

# Hinzufügen von Teilnehmern zu vorhandener Konferenz oder zu vorhandenem Speicherplatz im CMS-Cluster bei aktiviertem Lastenausgleich

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Methoden zum Hinzufügen von Teilnehmern zu einer vorhandenen CMS-Konferenz](#)

[Konfigurieren](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einführung

In diesem Dokument wird beschrieben, wie Sie Teilnehmer zu einer bestehenden CMS-Konferenz hinzufügen, wenn Clustered CMS mit aktiviertem Lastenausgleich bereitgestellt wird.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- CMS-Lastenausgleich (Cisco Meeting Server)
- Ad-hoc-CUCM-Konferenzen (Cisco Unified Communications Manager)

In diesem Dokument wird davon ausgegangen, dass der Lastenausgleich bereits für Ihre geclusterten Callbridges (CB) konfiguriert ist und für direkte Anrufe an diese CMS-Server (Anrufe direkt an einen vorhandenen CMS-Raum) funktioniert. Dies bedeutet, dass diese Anforderungen bereits konfiguriert sind:

- Alle CMS-Server, die für Ad-hoc-Konferenzen verwendet werden sollen, werden **CUCM > Media Resources > Conference Bridge** hinzugefügt und sind registriert.
- Eine **MRGL-Liste** (Media Resource Group List), die eine **Medienressourcengruppe (MRG)** enthält, wird erstellt. Sie umfasst nur die CMS-Server und ist die erste Gruppe in der **MRGL**.
- Eine **Weiterleitungsliste** mit einer **Weiterleitungsgruppe** wird erstellt, die über die CMS-Server verfügt, und der ausgewählte **Verteilungsalgorithmus** ist **Circular**

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und

Hardwareversionen:

- CMS 2.9.1
- CUCM 12.5.1

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Methoden zum Hinzufügen von Teilnehmern zu einer vorhandenen CMS-Konferenz

**Hinweis:** Es gibt drei Hauptmethoden, um einem Teilnehmer eine vorhandene CMS-Konferenz hinzuzufügen: Hinzufügen eines Teilnehmers über API, Hinzufügen eines Teilnehmers über Active Control und Hinzufügen eines Teilnehmers ohne Active Control.

### 1. Hinzufügen eines Teilnehmers über API

Um diese Methode verwenden zu können, muss **LoadbalanceOutgoingCalls** in der **Callbridge-Gruppe** aktiviert werden.

Um den Teilnehmer mithilfe dieser Methode hinzuzufügen, muss eine **API-POST-Anforderung** an **/Calls/<active-call-id>/Participants/** gestellt werden. Die **POST-Anforderung** muss die **Teilnehmer-ID** des **Teilnehmers** enthalten, die der Konferenz als Wert des **RemoteParty-Parameters** hinzugefügt wird, der Teil dieser **POST-Anforderung** ist.

Diese **POST-Anforderung** weist CMS an, einen ausgehenden Anruf an den Teilnehmer zu tätigen, der hinzugefügt wird. Wenn **LoadbalanceOutgoingCalls** auf der **Callbridge-Gruppe** aktiviert ist und das CMS seine Lastgrenze erreicht hat, findet es einen freien CMS-Server im Cluster, um einen ausgehenden Anruf an den hinzugefügten Teilnehmer zu tätigen, und ein verteilter Anruf wird zwischen den beiden Servern erstellt. Dies ist die gleiche Methode, die **CMM** verwendet, um Teilnehmer einer CMS-Konferenz hinzuzufügen.

### 2. Hinzufügen eines Teilnehmers über Active Control

Um Active Control-Teilnehmer-Add zu verwenden, muss Active Control zuerst zwischen dem CMS-Server und dem Benutzer, der den Teilnehmer hinzufügt, ausgehandelt werden.

Sie müssen Active Control für das **SIP-Trunk-Profil** aktivieren, das auf dem **SIP-Trunk** konfiguriert ist, der CUCM mit dem CMS verbindet, um den Parameter **Allow IX application media** zu aktivieren. Beachten Sie, dass **Standard-SIP-Profil für TelePresence-Konferenzen** standardmäßig aktiviert ist. Darüber hinaus müssen **LoadbalanceOutgoingCalls** in der **Callbridge-Gruppe** aktiviert werden.

Wenn ein Teilnehmer über Active Control zu einer bestehenden CMS-Konferenz hinzugefügt wird, wird CMS1 vom Benutzer (über eine aktive Kontrollmeldung) angewiesen, einen ausgehenden Anruf an den neuen Teilnehmer zu tätigen. Wenn der für CMS1 konfigurierte Lastgrenzwert erreicht ist und der Benutzer versucht, einen neuen Teilnehmer mit Active Control hinzuzufügen, zeigt CMS1 diese Fehlermeldung an (bis zu CMS Version 2.9.1):

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

Dies gilt für beide Anwendungsfälle, wenn der Teilnehmer einer Ad-hoc-Konferenz hinzugefügt wird und der Teilnehmer über Active Control einem vorhandenen CMS-Raum hinzugefügt wird.

Dies ist ein fehlerhaftes Verhalten, das unter dem Fehler nachverfolgt wird: [CSCvu72374](#)

### 3. Hinzufügen eines Teilnehmers ohne Active Control

Wenn ein Teilnehmer hinzugefügt wird, ohne aktive Kontrolle zu verwenden (**daher dürfen IX-Anwendungsmedien im SIP-Profil nicht aktiviert sein**), ruft CUCM zwischen dem Benutzer, der die Aktion initiiert, und dem neuen Teilnehmer auf. Wenn der Benutzer dann bereit ist, dem neuen Teilnehmer der Konferenz beizutreten, führt der CUCM einen ausgehenden Anruf zur Adhoc-Konferenz aus, die auf CMS1 ausgeführt wird. Wenn der Lastgrenzwert für CMS1 erreicht ist, kann der Teilnehmer nicht hinzugefügt werden, und CMS1 zeigt diese Fehlermeldung an (55 ist eine Beispielfonummer):

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

Diese Fehlermeldung ist eine normale Fehlermeldung, die von einem CMS-Server ausgegeben wird, wenn ein eingehender Anruf eingeht und die maximale Auslastungsgrenze erreicht ist. Anschließend muss der Anrufsteuerungsserver (CUCM oder VCS) den Anruf an andere Mitglieder im Cluster weiterleiten. Im Fall einer Ad-hoc-Konferenz funktioniert dies jedoch nicht, und dies ist nicht möglich, da CUCM keine **Routenliste** für Ad-hoc-Konferenzen besitzt.

## Konfigurieren

Dieses Dokument enthält die Konfigurationsschritte, die erforderlich sind, um Teilnehmer zur bestehenden Konferenz hinzuzufügen (**Hinzufügen eines Teilnehmers ohne Active Control**).

Das Verhalten, das mit den Konfigurationsschritten in diesem Dokument behandelt wird, ist:

1. Benutzer erstellt eine Adhoc-Konferenz, vom CMS1-Server wird diese gehostet
2. Nach der Einrichtung der Adhoc-Konferenz erreicht CMS1 schrittweise das konfigurierte Limit (über API konfiguriert über **/System/Konfiguration/Cluster**)
3. Der Benutzer versucht, der laufenden Ad-hoc-Konferenz einen neuen Teilnehmer hinzuzufügen. Der neue Benutzer wird jedoch nicht mit der Konferenz verbunden.

**Hinweis:** Dieses Konfigurationsverfahren ermöglicht es Benutzern, Teilnehmer einer bestehenden CMS-Adhoc-Konferenz hinzuzufügen, selbst wenn der CMS-Server, der die Adhoc-Konferenz hostet, seine Auslastungsgrenze erreicht hat, und kann verwendet werden, bis der aktive Steuerungsfehler behoben ist. Active Control wird in dieser Ad-hoc-Konferenz deaktiviert.

#### Schritt 1: Erstellen eines neuen SIP-Trunk-Sicherheitsprofils für Trunk1

- Navigieren Sie zu **System > Sicherheit > SIP-Trunk-Sicherheitsprofil**
- Wählen Sie **Neu hinzufügen** aus
- Legen Sie den **Namen** als **nicht sicheren Trunk1-Empfänger für 5040 fest**.
- Stellen Sie den **Gerätesicherheitsmodus** auf **"Nicht sicher"** ein.

- Legen Sie den **Eingangsport** auf **5040** fest.
- Wählen Sie **Speichern**

**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

Trunk1 SIP-

Sicherheitsprofil

**Schritt 2:** Erstellen eines neuen SIP-Trunk-Sicherheitsprofils für Trunk2

- Navigieren Sie zu **System > Sicherheit > SIP-Trunk-Sicherheitsprofil**
- Wählen Sie **Neu hinzufügen** aus
- Legen Sie den **Namen** als **nicht sicheren Trunk2-Empfänger für 5041** fest.
- Stellen Sie den **Gerätesicherheitsmodus** auf **"Nicht sicher"** ein.
- Legen Sie den **Eingangsport** auf **5041** fest.
- Wählen Sie **Speichern**

**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

Trunk2 SIP-

Sicherheitsprofil

### Schritt 3: Erstellen eines neuen SIP-Normungs-Skripts

- Navigieren Sie zu **Gerät > Geräteeinstellungen > SIP-Normalisierungsskripts**
- Wählen Sie **Neu hinzufügen** aus
- Legen Sie den Namen auf **remove\_Conference\_from\_call\_info\_header** fest.
- Verwenden Sie im **Inhalt** dieses Skript

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

- Wählen Sie **Speichern**

### Schritt 4: Neues SIP-Profil erstellen

- Navigieren Sie zu **Gerät > Geräteeinstellungen > SIP-Profil**
- Wählen Sie das **Standard-SIP-Profil für TelePresence-Konferenzen** aus, und kopieren Sie es.
- Legen Sie den Namen **No active control Telepresence conferencing** fest.
- Deaktivieren Sie das Kontrollkästchen **iX-Anwendungsmedien zulassen** unten auf der Seite.

- Wählen Sie **Speichern**

**Schritt 5:** Neue Partition erstellen

- Navigieren Sie zu **Call Routing > Class of Control > Partition**
- Wählen Sie **Neu hinzufügen aus**
- Legen Sie den **Namen** auf **cms\_adhoc\_numbers** fest.
- Wählen Sie **Speichern**

**Schritt 6:** Erstellen eines neuen CSS (Calling Search Space):

- Navigieren zu **Anrufweiterleitung > Class of Control > Calling Search Space**
- Wählen Sie **Neu hinzufügen aus**
- Legen Sie den **Namen** auf **CMS\_adhoc\_numbers** fest.
- Hinzufügen der in Schritt 5 erstellten Partition **cms\_adhoc\_numbers**
- Wählen Sie **Speichern**

Konfiguration des Call

Search Space

**Schritt 7:** Erstellen Sie einen neuen SIP-Trunk, **Trunk1**:

- Navigieren Sie zu **Gerät > Trunk**.
- Wählen Sie **Neu hinzufügen aus**
- Wählen Sie **SIP-Trunk** für den **Trunk-Typ** aus.
- **Weiter** auswählen
- Geben Sie diese Werte ein, und **speichern**

<b>Gerätename</b>	Geben Sie einen Namen für den SIP-Trunk, <b>Trunk1</b> ein.
<b>Auf allen aktiven Unified CM-Knoten ausführen</b>	Aktiviert
<b>Zieladresse</b>	Geben Sie die IP-Adresse des CUCM-Servers selbst ein, z. B. <b>10.48.36.50</b> .
<b>Zielport</b>	Geben Sie den Port ein, an dem der Trunk2 lauscht, <b>5041</b> .
<b>SIP-Trunk-Sicherheitsprofil</b>	Wählen Sie das Profil aus, das in Schritt 1 erstellt wurde, <b>Trunk1 unsicheres Empfangen auf 5040</b>
<b>SIP-Profil</b>	Wählen Sie das Profil aus, das in Schritt 4 erstellt wurde: <b>No Active Control Telepresence Conferencing</b> .
<b>DTMF-Signalisierungsverfahren</b>	Wählen Sie <b>RFC 2833</b>

SIP-Normalisierungsskript Wählen Sie das in Schritt 3 erstellte Skript aus,  
 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

**Normalization Script**

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

Trunk1 SIP settings

Trunk1 SIP-Einstellungen

**Schritt 8:** Erstellen Sie einen neuen SIP-Trunk, **Trunk2:**

- Navigieren Sie zu **Gerät > Trunk**.
- Wählen Sie **Neu hinzufügen aus**
- Wählen Sie **SIP-Trunk** für den **Trunk-Typ aus**.
- **Weiter** auswählen
- Geben Sie diese Werte ein, und **speichern**

**Gerätename** Geben Sie einen Namen für den SIP-Trunk, **Trunk2** ein.

**Auf allen aktiven Unified CM-Knoten ausführen** Aktiviert

**Calling Search Space** Wählen Sie den in Schritt 6 erstellten CSS aus, **CMS\_adhoc\_numbers**.

**Zieladresse** Geben Sie die IP-Adresse oder den FQDN des CUCM-Servers selbst ein, z. B. **10.48.36.50**.

**Zielport** Geben Sie den Port ein, an dem Trunk1 den **5040** abhört.

**SIP-Trunk-Sicherheitsprofil** Wählen Sie das Profil aus, das in Schritt 2 erstellt wurde, **Trunk2 unsicheres Empfangen auf 5041**

**SIP-Profil** Wählen Sie das Profil aus, das in Schritt 4 erstellt wurde: **No Active Control Telepresence Conferencing**.

**DTMF-Signalisierungsverfahren** Wählen Sie **RFC 2833**

**SIP-Normalisierungsskript** Wählen Sie das vorhandene Normalisierungsskript **cisco-meeting-server-interop** aus.

**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

unk2 SIP-Einstellungen

### Schritt 9: Erstellen eines neuen Routenmusters

- Navigieren Sie zu **Anrufweiterleitung > Route/Hunt > Routenmuster**
- Wählen Sie **Neu hinzufügen** aus
- Legen Sie **Routenmuster** auf !
- Legen Sie die **Route Partition** auf die in Schritt 5 erstellte Partition fest, **cms\_adhoc\_numbers**
- Aktivieren Sie das Kontrollkästchen **Dringlichkeit**
- Ändern Sie die **Anrufklassifizierung** in **OnNet**.
- Legen Sie als **Gateway/Routenliste** die bereits konfigurierte CMS-Routenliste fest (wie im Abschnitt "Anforderungen" weiter oben erwähnt).
- Wählen Sie **Speichern**

**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

Routenmuster

**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  
 Add Route Group

**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 Find  
 Available Devices\*\* 10.10.254.4  
 Cond1-rendez-vous  
 Cond2-rendez-vous  
 IMP  
 TO-EXP-3G-5N  
 Port(s) All  
 Add to Route Group

**Current Route Group Members**

Selected Devices (ordered by priority)\* cms-c1 (All Ports)  
 cms-c2 (All Ports)  
 cms-c3 (All Ports)

CMS-

Lastenausgleichs-Routenliste

CMS-Routengruppe für Lastenausgleich

Schritt 10: Ändern der CMS-Adhoc-Konferenzbrücken-Konfiguration

- Navigieren Sie zu **Medienressourcen > Konferenzbrücke**
- Wählen Sie den ersten CMS-Server aus.
- Ändern Sie **SIP-Trunk** an **Trunk1**, den in Schritt 7 erstellten SIP-Trunk
- Aktivieren Sie das Kontrollkästchen **SIP-Trunk-Ziel als HTTPS-Adresse überschreiben**
- Legen Sie im Feld **Hostname/IP-Adresse** den CMS Webadmin **FQDN** für diesen spezifischen CMS-Server fest, der auch im Webadmin-Zertifikat dieses Servers vorhanden sein muss.
- Wählen Sie **Speichern**
- Gleiches für alle anderen CMS-Server, **Trunk1** für alle festlegen, ändern Sie jedoch das **Hostname-/IP-Adressenfeld** in das spezifische **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\* cms\_c1  
 Description  
 Conference Bridge Prefix  
 SIP Trunk\* Trunk1   
 Allow Conference Bridge Control of the Call Security Icon

---

**- HTTPS Interface Info**

Override SIP Trunk Destination as HTTPS Address

**Hostname/IP Address**

1 cms-c1.nart.com 

Username\* admin  
 Password\* .....  
 Confirm Password\* .....  
 HTTPS Port\* 449

---

Save Delete Copy Reset Apply Config Add New

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\* cms\_c2  
 Description  
 Conference Bridge Prefix  
 SIP Trunk\* Trunk1  
 Allow Conference Bridge Control of the Call Security Icon

---

**HTTPS Interface Info**

Override SIP Trunk Destination as HTTPS Address

Hostname/IP Address

1 cms-c2.nart.com

Username\* admin  
 Password\* .....  
 Confirm Password\* .....  
 HTTPS Port\* 449

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\* cms\_c3  
 Description  
 Conference Bridge Prefix  
 SIP Trunk\* Trunk1  
 Allow Conference Bridge Control of the Call Security Icon

---

**HTTPS Interface Info**

Override SIP Trunk Destination as HTTPS Address

Hostname/IP Address

1 cms-c3.nart.com

Username\* admin  
 Password\* .....  
 Confirm Password\* .....  
 HTTPS Port\* 449

CMS3

### Schritt 11: SIP-Trunks Trunk1 und Trunk2 zurücksetzen

- Navigieren Sie zu **Gerät > Trunk**.
- Wählen Sie **Trunk1** und **Trunk2** aus
- **Ausgewählte Zurücksetzen** auswählen
- Warten Sie, bis beide **Full-Service** anzeigen.

### Schritt 12: CMS Adhoc-Server zurücksetzen

- Navigieren Sie zu **Medienressourcen >Konferenzbrücke**.
- Alle CMS-Server auswählen
- **Ausgewählte Zurücksetzen** auswählen
- Warten Sie, bis alle Server **Registrierte** Server anzeigen.

## Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

- Erstellen Sie eine Adhoc-Konferenz, und überprüfen Sie, welcher CMS-Server die Konferenz hostet.

### Active Calls

Filter   Show only calls with alarms

Conference: 001229340004 (3 active calls)		
<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)

1

CMS1 a

Gastgeber der Adhoc-Konferenz

- Überprüfen Sie die aktuelle **Medienverarbeitungslast** auf diesem CMS-Server, und verwenden Sie eine **API GET** für **/System/Laden**.

**/api/v1/system/load** ◀

**Object configuration**

mediaProcessingLoad 1525

Aktuelle

Medienlast

- Legen Sie den **Lastgrenzwert** auf dem Server auf einen Wert fest, der unter der **Medienverarbeitungslast** liegt, indem Sie einen **POST** an **/System/Konfiguration/Cluster** mit dem **Lastgrenzwert** für den **Partner** senden, z. B. 1000.

View or edit

Table view

XML view

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

Ändern des Limit

- Fügen Sie dem Meeting einen neuen Teilnehmer hinzu. Der Teilnehmer wird hinzugefügt und eine Verteilung zwischen CMS1 und einem anderen CMS-Server erstellt, da CMS1 den Grenzwert erreicht hat.

## Active Calls

Filter

Set

Show only calls with alarms

Set

Conference: 001229340004 (4 active calls; 3 local participants; 1 remote partic	
<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)
	distributed call from *cms-c3* <a href="#">[more]</a> (call 57, incoming, encrypted - AES-128)

1

Disconnect

Disconnect All

Verteilte

Anruf

## Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Sie können das [Collaboration Solutions Analyser](#)-Tool für Protokollanalysen verwenden.

## Zugehörige Informationen

- [Load Balancing-Logik auf Cisco Meeting Server](#)
- [CMS-Konfigurationsdokumentation](#)
- [Programmieranleitungen für CMS API und MMP](#)
- [CUCM-Konfigurationsdokumentation](#)