Richtlijnen voor probleemloze upgrade van Cisco Meeting Server 2.9 naar 3.0 (en hoger)

Inhoud

Inleiding

In dit document worden de uitdagingen beschreven waarmee u te maken heeft bij het upgraden van een Cisco Meeting Server-implementatie met versie 2.9 (of lager) of 3.0 (of hoger) en hoe u een vlot upgradeproces kunt garanderen.

Verwijderde functies: XMPP is verwijderd (wat invloed heeft op WebRTC), trunks/load balancers,

webbridge

Eigenschappen gewijzigd: Recorders en streamers zijn nu SIP en webbridge wordt vervangen door webbridge3

In dit document worden onderwerpen beschreven die uw aandacht verdienen voordat u een upgrade uitvoert. Niet alle nieuwe functies die in versie 3.X beschikbaar zijn worden behandeld.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CMS-beheer
- CMS-upgrades
- Maken en ondertekenen van certificaten

Alles wat hier wordt genoemd, wordt in verschillende documenten beschreven. Het is altijd raadzaam de release-opmerkingen van producten te lezen en onze programmeer- en implementatiehandleidingen door te nemen als u meer informatie nodig heeft over functies: Installatie- en configuratiehandleidingen voor CMS en Release-opmerkingen voor CMS-producten.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Meeting Server.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document is bedoeld als leidraad als u al CMS 2.9.x (of lager) heeft geïmplementeerd, ongeacht of dit in gecombineerd of veerkrachtig is, en u van plan bent te upgraden naar CMS 3.0. De informatie in dit document heeft betrekking op alle CMS-modellen.

> **Opmerking:** X-Series servers kunnen niet worden geüpgraded naar CMS 3.0. U moet X-Series servers zo snel mogelijk vervangen.

Belangrijke informatie over upgrades

De enige ondersteunde methode voor het upgraden van CMS is een stapsgewijze upgrade. Op het moment van schrijven is CMS 3.5 uitgebracht. Als u op CMS 2.9 bent, moet u op een stapsgewijze manier upgraden (2.9 —> 3.0 —> 3.1 —> 3.2 —> 3.3 —> 3.4 —> 3.5 (het upgradeproces van de opmerking heeft wijzigingen vanaf CMS 3.5, dus lees de release notities

zorgvuldig!!)

Als u geen stapsgewijze upgrade uitvoert en ongewoon gedrag ervaart, kan TAC u verzoeken te downgraden en opnieuw te beginnen.

Vanaf CMS 3.4 moet CMS ook slimme licenties gebruiken. U kunt niet upgraden naar CMS 3.4 of nieuwer en toch traditionele licenties gebruiken. Upgrade niet naar CMS 3.4 of nieuwer tenzij u Smart Licensing hebt ingesteld.

Samenvatting van aandachtspunten

Gebruik deze vragen om te navigeren naar de secties die betrekking hebben op uw eigen situatie. Bij elk aandachtspunt is een hyperlink opgenomen naar een gedetailleerdere beschrijving.

Licenties

Heeft u voldoende PMP- en SMP-licenties (Personal MultiParty/Shared MultiParty) op uw servers voorafgaand aan de upgrade?

In versie 3.0 worden de PMP-licenties toegewezen, zelfs als de gebruiker niet is aangemeld. Als u bijvoorbeeld 10000 gebruikers hebt geïmporteerd via LDAP, maar u slechts 100 PMP-licenties hebt, komt u niet meer aan de eisen te voldoen zodra u een upgrade naar 3.0 uitvoert. In deze use case moet u controleren op tenants met ingesteld userProfile en/of System/Profiles om na te gaan of een userProfile een hasLicense heeft die is ingesteld op true.

In deze sectie wordt gedetailleerder beschreven hoe u userProfiles op API kunt controleren om na te gaan of hasLicense=true is ingesteld (gelicentieerde PMP-gebruikers).

Heeft u PMP/SMP-licenties in uw huidige bestand cms.lic?

Als gevolg van wijzigingen in het licentiegedrag vanaf versie 3.0 moet u bevestigen dat u voldoende PMP/SMP-licenties heeft voordat u de upgrade uitvoert. Dit wordt in deze sectie **gedetailleerder beschreven.**

Heeft u Cisco Meeting Manager (CMM) geïmplementeerd?

CMS 3.0 vereist CMM 3.0 vanwege veranderingen in de manier waarop licenties worden verwerkt. Het wordt aanbevolen CMM 2.9 te implementeren voordat u een upgrade van uw omgeving naar versie 3.0 uitvoert, omdat u het 90-daagse rapport kunt controleren op licentieverbruik gedurende de afgelopen 90 dagen. Dit wordt in deze sectie gedetailleerder beschreven.

Gebruikt u Smart Licensing?

CMS 3.0 vereist CMM 3.0 vanwege veranderingen in de manier waarop licenties worden verwerkt. Als u al Smart Licensing via CMM gebruikt, moet u ervoor zorgen dat PMP- en SMP-licenties zijn gekoppeld aan uw cluster.

webBridge (WebRTC- en CMA-client)

Gebruikt u WebRTC in CMS 2.9?

Webbridge is aanzienlijk veranderd in CMS 3.0. In deze sectie is advies opgenomen over de migratie van webbridge2 naar webbridge3 en het gebruik van de webapp.

Gebruiken uw gebruikers de CMA thick client?

Aangezien deze clients op XMPP zijn gebaseerd, kunnen ze na de upgrade niet meer worden gebruikt aangezien de XMPP-server is verwijderd. U vindt meer informatie in deze sectie als dit van toepassing is op uw use case.

Gebruikt u de chatfunctie in WebRTC?

De chatfunctie is verwijderd uit de webapp in 3.0. De chatfunctie is weer beschikbaar in CMS 3.2, maar is niet permanent. U vindt meer informatie over deze functie in deze sectie.

Voeren uw gebruikers via WebRTC point-to-point oproepen uit naar apparaten?

In CMS 3.0 kan een webapp-gebruiker niet meer rechtstreeks naar een ander apparaat bellen. Nu moet u toetreden tot een vergaderruimte en de machtiging hebben om deelnemers aan de vergadering toe te voegen om dezelfde actie uit te voeren. U vindt meer informatie hierover in deze sectie.

Maken uw gebruikers hun eigen coSpaces via WebRTC?

In versie 3.0 moet in de API een coSpaceTemplate worden gemaakt en aan webapp-gebruikers worden toegewezen zodat ze via de client hun eigen ruimtes kunnen maken. Dit kan handmatig of automatisch plaatsvinden tijdens LDAP-import. CanCreateCoSpaces wordt uit userProfile verwijderd. U vindt meer informatie over deze functie in deze sectie.

Wijzigingen in web-GUI

Heeft u webBridge-instellingen geconfigureerd in de web-GUI?

De webBridge-instellingen worden in versie 3.0 uit de GUI verwijderd. U moet de webbridges dan ook configureren in de API en de huidige GUI-instellingen noteren, zodat u de webBridgeProfiles in de API dienovereenkomstig kunt configureren. U vindt meer informatie over deze wijziging in deze sectie.

Heeft u externe instellingen geconfigureerd in de web-GUI?

De externe instellingen zijn uit de GUI in CMS 3.1 verwijderd. Als u webBridge-URL of -IVR heeft ingesteld in de web-GUI in CMS 3.0 of lager (Configuration —> General —> External Settings (Configuratie —> Algemeen —> Externe instellingen)), zijn deze verwijderd van de webpagina en moeten nu worden geconfigureerd in de API. De instellingen voorafgaand aan de upgrade naar versie 3.1 worden NIET in de API opgenomen en moeten handmatig worden opgegeven. U vindt meer informatie over deze wijziging in deze sectie.

Recorders/streamers

Maakt u momenteel gebruik van CMS-recorder(s) en/of -streamer(s)?

De CMS-componenten recorder en streamer zijn nu op SIP gebaseerd in plaats van op XMPP. Aangezien XMPP wordt verwijderd, moeten deze na de upgrade worden aangepast. U vindt meer

informatie over deze wijziging in deze sectie.

Overwegingen voor Cisco Expressway

Wat is uw huidige versie van Cisco Expressway als u Expressway als proxy voor WebRTC gebruikt?

CMS 3.0 vereist Expressway 12.6 of hoger. U vindt meer informatie over de WebRTC-proxyfunctie in deze sectie.

CMS Edge

Gebruikt u momenteel CMS Edge in uw omgeving?

CMS Edge wordt opnieuw opgenomen in CMS 3.1 met hogere schaalbaarheid voor externe verbindingen. U vindt meer informatie hierover in deze sectie.

CMS (Acano) X-Series

Gebruikt u momenteel X-Series servers in uw omgeving?

Deze servers kunnen niet worden geüpgraded naar CMS 3.0 en u moet deze zo snel mogelijk vervangen (overstappen op een virtuele machine of een CMS-applicatie voordat u de upgrade naar versie 3.0 uitvoert). U vindt de end-of-life kennisgeving met betrekking tot deze server via deze link.

SIP Edge

Gebruikt u momenteel SIP Edge in uw omgeving?

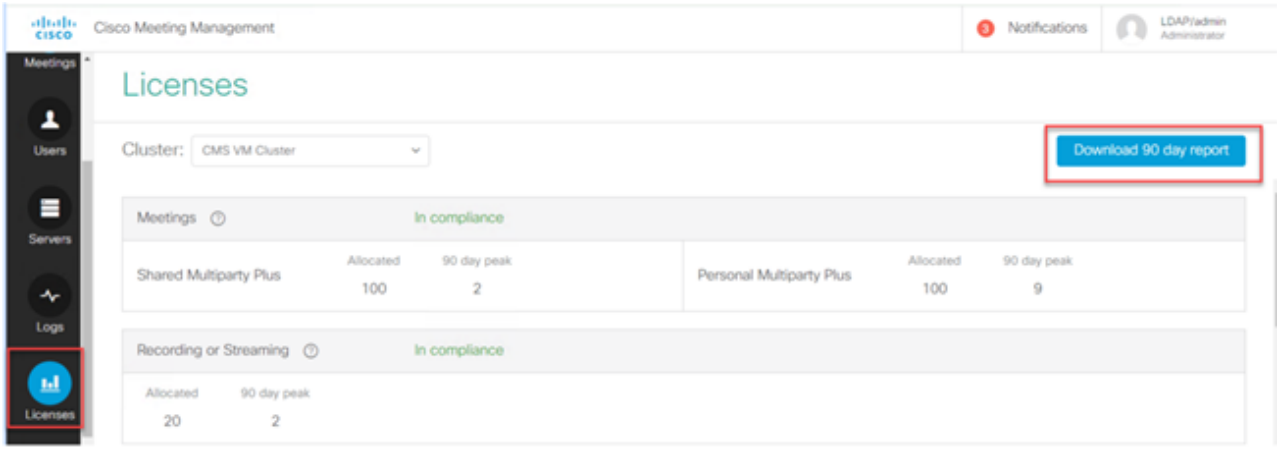
Sip Edge wordt vanaf CMS 3.0 volledig afgeschaft. U moet Cisco Expressway gebruiken om SIP-oproepen naar uw CMS mogelijk te maken. Neem contact op met uw Cisco-accountvertegenwoordiger over de inzet van Expressway in uw organisatie.

Meer informatie

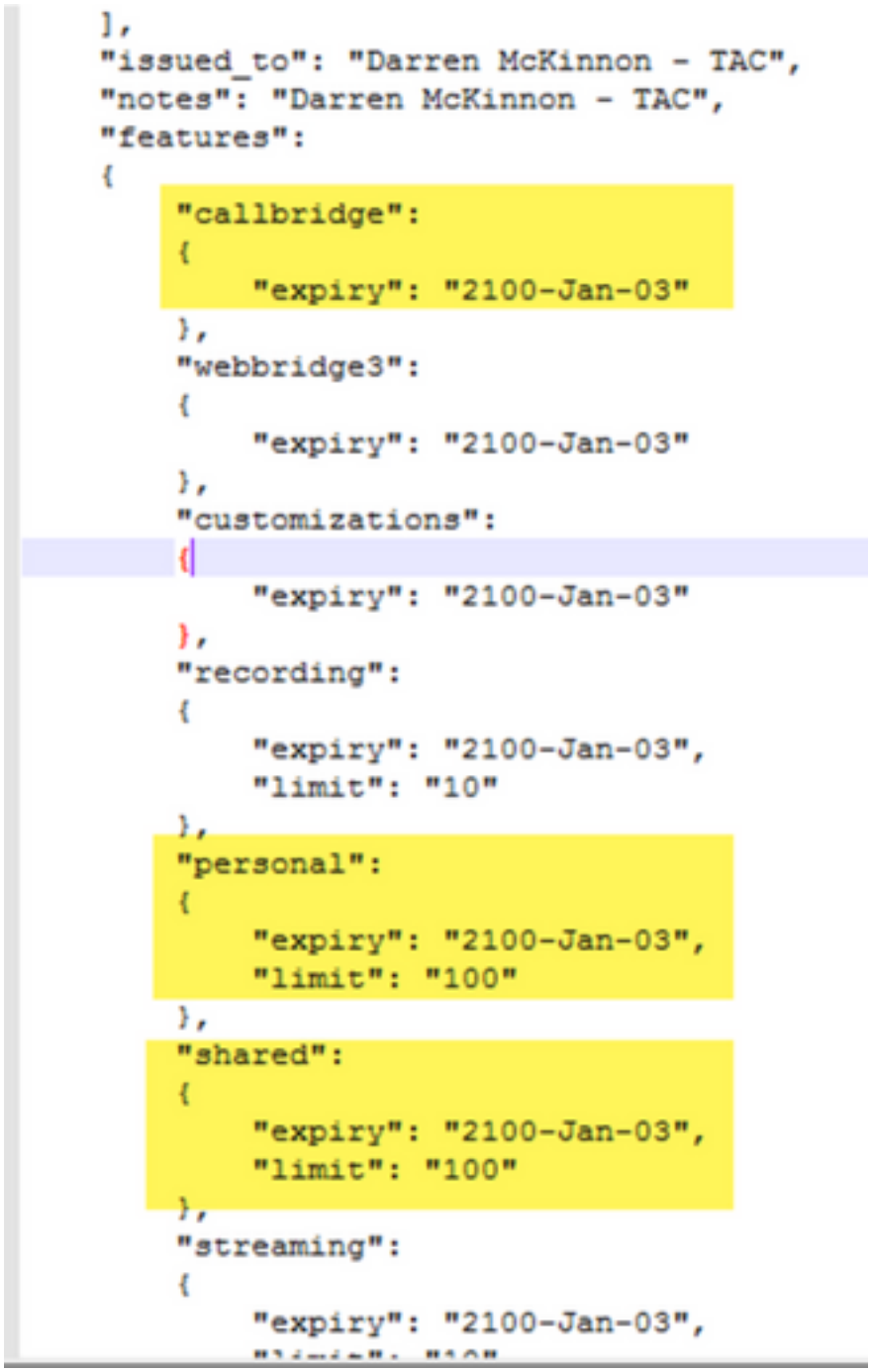
Licenties voorafgaand aan upgrade controleren

Als de status van de licentie niet compliant is, heeft dat een grote impact bij het upgraden van versie 2.x naar versie 3.0 of hoger. In deze sectie wordt beschreven hoe u het aantal PMP/SMP-licenties kunt bepalen dat nodig is voor een probleemloze upgrade.

Voordat u een upgrade uitvoert naar versie 3.0, kunt u CMM 2.9 implementeren en het **90-daagse rapport** controleren op het tabblad **Licenses** (Licenties) om na te gaan of het licentieverbruik onder het huidige toegewezen licentie-aantal op de CMS-knooppunten is gebleven:

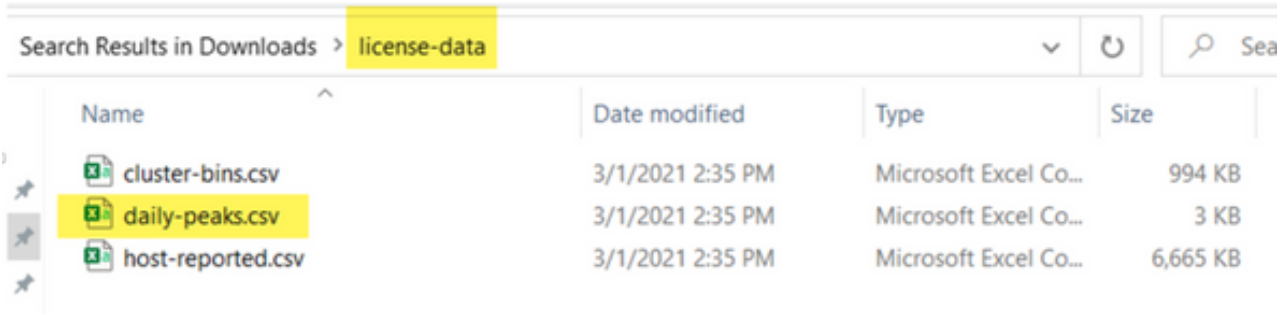


Als u traditionele licenties gebruikt (bestand cms.lic wordt lokaal geïnstalleerd op uw CMS-knooppunten), controleer dan het CMS-licentiebestand op het aantal persoonlijke en gedeelde licenties (in de afbeelding 100/100) op elk CMS-knooppunt (download van elk callBridge-knooppunt via WinSCP).



Als u al Smart Licensing gebruikt, controleer dan hoeveel PMP/SMP-licenties in de Smart-portal voor Cisco-software zijn toegewezen voor de CMS-servers.

Open het 90-daagse rapport (het bestand *license-data.zip*) en bekijk het bestand met de naam *daily-peaks.csv* in Excel.



Sorteer de kolom PMP van Z naar A om de hogere waarden bovenaan te zetten. Doet hetzelfde voor de kolom SMP. Zijn de waarden die u in dit bestand ziet lager dan het aantal licenties beschikbaar in het CMS-licentiebestand? Zo ja, dan is alles in orde en volledig compliant. Zo niet, dan geeft dit waarschuwingen en/of fouten aan zoals aangegeven in afbeelding 6 in paragraaf 1.7.3 van de CMS-implementatiegids waarvoor u meer informatie kunt vinden, evenals in paragraaf 1.7.4.

Volgens de afbeelding in dit voorbeeld werden er gedurende de afgelopen 90 dagen bij piekgebruik 2.1667 SMP-licenties gebruikt en geen PMP-licenties. In het bestand cms.lic wordt 100 eenheden van elk licentietype aangegeven, wat betekent dat alles volledig compliant is. Er zijn dan ook geen problemen met licenties wanneer deze setup-upgrades naar CMS 3.0 worden uitgevoerd. Er kan echter nog steeds een probleem zijn wanneer er op de setup 10.000 gebruikers met LDAP zouden zijn geïmporteerd. U heeft slechts 100 PMP-licenties maar wijst er 10.000 toe (met userProfile waarbij hasLicense=true). In dit geval bent u dus niet meer compliant na een upgrade naar versie 3.0. Dit wordt verder beschreven in de volgende sectie.

date	pmp	smp	rec/str
12/10/2020	0	2.166666667	0
12/3/2020	0	2	0
1/7/2021	0	2	0
1/8/2021	0	2	0
1/14/2021	0	2	0
1/15/2021	0	2	0
1/26/2021	0	2	0
1/27/2021	0	2	0
2/19/2021	0	2	0
2/20/2021	0	2	0
1/11/2021	0	1.333333333	0
12/9/2020	0	1.166666667	0
1/12/2021	0	1.166666667	0
1/21/2021	0	1.166666667	0
2/8/2021	0	1.166666667	0
2/25/2021	0	1.166666667	0

Bepalen hoeveel gebruikers een PMP-licentie krijgen wanneer u een upgrade heeft uitgevoerd

Alle gebruikers die worden geïmporteerd en een **userProfile** met **hasLicense=true** gebruiken, krijgen in CMS 3.0 automatisch een PMP-licentie toegewezen.

Controleer in de API hoeveel userProfiles er zijn en controleer of een of meer ervan de instelling hasLicense=true heeft. Zo ja, dan moet u controleren waar deze userProfiles zijn toegewezen.

De gebruikersprofielen kunnen op elk van deze niveaus worden toegewezen:

1. LdapSources
2. Tenants
3. System/Profiles

Controleer alle 3 locaties voor toegewezen userProfiles met hasLicense=true.

1. LdapSources/Tenants

Voor elke ldapSource die een tenant of een userProfile gebruikt wordt aan gebruikers die met die ldapSource worden geïmporteerd een PMP-licentie toegewezen wanneer de parameter hasLicense is ingesteld op true. Als er een tenant is, moet u op de tenant-ID klikken om na te gaan of er een userProfile aan is toegewezen en vervolgens controleren of dit is geconfigureerd met hasLicense=true. Als er geen tenant is maar wel een userProfile is ingesteld, moet u erop klikken om na te gaan of dit is ingesteld op License=true. Als er bij tenant/geen tenant sprake is van hasLicense=true, dan kunt u controleren hoeveel gebruikers zijn geïmporteerd door een opdracht GET uit te voeren op ‘api/v1/users’ en te filteren op het domein dat wordt gebruikt voor de jidMapping in de ldapMapping gekoppeld aan de ldapSource.

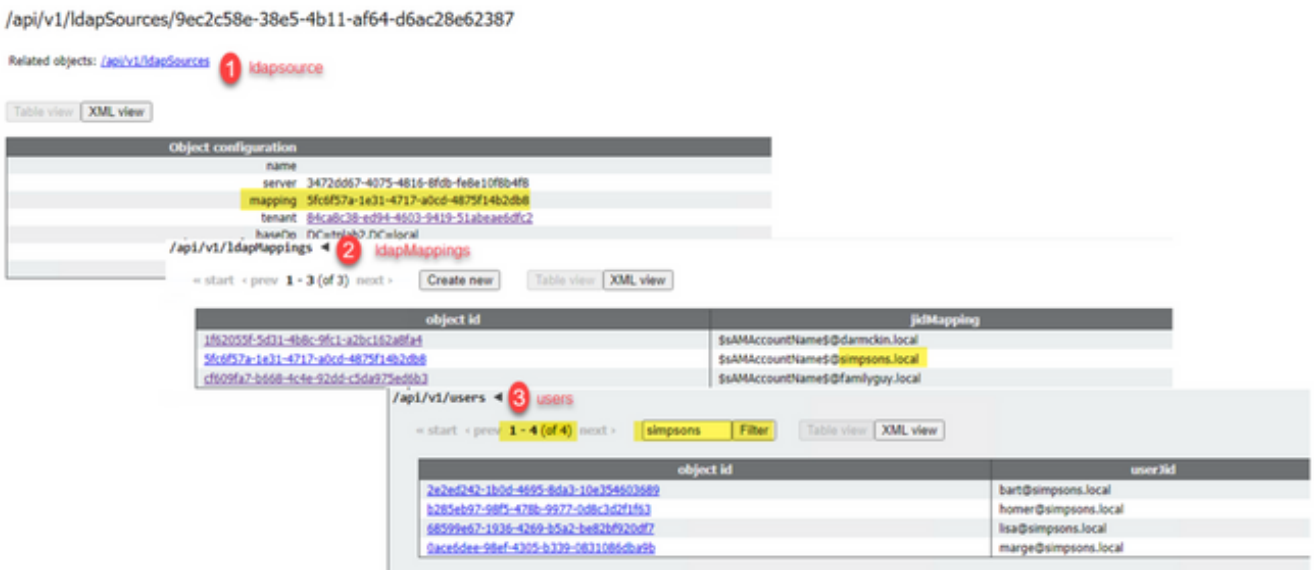
> **Opmerking:** Dit kan complexer zijn in andere situaties; in dat geval moet dit controleren met de ActiveDirectory-toewijzingen en -filters die u heeft gemaakt.

Stap 1. Zoek de toewijzings-ID via de ldapSource.

Stap 2. Zoek ldapMappings om de jidMapping te vinden.

Stap 3. Zoek in api/v1/users naar het domein dat in de jidMapping wordt gebruikt.

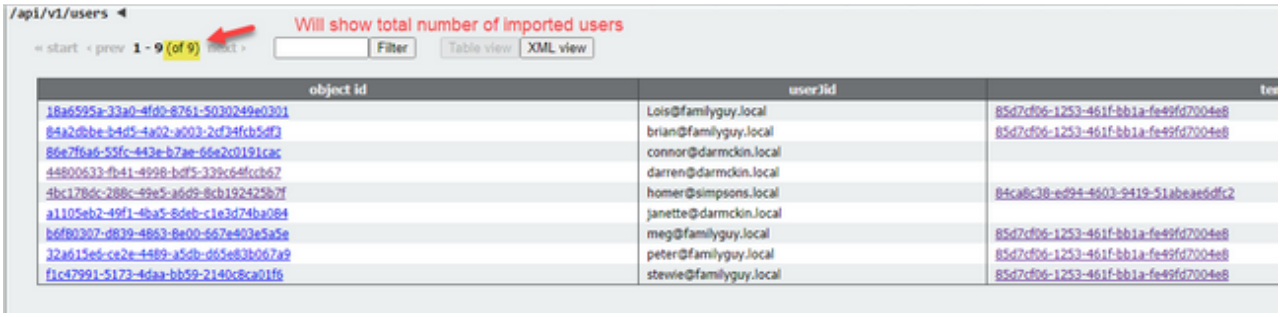
Stap 4. Tel de gebruikers op die in elke ldapSource zijn gevonden. Dit is hoeveel LDAP geïmporteerde gebruikers PMP-licenties nodig hebben.



2. System/Profiles

Als een gebruikersprofiel op systeem-/profielniveau is ingesteld en dat gebruikersprofiel "hasLicense=true" heeft, wordt aan elke gebruiker die in CMS is geïmporteerd, een PMP-licentie toegewezen wanneer de server wordt bijgewerkt. Als u 10.000 gebruikers hebt geïmporteerd, maar u slechts 100 PMP's hebt, is dit niet conform wanneer u upgradt naar CMS 3.0, en kan een 30 seconden bericht op het scherm te verschijnen en audio-prompt bij het begin van de oproepen.

Als het gebruikersprofiel op systeemniveau aangeeft dat gebruikers een PMP moeten krijgen, ga dan naar api/v1/gebruikers om te zien hoeveel gebruikers er in totaal zijn:



Als u alle gebruikers al uit ldap heeft geïmporteerd maar zich nu beseft dat u alleen een bepaalde subset van die lijst nodig heeft, maak dan een beter filter in ldapSource zodat alleen de gebruikers worden geïmporteerd waaraan u PMP-licenties wilt toewijzen. Wijzig het filter in ldapSource en voer vervolgens een nieuwe LDAP-synchronisatie uit in api/v1/ldapsync. Hierdoor worden alleen uw gewenste gebruikers geïmporteerd en alle anderen van deze eerdere import verwijderd.

> **Opmerking:** Als u dit correct doet en bij de nieuwe import alleen ongewenste gebruikers worden verwijderd, veranderen de coSpace callIds en geheimen van de resterende gebruikers niet. Als u echter een fout maakt, kunnen alle callIds en geheimen veranderen. Maak een back-up van uw database-knooppunten voordat u dit probeert als u zich hier zorgen over maakt!

Heeft u voldoende SMP-licenties?

Als u de dagelijkse pieken in het 90-daagse rapport van CMM bekijkt, heeft u dan voldoende

SMP-licenties om die pieken te kunnen verwerken? SMP-licenties worden gebruikt wanneer geen PMP-licentie is toegewezen aan de eigenaar van de vergadering (eigenaar van coSpace/ad-hoc vergadering/geplande TMS-vergadering). Als u bewust SMP gebruikt en er voldoende licenties zijn tijdens piekuren is alles in orde. Als u de dagelijkse SMP-pieken in het 90-daagse rapport controleert en het onduidelijk is waarom deze licenties worden verbruikt, moet u enkele zaken nagaan.

1. Ad-hocgesprekken (zoals verhoogd vanaf CUCM) gebruiken een SMP-licentie als het apparaat dat wordt gebruikt om samen te voegen niet is gekoppeld aan een gebruiker die via het gebruikersprofiel een PMP-licentie in CMS heeft toegewezen. CUCM verstrekt de GUID van de gebruiker die de vergadering escaleert. Als die GUID overeenkomt met een Meeting Server geïmporteerde LDAP-gebruiker met een toegewezen PMP-licentie, wordt de licentie van die gebruiker gebruikt.

2. Als een CoSpace-eigenaar geen PMP-licentie heeft gekregen, wordt bij oproepen naar die bepaalde coSpaces een SMP-licentie gebruikt.

3. Als de vergadering in TMS versie 15.6 of nieuwer was gepland, wordt de vergadereigenaar naar CMS verzonden en als die gebruiker geen PMP-licentie is toegewezen, gebruikt die vergadering een SMP-licentie.

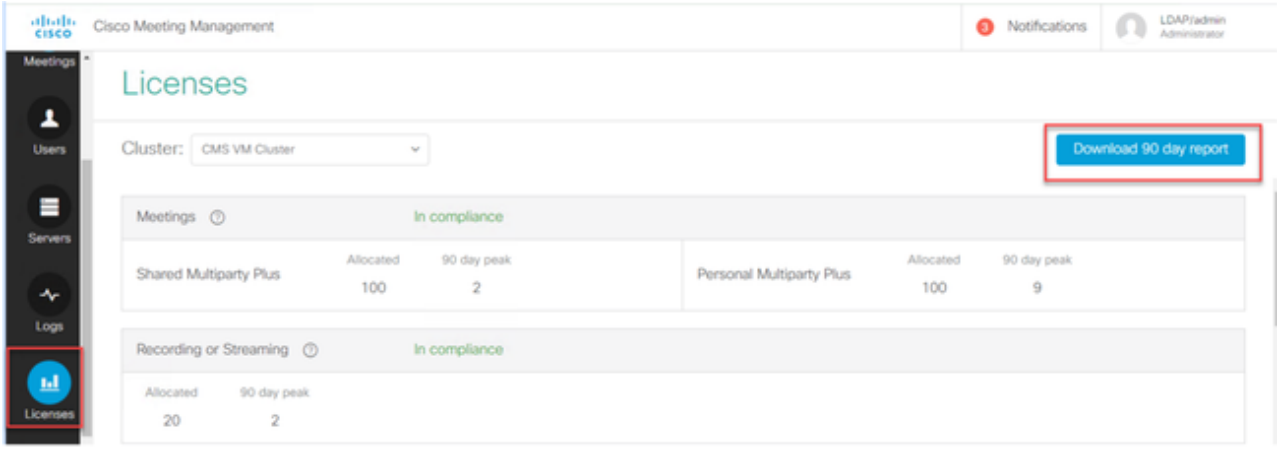
CMM configureren

Vanaf CMS 3.0 is CMM 3.0 nodig voor een goede werking van CMS. CMM is verantwoordelijk voor de licentiëring van CMS. Als u van plan bent CMS te upgraden naar versie 3.0, moet u een CMM-server hebben. Het wordt aanbevolen om CMM 2.9 te implementeren terwijl u CMS 2.9 gebruikt, zodat u het licentieverbruik kunt controleren voordat u de upgrade uitvoert.

CMM controleert alle toegevoegde callBridges voor SMP- en PMP-licenties en de callBridge-licentie. Het gebruikt het nummer dat het hoogste is over de verschillende apparaten binnen het cluster.

Als CMS1 bijvoorbeeld 20 PMP-licenties en 10 SMP-licenties heeft en CMS2 40 PMP-licenties en 5 SMP-licenties bij traditionele licentiëring, dan meldt de CMM dat u 40 PMP-licenties en 10 SMP-licenties te verbruiken heeft.

Als u meer PMP-licenties hebt dan geïmporteerde gebruikers, hebt u geen problemen met PMP- (of SMP-licenties), maar als u controleert dat piek van 90 dagen en u merkt dat u meer hebt gebruikt dan beschikbaar, kunt u nog steeds upgraden naar CMS 3.0 en de 90-dagen-proeflicentie op CMM gebruiken om zaken met uw licenties te regelen, of actie ondernemen vóór de upgrade.



Webbridge configureren (WebRTC- en CMA-client)

CMS 3.0 verwijdert de XMPP-servercomponent en daarmee wordt webBridge en de mogelijkheid om de CMA thick client te gebruiken ook verwijderd. webbridge3 wordt nu gebruikt om webapp-gebruikers (voorheen WebRTC-gebruikers) via de browser te verbinden met vergaderingen. Wanneer u upgrade naar 3.0, moet u webbridge3 configureren.

> **Opmerking:** CMA dikke client werkt niet na upgrade naar CMS 3.0!

In deze video wordt het proces voor het maken van de webbridge3-certificaten doorlopen.

https://video.cisco.com/video/6232772471001

Voorafgaand aan de upgrade naar versie 3.0 moeten klanten de configuratie van webbridge3 bepalen. De belangrijkste stappen worden hieronder aangegeven.

1. U heeft wel een sleutel- en certificaatketen nodig voor webbridge3. De oude webbridge cert kan worden gebruikt als de cert alle CMS server FQDN's of IP-adressen als Onderwerp Alternatieve Naam (SAN) / Gemeenschappelijke Naam (CN) bevat die webbridge3 uitvoeren, en als aan een van deze voorwaarden is voldaan:

a. Het certificaat omvat geen uitgebreid sleutelgebruik (dit betekent dat het als client of server kan worden gebruikt).

b. Het certificaat omvat zowel client- als serververificatie. Een HTTPS-certificaat vereist alleen serververificatie; een C2W-certificaat vereist zowel client- als serververificatie).

2. Als u een nieuw certificaat voor '**webbridge3 https**' wilt maken, wordt aangeraden het openbaar te ondertekenen (om certificaatwaarschuwingen op de client bij gebruik van de webapp te voorkomen). Dit zelfde cert kan worden gebruikt voor de "webbridge3 c2w cert", en de cert moet de FQDN van de webbrige servers in de SAN/CN hebben.

3. CallBridges moeten met de nieuwe webbridge3 communiceren via een poort die is geconfigureerd met de opdracht **webbridge3 c2w listen**. Dit kan elke beschikbare poort zijn, zoals 449. U moet er zeker van zijn dat de callBridges op deze poort kunnen communiceren met webbridge3 en waar nodig vooraf firewallwijzigingen doorvoeren. Het mag echter niet dezelfde poort zijn die door 'webbridge https' wordt gebruikt om te luisteren.

Voorafgaand aan de CMS-upgrade naar versie 3.0 is het raadzaam een back-up te maken met de opdracht 'backup snapshot <servername_date>' en vervolgens in te loggen bij de pagina webadmin op uw callBridge-knooppunten om alle XMPP- en webBridge-instellingen te verwijderen. Maak vervolgens verbinding met de MMP op uw servers en voer deze stappen uit op alle Core-servers met xmpp en webbridge via een SSH-verbinding:

1. **xmpp disable**
2. **xmpp reset**
3. **xmpp certs none**
4. **xmpp domain none**
5. **webbridge disable**
6. **webbridge listen none**
7. **webbridge certs none**

8. **webbridge trust none**

Nadat u een upgrade naar versie 3.0 heeft uitgevoerd, moet u webbridge3 configureren op alle servers waarop eerder webBridge werd uitgevoerd. Er zijn al DNS-records die naar deze servers verwijzen en op deze manier garandeert u dat als een gebruiker naar webbridge3 wordt omgeleid, de aanvraag kan worden afgehandeld.

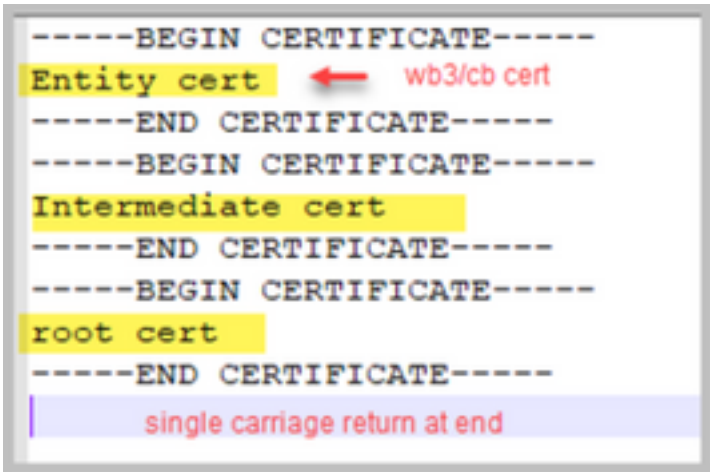
Configuratie van webbridge3 (via SSH-verbinding)

Stap 1. Configureer de http-luisterpoort voor webbridge3.

webbridge3 https listen a:443

Stap 2. Configureer certificaten voor webbridge3 voor browserverbindingen. Dit is het certificaat dat naar browsers wordt gestuurd, dat moet worden ondertekend door een openbare certificeringsinstantie (CA) en dat de FQDN bevat dat in de browser wordt gebruikt zodat de verbinding wordt vertrouwd.

webbridge3 https certs wb3.key wb3trust.cer (Dit moet een vertrouwensketen zijn: maak een vertrouwen zekerheid die eindentiteit bovenop heeft, gevolgd door Intermediate CAs in orde, eindigend met RootCA).



Stap 3. Configureer de poort die wordt gebruikt om te luisteren naar verbindingen van callBridge naar webBridge (c2w). Aangezien 443 wordt gebruikt als https-luisterpoort voor webbridge3, moet deze configuratie een andere, beschikbare poort zijn, bijvoorbeeld 449.

webbridge3 c2w listen a:449

4. Certificaten configureren die webbridge naar callbridge stuurt voor het c2w-vertrouwen

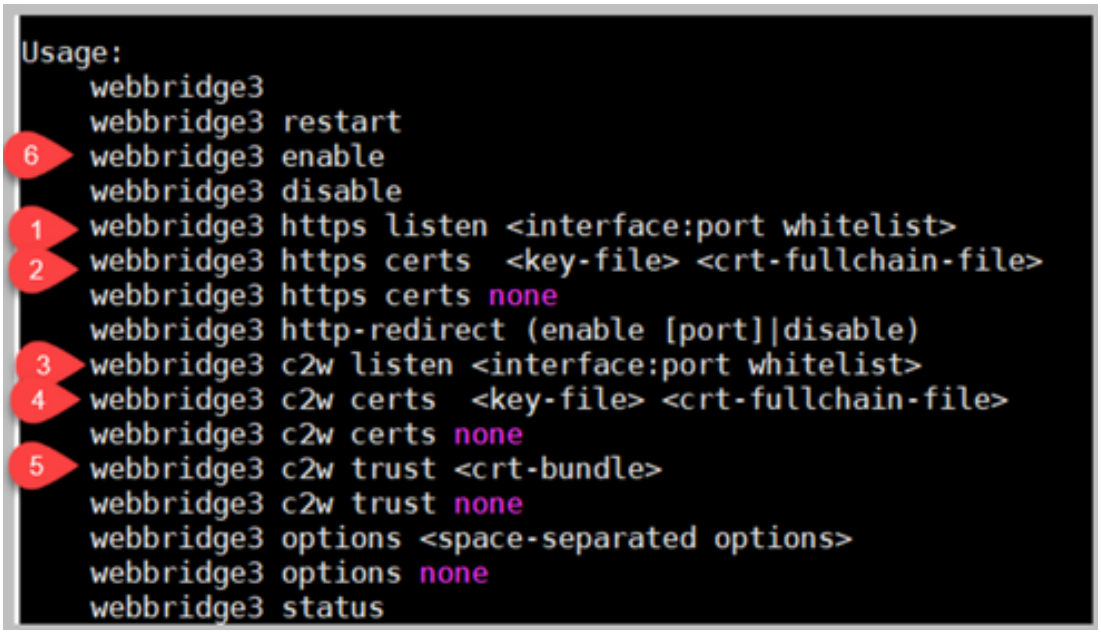
webbridge3 c2w certs wb3.key wb3trust.cer

5. Configureer de vertrouwensopslag WB3 gebruikt om het callBridge certificaat te vertrouwen. Dit moet hetzelfde certificaat zijn als wordt gebruikt in de CA-bundel van callBridge (en moet bovenaan een bundel van tussencertificaten en onderaan de basis-CA bevatten, gevolgd door één regelterugloop).

webbridge3 c2w trust rootca.cer

Stap 6. Schakel webbridge3 in.

webbridge3 enable



Wijzigingen in callBridge-configuratie (via SSH-verbinding)

Stap 1. Configureer het callBridge-vertrouwen met het CA-certificaat of de CA-bundel waarmee het webbridge3 c2w-certificaat is ondertekend.

callbridge trust c2w rootca.cer

Stap 2. Start de callBridge opnieuw om het nieuwe vertrouwen in werking te stellen. Alle oproepen naar deze specifieke callBridge worden hiermee afgewezen, dus ga voorzichtig te werk.

callbridge restart

API-configuratie voor verbinding van callBridges met webbridge3

1. Maak een nieuw webBridge object met POST in de API en geef het een URL-waarde met behulp van FQDN en poort geconfigureerd op de witte lijst van de webbridge c2w interface (stap 3 in de webbridge3-configuratie)

c2w://webbridge.darmckin.local:449

Op dit punt werkt Webbridge3 opnieuw, en u kunt zich als gast bij ruimtes aansluiten of als u eerder gebruikers hebt geïmporteerd, moeten ze kunnen inloggen.

Machtigingen voor het creëren van ruimte door webapp-gebruikers

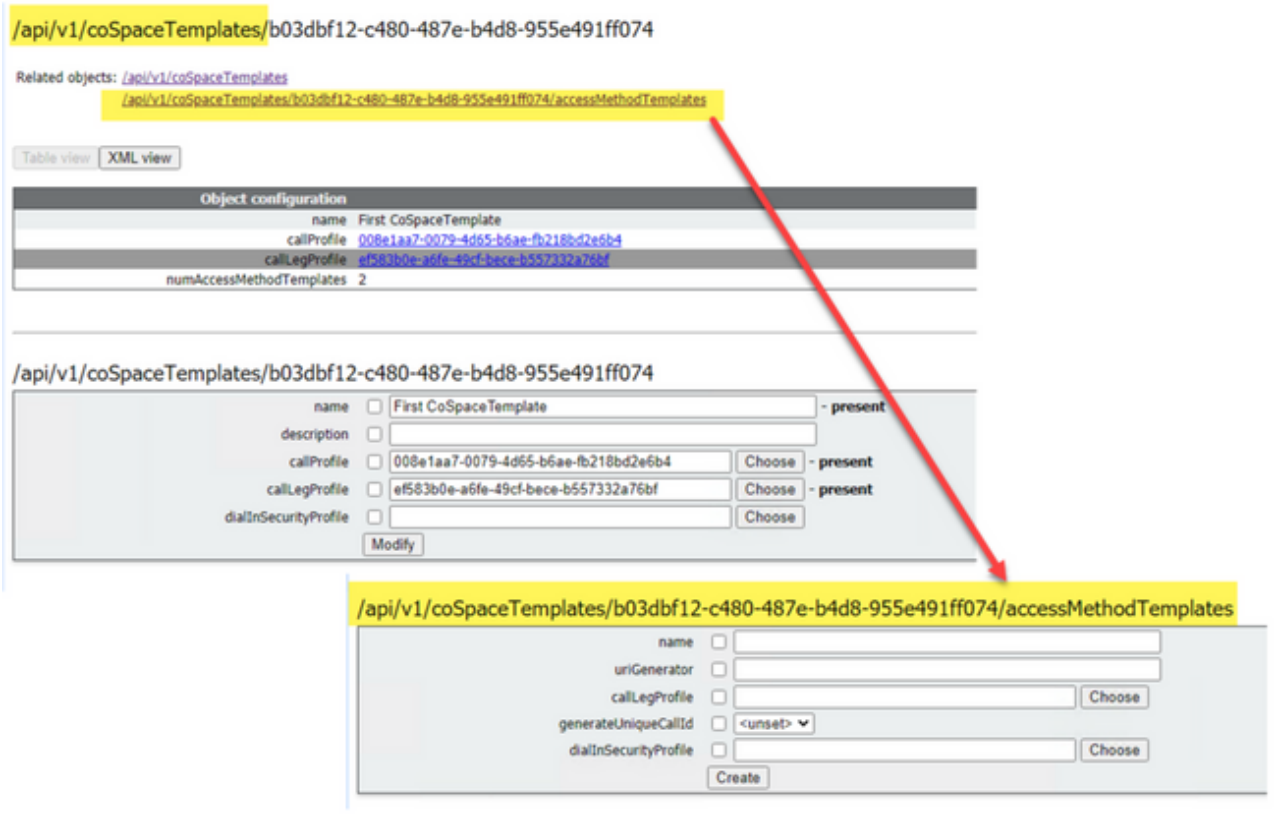
Kunnen uw gebruikers normaliter hun eigen ruimtes maken in WebRTC? Vanaf CMS 3.0 kunnen webapp-gebruikers niet hun eigen coSpaces maken, tenzij een coSpaceTemplate aan hen is toegewezen die dit toestaat.

Zelfs met een toegewezen coSpaceTemplate kunnen ze geen ruimte maken waar anderen kunnen inbellen (geen URI, geen callId of Passcode), maar als de coSpace een callLegProfile heeft met ‘addParticipantAllowed', kunnen ze wel via die ruimte uitbellen.

Als u kiesreeksen wilt creëren die kunnen worden gebruikt om in te bellen bij de nieuwe ruimte, moet de coSpaceTemplate worden gecombineerd met een accessMethodTemplate (zie 2.9 Release-opmerkingen – 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).

Maak in de API een of meer coSpaceTemplates en maak vervolgens een of meer accessMethodTemplates en wijs de coSpaceTemplate toe aan de ldapUserCoSpaceTemplateSources. U kunt ook handmatig een coSpaceTemplate toewijzen aan een gebruiker in api/v1/users.

U kunt meerdere coSpaceTemplates en accessMethodTemplates maken en toewijzen. Zie de API-referentiehandleiding van CMS voor meer informatie (https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html)



Gebruik van coSpaceTemplate (API-configuratie)

Name: Elke gewenste naam die u de coSpaceTemplate wilt geven.

Beschrijving: Beknopte omschrijving, indien gewenst.

callProfile: Welk callProfile moet worden gebruikt door ruimtes die met deze sjabloon worden gemaakt? Indien niets wordt opgegeven, wordt het profiel gebruikt dat is ingesteld op niveau System/Profiles.

callLegProfile: Welk callLegProfile moet worden gebruikt door ruimtes die met deze sjabloon zijn gemaakt? Indien niets wordt opgegeven, wordt het profiel gebruikt dat is ingesteld op niveau System/Profiles.

dialInSecurityProfile: Welk dialInSecurityProfile moet worden gebruikt door ruimtes die met deze

sjabloon zijn gemaakt? Indien niets wordt opgegeven, wordt het profiel gebruikt dat is ingesteld op niveau System/Profiles.

Gebruik van accessMethodTemplate (API-configuratie)

Name: Elke gewenste naam die u de coSpaceTemplate wilt geven.

uriGenerator: De expressie die moet worden gebruikt om URI-waarden te genereren voor de AccessMethodTemplate; de toegestane tekens zijn a t/m z, A t/m Z, 0 t/m 9, punt (.), koppelteken (-), onderstrepingsteken (_) en $; indien de expressie niet leeg is, moet deze precies één $-teken bevatten. Een voorbeeld hiervan is $.space, dat de naam gebruikt die door de gebruiker wordt opgegeven bij het maken van de ruimte en daar ".space" aan toevoegt. "Teamvergadering" maakt de url 'Team.Meeting.space@domain'.

callLegProfile: Welk callLegProfile worden gebruikt door accessMethods die met deze sjabloon zijn gemaakt? Indien niets wordt opgegeven, wordt het profiel gebruikt dat is ingesteld op het niveau coSpaceTemplate en anders wat is ingesteld op het niveau System/Profiles.

generateUniqueCallId: Hier geeft u aan of een unieke numerieke ID moet worden gegenereerd voor deze accessMethod die de algemene methode voor de coSpace overtreft.

dialInSecurityProfile: Welk dialInSecurityProfile worden gebruikt door accessMethods die met deze sjabloon zijn gemaakt? Indien niets wordt opgegeven, wordt het profiel gebruikt dat is ingesteld op het niveau coSpaceTemplate en anders wat is ingesteld op het niveau System/Profiles.

Chatfunctie

In CMS 3.0 is de permanente chatfunctie verwijderd, maar in CMS 3.2 is de niet-permanente chatfunctie weer opgenomen. De chatfunctie is beschikbaar voor webapp-gebruikers en de chats worden nergens opgeslagen. Nadat CMS 3.2 is geïnstalleerd, kunnen webapp-gebruikers elkaar standaard tijdens vergaderingen berichten sturen. Deze berichten zijn uitsluitend beschikbaar tijdens de vergadering en alleen berichten die worden uitgewisseld nadat gebruikers tot de vergadering zijn toegetreden, zijn zichtbaar. U kunt geen berichten zien die zijn uitgewisseld voordat u aan de vergadering deelnam.

WebRTC point-to-point oproepen

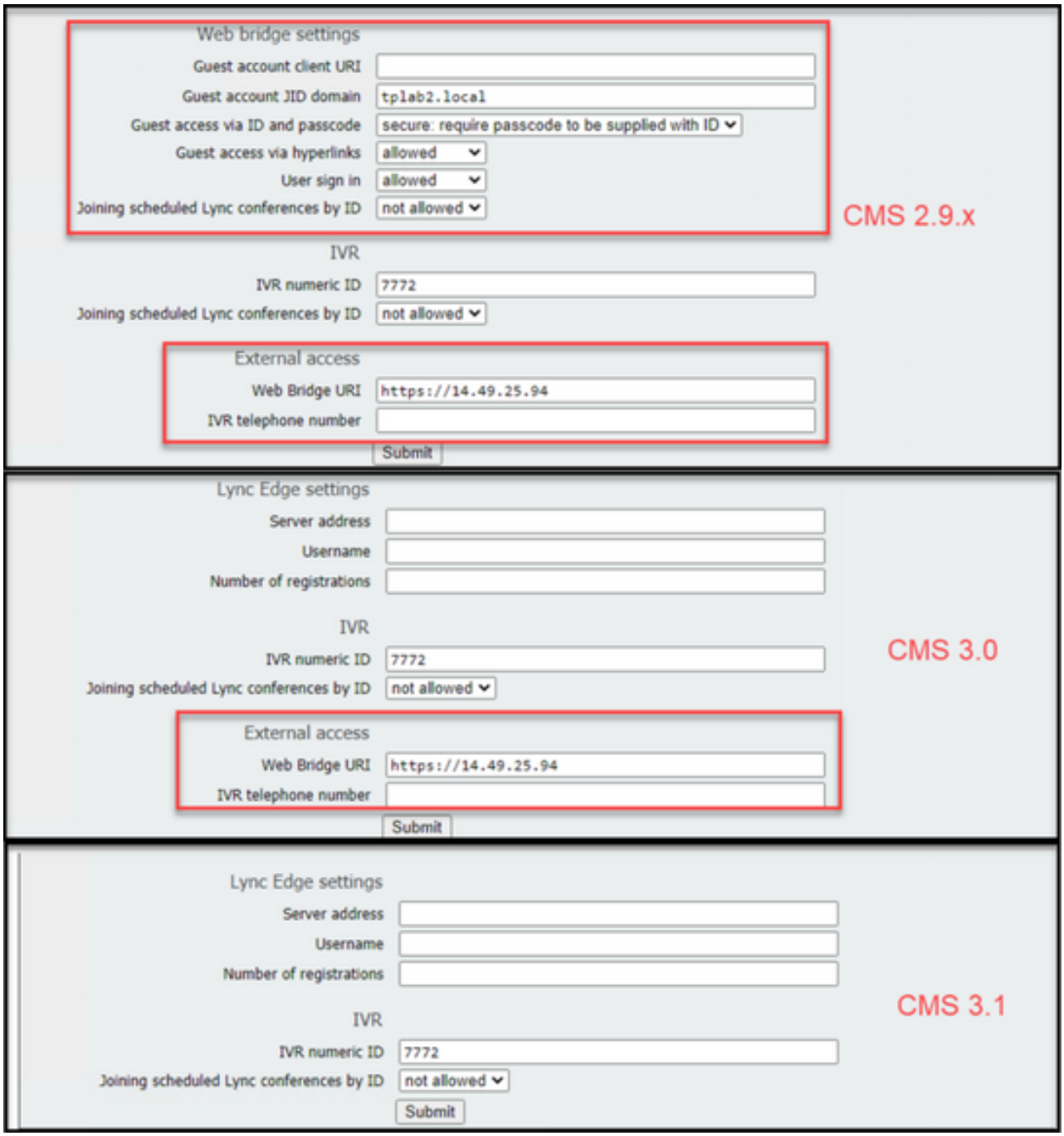
In CMS 2.9.x konden WebRTC-deelnemers direct via hun cliënt inbellen bij andere contactpersonen. Vanaf CMS 3.0 is dit niet langer mogelijk. Nu moeten gebruikers zich aanmelden en toetreden tot een ruimte. Als ze toestemming hebben in callLegProfile (parameter **addParticipants** ingesteld op true), kunnen ze andere contactpersonen toevoegen. Dit zorgt ervoor dat CMS uitbelt naar de deelnemer en ze elkaar kunnen ontmoeten in een ruimte in CMS.

Belangrijke veranderingen in webBridge-instellingen

In CMS 3.0 en 3.1 zijn enkele webBridge-instellingen uit de GUI verwijderd of verplaatst en deze moeten in de API worden geconfigureerd om gebruikers een consistente ervaring te bieden. Gebruik in 3.x **api/v1/webBridges** en **api/v1/webBridgeProfiles**.

Controleer wat momenteel is geconfigureerd, zodat u na de upgrade naar versie 3.0 de webBridge

en webBridgeProfiles in de API dienovereenkomstig kunt configureren.



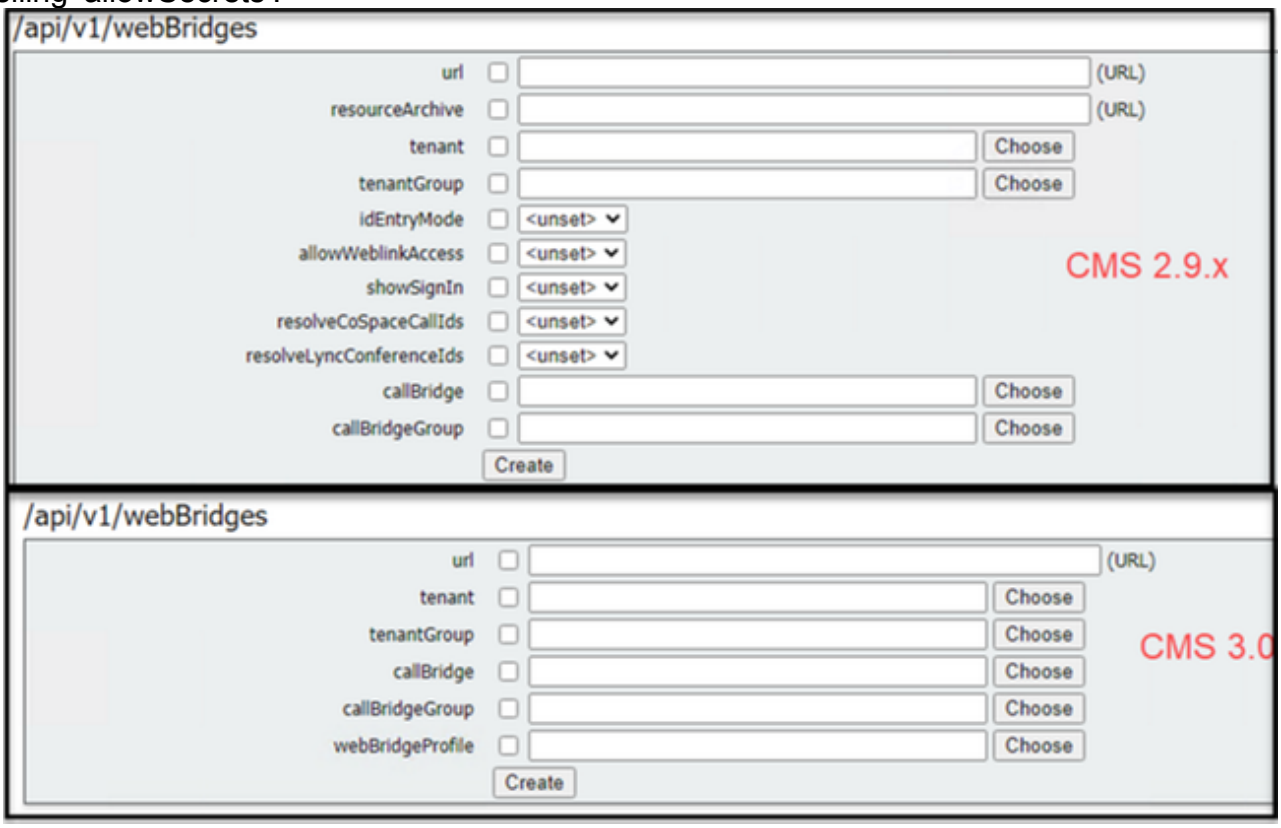
In 3.0 werden **de** bruginstellingen van het **Web** op de GUI verwijderd, dan in CMS 3.1, zijn de **Externe** toegangsvelden eveneens verwijderd.

webBridge-instellingen in GUI

- **Guest account client URI** – werd door de callBridge gebruikt om de webBridge te vinden. Als u meerdere webBridges in uw implementatie voor WebRTC had, moet dit veld al leeg zijn en moet u unieke URL's in api/v1/webbridges hebben voor elke webBridge waarmee de callBridge verbinding moet maken. Verwijdert alles in dit veld en zorg ervoor dat u de webBridges hebt geconfigureerd in de API.

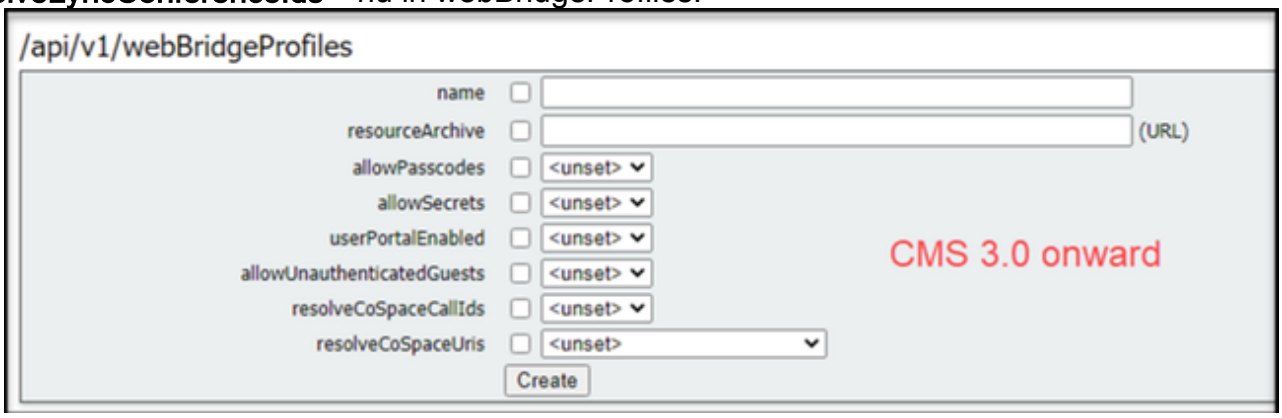
- **Guest Account JID Domain** – wordt niet meer gebruikt in CMS 3.0 en u kunt dit verwijderen.
- **Guest access via ID and passcode** – is verwijderd en wordt niet vervangen in CMS 3.0.
- **Guest access via hyperlinks** – is nu configureerbaar onder webBridgeProfiles in de API via de

instelling ‘allowSecrets’.



In CMS 3.0 zijn diverse velden verwijderd uit API/v1/webBridges.

- **resourceArchive** – nu in webBridgeProfiles.
- **idEntryMode** – nu afgeschaft.
- **allowWeblinkAccess** – nu in webBridgeProfiles als allowSecrets.
- **showSignIn** – nu in webBridgeProfiles als userPortalEnabled.
- **resolveCoSpaceCallIds** – nu in webBridgeProfiles.
- **resolveLyncConferenceIds** – nu in webBridgeProfiles.



<u>webBridgeProfile</u>

- **resourceArchive** – als u aangepaste achtergronden gebruikt en uw bronarchief op een webserver is opgeslagen, voer dan hier de URL in.
- **allowPasscodes** – indien ingesteld op ‘false’ kunnen gebruikers niet als gasten aan vergaderingen deelnemen. Ze kunnen zich alleen aanmelden of een URL gebruiken dat de ruimtegegevens en het geheim bevat.
- **allowSecrets** - Als dit is ingesteld op false, kunnen gebruikers zich niet aanmelden met spaties met een URL zoals

https://meet.company.com/meeting/040478?secret=gPDnucF8is4W1cS87_l.zw. Gebruikers moeten https://meet.company.com gebruiken en de callId/meetingId/URI en PIN/Passcode invoeren als deze is geconfigureerd.

- **userPortalEnabled** - als dit is ingesteld op false, de web app portal landing page toont niet de inlogoptie. Het toont slechts de velden voor het invoeren van de Call ID/Meeting ID/URI en PIN/Passcode als men is geconfigureerd.
- **allowUnauthenticatedGasten** - indien ingesteld op False, kunnen gasten niet deelnemen aan enige vergaderingen - zelfs met de volledige URL die de vergadering-ID en geheim bevat. Wanneer Vals, slechts kunnen de gebruikers die binnen kunnen ondertekenen zich bij een vergaderingen aansluiten. Voorbeeld. Gebruiker2 probeert de URL te gebruiken voor de vergadering van Gebruiker1. Na het invoeren van de URL moet Gebruiker2 zich aanmelden om aan de vergadering van Gebruiker1 deel te nemen.
- **resolveCoSpaceCallIds** – indien ingesteld op 'false' kunnen gasten alleen aan vergaderingen deelnemen door de URI en PIN/Passcode in te voeren, waar van toepassing. callId/meetingId/numericId worden niet geaccepteerd.
- **resolveCoSpaceUris** – drie mogelijke instellingen: off, domainSuggestionDisabled en domainSuggestionEnabled. Deze geven aan of deze webBridge coSpace en coSpaceAccessMethod SIP-URI's accepteert om bezoekers toe te staan deel te nemen aan coSpace-vergaderingen.

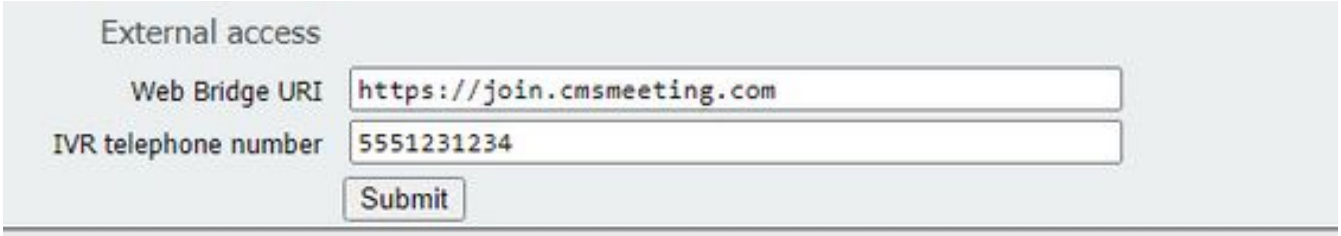
– Wanneer deze parameter is ingesteld op '*off*', is deelnemen via URI uitgeschakeld.

- Wanneer dit item wordt ingesteld op '*domainSuggestieDisabled*', wordt het domein van de URI ingeschakeld, maar wordt het niet automatisch ingevuld of geverifieerd op webBridges met behulp van dit webBridgeProfile.

– Wanneer deze parameter is ingesteld op '*domainSuggestionEnabled*', is deelname via URI ingeschakeld en wordt het domein van de URI automatisch aangevuld en geverifieerd op webBridges die dit webBridgeProfile gebruiken.

Sectie 'External access' (Externe toegang) verwijderd uit web-GUI

In CMS 3.1 is de sectie 'External access' (Externe toegang) verwijderd uit de web-GUI. Als u de externe toegang voorafgaand aan de upgrade had geconfigureerd, moet u deze in de API opnieuw configureren onder webBridgeProfiles.



Eerst moet u een webbridgeProfile maken zoals beschreven in de vorige sectie. Nadat u een webBridgeProfile heeft gemaakt, kunt u een IVR-nummer en/of Web Bridge URI maken via de links die in de API beschikbaar zijn onder het nieuwe webBridgeProfile.

U kunt maximaal 32 IVR-nummers of 32 webBridgeAdresses maken per webBridgeProfile.

Opnemen of streamen

De componenten recorder en streamer in CMS 2.9.x en lager waren XMPP-clients. Vanaf CMS 3.0 zijn deze SIP-gebaseerd. Hierdoor kunnen lay-outs voor opnemen en streamen worden gewijzigd op basis van de standaardversie in de API. Ook worden nu naamlabels getoond tijdens de sessie voor opnemen/streamen. Zie CMS 3.0 release-opmerkingen voor meer informatie over de functies voor opnemen/streamen: 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.

Als u in CMS 2.9.x een recorder of streamer heeft geconfigureerd, moet u de instellingen in de MMP en de API opnieuw configureren zodat deze na de upgrade blijven werken.

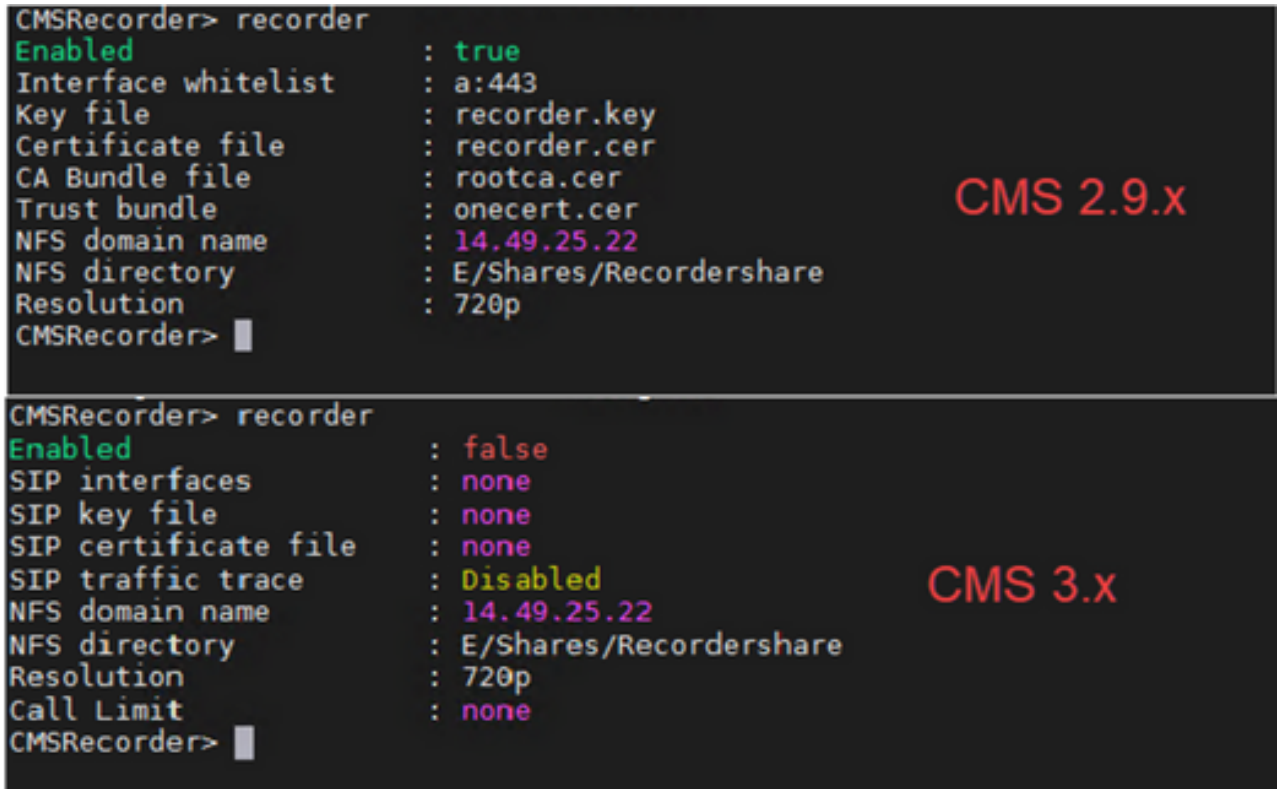
Voorafgaand aan de CMS-upgrade naar versie 3.0 is het raadzaam een back-up te maken met de opdracht ‘backup snapshot <servername_date>’ en vervolgens in te loggen bij de pagina webadmin op uw callBridge-knooppunten om alle XMPP-instellingen te verwijderen. Maak vervolgens verbinding met de MMP op uw servers en voer de volgende stappen uit op alle Core-servers met een SSH-verbinding:

1. **xmpp disable**
2. **xmpp reset**
3. **xmpp certs none**
4. **xmpp domain none**

Recorder

MMP

De afbeeldingen tonen een voorbeeld van de configuratie van de recorder in CMS 2.9.1 en hoe een en ander eruit ziet na de upgrade naar versie 3.0.



Na de upgrade moet u de recorder opnieuw configureren:

Stap 1. Configureer de SIP-luisterinterface.

recorder sip listen a 5060 5061 (De interface en poorten die zijn ingesteld voor de SIP-recorder om respectievelijk te luisteren naar TCP en TLS. Als u geen TLS wilt gebruiken, kunt u '**recorder sip listen a 5060 none**' gebruiken)

Stap 2. Configureer de certificaten die de recorder gebruikt als u een TLS-verbinding gebruikt.

recorder sip certs <key-file> <crt-file> [crt-bundle] (Zonder deze certificaten wordt de TLS-service niet gestart op de recorder. De recorder gebruikt de CRT-bundel om het callBridge-certificaat te verifiëren.)

Stap 3. Configureer de gesprekslimiet.

recorder limit <0-500|none> (Hiermee wordt het maximale aantal gelijktijdige opnamen ingesteld dat de server kan ondersteunen. Deze tabel is opgenomen in onze documentatie en de limiet voor de recorder moet worden afgestemd op de bronnen van de server.)

Table 6: Internal SIP recorder performance and resource usage

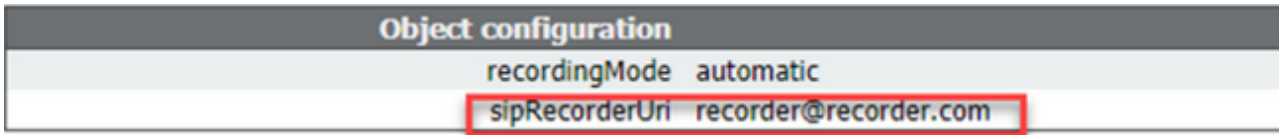
Recording Setting	Recordings per vCPU	RAM required per recording	Disk budget per hour	Maximum concurrent recording
720p	2	0.5GB	1GB	40
1080p	1	1GB	2GB	20
audio	16	100MB	150MB	100

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

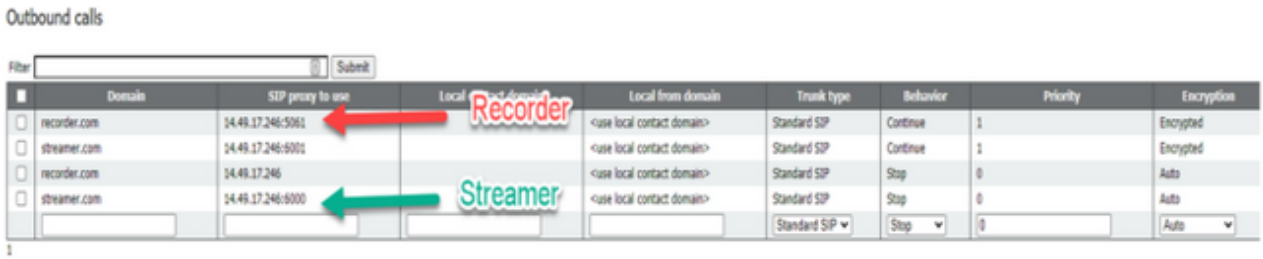
- Performance scales linearly adding vCPUs up to the number of host physical cores.

API

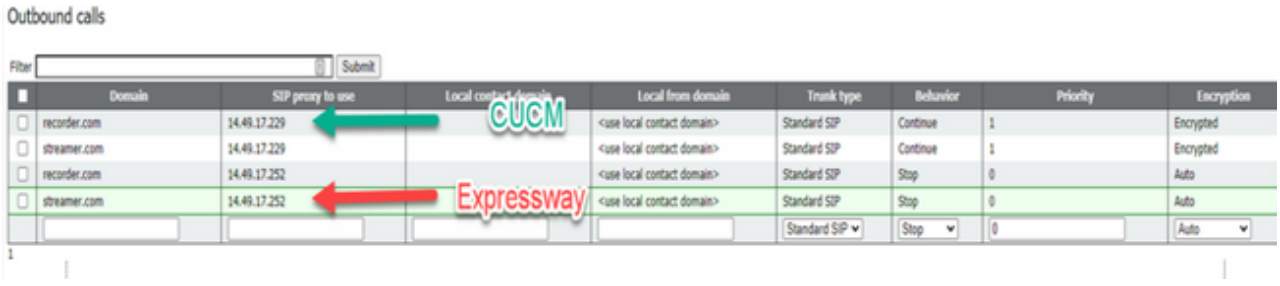
Op api/v1/callProfiles moet u de **sipRecorderUri** configureren. Dit is de URI die de callBridge aanroept wanneer een opname moet worden gestart. Het domein van deze URI moet aan uw tabel met uitgaande regels worden toegevoegd en naar de recorder (of gespreksbeheer) verwijzen als de te gebruiken SIP-proxy.



In deze afbeelding wordt een directe aanroep naar de component recorder getoond op basis van de uitgaande regels in **Configuration —> Outbound Calls** (Configuratie —> Uitgaande oproepen).



Deze afbeelding toont een oproep naar de component recorder via gespreksbeheer (zoals Cisco Unified Communications Manager (CUCM) of Expressway).



Opmerking: Als de recorder is geconfigureerd op het gebruik van SIP-TLS en oproepen vervolgens mislukken, controleer dan uw callBridge-knooppunt in MMP om na te gaan of TLS-SIP-verificatie is ingeschakeld. De MMP-opdracht is '**tls sip**'. Oproepen mislukken wellicht omdat het certificaat van de recorder niet wordt vertrouwd door de callBridge. U kunt dit testen door dit op de callBridge uit te schakelen met de opdracht '**tls sip verify disable**'.

Meerdere recorders?

Configureer elke individueel zoals beschreven en pas de uitgaande regels dienovereenkomstig aan. Als u een directe methode voor recorder gebruikt, wijzigt u de bestaande uitgaande regel om recorder regel te wijzigen in gedrag "Doorgaan" en voegt u een nieuwe uitgaande regel toe onder de vorige met de prioriteit minder dan de eerste. Wanneer de eerste recorder zijn call-limiet heeft bereikt, stuurt het een 488 Unacceptabele hier terug naar callBridge, en de callBridge beweegt zich naar de volgende regel.

Als u taken over de recorders wilt verdelen, pas dan de routing van gespreksbeheer zo aan dat oproepen bij meerdere recorders kunnen worden geplaatst.

Streamer

MMP

Na de upgrade van versie 2.9.x naar versie 3.0 moet u de streamer opnieuw configureren.

Stap 1. Configureer de SIP-luisterinterface.

streamer sip listen a 6000 6001 (De interface en poorten die zijn ingesteld voor de SIP-streamer om respectievelijk te luisteren naar TCP en TLS. Als u geen TLS wilt gebruiken, kunt u '**streamer sip listen a 6000 none**' gebruiken)

Stap 2. Configureer de certificaten die de streamer gebruikt als u een TLS-verbinding gebruikt.

streamer sip certs <key-file> <crt-file> [crt-bundle] (Zonder deze certificaten wordt de TLS-service niet gestart op de streamer. De streamer gebruikt CRT-bundel om het callBridge-certificaat te verifiëren.)

Stap 3. Configureer de gesprekslimiet.

streamer limit <0-500|none> (Hiermee wordt het maximale aantal gelijktijdige streams ingesteld dat de server kan ondersteunen. Deze tabel is opgenomen in onze documentatie en de limiet voor de streamer moet worden afgestemd op de bronnen van de server.)

Table 7: Internal SIP streamer recommended specifications

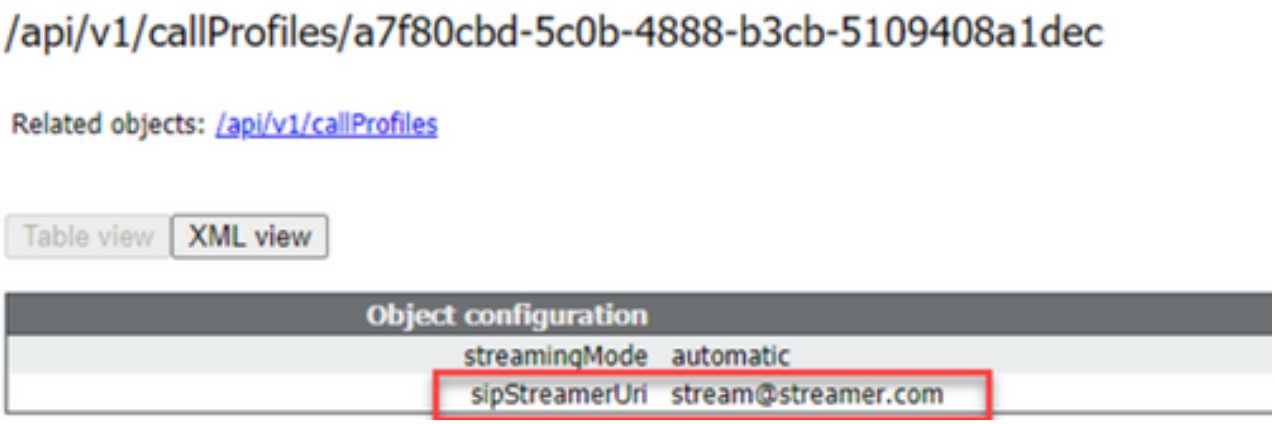
Number of vCPUs	RAM	Number of 720p streams	Number of 1080p streams	Number of audio-only streams
4	4GB	50	37	100
4	8GB	100	75	200
8	8GB	200	150	200

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

Op api/v1/callProfiles moet u de **sipStreamUri** configureren. Dit is de URI die de callBridge aanroept wanneer streaming moet worden gestart. Het domein van deze URI moet aan uw tabel met uitgaande regels worden toegevoegd en naar de streamer (of gespreksbeheer) verwijzen als de te gebruiken SIP-proxy.



In deze afbeelding wordt een directe aanroep naar de component streamer getoond op basis van de uitgaande regels in **Configuration —> Outbound Calls** (Configuratie —> Uitgaande oproepen).

Deze afbeelding toont een oproep naar de component recorder via gespreksbeheer (zoals Cisco Unified Communications Manager (CUCM) of Expressway).

Opmerking: Als de streamer is geconfigureerd voor het gebruik van SIP-TLS en oproepen vervolgens mislukken, controleer dan uw callBridge-knooppunt in MMP om na te gaan of TLS-SIP-verificatie is ingeschakeld. De MMP-opdracht is '**tls sip**'. Oproepen mislukken wellicht omdat het certificaat van de streamer niet wordt vertrouwd door de callBridge. U kunt dit testen door dit op de callBridge uit te schakelen met de opdracht '**tls sip verify disable**'.

Meerdere streamers?

Configureer elke individueel zoals beschreven en pas de uitgaande regels dienovereenkomstig aan. Als u een directe methode gebruikt om de methode te stroomlijnen, verander de bestaande uitgaand om recorder regel naar gedrag "Doorgaan" en voeg een nieuwe uitgaande regel toe

onder de vorige met de prioriteit minder dan de eerste. Wanneer de eerste streamer zijn oproeplimiet heeft bereikt, stuurt hij een 488 Unacceptabele terug naar callBridge, en de callBridge gaat naar de volgende regel.

Als u taken over de streamers wilt verdelen, pas dan de routing van gespreksbeheer zo aan dat oproepen bij meerdere streamers kunnen worden geplaatst.

Overweging snelweg

Als u Cisco Expressway voor webproxy gebruikt, moet u ervoor zorgen dat Expressway ten minste X12.6 gebruikt voorafgaand aan de CMS-upgrade. Dit is in CMS 3.0 vereist voor werking en ondersteuning van webproxy.

De capaciteit voor webapp-deelnemers via Expressways neemt toe in combinatie met CMS 3.0. Voor een grote OVA Expressway is de verwachte capaciteit 150 Full HD-oproepen (1080p30) of 200 andere typen oproepen (bijvoorbeeld 720p30). U kunt deze capaciteit vergroten door Expressways te clusteren, maximaal 6 knooppunten (4 voor schaling en 2 voor redundantie: maximaal 600 Full HD-oproepen of 800 andere typen oproepen).

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 Edge

CMS Edge wordt opnieuw geïntroduceerd in CMS 3.1 omdat deze een hogere capaciteit biedt dan de Expressway voor externe webapp-sessies. Er zijn twee aanbevolen configuraties.

Specificatie van kleine edge-server

4 GB RAM, 4 vCPU's, **1 Gbps** netwerkinterface

Deze VM-edge-server levert voldoende audio- en videolaadvermogen voor één CMS1000: 48 x 1080p, 96 x 720p, 192 x 480p en 1000 audio-oproepen.

Voor de implementatie wordt aanbevolen om per CMS1000-applicatie 1 kleine edge-server en per CMS2000-applicatie 4 kleine edge-servers aan te houden.

Specificatie van grote edge-server

8 GB RAM, 16 vCPU's, **10 Gbps** netwerkinterface

Deze VM-edge-server levert voldoende audio- en videolaadvermogen voor één CMS2000: 350 x 1080p, 700 x 720p, 1000 x 480p en 3000 audio-oproepen.

Voor de implementatie wordt aanbevolen om 1 grote edge-server per enkele CMS2000-applicatie of per 4 CMS1000-applicaties aan te houden.

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.