配置思科會議伺服器和CUCM臨時會議

目錄

簡介

本文檔介紹使用思科會議伺服器(CMS)和思科統一通訊管理器(CUCM)配置臨時會議的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- CMS部署和配置
- CUCM終端註冊和中繼建立
- 簽名的證書

採用元件

- CUCM
- CMS Server 2.0.X及更高版本
- 必須在CMS上配置Web管理元件和呼叫橋元件
- 呼叫網橋和Webadmin的內部域名系統(DNS)記錄，可解析為CMS伺服器IP地址
- 內部憑證授權單位(CA)，以使用Web伺服器的增強型金鑰使用和Web使用者端驗證來簽署憑證
- 用於傳輸層安全(TLS)通訊的簽名證書

   附註：此部署不支援自簽名證書，因為它們需要無法新增自簽名證書的Web伺服器和Web客戶端身份驗證

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。本檔案所述內容不限於特定軟體和硬體版本，但必須滿足最低軟體版本要求。

設定

配置CMS

步驟1.建立具有應用程式介面(API)許可權的管理員使用者帳戶。

- 開啟與主機板管理處理器(MMP)的安全殼層(SSH)作業階段
- 要新增管理員級別使用者帳戶,請運行命令**user add <username> <role>**
- 輸入密碼,如下圖所示。

```
cb1> user add apiadmin admin
Please enter new password:
Please enter new password again:
Success
```

步驟2.產生憑證。

- 運行命令**pki csr <file name> CN:<common name> subjectAltName:<subject alternative names>**
- 根據您的要求使用資訊

檔案名稱	certall
CN	tptac9.com
subjectAltName	cmsadhoc.tptac9.com,10.106.81.32

- 請勿使用萬用字元生成證書。CUCM不支援具有萬用字元的證書
- 確保使用增強型金鑰使用Web伺服器和Web客戶端身份驗證對證書進行簽名

附註:若要對所有服務使用相同的證書,公用名(CN)必須是域名,並且其他CMS服務的名稱必須包括為使用者替代名稱(SAN)。 在這種情況下,該IP地址也由證書簽名,並且由安裝了根證書的任何電腦信任。

配置CUCM

步驟1.將證書上傳到CUCM受信任儲存。

- 根證書可以從內部證書頒發機構Web介面下載

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

```
Current [tptac9-WIN-TI6UAFTSEEV-CA-1]
```

Encoding method:

○ DER
◉ Base 64

Install CA certificate
Download CA certificate

- 將呼叫網橋證書和捆綁證書（中間證書和根證書）新增到CallManager信任儲存中

Upload Certificate/Certificate chain

Upload   Close

Status

ⓘ Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose*	CallManager-trust ▼
Description(friendly name)	
Upload File	Choose File CA-cert.cer

Upload   Close

Upload   Close

Status

ⓘ Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose*	CallManager-trust ▼
Description(friendly name)	
Upload File	Choose File certall.cer

Upload   Close

如果您有用於Call Bridge和Webadmin的單獨證書，請確保上傳：

- CUCM上Call Manager信任儲存的Web管理、呼叫網橋和根證書

附註：可以將CUCM SIP中繼建立為非安全SIP中繼，在這種情況下，不需要將呼叫網橋證書上傳到CallManager-trust儲存，但需要將簽署Webadmin證書的根證書上傳到CallManager-trust儲存。

步驟2.配置安全SIP中繼配置檔案。

- 開啟CUCM Web介面
- 導覽至System > Security > SIP Trunk Security Profile
- 選擇Add New
- 輸入包含正確資訊的值

名稱　　　　　　　輸入名稱，例如CMS-Trunk-32
裝置安全模式　　選擇已加密
傳入傳輸型別　　選擇TLS
傳出傳輸型別　　選擇TLS
X.509使用者名稱 輸入呼叫網橋證書的CN，使用逗號分隔名稱
傳入連線埠　　　輸入接收TLS請求的埠。預設值為5061

- 選擇**儲存**

SIP Trunk Security Profile Information

Name*	CMS-Trunk-32
Description	10.106.81.32
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
☐ Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	cmsadhoc.tptac9.com,tptac9.com,10.106.81.32
Incoming Port*	5061

步驟3.建立SIP中繼

- 導覽至Device >Trunk
- 選擇Add New
- 選擇SIP Trunk作為中**繼型別**
- 選擇下**一步**
- 輸入適用的值

裝置名稱　　　　　　輸入SIP中繼的名稱，例如**CMS-Abhishek-32**
目的地位址　　　　　輸入CMS IP地址或呼叫網橋FQDN，例如**10.106.81.32**
目的地連線埠　　　　輸入CMS監聽TLS通訊的埠，例如**5061**
SIP中繼安全配置檔案 選擇在步驟2中建立的安全配置檔案CMS-Trunk-32
SIP配置檔案　　　　　選擇Standard SIP Profile for TelePresence Conferencing

步驟4.建立會議橋

- 導覽至Media Resources > Conference Bridge
- 選擇「Add New」
- 從Conference Bridge下拉選單中選擇Cisco TelePresence Conductor

附註：從CUCM版本11.5.1 SU3開始，可以在下拉選單中選擇Cisco Meeting Server 選項作為 Conference Bridge Type

- 輸入正確的資訊

會議橋名稱	輸入此裝置的名稱，例如CMS-Adhoc-32
說明	輸入此會議網橋的說明，例如10.106.81.32
SIP中繼	選擇在步驟3中建立的SIP中繼CMS-Abhishek-32
將SIP中繼目標覆蓋為HTTP地址	如果需要其他名稱，請選中此框
主機名/IP地址	輸入CMS的主機名或IP地址，例如10.106.81.32
使用者名稱	輸入使用API許可權在CMS中建立的使用者，例如admin
密碼	輸入API使用者的密碼
確認密碼	再次輸入密碼
使用HTTPS	覈取方塊，這是CMS連線所必需的
HTTP埠	輸入CMS webadmin埠，例如443

HTTP Interface Info

☑ Override SIP Trunk Destination as HTTP Address

Hostname/IP Address

1 `10.106.81.32` ➕

Username* `admin`

Password* `●●●●●●●●●●●●●●●●●●●●●●●●●`

Confirm Password* `●●●●●●●●●●●●●●●●●●●●●●●●●`

☑ Use HTTPS

HTTP Port* `443`

- 選擇**儲存**

  附註：**主機名（CMS的FQDN）和/或IP地址**欄位必須包含在Webadmin證書中、**Common Name**或**Subject Alternative Name**欄位中，才能允許安全連線

- 建立Conference Bridge後，開啟**Cisco Unified Serviceability** 部分
- 導覽至**Tools > Control Center - Feature Services**
- 從下拉選單中，選擇CUCM發佈器節點
- 選擇**Go**
- 選擇**Cisco CallManager服務**
- 選擇**Restart**

  注意：重新啟動CallManager服務後，連線的呼叫將保留，但某些功能在此重新啟動過程中不可用。無法進行新呼叫。服務重新啟動大約需要5到10分鐘，具體取決於CUCM工作負載。請謹慎執行此操作，並確保在維護時段執行此操作。

步驟5. CMS網橋已成功註冊到CUCM

- 轉至**Media Resources > Media Resource Group**
- 按一下**Add New**以建立新的介質資源組並輸入名稱
- 將會議網橋(cms)從**Available Media Resources**（可用媒體資源）框移至**Selected Media Resources**（選定媒體資源）框
- 按一下「**Save**」

步驟6.將媒體資源組(MRG)新增到媒體資源組清單(MRGL)

- 轉到**媒體資源 > 媒體資源組清單**
- 按一下**Add New**以建立新的媒體資源組清單並輸入名稱,或選擇現有MRGL並按一下進行編輯。
- 將一個或多個從「可用介質資源組」框建立**的介質資源組移**到「選定的**介質資源組」**中
- 按一下「**Save」**

第7步：將MRGL新增到裝置池或裝置

根據實施情況，可以配置裝置池並將其應用於終端，也可以將單個裝置（終端）分配給特定MRGL。**如果MRGL同時應用於裝置池和終結點，則終結點設定將優先。**

- 轉至System > Device Pool
- 建立新裝置池或使用現有裝置池。按一下「Add New」

Device Pool Configuration

💾 Save

ℹ️ Status: Ready

Device Pool Information

Device Pool: New

Device Pool Settings

Device Pool Name*	CMS-Adhoc-DevicePool
Cisco Unified Communications Manager Group*	Default
Calling Search Space for Auto-registration	< None >
Adjunct CSS	< None >
Reverted Call Focus Priority	Default
Intercompany Media Services Enrolled Group	< None >

Roaming Sensitive Settings

Date/Time Group*	CMLocal
Region*	Default
Media Resource Group List	CMS MRGL

第8步：將裝置池新增到終端並將MRGL新增到終端

- 轉到Device> Phones
- 按一下Find並選擇裝置以更改裝置池設定
- 按上述步驟應用建立的裝置池和MRGL
- **儲存、套用組態和重設**

終端將重新啟動並註冊

Phone Configuration

💾 Save ❌ Delete 📋 Copy 🔄 Reset ✏️ Apply Config ➕ Add New

Modify Button Items
1 ☎ Line [1] - 6000 (no partition)
--------- Unassigned Associated Items ---------
2 ☎ Line [2] - Add a new DN

Product Type: **Cisco Spark Room Kit**
Device Protocol: SIP

Real-time Device Status

Registration: Registered with Cisco Unified Communications Manager 10.104.215.207
IPv4 Address: 10.104.130.54
Active Load ID: ce-9.3.1-61bfa3834f2-2018-05-04
Inactive Load ID: None
Download Status: None

Device Information

✅ Device is Active
✅ Device is trusted

MAC Address*	0896AD2D9DB2	
Description	SPARK KiT	
Device Pool*	CMS-Adhoc-DevicePool	View Details
Common Device Configuration	< None >	View Details
Phone Button Template*	Standard Cisco Spark Room Kit	
Common Phone Profile*	Standard Common Phone Profile	View Details
Calling Search Space	< None >	
AAR Calling Search Space	< None >	
Media Resource Group List	CMS MRGL	

第9步：終端上的配置

- 登錄**終端的**web-gui
- 轉至Setup > Configuration > Conference > Multipoint Mode
- 選擇CUCMediaResourceGroupList

Multipoint Mode   CUCMMediaResourceGroupList ⇕

驗證

使用本節內容，確認您的組態是否正常運作。

- 開啟CUCM Web介面
- 導航到**Device > Trunks**
- 選擇指向CMS的SIP中繼
- 確保中繼處於**Full Service狀**態
- 導覽至**Media Resource > Conference Bridge**
- 選擇CMS會議網橋
- 確保已向CUCM註冊

進行臨時呼叫

- 從註冊到CUCM的EndpointA呼叫（新增MRGL）到另一個EndpointB
- 在EndpointA上，按一下**Add，**撥打EndpointC
- EndpointA將處於保留狀態
- 按一下**合併**
- 驗證呼叫是否已在CMS中連線
- 開啟CMS Web介面
- 導覽至**Status > Calls**

為了進行測試，將3個終端用於臨時音訊/視訊會議

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。