

將參與者新增到CMS集群部署中已啟用負載平衡的現有會議或空間

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[向現有CMS會議新增參與者的方法](#)

[設定](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹如何在部署啟用了負載均衡的群集CMS時將參與者新增到現有CMS會議中。

必要條件

需求

思科建議您瞭解以下主題：

- CMS負載平衡 (思科會議伺服器)
- CUCM臨時會議(Cisco Unified Communications Manager)

本文檔假定已為您的群集Callbridge(CB)配置負載均衡，並正在處理對這些CMS伺服器的直接呼叫 (直接呼叫現有CMS空間)。這表示已設定以下要求：

- 所有要用於Adhoc會議的CMS伺服器都將新增到CUCM > Media Resources > Conference Bridge中，並已註冊
- 將建立包含**媒體資源組(MRG)**的**媒體資源組清單(MRGL)**，該清單僅包含CMS伺服器，是MRGL中的**第一個組**
- 將建立包含**路由組**的**路由清單**，它具有CMS伺服器，並且所選的分發演算法為**循環**

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- CMS 2.9.1
- CUCM 12.5.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

向現有CMS會議新增參與者的方法

附註：向現有CMS會議新增參與者有三種主要方法：通過API新增參與者，通過Active Control新增參與者，以及新增沒有活動控制的參與者。

1.通過API新增參與者

若要使用此方法，必須啟用Callbridge組上的LoadbalanceOutgoingCalls。

若要使用此方法新增參與者，必須向/calls/<active-call-id>/participants/發出API POST請求。POST請求需要包括參與者的participantID，此參與者作為remoteParty引數的值新增到會議，此引數是此POST請求的一部分。

此POST請求指示CMS向正在新增的參與者發出撥出呼叫。如果在Callbridge Group上啟用了LoadbalanceOutgoingCalls，並且如果CMS已達到其負載限制，它將在群集中查詢一個空閒的CMS伺服器以向正在新增的參與者發出呼叫，並在兩個伺服器之間建立一個分散式呼叫。這是CMM用於向CMS會議添加參與者的相同方法。

2.通過活動控制元件新增參與者

若要使用活動控制參與者新增，必須首先在CMS伺服器和正在新增參與者的使用者之間協商活動控制。

您需要對在SIP中繼上配置的SIP Trunk Profile啟用Active Control，該配置檔案將CUCM與CMS連線，為此，請啟用引數Allow IX application media，並注意Standard SIP Profile For TelePresence Conferencing在預設情況下已啟用該配置。此外，必須啟用Callbridge組上的LoadbalanceOutgoingCalls。

當參與者通過Active Control新增到現有CMS會議時，使用者會指示CMS1 (通過活動控制消息) 向新參與者發出撥出呼叫。如果達到CMS1上配置的負載限制值，並且使用者嘗試新增具有主動控制的新參與者，則CMS1會顯示以下錯誤消息 (CMS版本2.9.1) ：

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

這同時適用於兩種使用情形 — 將參與者新增到臨時會議中，以及通過主動控制將其新增到現有CMS空間中。

這是一個缺陷行為，正在缺陷之下跟蹤：[CSCvu72374](#)

3.新增沒有活動控制的參與者

當新增參與者而不使用主動控制(因此在SIP配置檔案上未啟用Allow IX application media)時，CUCM會在發起操作的使用者和新參與者之間發出呼叫。然後，當使用者準備加入新的參與者參加會議時，CUCM發出對CMS1上運行的臨時會議的撥出呼叫。如果CMS1達到負載限制，則無法新增參與者，並且CMS1顯示以下錯誤消息 (55是示例呼叫號碼) ：

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

此錯誤消息是CMS伺服器在收到傳入呼叫並且達到其最大負載限制後要列印的一般錯誤消息。然後由呼叫控制伺服器 (CUCM或VCS) 繼續將呼叫路由到集群中的其他成員。但是，如果是臨時會議，則無法工作，因為CUCM沒有用於臨時會議的路由清單。

設定

本文檔提供了使用將參與者新增到現有會議的第三種方法(新增參與者而非活動控制)所需的配置步驟。

本文配置步驟所涉及的行為是：

- 1.使用者建立臨時會議，由CMS1伺服器託管
- 2.在臨時會議建立後，CMS1逐漸達到其配置的負載限制(通過/system/configuration/cluster上的API配置)
- 3.使用者嘗試向正在進行的臨時會議新增新的參與者，但新使用者未連線到會議

附註：此配置過程允許使用者向現有CMS臨時會議新增參與者，即使託管該臨時會議的CMS伺服器已達到其負載限制，並且它可以在修復活動控制缺陷之前使用。該臨時會議中禁用了活動控制。

步驟1。 為Trunk1建立新的SIP中繼安全配置檔案

- 導覽至System > Security> SIP中繼安全配置檔案
- 選擇Add New
- 將Name設定為Trunk1 non secure receiving on 5040
- 將Device Security Mode設定為Non-secure
- 將傳入埠設定為5040
- 選擇儲存

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安

置檔案

步驟2。 為Trunk2建立新的SIP中繼安全配置檔案

- 導覽至System > Security > SIP中繼安全配置檔案
- 選擇Add New
- 將5041上的名稱設定為Trunk2非安全接收
- 將Device Security Mode設定為Non-secure
- 將傳入埠設定為5041
- 選擇儲存

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安全

檔案

步驟3. 建立新的SIP規範化指令碼

- 導覽至Device > Device settings > SIP規範化指令碼
- 選擇Add New
- 將Name設定為remove_conference_from_call_info_header
- 在內容中，使用此指令碼

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

- 選擇儲存

步驟4. 建立新的SIP配置檔案

- 導覽至Device > Device settings > SIP配置檔案
- 選擇TelePresence Conferencing的標準SIP配置檔案並複製
- 將Name設定為No active control telepresence conferencing
- 取消選中頁面底部的Allow iX Application Media覈取方塊

- 選擇儲存

步驟5。 建立新分割槽

- 導航至**呼叫路由>控制類> 分割槽**
- 選擇Add New
- 將Name設定為**cms_adhoc_numbers**
- 選擇儲存

步驟6。 建立新的呼叫搜尋空間(CSS):

- 導航至 **呼叫路由>控制類別>呼叫搜尋空間**
- 選擇Add New
- 將Name設定為**CMS_adhoc_numbers**
- 新增在步驟5中建立的分割槽**cms_adhoc_numbers**
- 選擇儲存

呼叫搜尋空間配置

步驟7。 建立新的SIP中繼,Trunk1:

- 導覽至**Device > Trunk**
- 選擇Add New
- 選擇**SIP Trunk**作為中繼**型別**
- 選擇**下一步**
- 輸入這些值並保存

裝置名稱	輸入SIP中繼的名稱,Trunk1
在所有活動的Unified CM節點上運行	已檢查
目的地地址	輸入CUCM伺服器本身的IP, 例如10.48.36.50
目的地連線埠	輸入Trunk2偵聽的埠5041
SIP中繼安全配置檔案	選擇在步驟1中建立的配置檔案, Trunk1在5040上非安全接收
SIP配置檔案	選擇在步驟4 無活動控制網真會議 中建立的配置檔案
DTMF信令方法	選擇RFC 2833
SIP規範化指令碼	選擇在步驟3中建立的指令碼 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 setting

Trunk1 SIP設定

步驟8。 建立新的SIP中繼,Trunk2:

- 導覽至Device > Trunk
- 選擇Add New
- 選擇SIP Trunk作為中繼型別
- 選擇下一步
- 輸入這些值並保存

裝置名稱	輸入SIP中繼的名稱,Trunk2
在所有活動的Unified CM節點上運行	已檢查
呼叫搜尋空間	選擇在步驟6中建立的CSS, CMS_adhoc_numbers
目的地地址	輸入CUCM伺服器本身的IP地址或FQDN, 例如10.48.36.50
目的地連線埠	輸入Trunk1偵聽的埠5040
SIP中繼安全配置檔案	選擇在步驟2中建立的配置檔案,Trunk2在5041上非安全接收
SIP配置檔案	選擇在步驟4無活動控制網真會議中建立的配置檔案
DTMF信令方法	選擇RFC 2833
SIP規範化指令碼	選擇現有規範化指令碼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

unk2 SIP設定

步驟9。 建立新的路由模式

- 導覽至Call routing > Route/Hunt> 路由模式
- 選擇Add New
- 設定 路由模式 到!
- 將Route Partition 設定為步驟5中建立的分割槽cms_adhoc_numbers
- 啟用覈取方塊 緊急優先順序
- 將呼叫分類更改為OnNet
- 將Gateway/Route List設定為已配置的CMS路由清單 (如前面的「要求」部分所述)
- 選擇儲存

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

路由模式

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

CMS負載平衡路

單

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-JG-SN
 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負載平衡路由組

步驟10. 修改CMS臨時會議網橋配置

- 導覽至**媒體資源 > 會議橋接器**
- 選擇第一個CMS伺服器
- 更改 **SIP中繼** 到Trunk1，在第7步中建立的SIP中繼
- 啟用**覈取方塊** 將**SIP中繼目標**替換為**HTTPS地址**
- 在**主機名/IP地址**欄位中，設定該特定CMS伺服器的CMS Webadmin FQDN，該伺服器的Webadmin證書中也必須存在
- 選擇**儲存**
- 對所有其他CMS伺服器執行相同操作，將Trunk1設定為在所有伺服器上使用，但將**Hostname/IP Address**欄位更改為特定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*
 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	<input type="text" value="cms-c3.nart.com"/>	<input type="button" value="±"/>
---	--	----------------------------------

Username*
 Password*
 Confirm Password*
 HTTPS Port*

CMS3

步驟11。 重置SIP中繼中繼1和中繼2

- 導覽至Device > Trunk
- 選擇Trunk1和Trunk2
- 選擇Reset selected
- 等到兩者都顯示完整服務

步驟12。 重置CMS臨時伺服器

- 導覽至Media resources > Conference bridge
- 選擇所有CMS伺服器
- 選擇Reset selected
- 等到所有伺服器都顯示Registered

驗證

使用本節內容，確認您的組態是否正常運作。

- 建立臨時會議並檢查哪個CMS伺服器承載該會議

Active Calls

Filter Show only calls with alarms

Conference: 001229340004 (3 active calls)		
<input type="checkbox"/>	SIP 5002@nart.local [more]	(call 53, incoming, unencrypted)
<input type="checkbox"/>	SIP 5006@nart.local (packet loss) [more]	(call 54, outgoing, unencrypted)
<input type="checkbox"/>	SIP 5002@10.48.36.50 [more]	(call 55, outgoing, unencrypted)

1

主持臨時

的CMS1

- 檢查該CMS服務器上的當前媒體處理負載，使用API GET to/system/load

/api/v1/system/load ◀

Object configuration

mediaProcessingLoad	1525
---------------------	------

當前介質負

- 使用引數loadlimit(例如1000)將POST傳送到/system/configuration/cluster，將伺服器上的負載限制設定為低於媒體處理負載的值

/api/v1/system/configuration/cluster ◀

Object configuration

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

更改負載限制

- 向會議新增新參與者。將新增該參與者，並在CMS1和另一個CMS伺服器之間建立一個分發伺服器，因為CMS1已達到其限制

Active Calls

Filter Show only calls with alarms

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

1

分散式呼

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

您可以使用[Collaboration Solutions Analyzer工具](#)進行日誌分析。

相關資訊

- [思科會議伺服器上的負載平衡邏輯](#)
- [CMS配置文檔](#)
- [CMS API和MMP程式設計指南](#)
- [CUCM配置文檔](#)