從 Cisco Meeting Server 2.9 升級至 3.0（及更新版本）的順利升級指南

目錄

簡介

本文檔介紹將運行版本2.9（或更低版本）的思科會議伺服器部署升級到3.0（或更高版本）所面臨的挑戰，以及如何處理這些挑戰以實現平穩升級過程。

刪除的功能：刪除了XMPP（影響WebRTC）、中繼/負載均衡器、網橋

功能已更改：記錄器和流處理器現在是SIP，Webbridge由webbridge3取代

本文僅涵蓋升級前需要考慮的主題。它不包括3.X中的所有新功能。

必要條件

需求

思科建議您瞭解以下主題：

- CMS管理
- CMS升級
- 證書建立和簽名

這裡提到的一切都在各種檔案中作了概述。 如果您需要進一步闡明功能，建議您閱讀產品發行說明，並參閱我們的程式設計指南和部署指南：CMS安裝及設定指南和CMS產品發行說明。

採用元件

本檔案中的資訊是根據思科會議伺服器。

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。

背景資訊

本文檔旨在指導您已經部署了CMS 2.9.x（或更低版本），無論是否單獨組合部署，或是否具有恢復能力，以及您計畫升級到CMS 3.0的時間。 本文檔中的資訊涉及所有CMS型號。

註意：X系列無法升級到CMS 3.0。您需要計畫儘快更換X系列伺服器。

有關升級的重要資訊

唯一支援的CMS升級方法是步進式升級。 在撰寫本文時，CMS 3.5已發佈。 如果您在CMS 2.9上，您必須以階梯式方式升級(2.9 —> 3.0 —> 3.1 —> 3.2 —> 3.3 —> 3.4 —> 3.5(注意：自CMS 3.5起，升級過程已發生更改，因此請仔細閱讀發行說明!!)

如果不執行逐步升級，並且遇到異常行為，TAC可能會請求降級並重新開始。

此外，從CMS 3.4開始，CMS必須使用智慧許可。 您不能升級到CMS 3.4或更高版本，但仍使用傳統許可證。 除非您已設定智慧許可，否則請勿升級到CMS 3.4或更高版本。

要考慮的事項摘要

使用這些問題可以導航到與您自己的情況有關的部分。 每個考慮事項都指一個超連結，指向本文檔中提供的更詳細的說明。

授權

升級之前，您的伺服器上是否有足夠的個人多方(PMP)/共用多方(SMP)許可證？

在3.0中，即使使用者未登入，也會分配PMP許可證。例如，如果您已通過LDAP匯入了10000個使用者，但您只有100個PMP許可證，則一旦升級到3.0，就會使您不符合要求。 對於此使用案例，請確保確實檢查設定了使用者配置檔案和/或系統/配置檔案的租戶，以檢視是否設定了值為true的hasLicense的userProfile。

如何檢查API上的userProfile並檢視您是否設定了haveLicense=true（即PMP許可使用者），將在本節中詳細介紹介紹。

您當前的cms.lic檔案中是否有PMP/SMP許可證？

由於許可證行為在3.0之後發生更改，必須在執行升級之前確認是否具有足夠的PMP/SMP許可證。本節將對此進行更詳細描述。

您是否部署了思科會議管理器(CMM)?

由於處理許可證的方式發生變化，CMS 3.0需要CMM 3.0。建議在環境升級到3.0之前部署CMM 2.9，因為您可以檢視90天報告，瞭解過去90天的許可證使用情況。本節將對此進行更詳細描述。

您是否有智慧許可？

由於處理許可證的方式發生變化，CMS 3.0需要CMM 3.0。因此，如果您已經通過CMM使用智慧許可，請確保您擁有與群集關聯的PMP和SMP許可證。

Webbridge（WebRTC和CMA客戶端）

是否在CMS 2.9中使用WebRTC?

Webbridge在CMS 3.0中發生了重大變化。 有關從webbridge2遷移到webbridge3以及使用web app的指導，請參閱本部分。

您的使用者是否使用CMA胖客戶端？

由於這些客戶端基於XMPP，因此升級後無法再使用這些客戶端，因為XMPP伺服器已被刪除。如果這適用於您的使用情形，您可以在本節中查詢更多資訊。

是否在WebRTC中使用聊天？

在3.0中，會從Web應用中刪除聊天功能。在CMS 3.2中，聊天功能被重新引入，但它不是持久的。 您可以在本節中找到有關此功能的更多資訊。

您的使用者是否執行從WebRTC到裝置的點對點呼叫？

在CMS 3.0中，Web應用使用者不能再直接撥號到其他裝置。現在，您必須加入會議空間，並且擁

有向會議新增參與者的許可權，以便執行相同的操作。 您可以在此部分找到此部件的更多資訊。

您的使用者是否從WebRTC建立自己的coSpaces?

在3.0中，為了使Web應用使用者能夠從客戶端建立自己的空間，需要在API中建立coSpaceTemplate並將其分配給使用者。在LDAP匯入期間，可以手動或自動執行此操作。CanCreateCoSpaces已從UserProfile中刪除。 您可以在本節中找到有關此功能的更多資訊。

Web GUI更改

您是否在Web管理GUI中配置了WebBridge設定？

3.0版中的WebBridge設定將從GUI中刪除，因此您必須在API中配置WebBridge並注意GUI中的當前設定，以便相應地在API中配置WebBridgeProfiles。 您可以在此部分找到有關此變更的更多資訊。

您在Web管理GUI中是否配置了「外部設定」？

CMS 3.1中的外部設定已從GUI中刪除。 如果您在CMS 3.0或更早版本的Web管理GUI（配置 — >常規 — >外部設定）中配置了Webbridge URL或IVR，則這些設定已從網頁中刪除，現在需要在API中進行配置。升級到3.1之前的設定不會新增到API中，必須手動完成。 您可以在此部分找到有關此變更的更多資訊。

記錄器/串流器

您當前是否使用任何CMS錄製器和/或流處理器？

CMS記錄器和流處理器元件現在基於SIP而不是基於XMPP。因此，在刪除XMPP時，需要在升級後對其進行調整。您可以在此部分找到有關此變更的更多資訊。

Cisco Expressway注意事項

如果使用Expressway代理WebRTC，您當前的Cisco Expressway版本是什麼？

CMS 3.0需要Expressway 12.6或更高版本。 您可以在本節找到有關此WebRTC代理功能的更多資訊。

CMS邊緣

您的環境中當前是否有CMS邊緣？

CMS Edge在CMS 3.1上重新引入，具有更高的外部連線可擴充性。 您可以在此部分找到此部件的更多資訊。

CMS(Acano)X系列

您的環境中當前是否有x系列伺服器？

這些伺服器無法升級到CMS 3.0，您必須考慮儘快更換這些伺服器（在升級到3.0之前，請移至虛擬機器或CMS裝置）。您可以在此連結中找到有關這些伺服器的生命終止通知。

SIP邊緣

您當前是否在您的環境中使用SIP Edge?

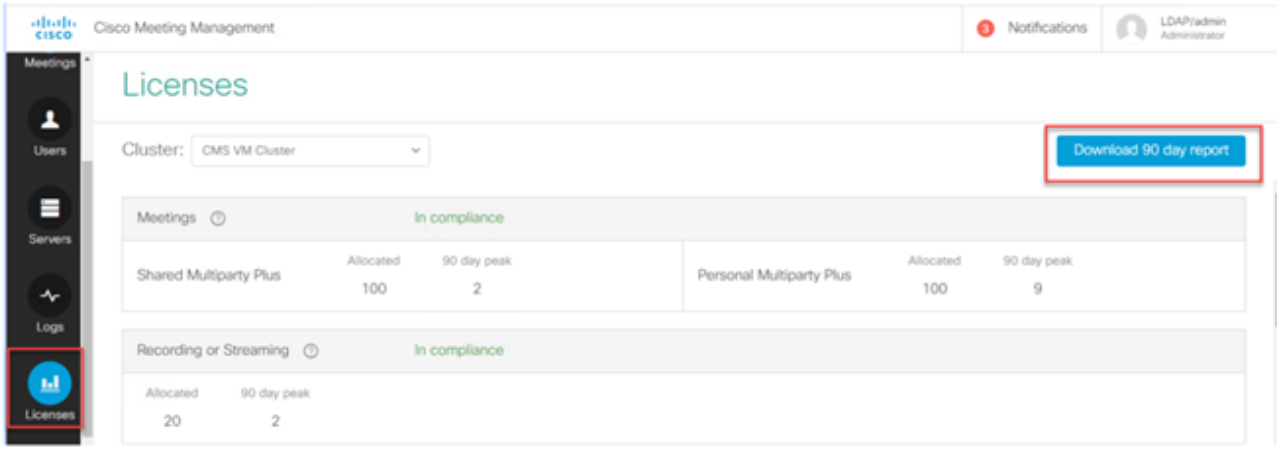
Sip Edge自CMS 3.0起已完全棄用。 您需要使用Cisco Expressway將SIP呼叫引入您的CMS。請與您的思科客戶代表聯絡，瞭解如何為您的組織獲取Expressway。

更多資訊

許可 — 升級前檢查許可證

從2.x版本升級到3.0或更高版本時，許可證狀態不合規，是最嚴重的問題。本節介紹如何確定平穩升級所需的PMP/SMP許可證數量。

將部署升級到3.0之前，部署CMM 2.9並檢查Licenses 頁籤下的90天報告，以檢視CMS節點上的許可證使用量是否保持在您當前分配的許可證數量下：

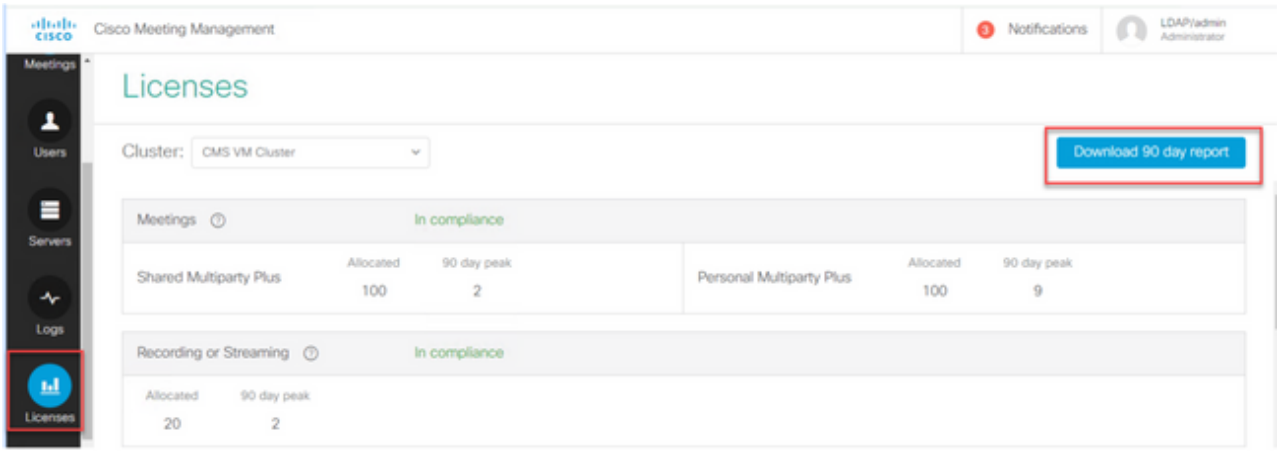


如果您使用Traditional licensing（cms.lic檔案安裝在CMS節點本地），請檢查CMS許可證檔案以查詢每個CMS節點上的個人和共用許可證數量（100/100，如下圖所示）（從每個callBridge節點通過WinSCP下載）。

```
    ],
    "issued_to": "Darren McKinnon - TAC",
    "notes": "Darren McKinnon - TAC",
    "features":
    {
        "callbridge":
        {
            "expiry": "2100-Jan-03"
        },
        "webbridge3":
        {
            "expiry": "2100-Jan-03"
        },
        "customizations":
        {
            "expiry": "2100-Jan-03"
        },
        "recording":
        {
            "expiry": "2100-Jan-03",
            "limit": "10"
        },
        "personal":
        {
            "expiry": "2100-Jan-03",
            "limit": "100"
        },
        "shared":
        {
            "expiry": "2100-Jan-03",
            "limit": "100"
        },
        "streaming":
        {
            "expiry": "2100-Jan-03",
```


如果您已經使用智慧許可，請檢查在思科軟體智慧門戶中為CMS伺服器分配了多少個PMP/SMP許可證。

許可證相關的問題，但如果您檢查了90天峰值，發現您使用的許可證多於可用許可證，您仍然可以升級到CMS 3.0並使用CMM上的90天試用許可證來整理您的許可問題，或者在升級之前執行操作。



配置Webbridge（WebRTC和CMA客戶端）

CMS 3.0移除XMPP伺服器元件，並隨之移除WebBridge和使用CMA胖客戶端的功能。 WebBridge3現在用於使用瀏覽器將Web應用使用者（以前稱為WebRTC使用者）連線到會議。 升級到3.0時，需要配置webbridge3。

注意：升級到CMS 3.0後，CMA胖客戶端無法正常工作！

此影片確實會引導您完成有關如何建立webbridge 3證書的過程。

https://video.cisco.com/detail/video/6232772471001?autoStart=true&q=cms

升級到3.0之前，客戶必須計畫如何配置Webbridge3。此處著重說明了最重要的步驟。

1.您確實需要webbridge3的金鑰和證書鏈。 如果證書包含運行webbridge3的所有CMS伺服器FQDN或IP地址作為主體替代名稱(SAN)/公用名稱(CN)，並且滿足以下任一條件，則可以使用舊的webbridge證書：

a.證書沒有增強型金鑰用法（意味著它可以用作客戶端或伺服器）。

b.證書具有客戶端身份驗證和伺服器身份驗證。 HTTPs證書實際上只需要伺服器身份驗證，而C2W證書需要伺服器和客戶端)。

2. 如果要為「webbridge3 https」證書建立新證書，建議對其進行公開簽名（以避免在使用Web應用時在客戶端上出現證書警告）。 此證書可用於「webbridge3 c2w證書」，並且證書必須具有SAN/CN中Webbridge伺服器的FQDN。

3. CallBridge需要使用在webbridge3 c2w listen命令中配置的埠與新webbridge3通信。這可以是任何可用的埠，如449。使用者需要確保呼叫網橋可以與此埠上的webbridge3通訊，並在必要時提前進行任何防火牆更改。 不能是「webbridge https」用於偵聽的相同埠。

在CMS升級到3.0之前，建議使用「backup snapshot <servername_date>」進行備份，然後登入callbridge節點上的webadmin頁面，以刪除所有XMPP設定和Webbridge設定。 然後連線到伺服器

上的MMP，並在所有通過SSH連線具有xmpp和webbridge的核心伺服器上執行以下步驟：

1. xmpp disable
2. xmpp reset
3. xmpp certs none
4. xmpp域無
5. webbridge disable
6. webbridge listen none
7. webbridge certs none
8. webbridge trust none

升級到3.0後，首先在以前運行webbridge的所有伺服器上配置webbridge3。 您必須這樣做，因為目前已經存在指向這些伺服器的DNS記錄，因此，通過這種方式，您可以確保如果使用者被傳送到webbridge3，它將準備處理請求。

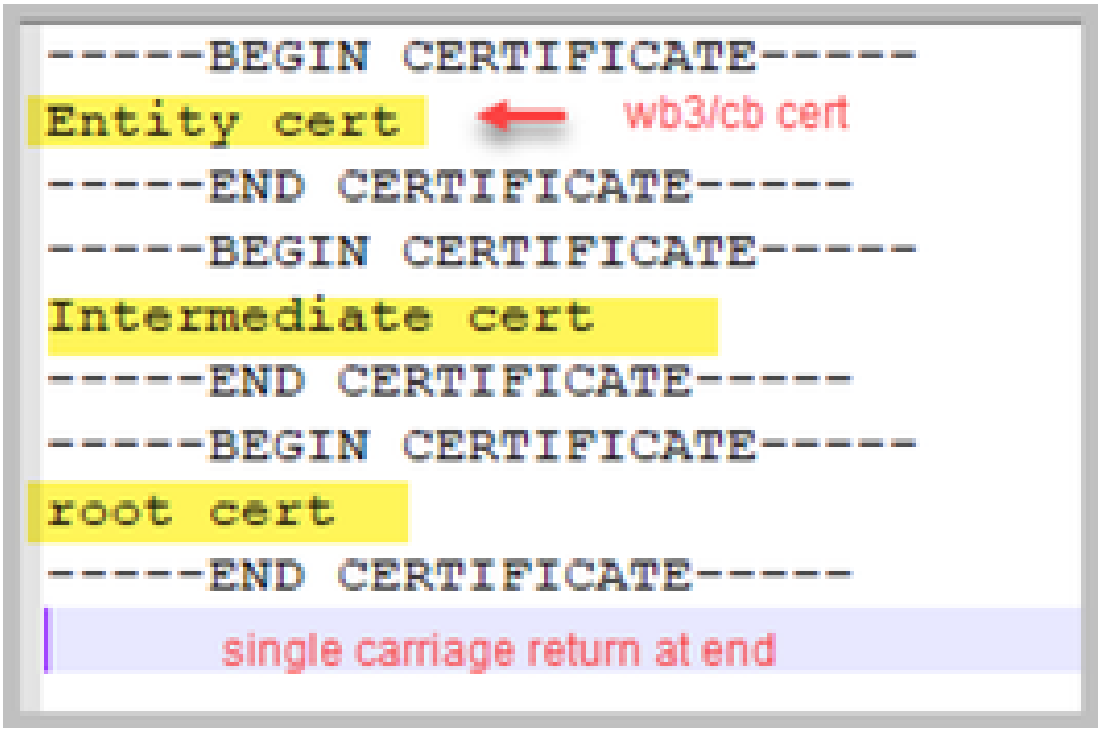
Webbridge3配置（全部通過SSH連線）

步驟 1.配置webbridge3 http偵聽埠。

Webbridge3 https偵聽a:443

步驟 2.為瀏覽器連線的webbridge3配置證書。 這是傳送給瀏覽器的證書，需要由公共證書頒發機構(CA)簽名並包含瀏覽器中用於瀏覽器信任連線的FQDN。

Webbridge3 https certs wb3.key wb3trust.cer（這必須是信任鏈：製作一個在頂部具有終端實體的信任證書，然後按順序排列中繼CA，最後使用RootCA）。



步驟 3.配置用於監聽callBridge與webbridge(c2w)連線的埠。 由於443用於webbridge3 https偵聽埠，因此此配置必須是不同的可用埠，例如449。

Webbridge3 c2w listen a:449

4.配置webbridge傳送到callbridge的c2w信任證書

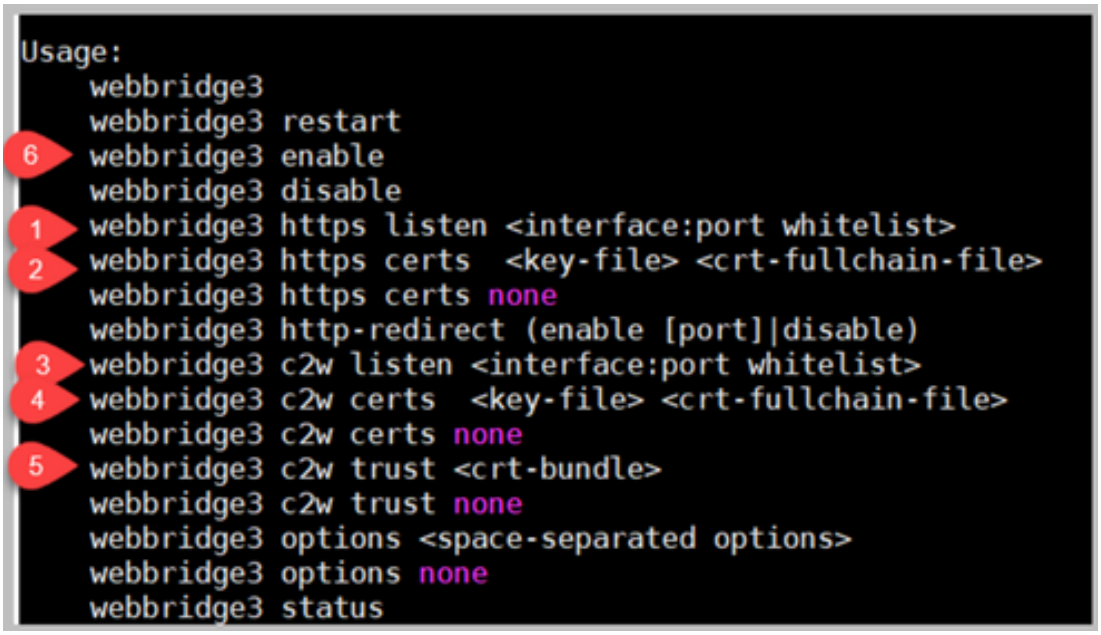
Webbridge3 c2w certs wb3.key wb3trust.cer

5.配置WB3用於信任callBridge證書的信任儲存。 這必須與callbridge CA捆綁包中使用的證書相同（並且必須是頂部中間證書的捆綁包，結尾為根CA，後跟一個回車位）。

Webbridge3 c2w信任rootca.cer

6.啟用webbridge3

Webbridge3 enable



CallBridge配置更改（全部通過SSH連線）

步驟 1.使用簽署webbridge3 c2w證書的CA證書/捆綁配置callBridge信任。

Callbridge trust c2w rootca.cer

步驟 2.重新啟動callBridge以使新信任生效。 這將丟棄此特定callBridge上的所有呼叫，因此請謹慎使用此選項。

Callbridge restart

用於連線WebBridge3的callBridge的API配置

1.使用API中的POST建立新的WebBridge對象，並使用WebBridge c2w介面白名單上的FQDN和埠為其賦予URL值（webbridge3配置中的步驟3）

c2w://webbridge.darmckin.local:449

此時，Webbridge3會再次運行，您可以作為訪客加入空間，或者，如果您以前匯入過使用者，他們

必須能夠登入。

Web應用使用者空間建立許可權

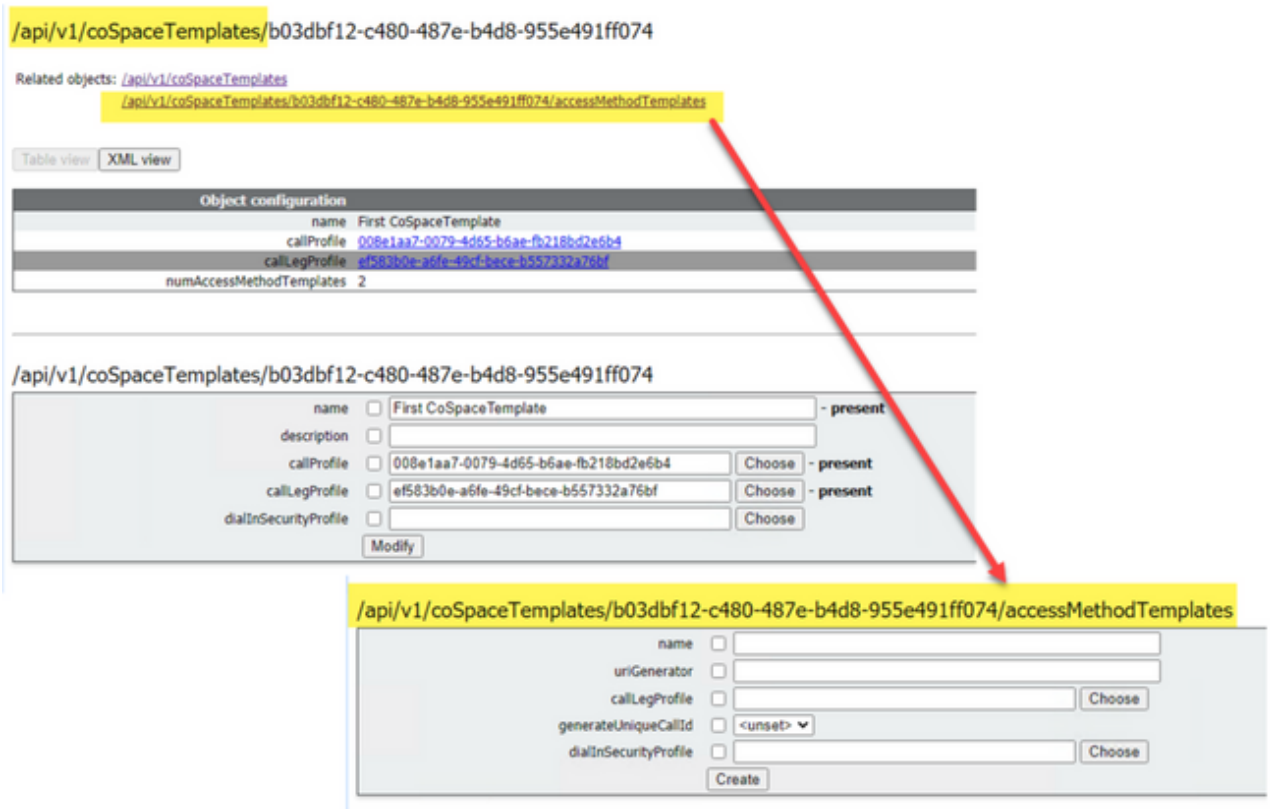
您的使用者是否習慣了在WebRTC中建立自己的空間？ 從CMS 3.0開始，Web應用使用者無法建立自己的coSpaces，除非他們分配了一個允許此操作的共用空間模板。

即使分配了coSpaceTemplate，這也不會建立其他人可以撥入的空間（無URI、無呼叫ID或密碼），但是如果coSpace具有帶「addParticipantAllowed」的callLegProfile，則他們可以從該空間撥出。

為了具有可用於呼叫新空間的撥號字串，coSpaceTemplate必須具有accessMethodTemplate設定(請參閱2.9發行說明 — https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Release_Notes/Version-2-9/Cisco-Meeting-Server-Release-Notes-2-9-6.pdf)。

在API中，建立coSpaceTemplate，然後建立accessMethodTemplate，並將coSpaceTemplate分配給ldapUserCoSpaceTemplateSources，或者您可以手動將coSpaceTemplate分配給api/v1/users中的使用者。

您可以建立和分配多個CoSpaceTemplates和accessMethodsTemplates。 有關詳細資訊，請參閱CMS API指南(https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html)



CoSpaceTemplate（API配置）

名稱：要為coSpaceTemplate指定的任何名稱。

說明：簡要說明（如果需要）。

callProfile:White callProfile您希望使用此模板建立的任何空間使用嗎？如果未提供，則使用在系統/配置檔案級別設定的內容。

calllegProfile：您希望使用此模板建立的任何空格使用哪個calllegProfile? 如果未提供，則使用在系統/配置檔案級別設定的內容。

dialInSecurityProfile：您希望使用此模板建立的任何空格使用哪個dialInSecurityProfile?如果未提供，則使用在系統/配置檔案級別設定的內容。

AccessMethodTemplate（API配置）

名稱：要為coSpaceTemplate指定的任何名稱。

uriGenerator：用於為此訪問方法模板生成URI值的表達式；允許的字符集為'a'到'z'、'A'到'Z'、'0'到'9'、'.'、'-'、'_'和'$'；如果不為空，則它必須正好包含一個'$'字元。 例如，$.space在建立空間時使用使用者提供的名稱並附加「.space」。「Team Meeting」建立url「Team.Meeting.space@domain」。

callLegProfile：您希望使用此模板建立的任何訪問方法使用哪個callegProfile? 如果未提供，則使用設定的CoSpaceTemplate級別；如果沒有提供，則使用系統/配置檔案級別上的內容。

generateUniqueCallId：是否為此訪問方法生成唯一數字ID，該訪問方法將覆蓋cospace的全域性數字ID。

dialInSecurityProfile：您希望使用此模板建立的任何訪問方法使用哪個dialInSecurityProfile?如果未提供，則使用設定的CoSpaceTemplate級別；如果沒有提供，則使用系統/配置檔案級別上的內容。

聊天功能

CMS 3.0刪除了持續聊天功能，但在CMS 3.2中返回了空間內的非持續聊天。 Web應用使用者可以使用「聊天」，但不會儲存在任何地方。 安裝CMS 3.2後，預設情況下，Web應用使用者能夠在會議期間相互傳送消息。 這些報文僅在會議期間可用，並且只能檢視加入後交換的報文。您不能延遲加入並回滾以檢視以前的消息。

WebRTC點對點呼叫

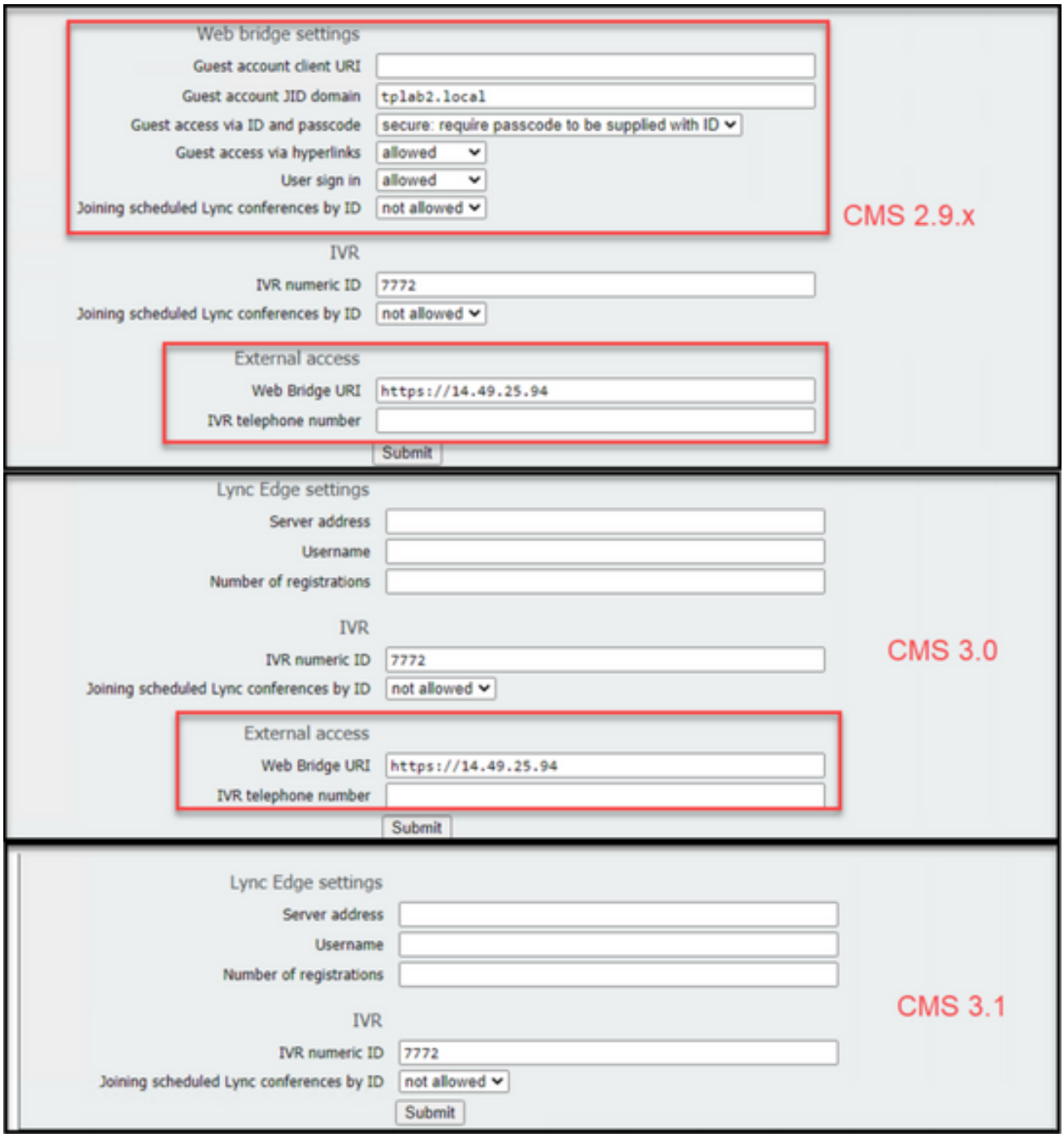
在CMS 2.9.x上，WebRTC參與者可以從其客戶端直接撥號到其他聯絡人。 從CMS 3.0開始，這不再可能。現在，使用者必須登入並加入空間。從這裡開始，如果他們對callLegProfile(將addParticipants引數設定為True)擁有許可權，則他們能夠新增其他聯絡人。 這會使CMS向參與者撥號，然後參與者在CMS的空間上會面。

顯著的WebBridge設定更改

CMS 3.0和3.1已從GUI中刪除或重新定位了某些Webbridge設定，並且需要在API中配置這些設定來保持使用者的一致體驗。 在3.x上，使用api/v1/webBridge和api/v1/webBridgeProfiles。

檢查您當前配置的內容，這樣在升級到3.0時，您可以相應地在API中配置Webbridge和

Webbridge配置檔案。

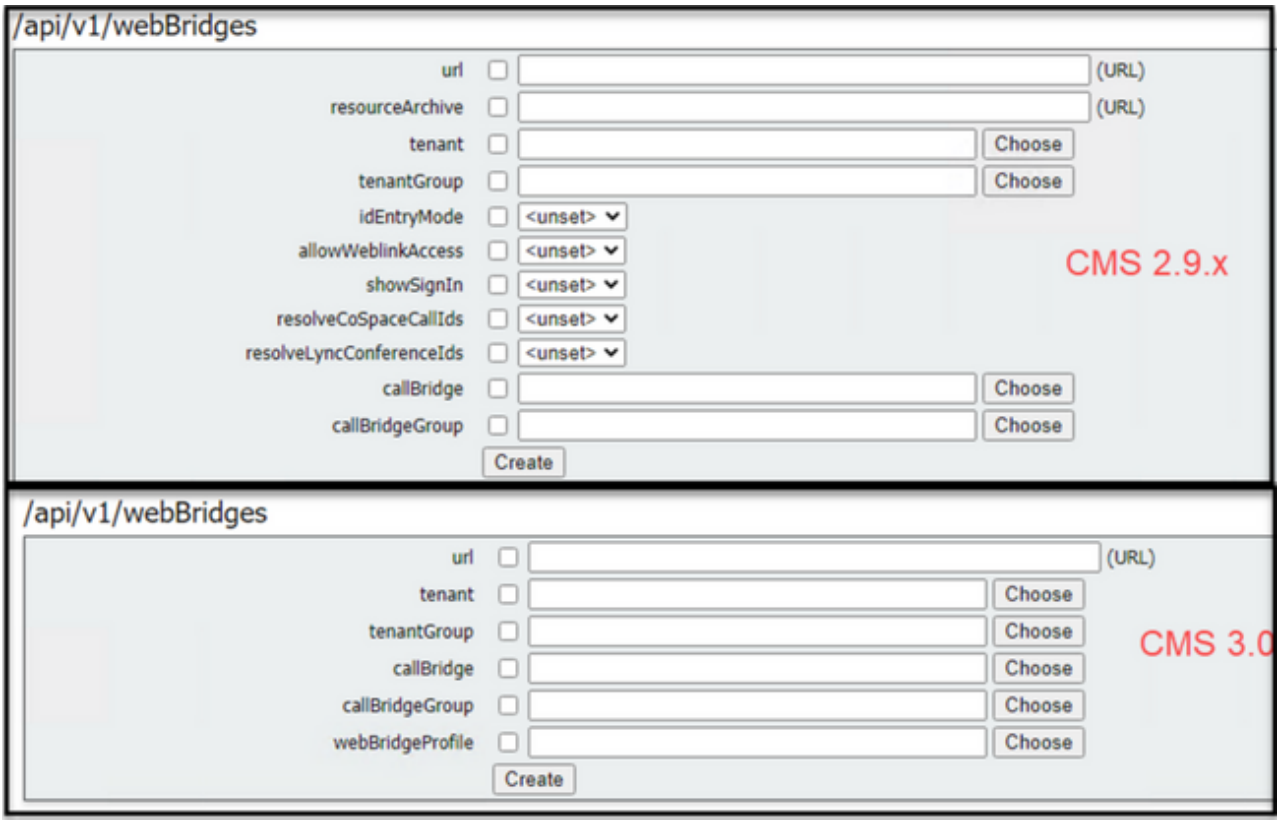


在3.0中，在GUI上刪除了Web橋接器設定，然後在CMS 3.1中，External access欄位也被刪除。

GUI中的Web網橋設定

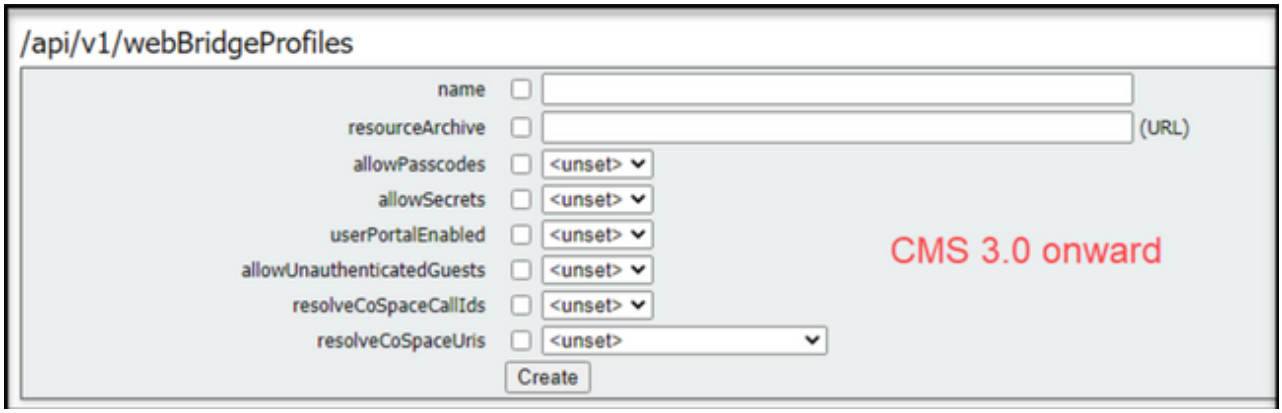
- 訪客帳戶客戶端URI - callBridge已使用此項來查詢webBridge。 如果您為WebRTC部署了多個WebBridge，則此欄位必須已經為空，並且對於callBridge需要連線的每個WebBridge，您必須在api/v1/webbridge中具有唯一的URL。 刪除此欄位中的任何內容，並確保已在API中配置WebBridge。

- Guest Account Jid Domain — 這在CMS 3.0中不再使用，您可以刪除它。
- 訪客通過ID和密碼訪問 — 已在CMS 3.0中刪除且未替換。
- 通過超級連結訪客訪問 — 現在可在API中的webBridgeProfiles下設定「AllowSecrets」。



注意，在CMS 3.0中，已從api/v1/webBridge中刪除了多個欄位。

- resourceArchive — 現在位於webbridgeProfiles中。
- idEntryMode — 現在已棄用。
- allowWeblinkAccess — 現在在webBridgeProfiles中作為allowSecrets。
- showSignin — 現在以userPortalEnabled身份出現在webBridgeProfiles中。
- resolveCoSpaceCallIds-現在位於webbridgeProfiles中。
- resolveLyncConferenceIDs — 現在位於webbridgeProfiles中。



WebBridgeProfile

- resourceArchive — 如果您使用自定義背景並且您的資源存檔儲存在Web伺服器上，請在此處輸入URL。
- allowPasscodes — 如果為false，則使用者無權選擇作為來賓加入會議。 他們只能登入或使用包含空間資訊和金鑰的URL
- allowSecrets — 如果設定為false，則使用者無法使用URL(如

https://meet.company.com/meeting/040478?secret=gPDnucF8is4W1cS87_I.zw)加入空格。使用者需要使用https://meet.company.com，並輸入呼叫ID/會議ID/URI和PIN/密碼（如果已配置）。

- userPortalEnabled — 如果設定為false，則web應用門戶登入頁面不顯示登入選項。它只顯示用於輸入呼叫ID/會議ID/URI和PIN/密碼的欄位（如果已配置）。
- allowUnauthenticatedGuests — 如果設定為False，則訪客無法加入任何會議 — 即使包含會議ID和機密的完整URL也是如此。 如果為False，則只有可以登入的使用者才能加入會議。範例. 使用者2正在嘗試使用User1會議的URL。 輸入URL後，User2必須登入才能繼續參加User1的會議。
- resolveCoSpaceCallIds — 如果設定為False，則訪客只能通過輸入URI和PIN/密碼（如果使用）來加入會議。 不接受呼叫ID/會議ID/數字ID。
- resolveCoSpaceUri - 3個可能的設定：off、domainSuggestionDisabled和domainSuggestionEnabled。此webBridge是否接受coSpace和coSpace訪問方法SIP URI，以便允許訪問者加入共用空間會議。

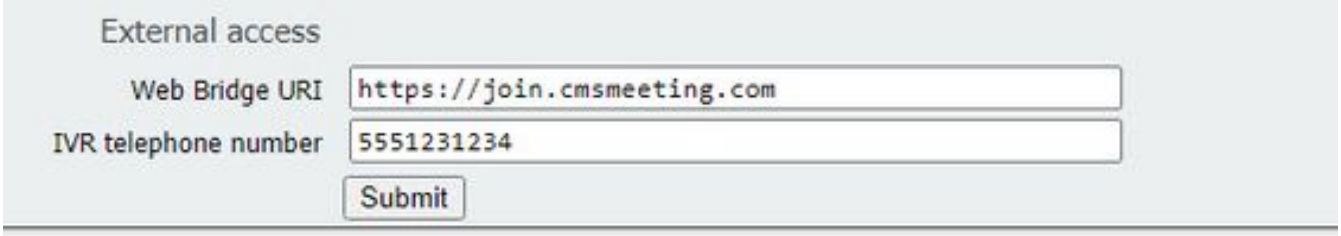
— 當設定為「off」時，URI的聯接被禁用。

— 如果設定為「domainSuggestionDisabled」，則啟用通過URI加入，但該URI的域未自動完成或在使用此webBridgeProfile的webBridge上驗證。

— 如果設定為「domainSuggestionEnabled」，則啟用URI加入，並且可以使用此webBridgeProfile在webBridge上自動完成並驗證URI的域。

從Web GUI中刪除的外部訪問部分

在CMS 3.1中，已從Web GUI中刪除外部訪問部分。如果在升級之前配置了這些部分，則您需要在API的webbridgeProfiles下重新配置它們。



首先，您需要建立上一節中介紹的webbridgeProfile。一旦建立了webbridgeProfile，就可以通過新建立的webBridgeProfile下的API中的可用連結建立IVR號碼和/或Web Bridge URI。

每個webBridgeProfile最多可建立32個IVR號碼或32個webbridgeAddresses

錄製或串流

CMS 2.9.x及更早版本上的記錄器和串流器元件是XMPP客戶端，而從CMS 3.0開始，它們都是基於SIP的。 現在，這允許使用API中的預設佈局更改錄製和流式處理的佈局。此外，現在名稱標籤顯示在錄製/流式處理會話中。 請參閱CMS 3.0版本說明，瞭解有關錄製器/流功能的詳細資訊 — https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Release_Notes/Version-3-0/Cisco-Meeting-Server-Release-Notes-3-0.pdf。

如果您在2.9.x中配置了錄製器或串流器，則需要重新配置MMP和API中的設定，以便在升級後繼續使用這些設定。

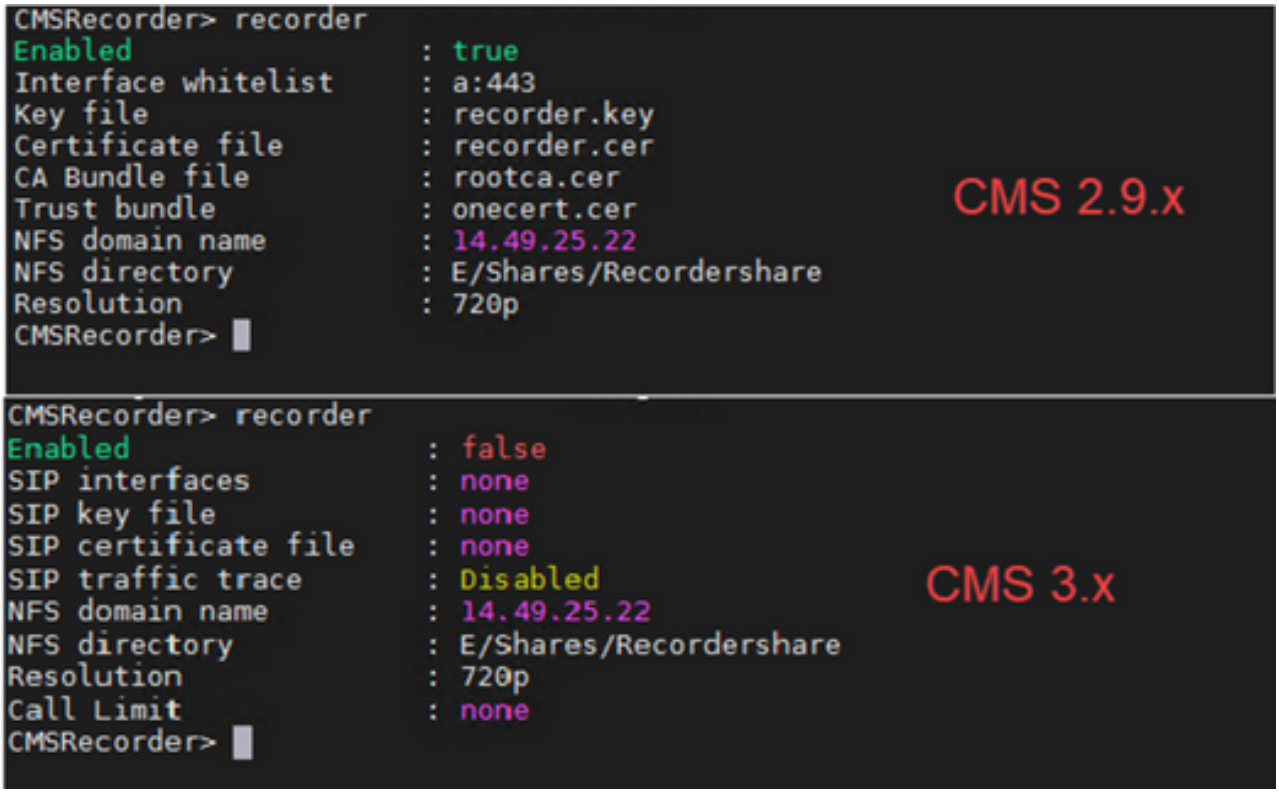
在CMS升級到3.0之前，建議使用「backup snapshot <servername_date>」進行備份，然後登入callbridge節點上的webadmin頁面以刪除所有XMPP設定。 然後連線到伺服器上的MMP，並在所有通過SSH連線具有xmpp的核心伺服器上執行以下步驟：

1. xmpp disable
2. xmpp reset
3. xmpp certs none
4. xmpp域無

記錄器

MMP

圖中顯示了配置記錄器時在CMS 2.9.1上看到的配置示例，以及升級到3.0後其立即顯示的樣子。



升級後，您必須重新設定錄製器：

步驟 1.配置SIP偵聽介面。

記錄器sip偵聽5060 5061(SIP記錄器設定為分別偵聽TCP和TLS的介面和埠)。如果您不想使用TLS，可以使用「錄製器sip listen a 5060 none」)

步驟 2.配置錄製器使用的證書（如果您使用的是TLS連線）。

recorder sip certs <key-file> <crt-file> [crt-bundle](如果沒有這些證書，tls服務不會在錄製器上啟動。錄製器使用crt捆綁包驗證callBridge證書。)

步驟 3.配置呼叫限制。

recorder limit <0-500|none>(設定伺服器可同時提供的記錄數限制。此表位於我們的文檔中，記錄器的限制必須與伺服器上的資源一致。)

Table 6: Internal SIP recorder performance and resource usage

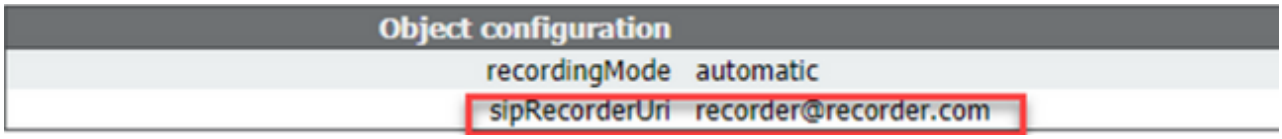
Recording Setting	Recordings per vCPU	RAM required per recording	Disk budget per hour	Maximum concurrent recording
720p	2	0.5GB	1GB	40
1080p	1	1GB	2GB	20
audio	16	100MB	150MB	100

Key point to note (applies to new internal recorder component only):

- Performance scales linearly adding vCPUs up to the number of host physical cores.

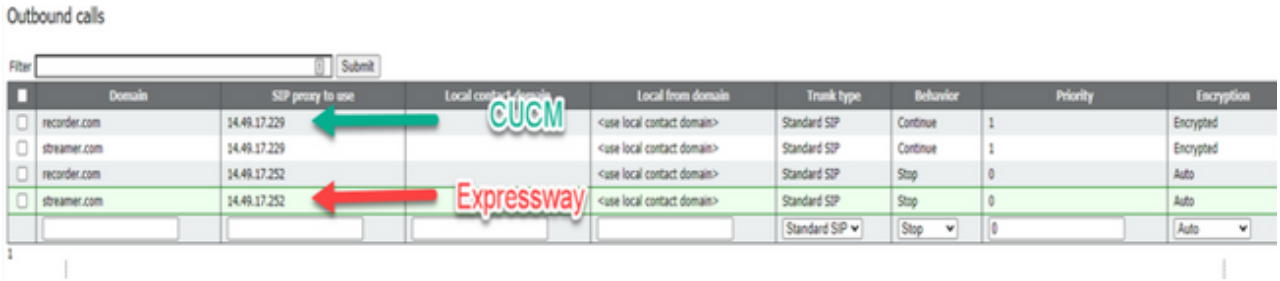
API

在api/v1/callProfiles上，您需要配置sipRecorderUri。這是callBridge在必須開始錄製時撥打的URI。此URI的域需要新增到出站規則表，並指向錄製器（或呼叫控制）作為要使用的SIP代理。



下圖顯示直接撥號到Configuration > Outbound Calls中找到的出站規則上的記錄器元件。

下圖顯示通過呼叫控制(例如Cisco Unified Communications Manager(CUCM)或Expressway)對記錄器元件的呼叫。



注意：如果將錄製器配置為使用SIP TLS，並且呼叫失敗，請檢查MMP中的callBridge節點，以檢視是否啟用了TLS SIP驗證。 MMP命令是「tls sip」。 呼叫可能失敗，因為callBridge不信任記錄器證書。 您可以通過使用「tls sip verify disable」在callBridge上禁用此選項來測試此功能。

多個記錄器？

按照說明配置每個規則，並相應地調整出站規則。 如果您使用直接到記錄器方法，請將現有的出站到記錄器規則更改為行為「繼續」，並在前一個出站規則下新增新的出站規則，該規則的優先順序比第一個出站規則低。 當第一個記錄器達到其呼叫限制時，它會將488 Unreceptable發回到callBridge，並且callBridge會移動到下一個規則。

如果要對記錄器進行負載平衡，請使用呼叫控制並調整呼叫控制路由，以便它能夠呼叫多個記錄器。

串流器

MMP

從2.9.x升級到3.0後，需要重新配置流處理器。

步驟 1.配置SIP偵聽介面。

串流器sip listen a 6000 6001(SIP串流器設定為分別偵聽TCP和TLS的介面和埠)。 如果您不想使用TLS，可以使用「streamer sip listen a 6000 none」)

步驟 2.配置在使用TLS連線時串流器使用的證書。

streamer sip certs <key-file> <crt-file> [crt-bundle](如果沒有這些證書，tls服務不會在串流器上啟動。串流器使用crt套件組合來驗證callBridge證書。)

步驟 3.配置呼叫限制

streamer limit <0-500|none>(設定伺服器可同時服務的流數限制。此表格位於我們的文檔中，串流器限制必須與伺服器上的資源一致。)

Table 7: Internal SIP streamer recommended specifications

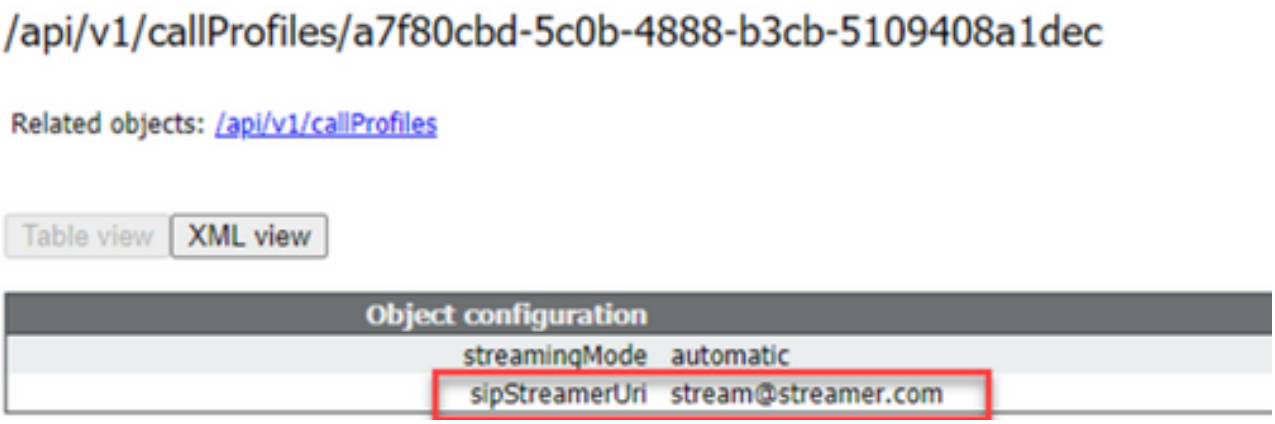
Number of vCPUs	RAM	Number of 720p streams	Number of 1080p streams	Number of audio-only streams
4	4GB	50	37	100
4	8GB	100	75	200
8	8GB	200	150	200

Key points to note (applies to both new internal recorder and streamer components):

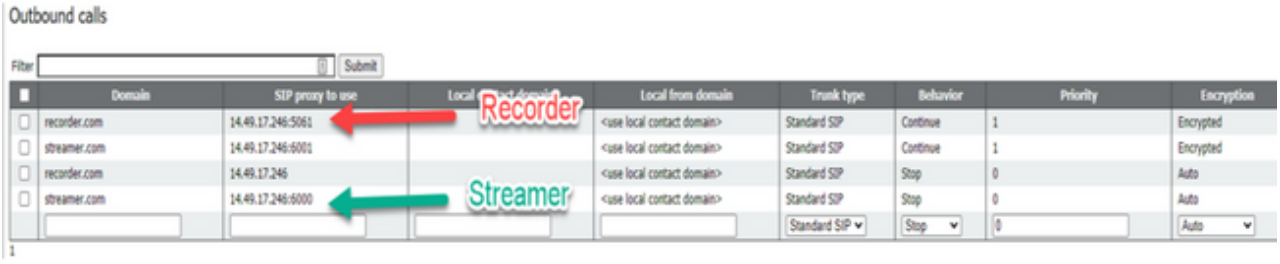
- Number of vCPUs should not oversubscribe the number of physical cores.
- Maximum number of 720p streams supported is 200 regardless of adding more vCPUs
- Maximum number of 1080p streams supported is 150 regardless of adding more vCPUs.
- Maximum number of audio-only streams supported is 200 regardless of adding more vCPUs.

API

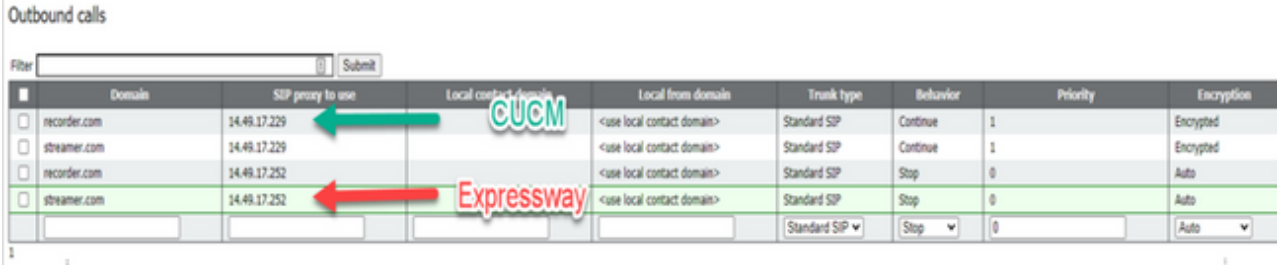
在api/v1/callProfiles上，您需要配置sipStreamUri。這是callBridge在必須啟動流式處理時撥打的URI。此URI的域需要新增到您的出站規則表，並指向流器（或呼叫控制）作為要使用的SIP代理。



下圖顯示直接撥號到Configuration > Outbound Calls中找到的出站規則上的流器元件。



下圖顯示通過呼叫控制(例如Cisco Unified Communications Manager(CUCM)或Expressway)對記錄器元件的呼叫。



注意：如果將流程式配置為使用SIP TLS，並且呼叫失敗，請檢查MMP中的callBridge節點，以檢視是否啟用了TLS SIP驗證。 MMP命令是「tls sip」。 呼叫可能失敗，因為callBridge不信任流處理器證書。 您可以通過使用「tls sip verify disable」在callBridge上禁用此選項來測試此功能。

多個串流器？

按照說明配置每個規則，並相應地調整出站規則。 如果您使用直接到串流器方法，請將現有的「出站到記錄器」規則更改為行為「繼續」，並在前一個出站規則下新增新的出站規則，該規則的優先順序比第一個出站規則低。 當第一個串流器達到其呼叫限制時，它會將488 Unreceptable發回到callBridge，而callBridge會移動到下一個規則。

如果要對資料流進行負載均衡，請使用呼叫控制並調整您的呼叫控制路由，以便它能夠向多個資料流發出呼叫。

Expressway注意事項

如果使用Cisco Expressway for Web Proxy，則必須確保Expressway在CMS升級之前至少運行X12.6。CMS 3.0需要該選項才能使Web代理運行並受到支援。

與CMS 3.0配合使用時，Web應用參與者的容量比Expressway有所增加。 對於大型OVA Expressway，預期容量為150個全高畫質呼叫(1080p30)或200個其他型別呼叫（例如720p30）。您可以通過將Expressway集群來增加此容量，最多6個節點（其中4個用於擴展，2個用於冗餘，因此最多600個全高畫質呼叫，或800個其他型別呼叫）。

Table 3: Cisco Meeting Server web app call capacities – external calling

Setup	Call Type	CE1200 Platform	Large OVA Expressway
Cisco Expressway Pair (X12.6 or later)	Full HD	150	150
	Other	200	200

CMS邊緣

CMS Edge在CMS 3.1中重新引入，因為它提供了比Expressway更高的容量用於外部Web應用會話。有兩種推薦的配置。

小型邊緣規格

4 GB RAM、4個vCPU、1Gbps網路介面

此VM Edge規格具有足夠的電源以覆蓋單個CMS1000音訊和影片負載容量，即48 x 1080p、96 x 720p、192 x 480p和1000音訊呼叫。

對於部署，建議每個CMS1000有1台小型邊緣伺服器，或者每個CMS2000有4台小型邊緣伺服器。

大型邊緣規格

8 GB RAM、16個vCPU、10Gbps網路介面

此VM Edge規格具有足夠的電源以覆蓋單個CMS2000音訊和影片容量，即350 x 1080p、700 x 720p、1000 x 480p和3000 x音訊呼叫。

對於部署，建議每個CMS2000或每個4個CMS1000配備1個大型邊緣伺服器。

Type of Calls	1 x 4 vCPU VM call capacity	1 x 16 vCPU VM call capacity
Full HD calls, 1080p30 video	100	350
HD calls, 720p30 video	175	700
SD calls, 448p30 video	250	1000
Audio Calls (G.711)	850	3000

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。