Orientación para una actualización sin inconvenientes de Cisco Meeting Server 2.9 a 3.0 (y versiones posteriores)

Contenido

Introducción

Este documento describe los desafíos de actualizar una implementación de Cisco Meeting Server que ejecuta la versión 2.9 (o anterior) a la 3.0 (o posterior) y cómo manejarlos para un proceso de actualización fluido.

Funciones eliminadas: se eliminó XMPP (que afecta a WebRTC), trunks/equilibradores de carga, webbridge

Funciones cambiadas: los grabadores y las transmisiones ahora son SIP, y webbridge se sustituye por webbridge3

Este documento sólo trata temas que debe tener en cuenta antes de actualizar. No cubre todas las nuevas funciones disponibles en 3.X.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- administración de CMS
- Actualizaciones de CMS
- Creación y firma de certificados

Todo lo que aquí se menciona está esbozado en varios documentos. Siempre es recomendable leer las notas de la versión del producto y consultar nuestras guías de programación e implementación si necesita más información sobre las funciones: Guías de instalación y configuración de CMS y Notas de la versión del producto de CMS.

Componentes Utilizados

La información de este documento se basa en Cisco Meeting Server.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento sirve de guía en caso de que ya tenga una implementación de CMS 2.9.x (o anterior), independientemente de si es única, combinada o resistente, y cuando planee actualizar a CMS 3.0. La información de este documento pertenece a todos los modelos de CMS.

Nota: La serie X no se puede actualizar a CMS 3.0. Debe planificar la sustitución de los servidores de la serie X lo antes posible.

Información importante sobre las actualizaciones

El único método admitido para actualizar CMS es una actualización escalonada. En el momento de escribir esto, CMS 3.5 ha sido lanzado. Si está en CMS 2.9, debe actualizar de forma escalonada (2.9 —> 3.0 —> 3.1 —> 3.2 —> 3.3 —> 3.4 —> 3.5 (Tenga en cuenta que el proceso de actualización tiene cambios desde CMS 3.5, por lo que debe leer atentamente las notas de la versión!!)

Si no realiza una actualización escalonada y experimenta un comportamiento inusual, el TAC podría solicitarle una reversión y empezar de nuevo.

Además, a partir de CMS 3.4, CMS DEBE utilizar Smart Licensing. No puede actualizar a CMS 3.4 o posterior y seguir utilizando licencias tradicionales. No actualice a CMS 3.4 o posterior a menos que haya configurado Smart Licensing.

Resumen de cosas a considerar

Utilice estas preguntas para desplazarse a las secciones relacionadas con su propia situación. Cada consideración se refiere a un hipervínculo a una descripción más detallada presentada en este documento.

Licencias

¿Dispone de suficientes licencias Personal MultiParty (PMP)/Shared MultiParty (SMP) en sus servidores antes de la actualización?

En la versión 3.0 se asignan las licencias de PMP, incluso si el usuario no ha iniciado sesión. Por ejemplo, si ha importado 10000 usuarios a través de LDAP, pero sólo tiene 100 licencias de PMP, esto le dejará sin cumplimiento tan pronto como actualice a 3.0. Para este caso de uso, asegúrese de verificar si los inquilinos tienen definido un perfil de usuario y/o un sistema/perfiles para ver si un perfil de usuario con tiene una licencia con un valor de true está configurado.

En esta sección se explica con más detalle cómo comprobar el perfil de usuario en la API y ver si tieneLicense=true set (es decir, usuarios con licencia de PMP).

¿Dispone de licencias PMP/SMP en su archivo cms.lic actual?

Debido a los cambios en el comportamiento de la licencia a partir de la versión 3.0, debe confirmar si dispone de suficientes licencias PMP/SMP antes de realizar la actualización. Esto se describe con más detalle en esta sección.

¿Tiene implementado Cisco Meeting Manager (CMM)?

CMS 3.0 requiere CMM 3.0 debido a los cambios en la forma en que se gestionan las licencias. Se recomienda implementar CMM 2.9 antes de realizar una actualización de su entorno a 3.0, ya que puede comprobar su informe de 90 días para ver si ha consumido licencias durante los últimos 90 días. Esto se describe con más detalle en esta sección.

¿Dispone de Smart Licensing?

CMS 3.0 requiere CMM 3.0 debido a los cambios en la forma en que se gestionan las licencias. Por lo tanto, si ya utiliza Smart Licensing a través de CMM, asegúrese de que tiene licencias PMP y SMP asociadas al clúster.

Webbridge (cliente WebRTC y CMA)

¿Utiliza WebRTC en CMS 2.9?

Webbridge ha cambiado significativamente en CMS 3.0. Para obtener orientación sobre la migración de webbridge2 a webbridge3 y el uso de la aplicación web, la información se encuentra en esta sección.

¿Utilizan sus usuarios el cliente pesado CMA?

Como estos clientes están basados en XMPP, estos clientes ya no se pueden utilizar después de la actualización, ya que el servidor XMPP se ha eliminado. Si esto es aplicable a su caso práctico, puede encontrar más información en esta sección.

¿Utiliza el chat en WebRTC?

La funcionalidad de chat se elimina de la aplicación web en 3.0. En CMS 3.2, el chat se vuelve a introducir, pero no es persistente. Puede encontrar más información sobre esta función en esta sección.

¿Realizan los usuarios llamadas punto a punto desde WebRTC a los dispositivos?

En CMS 3.0, un usuario de una aplicación web ya no puede marcar directamente a otro dispositivo. Ahora debe unirse a un espacio de reunión y tener permiso para agregar participantes a la reunión para realizar la misma acción. Puede encontrar más información sobre esta parte en esta sección.

¿Crean sus usuarios sus propios coSpaces a partir de WebRTC?

En la versión 3.0, para que los usuarios de aplicaciones web puedan crear sus propios espacios desde el cliente, se debe crear una plantilla coSpaceTemplate en la API y asignarla al usuario. Puede ser manual o automático durante la importación LDAP. CanCreateCoSpaces se elimina de UserProfile. Puede encontrar más información sobre esta función en esta sección.

Cambios de GUI web

¿Tiene los parámetros de webBridge configurados en la GUI de administración web?

Los ajustes de webBridge se eliminan de la GUI en 3.0, por lo que debe configurar los webbridges en la API y tener en cuenta cuáles son sus ajustes actuales en la GUI para que pueda configurar los webBridgeProfiles en la API en consecuencia. Puede encontrar más información sobre este cambio en esta sección.

¿Dispone de parámetros externos configurados en la GUI de administración web?

La configuración externa se ha eliminado de la GUI en CMS 3.1. Si tiene la URL de Webbridge o la IVR configurada en CMS 3.0 o en una GUI de administración web anterior (Configuration —> General —> External Settings), se han eliminado de la página web y ahora deben configurarse en la API. La configuración anterior antes de actualizar a 3.1 NO se agrega a la API y debe realizarse manualmente. Puede encontrar más información sobre este cambio en esta sección.

Grabadores/Streamers

¿Utiliza actualmente algún grabador o transmisores de CMS?

El grabador CMS y el componente de transmisión ahora se basan en SIP en lugar de en XMPP. Por lo tanto, a medida que se elimina el XMPP, es necesario modificarlo después de la actualización. Puede encontrar más información sobre este cambio en esta sección.

Consideraciones sobre Cisco Expressway

¿Cuál es su versión actual de Cisco Expressway si utiliza Expressway para proxy WebRTC?

CMS 3.0 requiere Expressway 12.6 o posterior. Puede encontrar más información sobre esta función de proxy de WebRTC en esta sección.

Perímetro CMS

¿Tiene actualmente un CMS Edge en su entorno?

CMS Edge se vuelve a introducir en CMS 3.1 con mayor escalabilidad para conexiones externas. Puede encontrar más información sobre esta parte en esta sección.

CMS (Acano) serie X

¿Tiene actualmente servidores de la serie x en su entorno?

Estos servidores no se pueden actualizar a CMS 3.0 y debe plantearse sustituirlos pronto (cambie a una máquina virtual o a un dispositivo CMS antes de actualizar a 3.0). Puede encontrar el aviso de fin de vida útil de estos servidores en este enlace.

Perímetro SIP

¿Utiliza actualmente SIP Edge en su entorno?

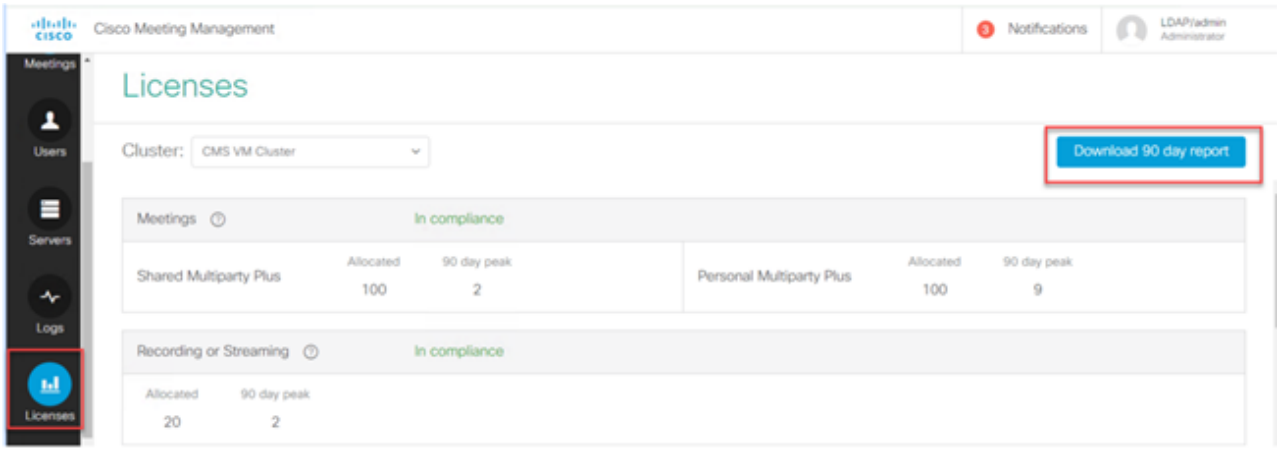
Sip Edge está totalmente obsoleto desde CMS 3.0. Debe usar Cisco Expressway para llevar las llamadas SIP a su CMS. Póngase en contacto con su representante de cuentas de Cisco para obtener Expressway para su organización.

Más información

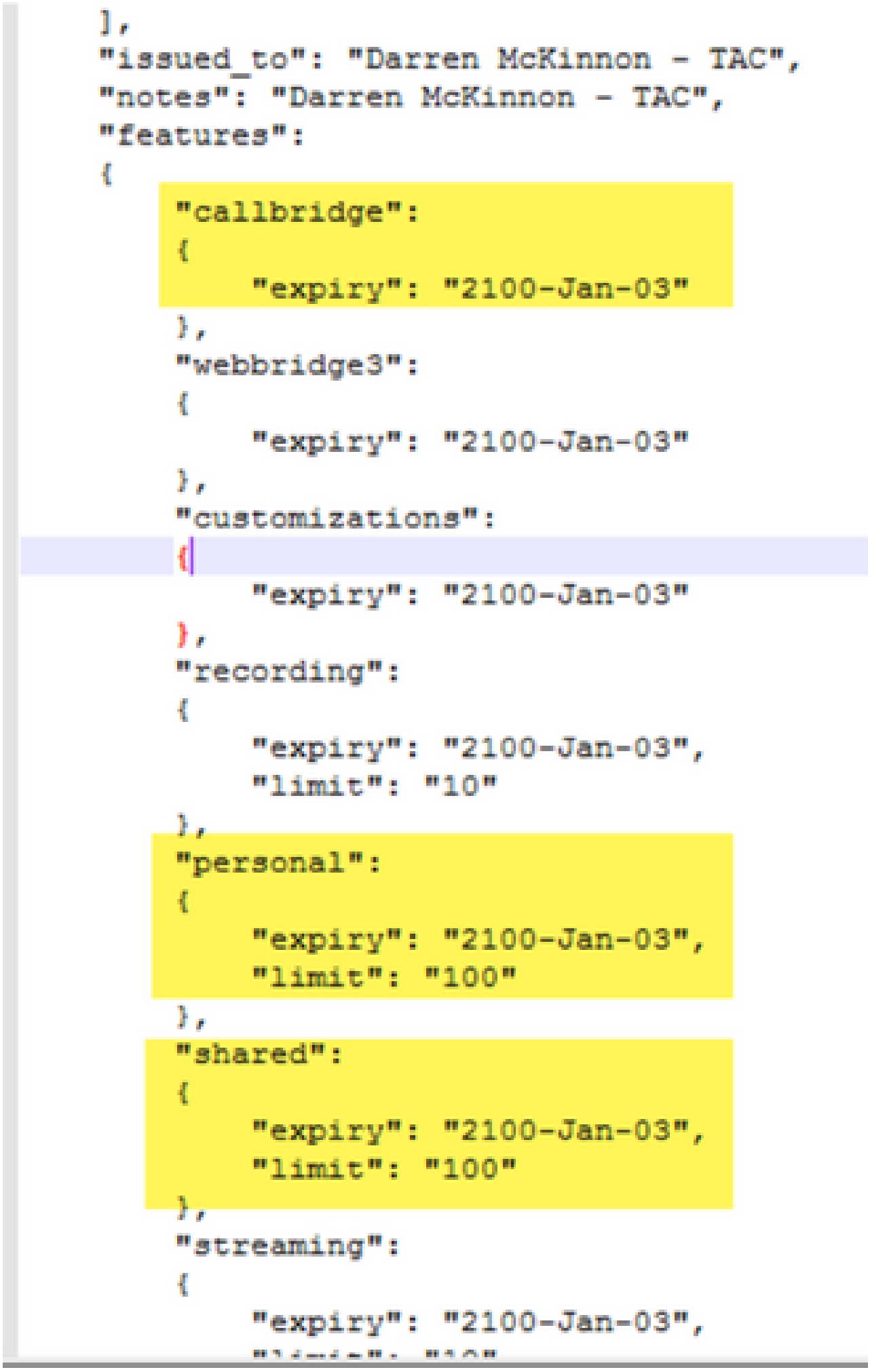
Licencias: comprobar las licencias antes de la actualización

El estado de la licencia sin cumplimiento es el problema más importante al actualizar a 3.0 o superior desde una versión 2.x. En esta sección se describe cómo determinar la cantidad de licencias PMP/SMP que necesita para realizar una actualización sin problemas.

Antes de actualizar su implementación a 3.0, implemente CMM 2.9 y verifique el informe de 90 días en la pestaña Licencias para ver si el uso de la licencia permaneció por debajo de la cantidad de licencia asignada actualmente en los nodos CMS:



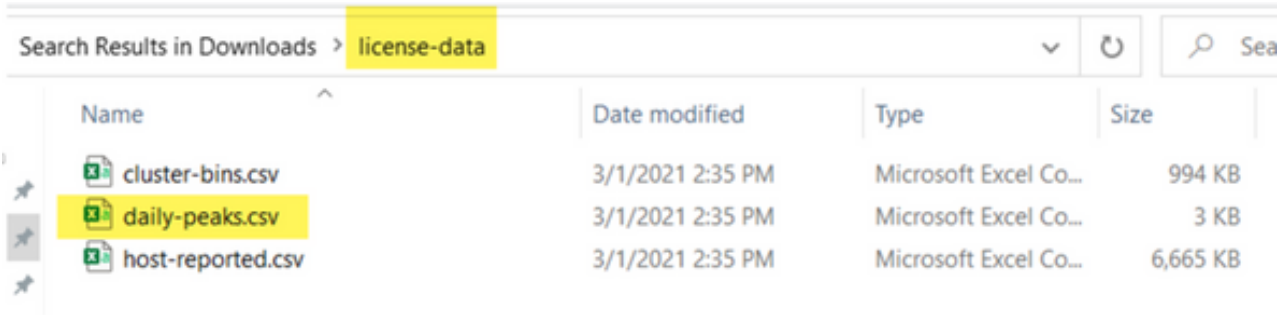
Si utiliza la licencia tradicional (el archivo cms.lic se instala localmente en los nodos CMS), compruebe en el archivo de licencia CMS las cantidades de licencias personales y compartidas (100 / 100 según la imagen que aparece aquí) en cada uno de los nodos CMS (descargue a través de WinSCP desde cada nodo de callBridge).



Si ya utiliza Smart
Licensing

, compruebe cuántas licencias PMP/SMP se asignan en el portal inteligente de software de Cisco para los servidores CMS.

Abra el informe de 90 días (el archivo Zip se denomina license-data.zip) y abra el archivo daily-peaks.csv.



En Excel, ordene la columna PMP por Z a A para obtener los valores más altos en la parte superior y, a continuación, realice el mismo procedimiento para la columna SMP. ¿Son los valores que ve en este archivo inferiores a las licencias disponibles en el archivo de licencia de CMS? Si la respuesta es sí, está bien y cumple plenamente las normas. Si no es así, se crean advertencias o errores, como se indica en la figura 6 de la sección 1.7.3 de la guía de implementación de CMS, de la que también puede encontrar más información en la sección 1.7.4.

En cuanto a la imagen como ejemplo, se utilizaron 2.1667 licencias SMP y no se utilizaron licencias PMP durante el período máximo de los últimos 90 días. El archivo cms.lic indicó 100 unidades de cada tipo de licencia, por lo que esta configuración es totalmente compatible. Por lo tanto, no hay problemas con las licencias cuando esta configuración se actualiza a CMS 3.0. Sin embargo, todavía puede haber un problema cuando en la configuración se habrían importado 10,000 usuarios a través de LDAP. Como entonces solo tiene 100 licencias de PMP, pero asigna 10000 (con userProfile con hasLicense establecido en True), en este caso dejará de cumplir las normativas en cuanto actualice a 3.0. Más información al respecto en la siguiente sección.

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

Determine cuántos usuarios tienen asignada una licencia de PMP una vez que realiza la actualización

A todos los usuarios que se importan y utilizan un userProfile con hasLicense=true se les asigna automáticamente una licencia PMP en CMS 3.0.

En la API, verifique cuántos userProfiles tiene y verifique si alguno de ellos tiene configurado "hasLicense=true". Si es así, debe comprobar dónde están asignados esos perfiles de usuario.

Los perfiles de usuario se pueden asignar en cualquiera de estos niveles:

1. LdapSources
2. Arrendatarios
3. Sistema/perfiles

Verifique las 3 ubicaciones para los userProfiles asignados que tengan hasLicense=true.

1. LdapSources/Tenants

Para cada ldapSource que utilice un arrendatario o un userProfile, a los usuarios importados con ese ldapSource se les asignará una licencia PMP cuando el parámetro hasLicense se establezca en True. Si hay un arrendatario, debe hacer clic en el ID de arrendatario para ver si tiene

asignado un perfil de usuario y, a continuación, comprobar si ese perfil de usuario está configurado con 'hasLicense=true'. Si no hay ningún arrendatario, pero hay un conjunto userProfile, haga clic en él para ver si tiene 'hasLicense=true'. Si 'hasLicense=true' en cualquiera de los dos sentidos, puede comprobar cuántos usuarios se han importado realizando una operación GET para 'api/v1/users' y filtrando por el dominio utilizado para jidMapping en ldapmapping asociado a ldapSource, por ejemplo.

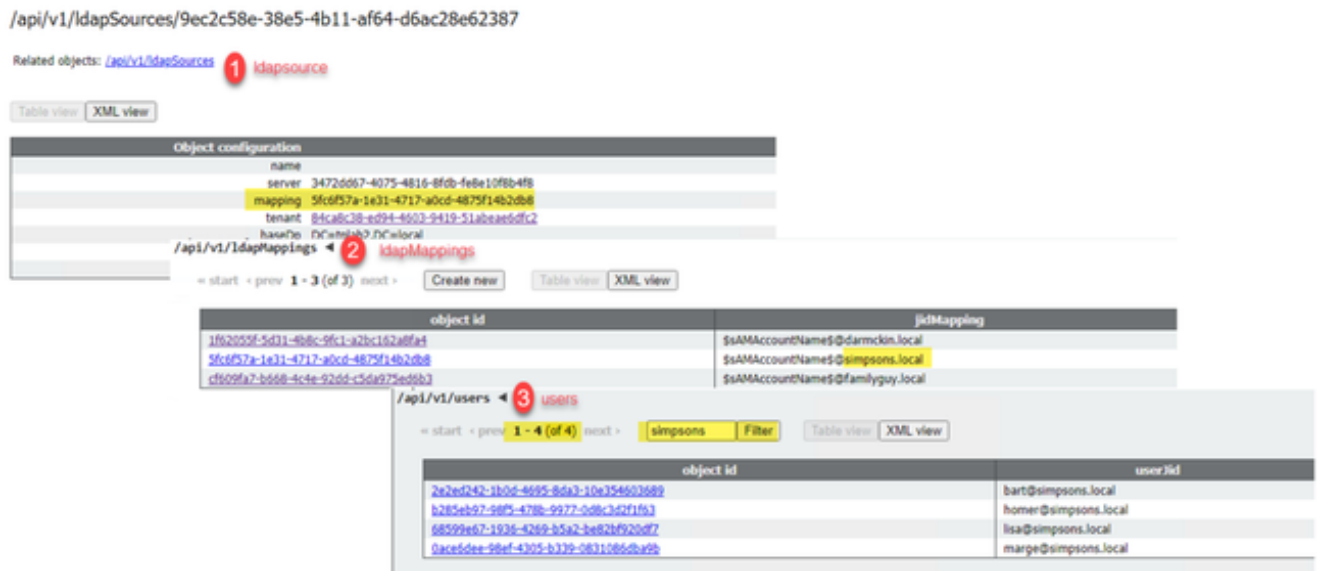
Nota: Esto puede ser más complejo en otras situaciones, en cuyo caso necesita verificar esto con las asignaciones y filtros de Active Directory que creó.

Paso 1. Busque el ID de asignación de ldapSource.

Paso 2. Busque ldapMappings para encontrar jidMapping.

Paso 3. Busque en api/v1/users el dominio utilizado en jidMapping.

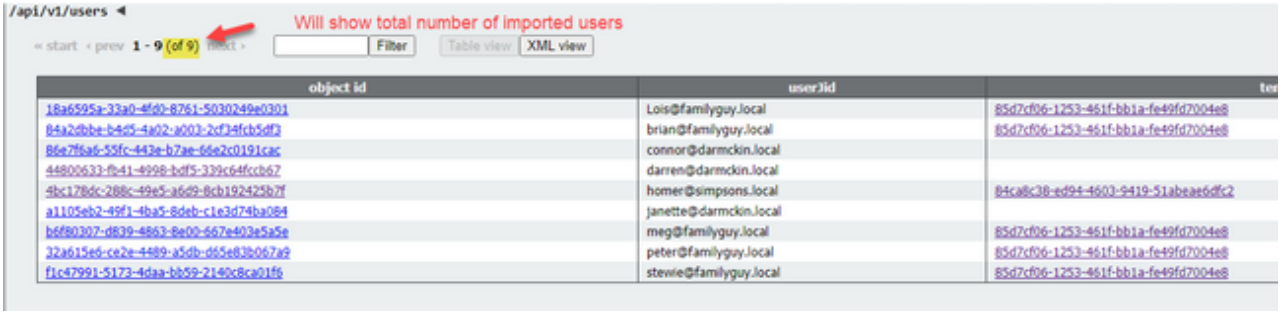
Paso 4. Sume los usuarios encontrados de cada ldapSource. Este es el número de usuarios LDAP importados que necesitan licencias PMP.



2. Sistema/Perfiles

Si un userProfile se establece en el nivel de sistema/perfiles y dicho userProfile tiene "hasLicense=true", a cualquier usuario importado a CMS se le asignará una licencia PMP cuando se actualice el servidor. Si importó 10 000 usuarios pero sólo tiene 100 PMP, esto provoca que no cumpla las normas cuando actualice a CMS 3.0 y puede hacer que aparezca un mensaje en pantalla de 30 segundos y un mensaje de audio al inicio de las llamadas.

Si userProfile en el nivel del sistema indica que los usuarios van a obtener un PMP, vaya a api/v1/users para ver cuántos usuarios hay en total:



Si previamente había importado todos los usuarios de su ldap, pero ahora se da cuenta de que sólo necesita un cierto subconjunto de esa lista, cree un filtro mejor en su ldapSource para que importe sólo los usuarios a los que desea que se le asignen licencias PMP. Revise su filtro en ldapSource y luego realice una nueva sincronización LDAP en api/v1/ldapsync. De este modo, sólo se importarán los usuarios deseados y se eliminarán todos los demás usuarios de la importación anterior.

✎ Nota: Si lo hace correctamente y la nueva importación solo elimina usuarios no deseados, los usuarios restantes de coSpace CallIDs y secretos no cambian, pero si comete un error, esto puede dar lugar a que todos los callID y secretos cambien. Realice una copia de seguridad de los nodos de la base de datos antes de intentarlo si le preocupa esto.

¿Dispone de suficientes licencias SMP?

Cuando analizaba los picos diarios del informe de 90 días de CMM, ¿ya dispone de suficientes licencias de SMP para cubrir su pico máximo? Las licencias de SMP se utilizan cuando al propietario de la reunión no se le ha asignado una licencia de PMP (como propietario de coSpace, reunión ad-hoc o reunión programada de TMS). Si está usando SMP intencionalmente y tiene suficiente para cubrir sus horas pico, entonces todo esto está bien. Si verifica el pico de 90 días para SMP y no está claro por qué se consumen, aquí hay algunas cosas que debe verificar.

1. Las llamadas ad hoc (según se derivan de CUCM) utilizan una licencia SMP si el dispositivo utilizado para la fusión no está asociado a un usuario al que se ha asignado una licencia PMP en CMS a través del perfil de usuario. CUCM proporciona el GUID del usuario que va a escalar la reunión. Si ese GUID corresponde a un usuario LDAP importado de Meeting Server con una licencia PMP asignada, se utilizará la licencia de ese usuario.

2. Si a un propietario de coSpace no se le ha asignado una licencia PMP, las llamadas a esos coSpaces en particular utilizan una licencia SMP.

3. Si la reunión se programó en la versión 15.6 de TMS o posterior, el propietario de la reunión se envía a CMS y, si a ese usuario no se le asignó una licencia PMP, la reunión usará una licencia SMP.

Configurar CMM

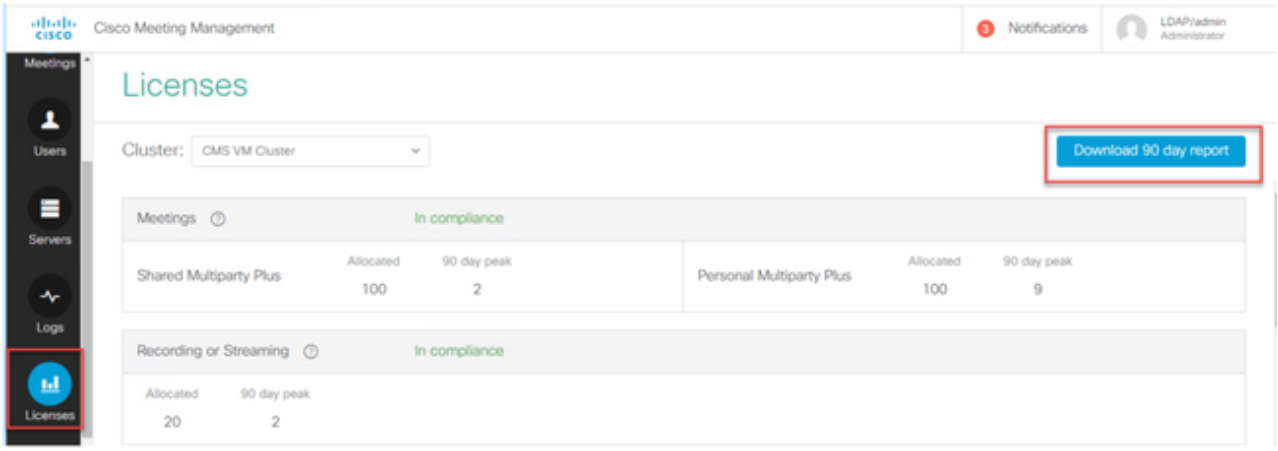
A partir de CMS 3.0, CMS 3.0 es necesario para que CMS funcione correctamente. CMM es responsable de la licencia de CMS, por lo que si planea actualizar CMS a 3.0, debe tener un

servidor CMM. Se recomienda implementar CMM 2.9 mientras se está en CMS 2.9 para poder comprobar el consumo de licencias antes de actualizar.

CMM verifica todos los CallBridges agregados para las licencias SMP y PMP y la licencia de callBridge. Utiliza el número más alto en los distintos dispositivos del clúster.

Por ejemplo, si CMS1 tiene 20 licencias PMP y 10 SMP y CMS2 tiene 40 licencias PMP y 5 SMP en las licencias tradicionales, CMM indica que tiene que utilizar 40 licencias PMP y 10 SMP.

Si tiene más licencias de PMP que usuarios importados, no tiene ningún problema relacionado con las licencias de PMP (o SMP), pero si comprueba ese pico de 90 días y descubre que utilizó más de lo disponible, todavía puede actualizar a CMS 3.0 y utilizar la licencia de prueba de 90 días en CMM para solucionar los problemas con su licencia o tomar medidas antes de la actualización.



Configuración de Webbridge (cliente WebRTC y CMA)

CMS 3.0 elimina el componente de servidor XMPP y, con ello, elimina webBridge y la capacidad de utilizar el cliente pesado CMA. WebBridge3 es lo que se utiliza ahora para conectar a los usuarios de aplicaciones web (anteriormente conocidos como usuarios de WebRTC) a reuniones mediante el navegador. Cuando actualice a 3.0, debe configurar webbridge3.

Nota: el cliente pesado de CMA no funciona después de actualizar a CMS 3.0.

Este vídeo le guía a través del proceso de creación de los certificados de webbridge 3.

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

Antes de la actualización a 3.0, los clientes deben planificar cómo configurar Webbridge3. Los pasos más importantes se destacan aquí.

1. Necesita una llave y una cadena de certificados para webbridge3. El certificado de webbridge antiguo se puede utilizar si el certificado contiene todos los FQDN de servidor CMS o direcciones IP como Nombre alternativo del sujeto (SAN)/ Nombre común (CN) que ejecutan webbridge3 y si se cumple alguno de estos criterios:

a. El certificado no tiene uso mejorado de clave (lo que significa que se puede usar como cliente o servidor).

b. El certificado tiene autenticación de cliente y de servidor. El certificado HTTPs sólo necesita realmente la autenticación de servidor, mientras que el certificado C2W requiere tanto servidor como cliente).

2. Si desea crear un nuevo certificado para el certificado "webbridge3 https", se recomienda firmarlo públicamente (para evitar advertencias de certificado en el cliente al usar la aplicación web). Este mismo certificado se puede utilizar para el "certificado c2w de webbridge3" y el certificado debe tener el FQDN de los servidores de webbrige en SAN/CN.

3. CallBridges debe comunicarse con el nuevo webbridge3 mediante un puerto configurado en el comando webbridge3 c2w listen. Puede ser cualquier puerto disponible, como 449. Los usuarios deben asegurarse de que los callbridges puedan comunicarse con webbridge3 en este puerto y de que se realicen los cambios de firewall por adelantado, si es necesario. No puede ser el mismo puerto utilizado por "webbridge https" para escuchar.

Antes de la actualización de CMS a 3.0, se recomienda realizar una copia de seguridad mediante 'backup snapshot <servername_date>' y, a continuación, iniciar sesión en la página webadmin de los nodos de callbridge para eliminar toda la configuración de XMPP y Webbridge. A continuación, conéctese al MMP en sus servidores y realice estos pasos en todos los servidores Core que tienen xmpp y webbridge en una conexión SSH:

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

Una vez que actualice a 3.0, comience configurando webbridge3 en todos los servidores que anteriormente ejecutaban webbridge. Debe hacer esto porque ya hay registros DNS que apuntan a estos servidores, así que de esa manera se asegura de que si un usuario es enviado a un webbridge3, esté preparado para manejar la solicitud.

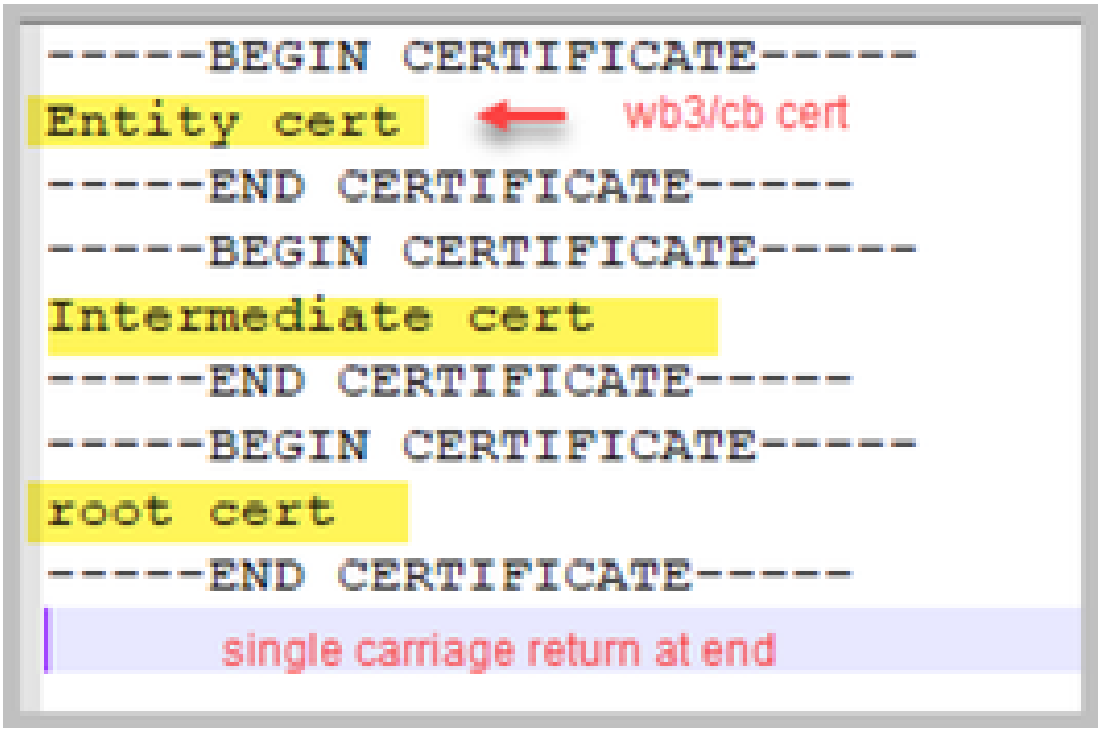
Configuración de Webbridge3 (en toda la conexión SSH)

Paso 1. Configure el puerto de escucha http de webbridge3.

Webbridge3 https listen a:443

Paso 2. Configure los certificados para webbridge3 para las conexiones del explorador. Este es el certificado enviado a los exploradores y debe estar firmado por una autoridad de certificación (CA) pública que contenga el FQDN utilizado en el explorador para que el explorador confíe en la conexión.

Webbridge3 https certs wb3.key wb3trust.cer (Esto debe ser una cadena de confianza: haga un certificado de confianza que tenga la entidad final en la parte superior, seguido por las CA intermedias en orden, terminando con la CA raíz).



Paso 3. Configure el puerto que se utilizará para escuchar las conexiones de callBridge a webbridge (c2w). Dado que 443 se utiliza para el puerto de escucha https de webbridge3, esta configuración debe ser un puerto disponible diferente como, por ejemplo, 449.

Webbridge3 c2w listen a:449

4. Configure los certificados que webbridge envía a callbridge para la confianza c2w

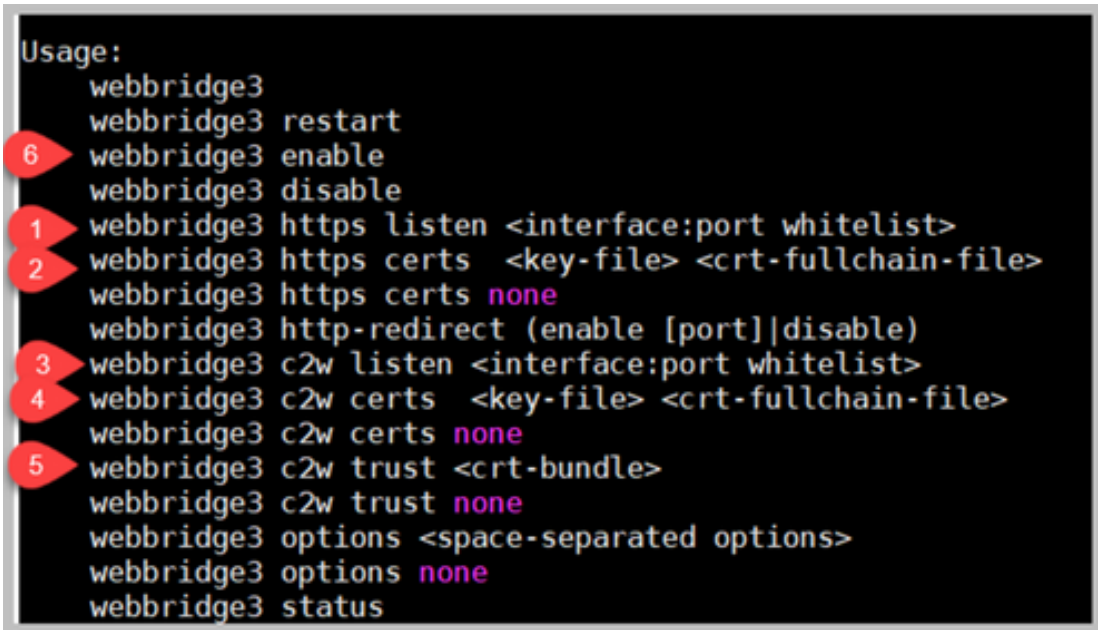
Webbridge3 c2w certs wb3.key wb3trust.cer

5. Configure el almacén de confianza que utiliza WB3 para confiar en el certificado de callBridge. Debe ser el mismo que el certificado utilizado en el conjunto de CA de callbridge (y debe ser un conjunto de certificados intermedios en la parte superior y una CA raíz al final, seguido de un único retorno de carro).

Webbridge3 c2w trust rootca.cer

6. Habilite webbridge3

Webbridge3 enable



Cambios en la configuración de CallBridge (en toda la conexión SSH)

Paso 1. Configure la confianza de callBridge con el certificado/conjunto de CA que firmó el certificado c2w de webbridge3.

Callbridge trust c2w rootca.cer

Paso 2. Reinicie el CallBridge para que la nueva confianza surta efecto. Esto descarta todas las llamadas en este callBridge en particular, así que utilícelo con precaución.

Callbridge restart

Configuración de API para que callBridges se conecte a webBridge3

1. Cree un nuevo objeto webBridge mediante POST en la API y asígnele un valor de URL mediante FQDN y un puerto configurado en la lista blanca de la interfaz webbridge c2w (paso 3 en la configuración de webbridge3)

c2w://webbridge.darmckin.local:449

En este punto, Webbridge3 vuelve a funcionar y puede unir espacios como invitado o, si ya ha importado usuarios, debe poder iniciar sesión.

Permisos de creación de espacio de usuario de aplicación web

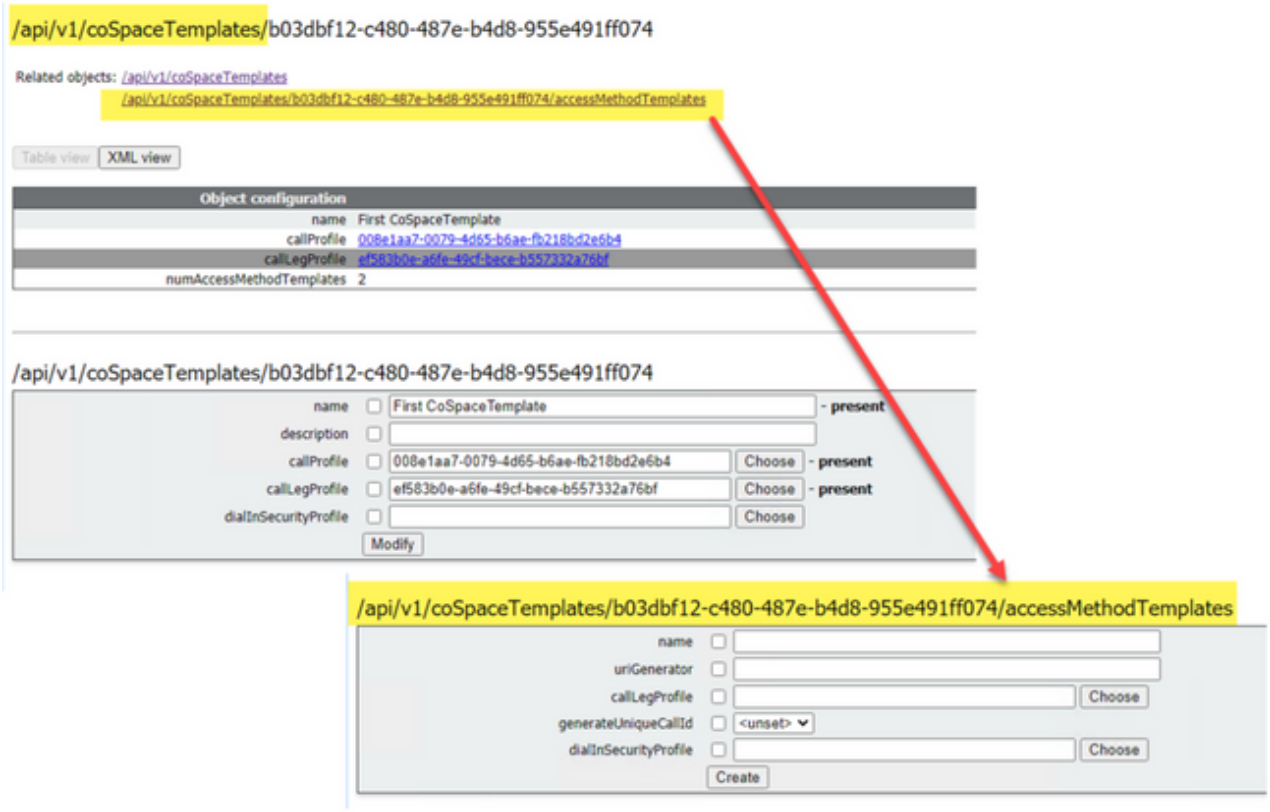
¿Están acostumbrados los usuarios a crear sus propios espacios en WebRTC? A partir de CMS 3.0, los usuarios de aplicaciones web no pueden crear sus propios coSpaces a menos que tengan una plantilla cospace asignada que lo permita.

Incluso con una plantilla coSpaceTemplate asignada, esto no crea un espacio al que otros puedan marcar (sin URI, sin ID de llamada o código de acceso), pero si la plantilla coSpace tiene un callLegProfile con ‘addParticipantAllowed’, entonces pueden marcar desde el espacio.

Para tener cadenas de marcado que se puedan utilizar para llamar al nuevo espacio, coSpaceTemplate debe tener una configuración accessMethodTemplate (consulte 2.9 release notes - 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).

En la API, cree coSpaceTemplate y, a continuación, cree accessMethodTemplate y asigne coSpaceTemplate a ldapUserCoSpaceTemplateSources o puede asignar manualmente coSpaceTemplate a un usuario de api/v1/users.

Puede crear y asignar varias plantillas CoSpaceTemplates y accessMethodsTemplates. Consulte la guía de la API de CMS para obtener más información (https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html)



CoSpaceTemplate (configuración de API)

Nombre: cualquier nombre que desee asignar a coSpaceTemplate.

Descripción: Breve descripción si lo desea.

callProfile: Perfil de llamada en blanco ¿Desea que use algún espacio creado con esta plantilla? Si no se proporciona, utiliza lo que se ha establecido en el nivel de sistema/perfil.

calllegProfile: ¿Qué calllegProfile desea que utilicen los espacios creados con esta plantilla? Si no se proporciona, utiliza lo que se ha establecido en el nivel de sistema/perfil.

dialInSecurityProfile: ¿Qué dialInSecurityProfile desea que utilicen los espacios creados con esta

plantilla? Si no se proporciona, utiliza lo que se ha establecido en el nivel de sistema/perfil.

AccessMethodTemplate (configuración de API)

Nombre: cualquier nombre que desee asignar a coSpaceTemplate.

uriGenerator: expresión que se va a utilizar para generar valores URI para esta plantilla de método de acceso; el conjunto de caracteres permitidos es 'a' a 'z', 'A' a 'Z', '0' a '9', '.', '-', '_' y '$'; si no está vacío, debe contener exactamente un carácter '$'. Ejemplo de esto es $.space, que utiliza el nombre proporcionado por el usuario al crear el espacio y le agrega ".space". "Reunión de equipo" crea la dirección URL 'Team.Meeting.space@domain'.

callLegProfile: ¿Qué callIegProfile desea que utilicen los accessMethods creados con esta plantilla? Si no se proporciona, utiliza lo que se establece en el nivel CoSpaceTemplate y, si no hay ninguno, utiliza lo que está en el nivel de sistema/perfil.

generateUniqueCallId: Indica si se debe generar un identificador numérico único para este método de acceso que reemplaza el global para el cospace.

dialInSecurityProfile: ¿Qué dialInSecurityProfile desea que utilicen los métodos de acceso creados con esta plantilla? Si no se proporciona, utiliza lo que se establece en el nivel CoSpaceTemplate y, si no hay ninguno, utiliza lo que está en el nivel de sistema/perfil.

Función de chat

CMS 3.0 eliminó la función de chat persistente, pero en CMS 3.2 devolvió el chat no persistente dentro de los espacios. El chat está disponible para los usuarios de aplicaciones web y no se almacena en ningún lugar. Una vez instalado CMS 3.2, los usuarios de aplicaciones web pueden comunicarse entre sí durante las reuniones de forma predeterminada. Estos mensajes solo están disponibles durante la reunión, y solo se ven los mensajes intercambiados después de unirse. No puede unirse más tarde y retroceder para ver los mensajes anteriores.

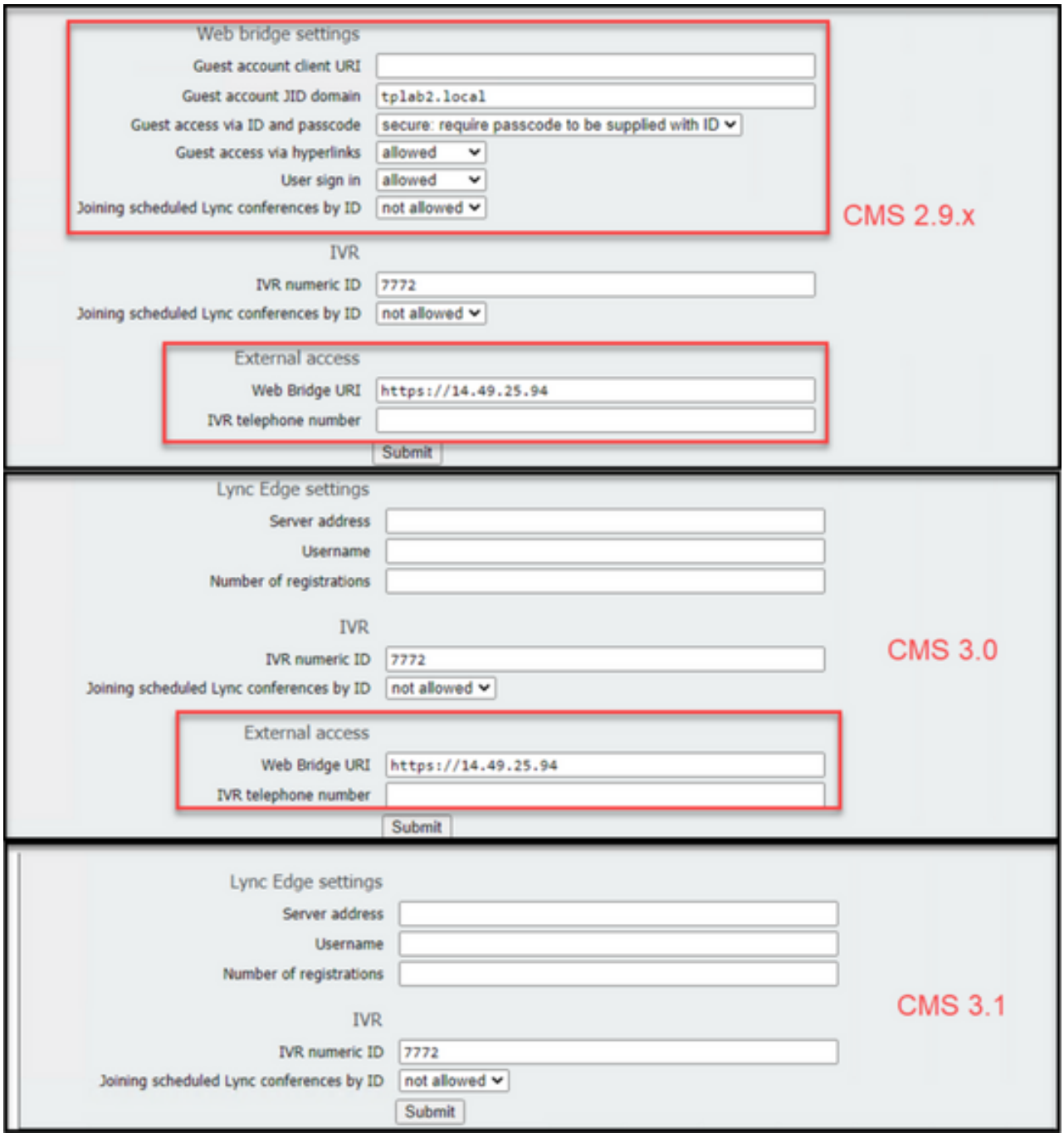
Llamadas punto a punto WebRTC

En CMS 2.9.x, los participantes de WebRTC podían marcar desde su cliente directamente a otros contactos. A partir de CMS 3.0, esto ya no es posible. Ahora los usuarios deben iniciar sesión y unirse a un espacio. A partir de ahí, si tienen permiso en callLegProfile (parámetro addParticipantes establecido en True), podrán agregar otros contactos. Esto hace que los CMS marquen al participante y se reúnan en un espacio de CMS.

Cambios notables en la configuración de WebBridge

CMS 3.0 y 3.1 ha eliminado o reubicado algunos de los ajustes de webbridge de la GUI y deben configurarse en la API para mantener la experiencia uniforme para los usuarios. En 3.x, utilice api/v1/webBridges y api/v1/webBridgeProfiles.

Compruebe lo que ha configurado actualmente para que, al actualizar a 3.0, pueda configurar los perfiles de webbridge y webbridge en la API en consecuencia.



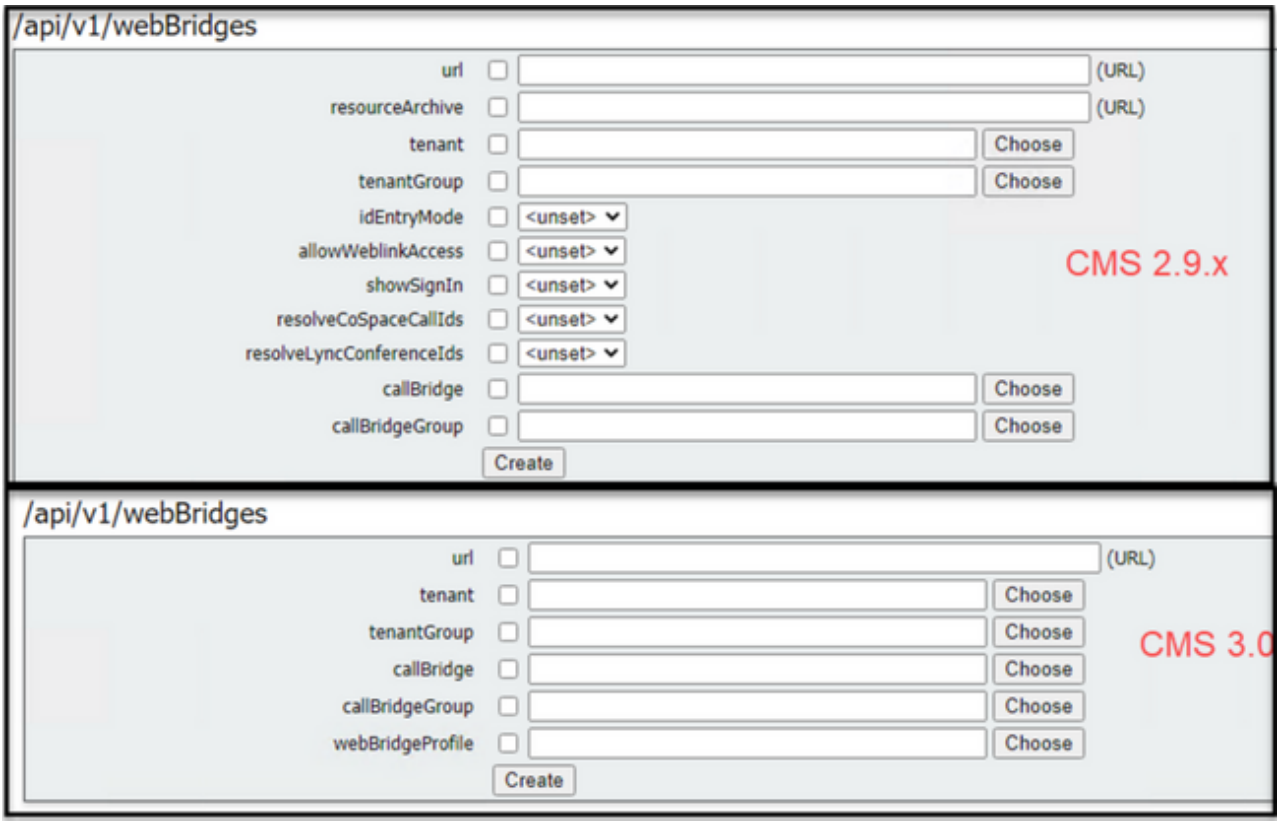
En la versión 3.0, la configuración del puente web se quitó en la GUI y, a continuación, en la versión 3.1 de CMS, también se quitaron los campos External access.

Configuración del puente web en la GUI

- URI de cliente de cuenta de invitado: el callBridge lo utilizó para buscar el webBridge. Si tenía varios WebBridges en su implementación para WebRTC, este campo ya debe estar en blanco y debe tener URL únicas en api/v1/webbridges para cada WebBridge al que el callBridge necesita conectarse. Elimine cualquier elemento de este campo y asegúrese de que WebBridges está configurado en la API.

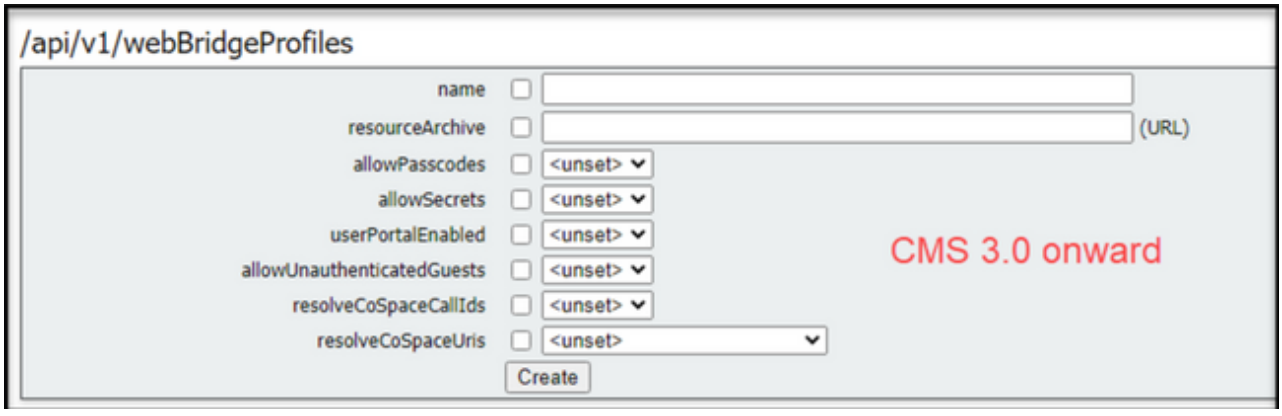
- Guest Account Jid Domain: ya no se utiliza en CMS 3.0 y puede eliminarlo.
- Acceso de invitado a través de ID y contraseña: eliminado y no sustituido en CMS 3.0.
- Acceso de invitado a través de hipervínculos: ahora configurable en webBridgeProfiles en

API al establecer "AllowSecrets".



En CMS 3.0, se han eliminado varios campos de api/v1/webBridges.

- resourceArchive: ahora en webbridgeProfiles.
- idEntryMode - ahora obsoleto.
- allowWebLinkAccess - ahora en webBridgeProfiles como allowSecrets.
- showSign: ahora en webBridgeProfiles como userPortalEnabled.
- resolverCoSpaceCallIds: ahora en webbridgeProfiles.
- resolverLyncConferenceIDs - ahora en webbridgeProfiles.



PerfilDeWebBridge

- resourceArchive: si utiliza fondos personalizados y el archivo de recursos está almacenado en un servidor web, introduzca aquí la URL.
- allowPasscodes: si es false, los usuarios no tienen la opción de unirse a las reuniones como invitados. Solo pueden iniciar sesión o utilizar una URL que contenga la información de

espacio y el secreto

- allowSecrets: si se establece en false, los usuarios no podrán unir espacios mediante una URL como https://meet.company.com/meeting/040478?secret=gPDnucF8is4W1cS87_l.zw. Los usuarios deben utilizar https://meet.company.com e introducir el ID de llamada/ID de reunión/URI y el PIN/contraseña, si hay alguno configurado.
- userPortalEnabled : si se establece en false, la página de inicio del portal de aplicaciones web no muestra la opción de inicio de sesión. Solo muestra los campos para introducir la ID de llamada/ID de reunión/URI y el PIN/contraseña, si hay alguno configurado.
- allowUnauthenticatedInvitados: si se establece en Falso, los invitados no pueden unirse a ninguna reunión, incluso con la URL completa que contiene el ID de la reunión y el secreto. Si su valor es False, sólo los usuarios que pueden iniciar sesión pueden unirse a una reunión. Ejemplo. El usuario 2 está intentando utilizar la dirección URL para la reunión del usuario 1. Después de introducir la URL, el usuario 2 debe iniciar sesión para continuar con la reunión del usuario 1.
- resolutionCoSpaceCallIds: si se establece en False, los invitados solo pueden unirse a las reuniones introduciendo el URI y el PIN/contraseña, si se utilizan. No se aceptan ID de llamada/ID de reunión/ID numérica.
- resolutionCoSpaceUri - 3 valores posibles: off, domainSuggestionDisabled y domainSuggestionEnabled. Si este webBridge acepta o no URI de SIP de accessMethod de coSpace y coSpace con el fin de permitir a los visitantes unirse a reuniones de cospace.

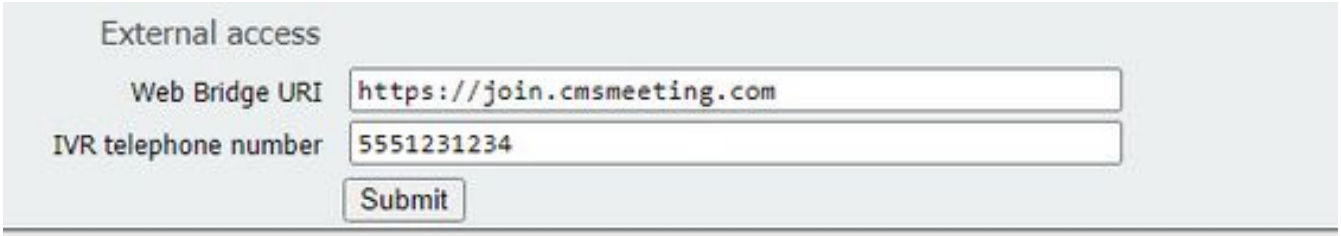
- Cuando se establece en 'off', la unión por URI está deshabilitada.

- Cuando se establece en 'domainSuggestionDisabled' se habilita la unión mediante URI, pero el dominio del URI no se completa automáticamente ni se verifica en webBridges mediante este webBridgeProfile.

- Cuando se establece en 'domainSuggestionEnabled' se habilita la unión mediante URI y el dominio del URI se puede completar automáticamente y verificar en webBridges mediante este perfil de webBridge.

Sección de acceso externo eliminada de la GUI web

En CMS 3.1, la sección Acceso Externo se ha eliminado de la GUI web. Si las tenía configuradas antes de la actualización, debe volver a configurarlas en la API bajo webbridgeProfiles.



En primer lugar, debe crear un webbridgeProfile como se describe en la sección anterior. Una vez que haya creado un webbridgeProfile, puede crear un número IVR o un URI de puente web mediante los enlaces disponibles en la API bajo el webBridgeProfile recién creado.

Puede crear hasta 32 números IVR o 32 direcciones webbridge por perfilWebBridge

Grabación o transmisión

El grabador y el componente de streaming en CMS 2.9.x y versiones anteriores eran clientes XMPP, y desde CMS 3.0, están basados en SIP. Esto ahora permite cambiar los diseños de las grabaciones y la transmisión mediante el diseño predeterminado de la API. Además, ahora las etiquetas de nombre se muestran en la sesión de grabación/transmisión. Consulte las notas de la versión de CMS 3.0 para obtener más información sobre las funciones de grabadora/transmisión: 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.

Si tiene una grabadora o una transmisora configurada en 2.9.x, debe volver a configurar los ajustes en MMP y API para que continúen funcionando después de la actualización.

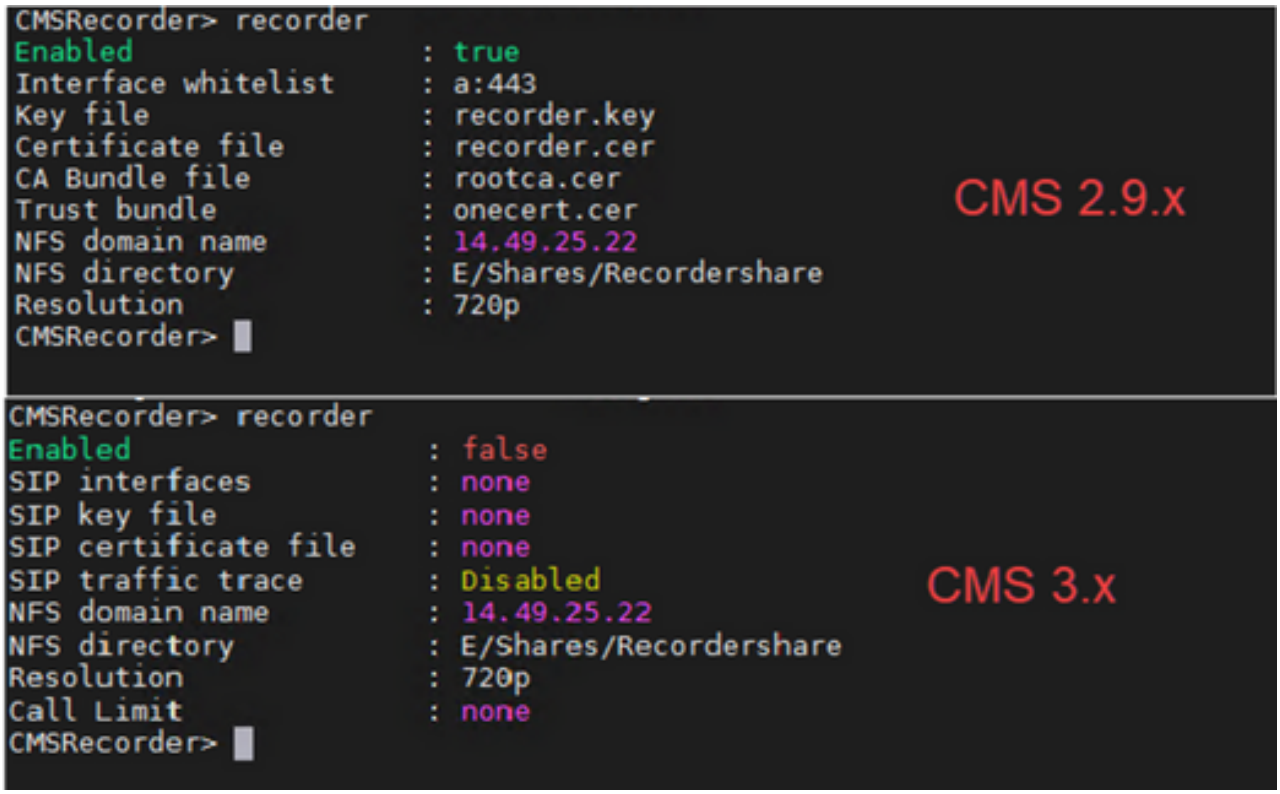
Antes de actualizar CMS a 3.0, se recomienda realizar una copia de seguridad mediante 'backup snapshot <servername_date>' y, a continuación, iniciar sesión en la página webadmin de los nodos de callbridge para eliminar toda la configuración de XMPP. A continuación, conéctese al MMP en sus servidores y realice estos pasos en todos los servidores Core que tienen xmpp a través de una conexión SSH:

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

Grabadora

MMP

Las Figuras muestran un ejemplo de las configuraciones que se ven en CMS 2.9.1 cuando se configuró el grabador, y cómo se ve inmediatamente después de la actualización a 3.0.



Después de la actualización, debe volver a configurar la grabadora:

Paso 1. Configure la interfaz de escucha SIP.

grabadora sip listen a 5060 5061 (La interfaz y los puertos que la grabadora SIP está configurada para escuchar TCP y TLS, respetuosamente. Si no desea utilizar TLS, puede utilizar 'recorder sip listen a 5060 none')

Paso 2. Configure los certificados que utiliza la grabadora si utiliza una conexión TLS.

recorder sip certs <key-file> <crt-file> [crt-bundle] (sin estos certificados, el servicio tls no se inicia en la grabadora. La grabadora utiliza el paquete crt para verificar el certificado de callBridge.)

Paso 3. Configure el límite de llamadas.

límite de grabadora <0-500|none> (Establece el límite del número de grabaciones simultáneas que puede servir el servidor. Esta tabla se encuentra en nuestra documentación y el límite del grabador debe coincidir con los recursos del servidor.)

Table 6: Internal SIP recorder performance and resource usage

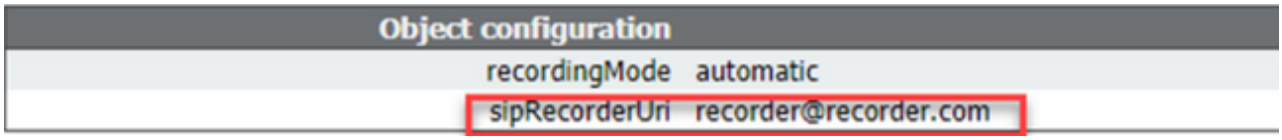
Recording Setting	Recordings per vCPU	RAM required per recording	Disk budget per hour	Maximum concurrent recording
720p	2	0.5GB	1GB	40
1080p	1	1GB	2GB	20
audio	16	100MB	150MB	100

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

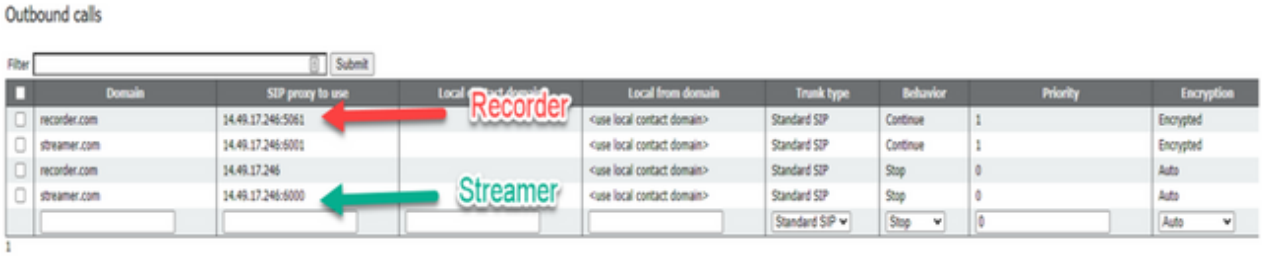
- Performance scales linearly adding vCPUs up to the number of host physical cores.

API

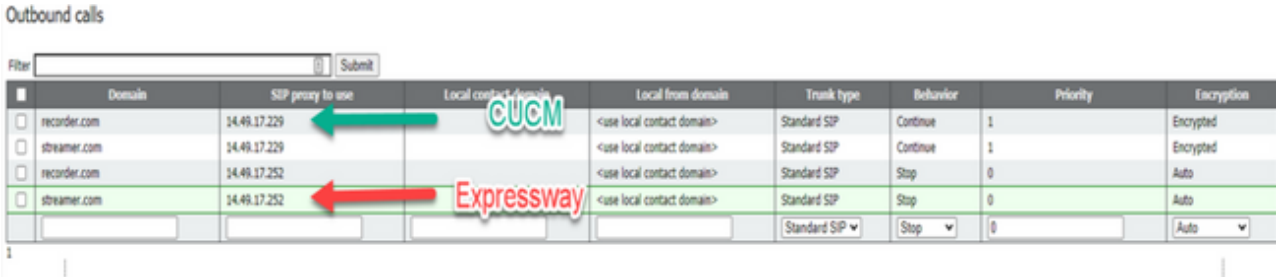
En api/v1/callProfiles, debe configurar el sipRecorderUri. Este es el URI que el callBridge marca cuando tiene que iniciar una grabación. El dominio de este URI debe agregarse a la tabla de reglas de salida y señalar al grabador (o control de llamada) como el proxy SIP que se va a utilizar.



Esta figura muestra una marcación directa al componente del grabador en las reglas salientes encontradas en Configuration > Outbound Calls.



En esta figura se muestra una llamada al componente del grabador a través de un control de llamada (por ejemplo, Cisco Unified Communications Manager (CUCM) o Expressway).



Nota: Si ha configurado la grabadora para utilizar SIP TLS y si las llamadas fallan, compruebe su nodo de CallBridge en MMP para ver si tiene habilitada la verificación de SIP de TLS. El comando MMP es 'tls sip'. Las llamadas pueden fallar porque el callBridge no

confía en el certificado de la grabadora. Puede probar esto desactivándolo en el callBridge usando 'tls sip verify disable'.

¿Múltiples grabadoras?

Configure cada una de ellas tal y como se ha explicado y ajuste las reglas de salida según corresponda. Si utiliza un método de grabación directa a, cambie la regla de grabación saliente a saliente existente a "Continuar" y agregue una nueva regla saliente debajo de la anterior con la prioridad uno menos que la primera. Cuando la primera grabadora ha alcanzado su límite de llamada, envía un 488 Inaceptable aquí de vuelta a callBridge, y callBridge pasa a la siguiente regla.

Si desea equilibrar la carga de las grabadoras, utilice un control de llamadas y ajuste el enrutamiento del control de llamadas para que pueda realizar llamadas a varias grabadoras.

Transmisor

MMP

Después de la actualización de 2.9.x a 3.0, debe volver a configurar la transmisión.

Paso 1. Configure la interfaz de escucha SIP.

streamer sip listen a 6000 6001 (La interfaz y los puertos que el streamer SIP está configurado para escuchar TCP y TLS, respetuosamente. Si no desea utilizar TLS, puede utilizar 'streamer sip listen a 6000 none')

Paso 2. Configure los certificados que utiliza el transmisor si utiliza una conexión TLS.

streamer sip certs <key-file> <crt-file> [crt-bundle] (sin estos certificados, el servicio tls no se inicia en el streamer. El transmisor utiliza el paquete crt para verificar el certificado de callBridge.)

Paso 3. Configurar el límite de llamadas

streamer limit <0-500|none> (Establece el límite para el número de secuencias simultáneas que puede servir el servidor. Esta tabla se encuentra en nuestra documentación y el límite de la secuencia debe alinearse con los recursos del servidor.)

Table 7: Internal SIP streamer recommended specifications

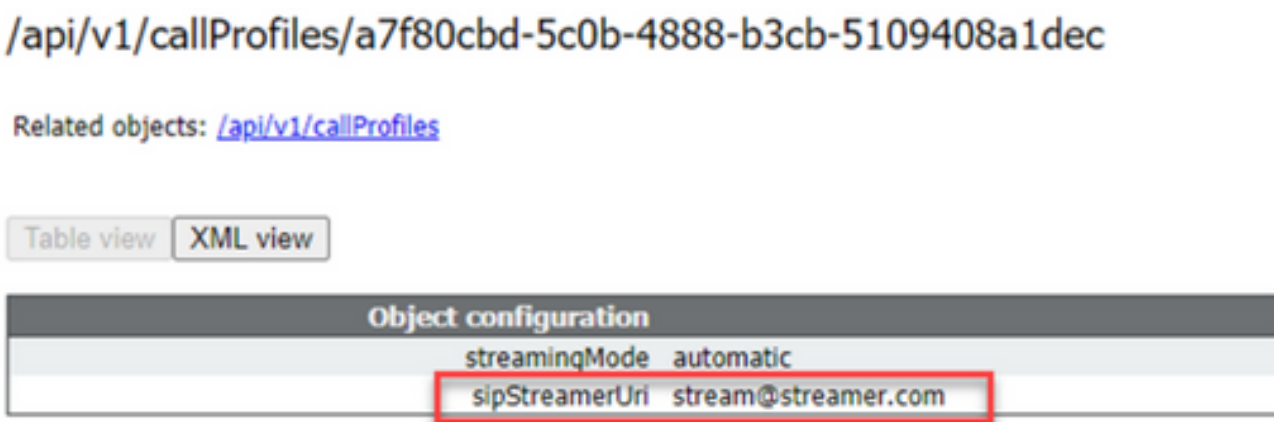
Number of vCPUs	RAM	Number of 720p streams	Number of 1080p streams	Number of audio-only streams
4	4GB	50	37	100
4	8GB	100	75	200
8	8GB	200	150	200

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.

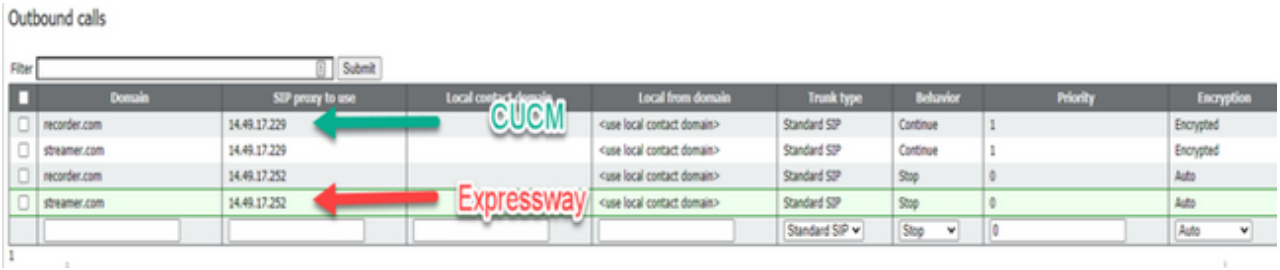
API

En api/v1/callProfiles, debe configurar el sipStreamUri. Este es el URI que el callBridge marca cuando tiene que iniciar la transmisión. El dominio de este URI debe agregarse a la tabla de reglas de salida y señalar al transmisor (o control de llamada) como el proxy SIP que se va a utilizar.



Esta figura muestra una marcación directa al componente de la transmisión en las reglas salientes encontradas en Configuration > Outbound Calls.

En esta figura se muestra una llamada al componente del grabador a través de un control de llamada (por ejemplo, Cisco Unified Communications Manager (CUCM) o Expressway).



Nota: Si ha configurado el transmisor para utilizar SIP TLS y si las llamadas fallan, compruebe su nodo de CallBridge en MMP para ver si tiene habilitada la verificación de SIP de TLS. El comando MMP es 'tls sip'. Las llamadas pueden fallar porque el callBridge no confía en el certificado de la transmisión. Puede probar esto desactivándolo en el callBridge usando 'tls sip verify disable'.

¿Varios Streamers?

Configure cada una de ellas tal y como se ha explicado y ajuste las reglas de salida según corresponda. Si utiliza un método directo a la secuencia, cambie la regla de salida a la grabadora existente a "Continuar" y agregue una nueva regla de salida por debajo de la anterior con la prioridad una menos que la primera. Cuando la primera transmisión ha alcanzado su límite de llamada, envía un 488 Inaceptable aquí de vuelta a callBridge, y callBridge pasa a la siguiente regla.

Si desea equilibrar la carga de las transmisiones, utilice un control de llamadas y ajuste el enrutamiento del control de llamadas para que pueda realizar llamadas a varias transmisiones.

Consideración de Expressway

Si utiliza Cisco Expressway para proxy web, debe asegurarse de que Expressway ejecuta al menos X12.6 antes de la actualización de CMS. CMS 3.0 lo requiere para que el proxy web funcione y sea compatible.

La capacidad de los participantes de las aplicaciones web ha aumentado en Expressways cuando se utiliza con CMS 3.0. Para un Expressway OVA de gran tamaño, la capacidad esperada es de 150 llamadas Full HD (1080p30) o 200 llamadas de otro tipo (por ejemplo, 720p30). Puede aumentar esta capacidad agrupando Expressway, hasta 6 nodos (donde 4 se utilizan para escalar y 2 para redundancia, por lo que hasta un máximo de 600 llamadas Full HD u 800 llamadas de otro tipo).

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

Perímetro CMS

CMS Edge se vuelve a introducir en CMS 3.1 ya que ofrece capacidades más altas que Expressway para sesiones de aplicaciones web externas. Hay dos configuraciones recomendadas.

Especificaciones de borde pequeño

4 GB de RAM, 4 vCPU y interfaz de red de 1 Gbps

Esta especificación VM Edge tiene suficiente potencia para cubrir una única capacidad de carga de audio y vídeo CMS1000 de 48 x 1080p, 96 x 720p, 192 x 480p y 1000 llamadas de audio.

Para la implementación, se recomienda disponer de 1 servidor de extremo pequeño por CMS1000 o 4 servidores de extremo pequeño por CMS2000.

Especificaciones de borde grande

8 GB de RAM, 16 vCPU y interfaz de red de 10 Gbps

Esta especificación VM Edge tiene suficiente potencia para cubrir una única capacidad de audio y vídeo CMS2000 de 350 x 1080p, 700 x 720p, 1000 x 480p y 3000 x llamadas de audio.

Para la implementación, se recomienda disponer de un servidor perimetral grande por CMS2000 o por cada 4 CMS1000.

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).