)

**SIP Trunk Security Profile Information**

Name\* Trunk2 non secure receiving on 5041

Description Trunk2 non secure receiving on 5041

Device Security Mode Non Secure

Incoming Transport Type\* TCP+UDP

Outgoing Transport Type TCP

Enable Digest Authentication

Nonce Validity Time (mins)\* 600

Secure Certificate Subject or Subject Alternate Name

Incoming Port\* 5041

Enable Application level authorization

Accept presence subscription

Accept out-of-dialog refer\*\*

Accept unsolicited notification

Accept replaces header

Transmit security status

Allow charging header

SIP V.150 Outbound SDP Offer Filtering\* Use Default Filter

Profil de sécurité SIP Trunk2

### Étape 3 : création d'un script de normalisation SIP

- Accédez à Device > Device settings > Scripts de normalisation SIP
- Sélectionnez Add New (ajouter nouveau)
- Définissez le nom sur remove\_conference\_from\_call\_info\_header
- Dans le contenu, utilisez ce script

```
M = {}
function M.outbound_INVITE(msg)
    msg:removeHeaderValue("Call-Info", "<urn:x-cisco-remotecc:conference>")
end
return M
```

- Sélectionnez Save (enregistrer)

### Étape 4. Créer un nouveau profil SIP

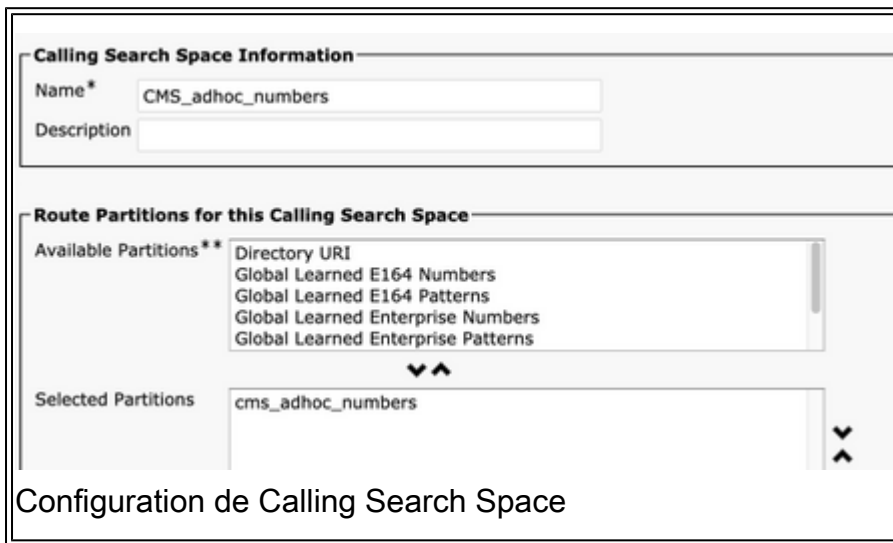
- Accédez à Device > Device settings > Profil SIP
- Sélectionnez le profil SIP standard pour les conférences TelePresence et copiez-le
- Définissez le nom sur Aucune téléprésence de contrôle active
- Décochez la case Allow iX Application Media au bas de la page
- Sélectionnez Save (enregistrer)

### Étape 5. Créer une nouvelle partition

- Accédez à Routage des appels > Classe de contrôle > Partition
- Sélectionnez Add New (ajouter nouveau)
- Définissez le nom sur cms\_adhoc\_numbers
- Sélectionnez Save (enregistrer)

Étape 6. Création d'un espace de recherche d'appels (CSS) :

- Naviguez jusqu'à Routage des appels > Classe de contrôle > Espace de recherche des appels
- Sélectionnez Add New (ajouter nouveau)
- Définissez le nom sur CMS\_adhoc\_numbers
- Ajoutez la partition créée à l'étape 5 cms\_adhoc\_numbers
- Sélectionnez Save (enregistrer)



Étape 7. Créez une nouvelle ligne principale SIP, Trunk1 :

- Naviguez jusqu'à Device >Trunk (Périphérique > Ligne principale)
- Sélectionnez Add New (ajouter nouveau)
- Sélectionnez SIP Trunk (ligne principale SIP) pour le Trunk Type (type de ligne principale)
- Sélectionnez Next (suivant)
- Saisissez ces valeurs et enregistrez

Nom du périphérique	Entrez un nom pour la ligne principale SIP, Trunk1
Exécuter sur tous les noeuds Unified CM actifs	Coché
Adresse de destination	Saisissez l'adresse IP du serveur CUCM lui-même, par exemple 10.48.36.50
Port de destination	Entrez le port sur lequel Trunk2 écoute, 5041
Profil de sécurité de la ligne principale SIP	Sélectionnez le profil créé à l'étape 1, Trunk1 non secure receive on 5040
Profil SIP	Sélectionnez le profil créé à l'étape 4, Aucune téléprésence de contrôle active

Méthode de signalisation DTMF	Sélectionnez RFC 2833
Script de normalisation SIP	Sélectionnez le script créé à l'étape 3, remove_conference_from_call_info_header

**SIP Information**

**Destination**

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.48.36.50		5041

MTP Preferred Originating Codec\* 711ulaw

BLF Presence Group\* Standard Presence group

SIP Trunk Security Profile\* Trunk1 non secure receiving on 5040

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile\* No active control telepresence conferencing [View Details](#)

DTMF Signaling Method\* RFC 2833

Trunk1 SIP settings

---

**Normalization Script**

Normalization Script remove\_conference\_from\_call\_info\_header

Paramètres SIP de Trunk1

Étape 8. Créez une nouvelle ligne principale SIP, Trunk2 :

- Naviguez jusqu'à Device >Trunk (Périphérique > Ligne principale)
- Sélectionnez Add New (ajouter nouveau)
- Sélectionnez SIP Trunk (ligne principale SIP) pour le Trunk Type (type de ligne principale)
- Sélectionnez Next (suivant)
- Saisissez ces valeurs et enregistrez

Nom du périphérique	Entrez un nom pour la ligne principale SIP, Trunk2
Exécuter sur tous les noeuds Unified CM actifs	Coché
Espace de recherche d'appels	Sélectionnez le CSS créé à l'étape 6, CMS_adhoc_numbers
Adresse de destination	Entrez l'adresse IP ou le nom de domaine complet du serveur CUCM lui-même, par exemple 10.48.36.50
Port de destination	Entrez le port sur lequel Trunk1 écoute, 5040
Profil de sécurité de la ligne principale SIP	Sélectionnez le profil créé à l'étape 2, Trunk2 non secure receive on 5041
Profil SIP	Sélectionnez le profil créé à l'étape 4, Aucune téléprésence de contrôle active
Méthode de signalisation DTMF	Sélectionnez RFC 2833
Script de normalisation SIP	Sélectionnez le script de normalisation existant cisco-meeting-server-interop

**SIP Information**

**Destination**

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 10.48.36.50		5040

MTP Preferred Originating Codec\* 711ulaw

BLF Presence Group\* Standard Presence group

SIP Trunk Security Profile\* Trunk2 non secure receiving on 5041 **Trunk2 SIP settings**

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile\* No active control telepresence conferencing [View Details](#)

DTMF Signaling Method\* RFC 2833

**Normalization Script**

Normalization Script cisco-meeting-server-interop

Paramètres SIP du trunk2

## Étape 9. Création d'un modèle de route

- Accédez à Routage d'appel > Route/Hunt > Modèle de route
- Sélectionnez Add New (ajouter nouveau)
- Définissez la Modèle de route par !
- Définissez la partition Route Partition sur la partition créée à l'étape 5, cms\_adhoc\_numbers
- Cochez cette case Priorité urgente
- Remplacer la classification des appels par OnNet
- Définissez la passerelle/liste de routage comme étant la liste de routage CMS déjà configurée (comme mentionné dans la section Spécifications ci-dessus)
- Sélectionnez Save (enregistrer)

**Pattern Definition**

Route Pattern\* !

Route Partition cms\_adhoc\_numbers

Description

Numbering Plan -- Not Selected --

Route Filter < None >

MLPP Precedence\* Default

Apply Call Blocking Percentage

Resource Priority Namespace Network Domain < None >

Route Class\* Default

Gateway/Route List\* CMS-loadbalancing-RL [\(Edit\)](#)

Route Option

Route this pattern

Block this pattern No Error

Call Classification\* OnNet

External Call Control Profile < None >

Allow Device Override  Provide Outside Dial Tone  Allow Overlap Sending  Urgent Priority

Modèle de route



**Route List Information**

Registration: Registered with Cisco Unified Communications Manager 10.48.36.50  
 IPv4 Address: 10.48.36.50

Device is trusted

Name\* CMS-loadbalancing-RL

Description

Cisco Unified Communications Manager Group\* Default

Enable this Route List (change effective on Save; no reset required)

Run On All Active Unified CM Nodes

---

**Route List Member Information**

Selected Groups\*\* CMS-loadbalancing

Liste de routage d'équilibrage de charge CMS

**Route Group Information**

Route Group Name\* CMS-loadbalancing

Distribution Algorithm\* Circular

---

**Route Group Member Information**

**Find Devices to Add to Route Group**

Device Name contains

Available Devices\*\*

- 10.10.254.4
- Cond1-rendez-vous
- Cond2-rendez-vous
- IMP
- TO-EXP-JG-SN

Port(s) All

---

**Current Route Group Members**

Selected Devices (ordered by priority)\*

- cms-c1 (All Ports)
- cms-c2 (All Ports)
- cms-c3 (All Ports)

Groupe de routes d'équilibrage de charge CMS


## Étape 10. Modification de la configuration du pont de conférence ad hoc CMS

- Accédez à Ressources multimédias > Pont de conférence
- Sélectionnez le premier serveur CMS
- Modifiez le SIP Trunk (ligne principale SIP) vers Trunk1, la ligne principale SIP créée à l'étape 7
- Cochez cette case Remplacer la destination de la liaison SIP par une adresse HTTPS
- Dans le champ Hostname/IP Address, définissez le FQDN Webadmin du serveur CMS pour ce serveur CMS spécifique qui doit également exister dans le certificat Webadmin de ce serveur
- Sélectionnez Save (enregistrer)
- Faites de même pour tous les autres serveurs CMS, définissez Trunk1 à utiliser sur chacun d'eux, mais changez le champ Hostname/IP Address à la valeur spécifique CMS FQDN

Conference Bridge : cms\_c1  
 Registration: Registered with Cisco Unified Communications Manager 10.48.36.50  
 IPv4 Address: 10.48.36.50

---

**Device Information**


Conference Bridge Type\* Cisco Meeting Server  
 Device is trusted  
 Conference Bridge Name\*   
 Description   
 Conference Bridge Prefix   
 SIP Trunk\*    
 Allow Conference Bridge Control of the Call Security Icon

---

**HTTPS Interface Info**

Override SIP Trunk Destination as HTTPS Address

Hostname/IP Address

1  

Username\*   
 Password\*   
 Confirm Password\*   
 HTTPS Port\*


## CMS1

**Conference Bridge Information**

Conference Bridge : cms\_c2  
 Registration: Registered with Cisco Unified Communications Manager 10.48.36.50  
 IPv4 Address: 10.48.36.50

---

**Device Information**


Conference Bridge Type\* Cisco Meeting Server  
 Device is trusted  
 Conference Bridge Name\*   
 Description   
 Conference Bridge Prefix   
 SIP Trunk\*    
 Allow Conference Bridge Control of the Call Security Icon

---

**HTTPS Interface Info**

Override SIP Trunk Destination as HTTPS Address

Hostname/IP Address

1  

Username\*   
 Password\*   
 Confirm Password\*   
 HTTPS Port\*


## CMS2

**Conference Bridge Information**

Conference Bridge : cms\_c3  
 Registration: Registered with Cisco Unified Communications Manager 10.48.36.50  
 IPv4 Address: 10.48.36.50

---

**Device Information**


Conference Bridge Type\* Cisco Meeting Server  
 Device is trusted  
 Conference Bridge Name\*   
 Description   
 Conference Bridge Prefix   
 SIP Trunk\*    
 Allow Conference Bridge Control of the Call Security Icon

---

**HTTPS Interface Info**

Override SIP Trunk Destination as HTTPS Address

Hostname/IP Address

1  

Username\*   
 Password\*   
 Confirm Password\*   
 HTTPS Port\*

CMS3

## Étape 11. Réinitialisation des liaisons SIP Trunk1 et Trunk2

- Naviguez jusqu'à Device >Trunk (Périphérique > Ligne principale)
- Sélectionnez Trunk1 et Trunk2
- Sélectionnez Réinitialiser la sélection
- Patientez jusqu'à ce que tous deux affichent Full service

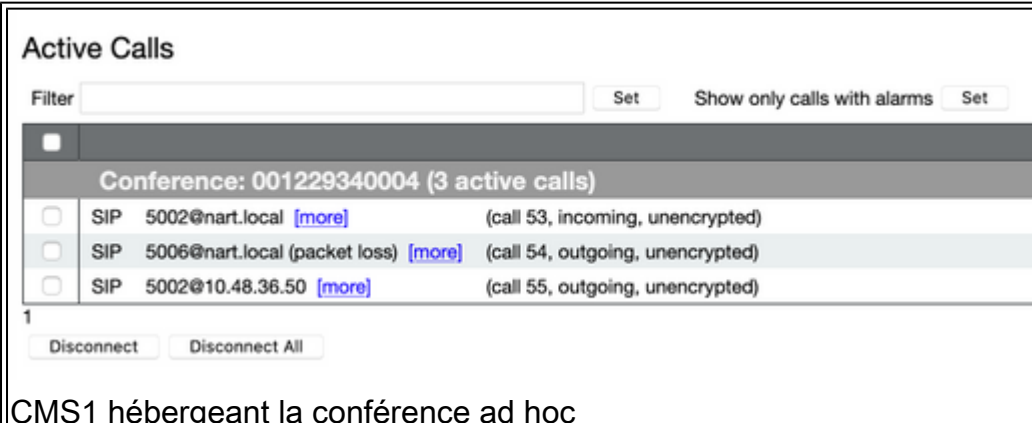
## Étape 12. Réinitialiser les serveurs ad hoc CMS

- Naviguez jusqu'à Media Resources > Conference Bridge (Ressources multimédias > Passerelle de conférence)
- Sélectionner tous les serveurs CMS
- Sélectionnez Réinitialiser la sélection
- Patientez jusqu'à ce que tous les serveurs soient enregistrés

## Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

- Créez une conférence ad hoc et vérifiez quel serveur CMS héberge la conférence



The screenshot shows the 'Active Calls' interface. At the top, there is a 'Filter' input field and a 'Set' button. To the right, there is a 'Show only calls with alarms' checkbox and another 'Set' button. Below this, a table lists active calls. The first row is a header: 'Conference: 001229340004 (3 active calls)'. The table contains three rows of call details:

Call ID	Details
<input type="checkbox"/> SIP 5002@nart.local <a href="#">[more]</a>	(call 53, incoming, unencrypted)
<input type="checkbox"/> SIP 5006@nart.local (packet loss) <a href="#">[more]</a>	(call 54, outgoing, unencrypted)
<input type="checkbox"/> SIP 5002@10.48.36.50 <a href="#">[more]</a>	(call 55, outgoing, unencrypted)

At the bottom of the table, there is a '1' and two buttons: 'Disconnect' and 'Disconnect All'.

CMS1 hébergeant la conférence ad hoc

- Vérifier la charge de traitement multimédia actuelle sur ce serveur CMS, utiliser une API GET vers /system/load



The screenshot shows the API endpoint '/api/v1/system/load'. At the top, there are three buttons: 'View', 'Table view', and 'XML view'. Below these buttons, there is a section titled 'Object configuration' with the following data:

```
mediaProcessingLoad 1525
```

Chargement du support actuel

- Définissez la limite de charge sur le serveur sur une valeur inférieure à la charge de

traitement du support en envoyant un POST à /system/configuration/cluster avec le paramètre loadlimit, par exemple 1000

**/api/v1/system/configuration/cluster** ◀

View or edit   Table view   XML view

Object configuration	
uniqueName	cms-c1
maxPeerVideoStreams	
participantLimit	
loadLimit	1000
newConferenceLoadLimitBasisPoints	5000
existingConferenceLoadLimitBasisPoints	8000

Modification de la limite de charge

- Ajouter un nouveau participant à la téléconférence. Le participant est ajouté et un serveur distribué est créé entre CMS1 et un autre serveur CMS, car CMS1 a atteint sa limite

**Active Calls**

Filter  Set   Show only calls with alarms  Set

Conference: 001229340004 (4 active calls; 3 local participants; 1 remote participant)	
<input type="checkbox"/>	SIP 5002@nart.local <a href="#">[more]</a> (call 53, incoming, unencrypted)
<input checked="" type="checkbox"/>	SIP 5006@nart.local <a href="#">[more]</a> (call 54, outgoing, unencrypted)
<input type="checkbox"/>	SIP 5002@10.48.36.50 <a href="#">[more]</a> (call 55, outgoing, unencrypted)
<input type="checkbox"/>	distributed call from "cms-c3" <a href="#">[more]</a> (call 57, incoming, encrypted - AES-128)

1

Disconnect   Disconnect All

Appel distribué

## Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Vous pouvez utiliser l'outil [Collaboration Solutions Analyzer](#) pour l'analyse des journaux.

## Informations connexes

- [Logique d'équilibrage de charge sur Cisco Meeting Server](#)
- [Documentation de configuration CMS](#)
- [Guide de programmation CMS API et MMP](#)
- [Documentation de configuration CUCM](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.