

Linee guida per effettuare l'aggiornamento di Cisco Meeting Server dalla versione 2.9 alla versione 3.0 o successive

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Informazioni importanti sugli aggiornamenti](#)

[Riepilogo degli elementi da considerare](#)

[Licenze](#)

[Webbridge \(client WebRTC e CMA\)](#)

[Modifiche alla GUI Web](#)

[Registratori / Streamer](#)

[Considerazioni su Cisco Expressway](#)

[CMS Edge](#)

[CMS \(Acano\) serie X](#)

[SIP Edge](#)

[Ulteriori informazioni](#)

[Licenze - Controllo delle licenze prima dell'aggiornamento](#)

[Determinare il numero di utenti a cui viene assegnata una licenza PMP dopo l'aggiornamento](#)

[Disponete di un numero sufficiente di licenze SMP?](#)

[Configura CMM](#)

[Configurazione di Webbridge \(client WebRTC e CMA\)](#)

[Autorizzazioni creazione spazio utente app Web](#)

[Funzione Chat](#)

[Chiamate point-to-point WebRTC](#)

[Modifiche alle impostazioni di webBridge di rilievo](#)

[Sezione Accesso esterno rimossa dalla GUI Web](#)

[Registrazione o streaming](#)

[Registratore](#)

[Streamer](#)

[Considerazioni su Expressway](#)

[CMS Edge](#)

Introduzione

In questo documento vengono descritte le problematiche relative all'aggiornamento di

un'implementazione di Cisco Meeting Server con versione 2.9 (o precedente) alla versione 3.0 (o successiva) e viene spiegato come gestirle per un processo di aggiornamento senza problemi.

Funzionalità rimosse: XMPP è stato rimosso (influisce su WebRTC), trunk/bilanciamenti del carico, webbridge

Funzionalità modificate: registratori e streamer sono ora SIP e webbridge è stato sostituito da webbridge3

Questo documento tratta solo gli argomenti che è necessario prendere in considerazione prima di eseguire l'aggiornamento. Non copre tutte le nuove funzioni disponibili in 3.X.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione CMS
- Aggiornamenti CMS
- Creazione e firma di certificati

Tutto quanto qui menzionato è delineato in vari documenti. Si consiglia sempre di leggere le note di rilascio del prodotto e di consultare le nostre guide alla programmazione e guide all'installazione per ulteriori chiarimenti sulle funzioni: [Guide all'installazione e alla configurazione del CMS](#) e [note di rilascio del prodotto CMS](#).

Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Meeting Server.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questo documento è da considerarsi di riferimento nel caso in cui si disponga già di un'implementazione di CMS 2.9.x (o precedente), indipendentemente dal fatto che sia stata eseguita una singola installazione combinata o resiliente e quando si prevede di eseguire l'aggiornamento a CMS 3.0. Le informazioni di questo documento si riferiscono a tutti i modelli di CMS.



Nota: la serie X non può essere aggiornata a CMS 3.0. È necessario pianificare la sostituzione dei server serie X il prima possibile.

Informazioni importanti sugli aggiornamenti

L'unico metodo supportato per l'aggiornamento di CMS è un aggiornamento graduale. Al momento della stesura di questo articolo, è stato pubblicato CMS 3.5. Se si utilizza CMS 2.9, è necessario eseguire l'aggiornamento in modo graduale (2.9 → 3.0 → 3.1 → 3.2 → 3.3 → 3.4 → 3.5 (il processo di aggiornamento nota presenta modifiche rispetto a CMS 3.5, quindi leggere attentamente le note sulla versione)).

Se non si esegue un aggiornamento graduale e si verifica un comportamento insolito, TAC potrebbe richiedere il downgrade e la ripresa dell'attività.

Inoltre, a partire da CMS 3.4, CMS DEVE utilizzare Smart Licensing. Non è possibile eseguire l'aggiornamento a CMS 3.4 o versioni successive e continuare a utilizzare le licenze tradizionali. Non eseguire l'aggiornamento a CMS 3.4 o versione successiva a meno che non sia stato configurato Smart Licensing.

Riepilogo degli elementi da considerare

Utilizzare queste domande per passare alle sezioni relative alla propria situazione. Ogni considerazione fa riferimento a un collegamento ipertestuale a una descrizione più dettagliata contenuta nel presente documento.

Licenze

Si dispone di un numero sufficiente di licenze Personal MultiParty (PMP) / Shared MultiParty (SMP) sui server prima dell'aggiornamento?

Nella versione 3.0 le licenze PMP vengono assegnate, anche se l'utente non ha eseguito l'accesso. Ad esempio, se sono stati importati 10000 utenti tramite LDAP, ma si dispone solo di 100 licenze PMP, non sarà possibile ottenere la conformità non appena si esegue l'aggiornamento alla versione 3.0. In questo caso, accertarsi di controllare i tenant con userProfile impostato e/o system/profiles per verificare se è impostato un userProfile con hasLicense con un valore true.

In [questa sezione](#) vengono illustrate in dettaglio le modalità di controllo di userProfile sull'API e di verifica della presenza di hasLicense=true impostato (ovvero utenti con licenza PMP).

Il file cms.lic corrente contiene licenze PMP/SMP?

A causa delle modifiche del comportamento della licenza nella versione 3.0 e successive, è necessario verificare di disporre di un numero sufficiente di licenze PMP/SMP prima di eseguire l'aggiornamento. Questa procedura viene descritta più dettagliatamente in [questa sezione](#).

È stato implementato Cisco Meeting Manager (CMM)?

CMS 3.0 richiede CMM 3.0 a causa di modifiche nella gestione delle licenze. Si consiglia di distribuire CMM 2.9 prima di eseguire un aggiornamento dell'ambiente alla versione 3.0, in quanto è possibile controllare il report di 90 giorni per verificare l'utilizzo della licenza negli ultimi 90 giorni.

Questa procedura viene descritta più dettagliatamente in [questa sezione](#).

Si dispone di licenze Smart?

CMS 3.0 richiede CMM 3.0 a causa di modifiche nella gestione delle licenze. Pertanto, se si utilizza già Smart Licensing tramite CMM, assicurarsi di disporre di licenze PMP e SMP associate al cluster.

Webbridge (client WebRTC e CMA)

Si utilizza WebRTC in CMS 2.9?

Webbridge è notevolmente cambiato in CMS 3.0. Per ulteriori informazioni sulla migrazione da webbridge2 a webbridge3 e sull'utilizzo delle app Web, vedere [questa sezione](#).

Gli utenti utilizzano il CMA thick client?

Poiché questi client sono basati su XMPP, non possono più essere utilizzati dopo l'aggiornamento, poiché il server XMPP è stato rimosso. In [questa sezione](#) sono disponibili ulteriori informazioni relative allo Use Case in uso.

Utilizzate Chat in WebRTC?

La funzionalità chat viene rimossa dall'app Web in 3.0. In CMS 3.2, la chat viene reintrodotta, ma non è persistente. Per ulteriori informazioni su questa funzione, consultare [questa sezione](#).

Gli utenti eseguono chiamate Point to Point da WebRTC ai dispositivi?

In CMS 3.0, un utente dell'app Web non può più connettersi direttamente a un altro dispositivo. A questo punto è necessario accedere a un'area riunioni e disporre dell'autorizzazione per aggiungere partecipanti alla riunione per eseguire la stessa azione. Per ulteriori informazioni su questa parte, consultare [questa sezione](#).

Gli utenti creano i propri coSpaces da WebRTC?

Nella versione 3.0, affinché gli utenti dell'app Web possano creare i propri spazi dal client, è necessario creare un coSpaceTemplate nell'API e assegnarlo all'utente. Questa operazione può essere manuale o automatica durante l'importazione LDAP. CanCreateCoSpaces viene rimosso da UserProfile. Per ulteriori informazioni su questa funzione, consultare [questa sezione](#).

Modifiche alla GUI Web

Le impostazioni di webBridge sono configurate nella GUI di amministrazione Web?

Le impostazioni di webBridge vengono rimosse dalla GUI in 3.0, quindi è necessario configurare i webbridge nell'API e prendere nota delle impostazioni correnti nella GUI, in modo da poter configurare di conseguenza i webBridgeProfiles nell'API. Per ulteriori informazioni su questa modifica, vedere [questa sezione](#).

Nella GUI di amministrazione Web sono configurate le impostazioni esterne?

Le impostazioni esterne sono state rimosse dalla GUI in CMS 3.1. Se nella GUI di CMS 3.0 o di una versione precedente di Web Admin è stato configurato l'URL o l'IVR di Webbridge (Configurazione → Generale → Impostazioni esterne), tali impostazioni sono state rimosse dalla pagina Web e devono essere configurate nell'API. Le impostazioni precedenti all'aggiornamento alla versione 3.1 NON vengono aggiunte all'API e devono essere eseguite manualmente. Per ulteriori informazioni su questa modifica, vedere [questa sezione](#).

Registratori / Streamer

Attualmente si utilizzano registratori CMS e/o streamer?

Il registratore CMS e il componente Streamer ora sono basati su SIP invece che su XMPP. Pertanto, mentre il file XMPP viene rimosso, è necessario modificarlo dopo l'aggiornamento. Per ulteriori informazioni su questa modifica, vedere [questa sezione](#).

Considerazioni su Cisco Expressway

Qual è la versione corrente di Cisco Expressway se si utilizza Expressway per il proxy WebRTC?

CMS 3.0 richiede Expressway 12.6 o versione successiva. Per ulteriori informazioni su questa funzionalità proxy WebRTC, vedere [questa sezione](#).

CMS Edge

Si dispone attualmente di un CMS Edge nell'ambiente?

CMS Edge è stato reintrodotta su CMS 3.1 con una maggiore scalabilità per le connessioni esterne. Per ulteriori informazioni su questa parte, consultare [questa sezione](#).

CMS (Acano) serie X

L'azienda dispone attualmente di server serie x nel proprio ambiente?

Questi server non possono essere aggiornati a CMS 3.0 ed è necessario provare a sostituirli presto (passare a una macchina virtuale o a un accessorio CMS prima di eseguire l'aggiornamento a 3.0). In [questo link](#) è possibile trovare l'avviso di fine ciclo di vita relativo a questi server.

SIP Edge

Attualmente si utilizza SIP Edge nell'ambiente in uso?

Sip Edge è completamente deprecato a partire da CMS 3.0. È necessario utilizzare Cisco Expressway per trasferire le chiamate SIP nel CMS. Contattare il rappresentante commerciale Cisco per informazioni su come ottenere Expressway per l'organizzazione.

Ulteriori informazioni

Licenze - Controllo delle licenze prima dell'aggiornamento

Lo stato della licenza non conforme è il problema più grave quando si esegue l'aggiornamento alla versione 3.0 o successive da una versione 2.x. In questa sezione viene descritto come determinare il numero di licenze PMP/SMP necessarie per un aggiornamento senza problemi.

Prima di aggiornare la distribuzione alla versione 3.0, distribuire CMM 2.9 e controllare il report di 90 giorni nella scheda Licenze per verificare se l'utilizzo della licenza è rimasto al di sotto del numero di licenze allocate nei nodi CMS:

The screenshot displays the Cisco Meeting Management interface for the 'Licenses' section. The cluster is identified as 'CMS VM Cluster'. A 'Download 90 day report' button is highlighted with a red box. The 'Meetings' section is 'In compliance' and shows the following data:

License Type	Allocated	90 day peak
Shared Multiparty Plus	100	2
Personal Multiparty Plus	100	9

The 'Recording or Streaming' section is also 'In compliance' and shows the following data:

Category	Allocated	90 day peak
Recording or Streaming	20	2

Se si utilizza la licenza Traditional (il file cms.lic viene installato localmente nei nodi CMS), controllare nel file di licenza CMS le quantità di licenze personali e condivise (100 / 100 come nell'immagine qui) su ciascuno dei nodi CMS (scaricarlo tramite WinSCP da ciascun nodo callBridge).

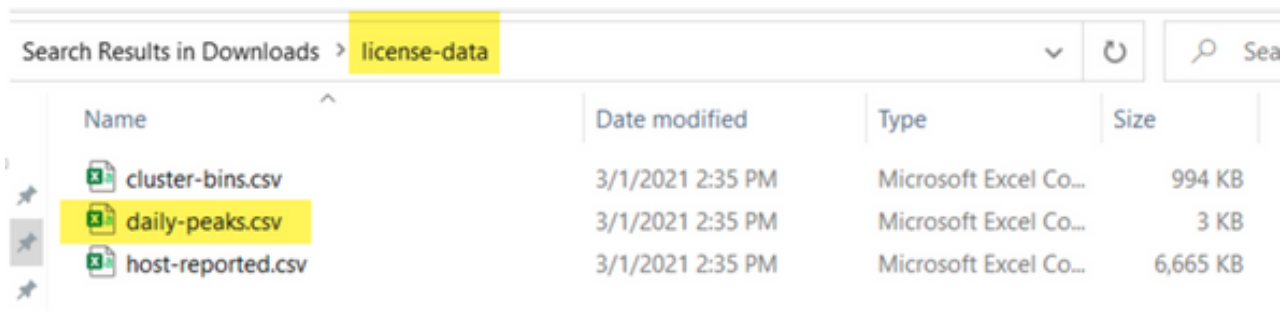
```

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

```

, verificare il numero di licenze PMP/SMP assegnate nel portale Cisco Software Smart per i server CMS.

Aprire il report di 90 giorni (il file Zip è denominato license-data.zip) e aprire il file daily-peaks.csv.



Name	Date modified	Type	Size
cluster-bins.csv	3/1/2021 2:35 PM	Microsoft Excel Co...	994 KB
daily-peaks.csv	3/1/2021 2:35 PM	Microsoft Excel Co...	3 KB
host-reported.csv	3/1/2021 2:35 PM	Microsoft Excel Co...	6,665 KB

In Excel, ordinare la colonna PMP per Z in A per ottenere i valori più alti nella parte superiore e quindi eseguire la stessa operazione per la colonna SMP. I valori visualizzati in questo file sono inferiori alle licenze disponibili nel file di licenza CMS? In caso affermativo, la conformità è garantita. In caso contrario, si creano avvisi e/o errori come indicato nella Figura 6 della sezione 1.7.3 della [guida alla distribuzione del CMS](#) per la quale è possibile trovare ulteriori informazioni anche nella sezione 1.7.4.

Come per l'immagine, ad esempio, sono state usate 2.1667 licenze SMP e nessuna licenza PMP negli ultimi 90 giorni. Il file cms.lic indicava 100 unità di ciascun tipo di licenza, pertanto l'installazione è completamente conforme. Pertanto, non vi sono problemi con la licenza quando questa installazione viene aggiornata a CMS 3.0. Tuttavia, potrebbe ancora esserci un problema quando nella configurazione sarebbero stati importati 10.000 utenti tramite LDAP. Poiché si hanno solo 100 licenze PMP, si allocano 10000 licenze (con userProfile con hasLicense impostato su True), in questo caso non si è conformi quando si esegue l'aggiornamento alla versione 3.0. Per ulteriori informazioni, vedere la sezione successiva.

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

Determinare il numero di utenti a cui viene assegnata una licenza PMP dopo l'aggiornamento

A tutti gli utenti importati che utilizzano un profilo utente con hasLicense=true viene automaticamente assegnata una licenza PMP in CMS 3.0.

Nell'API, controllare quanti profili utente si hanno e verificare se in uno di essi "hasLicense=true" è impostato. In caso affermativo, è necessario verificare dove sono assegnati tali profili utente.

I profili utente possono essere assegnati a uno dei seguenti livelli:


1. LdapSources
2. Affittuari
3. Sistema/Profili

Verificare in tutte e 3 le posizioni i profili utente assegnati con hasLicense=true.

1. LdapSources/tenant

Per ogni LdapSource che utilizza un tenant o un profilo utente, agli utenti importati con tale LdapSource viene assegnata una licenza PMP quando il parametro hasLicense è impostato su True. Se è presente un tenant, è necessario fare clic sull'ID tenant per verificare se è stato assegnato un profilo utente, quindi verificare se tale profilo utente è configurato con

'hasLicense=true'. Se non è presente alcun tenant, ma è stato impostato un profilo utente, fare clic su di esso per verificare se dispone di 'hasLicense=true'. Se in entrambi i casi viene utilizzato 'hasLicense=true', è possibile verificare il numero di utenti importati eseguendo un'operazione GET per 'api/v1/users' e un filtro per il dominio utilizzato per jidMapping, ad esempio, nel mapping LDAP associato a ldapSource.

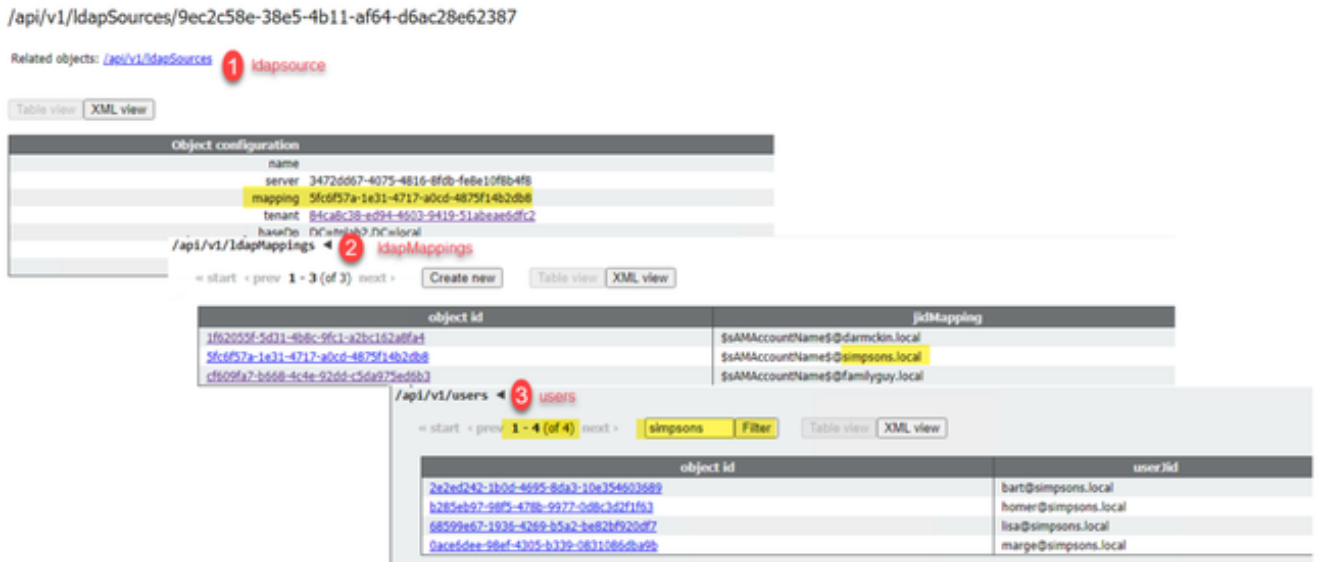
 Nota: questa operazione può risultare più complessa in altre situazioni, nel qual caso è necessario verificarla con i mapping e i filtri di Active Directory creati.

Passaggio 1. Trovare l'ID mapping da ldapSource.

Passaggio 2. Cercare ldapMappings per trovare jidMapping.

Passaggio 3. Cercare in api/v1/users il dominio utilizzato in jidMapping.

Passaggio 4. Aggiungere gli utenti trovati da ogni ldapSource. Il numero di utenti LDAP importati che necessitano di licenze PMP.



The screenshot shows a web interface with three main sections:

- Section 1:** Object configuration for an ldapSource. Fields include name, server, mapping, tenant, and baseDn. The mapping field is highlighted in yellow.
- Section 2:** A table of ldapMappings. The table has two columns: object id and jidMapping. The jidMapping column contains values like \$SAMAAccountName@damckin.local and \$SAMAAccountName@simpsons.local.
- Section 3:** A table of users. The table has two columns: object id and user/id. The user/id column contains values like bart@simpsons.local, homer@simpsons.local, lisa@simpsons.local, and marge@simpsons.local. A filter 'simpsons' is applied to the table.

2. Sistema/Profili

Se un profilo utente è impostato a livello di sistema/profili e quel profilo utente ha "hasLicense=true", a qualsiasi utente importato in CMS verrà assegnata una licenza PMP quando il server viene aggiornato. Se sono stati importati 10.000 utenti, ma si dispone solo di 100 PMP, si verificheranno problemi di conformità quando si esegue l'aggiornamento a CMS 3.0 e potrebbe essere visualizzato un messaggio sullo schermo di 30 secondi e l'audio viene richiesto all'inizio delle chiamate.


Se il profilo utente a livello di sistema indica che gli utenti devono ottenere un piano di gestione delle prestazioni, passare a api/v1/users per visualizzare il numero totale di utenti:

/api/v1/users ◀ Will show total number of imported users

◀ start ◀ prev 1 - 9 (of 9) next ▶ Filter Table view XML view

object id	user/jid	ten
18a6595a-33a0-4fd0-8761-5030249e0301	Lois@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8
84a2d8be-b4d5-4a02-a003-2cf34fcb5df3	brian@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8
86e7f8a6-55fc-443e-b7ae-66e2c0191cac	connor@darmskin.local	
44800633-fb41-4998-bdf5-339c64fccb67	darren@darmskin.local	
4bc178dc-288c-49e5-a6d9-8cb192425b7f	homer@simpsons.local	84ca8c38-ed94-4603-9419-51abaa6dfc2
a1105eb2-49f1-4ba5-8deb-c1e3d74ba084	janette@darmskin.local	
b6f80307-d839-4863-8e00-667e403a5a5e	meg@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8
32a615e6-ce2e-4489-a5db-d65e83e067a9	peter@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8
f1c47991-5173-4daa-bb59-2140c8ca01f6	stewie@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8

Se in precedenza erano stati importati tutti gli utenti dal ldap, ma ora è necessario solo un determinato sottoinsieme da tale elenco, creare un filtro migliore nel ldapSource in modo che importi solo gli utenti a cui si desidera assegnare licenze PMP. Modificare il filtro su ldapSource e quindi eseguire una nuova sincronizzazione LDAP in api/v1/ldapsync. In questo modo vengono importati solo gli utenti desiderati e tutti gli altri utenti dell'importazione precedente vengono rimossi.

 Nota: se si esegue questa operazione correttamente e la nuova importazione rimuove solo gli utenti indesiderati, gli altri utenti coSpace CallID e i segreti non cambiano, ma se si commette un errore, questo può comportare la modifica di tutti gli ID chiamata e i segreti. Eseguire un backup dei nodi del database prima di tentare di eseguire questa operazione se si è preoccupati per questo problema.

Disponete di un numero sufficiente di licenze SMP?

Quando si esaminano i picchi giornalieri dal report CMM 90 Day, si dispone già di licenze SMP sufficienti per coprire i picchi? Le licenze SMP vengono utilizzate quando al proprietario della riunione non è stata assegnata una licenza PMP (come proprietario di coSpace / riunione ad hoc / riunione pianificata TMS). Se si utilizza intenzionalmente il protocollo SMP e si dispone di spazio sufficiente per coprire gli orari di punta, tutto ciò è corretto. Se si controlla il picco di 90 giorni per il protocollo SMP e non è chiaro perché questi vengono consumati, di seguito sono riportate alcune informazioni da controllare.

1. Le chiamate ad hoc (come inoltrate da CUCM) utilizzano una licenza SMP se il dispositivo utilizzato per l'unione non è associato a un utente a cui è stata assegnata una licenza PMP in CMS tramite userProfile. CUCM fornisce il GUID dell'utente che esegue l'escalation della riunione. Se tale GUID corrisponde a un utente LDAP importato di Meeting Server con una licenza PMP assegnata, verrà utilizzata la licenza di tale utente.
2. Se a un proprietario di coSpace non è stata assegnata una licenza PMP, le chiamate a quei particolari coSpaces utilizzano una licenza SMP.
3. Se la riunione è stata pianificata in TMS versione 15.6 o successive, il proprietario della riunione viene inviato a CMS e, se a tale utente non è stata assegnata una licenza PMP, la riunione utilizza una licenza SMP.

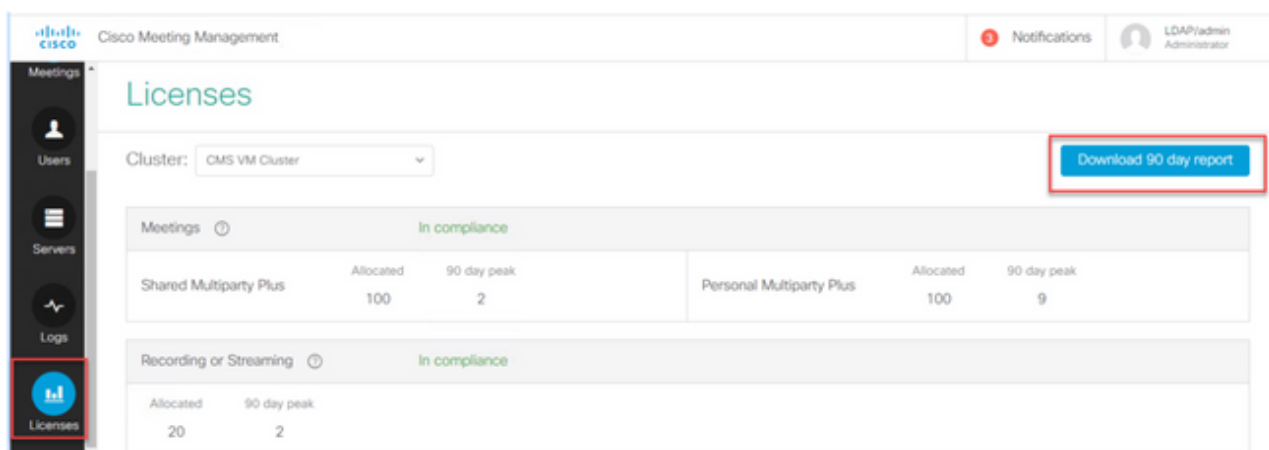
Configura CMM

A partire da CMS 3.0, CMM 3.0 è necessario per il corretto funzionamento di CMS. CMM è responsabile della gestione delle licenze di CMS, quindi se si intende aggiornare CMS alla versione 3.0, è necessario disporre di un server CMS. Si consiglia di distribuire CMM 2.9 mentre si è su CMS 2.9 in modo da poter controllare l'utilizzo della licenza prima dell'aggiornamento.

CMM controlla tutti i callBridge aggiunti per le licenze SMP e PMP e per la licenza callBridge. Viene utilizzato il numero più alto tra i vari dispositivi all'interno del cluster.

Ad esempio, se CMS1 ha 20 licenze PMP e 10 licenze SMP e CMS2 ha 40 licenze PMP e 5 licenze SMP nelle licenze tradizionali, CMM segnala che si hanno 40 licenze PMP e 10 licenze SMP da utilizzare.

Se si dispone di un numero di licenze PMP superiore a quello degli utenti importati, non si verificano problemi relativi alle licenze PMP (o SMP). Tuttavia, se si controlla il picco di 90 giorni e si scopre di aver utilizzato più di quanto disponibile, è comunque possibile eseguire l'aggiornamento a CMS 3.0 e utilizzare la licenza di prova di 90 giorni su CMM per risolvere i problemi relativi alla licenza o eseguire un'azione prima dell'aggiornamento.



The screenshot displays the Cisco Meeting Management interface. The main heading is 'Licenses'. Below it, a dropdown menu shows 'Cluster: CMS VM Cluster'. A 'Download 90 day report' button is highlighted with a red box. The interface shows two sections: 'Meetings' and 'Recording or Streaming', both marked as 'In compliance'. The 'Meetings' section contains a table with columns for 'Shared Multiparty Plus' and 'Personal Multiparty Plus', each with sub-columns for 'Allocated' and '90 day peak'. The 'Recording or Streaming' section has a table with 'Allocated' and '90 day peak' columns.

Meeting Type	Allocated	90 day peak
Shared Multiparty Plus	100	2
Personal Multiparty Plus	100	9

Category	Allocated	90 day peak
Recording or Streaming	20	2

Configurazione di Webbridge (client WebRTC e CMA)

CMS 3.0 rimuove il componente server XMPP e, con questo, rimuove webBridge e la possibilità di utilizzare il client thick CMA. WebBridge3 è quello che viene ora utilizzato per connettere gli utenti delle app Web (in precedenza denominati utenti WebRTC) alle riunioni che utilizzano il browser. Quando si esegue l'aggiornamento alla versione 3.0, è necessario configurare webbridge3.

 Nota: il client spesso CMA non funziona dopo l'aggiornamento a CMS 3.0!

In questo video viene illustrato il processo di creazione dei certificati di webbridge 3.

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

Prima dell'aggiornamento alla versione 3.0, i clienti devono pianificare come configurare Webbridge3. Qui vengono evidenziati i passi più importanti.

1. Per webbridge3 è necessaria una catena di chiavi e certificati. È possibile utilizzare il vecchio certificato webbridge se il certificato contiene tutti i nomi di dominio completi (FQDN) o gli indirizzi

IP del server CMS come nome alternativo del soggetto (SAN)/nome comune (CN) che eseguono webbridge3 e se uno di questi è soddisfatto:

a. Il certificato non prevede l'utilizzo chiavi avanzato (ovvero può essere utilizzato come client o server).

b. Il certificato prevede sia l'autenticazione client che quella server. Il certificato HTTP richiede solo l'autenticazione server, mentre il certificato C2W richiede sia server che client.

2. Se si desidera creare un nuovo certificato per il certificato "webbridge3 https", si consiglia di apporre la firma pubblica (per evitare avvisi sui certificati sul client quando si utilizza l'app Web). Lo stesso certificato può essere utilizzato per il "certificato c2w webbridge3" e il certificato deve avere il nome di dominio completo (FQDN) dei server webbridge nella rete SAN/CN.
3. CallBridge deve comunicare con il nuovo webbridge3 utilizzando una porta configurata nel comando di ascolto webbridge3 c2w. Può trattarsi di una qualsiasi porta disponibile, ad esempio 449. Gli utenti devono accertarsi che i callbridge possano comunicare con webbridge3 su questa porta e, se necessario, che le modifiche del firewall siano state apportate in anticipo. Non può essere la stessa porta utilizzata da "webbridge https" per l'ascolto.

Prima dell'aggiornamento di CMS alla versione 3.0, è consigliabile eseguire un backup utilizzando 'backup snapshot <servername_date>' e quindi accedere alla pagina webadmin nei nodi callbridge per rimuovere tutte le impostazioni XMPP e le impostazioni Webbridge. Quindi, collegarsi al pannello di gestione dei server ed eseguire la procedura seguente su tutti i server Core dotati di xmpp e webbridge su una connessione SSH:

1. xmpp disable
2. reimpostazione xmpp
3. certificati xmpp nessuno
4. dominio xmpp nessuno
5. webbridge disabilitato
6. ascolto webbridge nessuno
7. certificati webbridge nessuno
8. attendibilità webbridge nessuna

Una volta eseguito l'aggiornamento alla versione 3.0, iniziare configurando webbridge3 su tutti i server che in precedenza eseguivano webbridge. È necessario eseguire questa operazione perché esistono già record DNS che puntano a questi server, in modo da garantire che se un utente viene inviato a un webbridge3, sia pronto a gestire la richiesta.

Configurazione Webbridge3 (su tutte le connessioni SSH)

Passaggio 1. Configurare la porta di ascolto http di webbridge3.

Webbridge3 https ascolta a:443

Passaggio 2. Configurare i certificati per webbridge3 per le connessioni del browser. Questo è il

certificato inviato ai browser e deve essere firmato da un'Autorità di certificazione (CA) pubblica e contenente il nome di dominio completo (FQDN) utilizzato nel browser affinché il browser consideri attendibile la connessione.

Webbridge3 https certs wb3.key wb3trust.cer (deve trattarsi di una catena di trust: creare un certificato di trust con entità finale in primo piano, seguita da CA intermedie in ordine, terminante con RootCA).

```
-----BEGIN CERTIFICATE-----  
Entity cert ← wb3/cb cert  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
Intermediate cert  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
root cert  
-----END CERTIFICATE-----  
single carriage return at end
```

Passaggio 3. Configurare la porta da utilizzare per l'ascolto delle connessioni da callBridge a webbridge (c2w). Poiché per la porta di ascolto webbridge3 https viene utilizzato 443, questa configurazione deve essere una porta diversa disponibile, come ad esempio 449.

Webbridge3 c2w ascolto a:449

4. Configurare i certificati inviati da webbridge al callbridge per l'attendibilità c2w

certificati c2w Webbridge3 wb3.key wb3trust.cer

5. Configurare l'archivio di attendibilità utilizzato da WB3 per considerare attendibile il certificato callBridge. Deve essere lo stesso certificato utilizzato sul bundle della CA callbridge (e deve essere un bundle di certificati intermedi nella parte superiore e CA radice alla fine, seguito da un singolo ritorno a capo).

Webbridge3 c2w trust rootca.cer

6. Abilitare webbridge3

Webbridge3 attiva

```
Usage:
  webbridge3
  webbridge3 restart
  6 webbridge3 enable
  webbridge3 disable
  1 webbridge3 https listen <interface:port whitelist>
  2 webbridge3 https certs <key-file> <cert-fullchain-file>
  webbridge3 https certs none
  webbridge3 http-redirect (enable [port]|disable)
  3 webbridge3 c2w listen <interface:port whitelist>
  4 webbridge3 c2w certs <key-file> <cert-fullchain-file>
  webbridge3 c2w certs none
  5 webbridge3 c2w trust <cert-bundle>
  webbridge3 c2w trust none
  webbridge3 options <space-separated options>
  webbridge3 options none
  webbridge3 status
```

Modifiche alla configurazione di CallBridge (su tutta la connessione SSH)

Passaggio 1. Configurare il trust callBridge con il certificato/bundle CA che ha firmato il certificato c2w webbridge3.

```
Callbridge trust c2w rootca.cer
```

Passaggio 2. Riavviare il callBridge per rendere effettiva la nuova relazione di trust. In questo modo vengono interrotte tutte le chiamate su questo particolare callBridge. Utilizzare questa opzione con cautela.

Riavvio di Callbridge

Configurazione API per callBridge per la connessione a webBridge3

1. Creare un nuovo oggetto webBridge utilizzando POST nell'API e assegnargli un valore URL utilizzando FQDN e la porta configurata nell'elenco di colori dell'interfaccia c2w di webbridge (passaggio 3 della configurazione di webbridge3)

```
c2w://webbridge.darmckin.local:449
```

A questo punto, Webbridge3 funziona di nuovo ed è possibile unirsi agli spazi come guest o, se gli utenti sono stati importati in precedenza, devono essere in grado di accedere.

Autorizzazioni creazione spazio utente app Web

Gli utenti sono abituati a creare spazi propri in WebRTC? A partire dalla versione CMS 3.0, gli utenti dell'app Web non possono creare i propri coSpaces a meno che non dispongano di un modello di cospace assegnato che lo consenta.

Anche se è stato assegnato un coSpaceTemplate, non viene creato uno spazio in cui gli altri utenti possono comporre (nessun URI, nessun ID chiamata o passcode), ma se il coSpace ha un callLegProfile con 'addParticipantAllowed', possono comporre il numero dallo spazio.

Per poter utilizzare le stringhe di composizione per chiamare il nuovo spazio, coSpaceTemplate deve disporre di un accessMethodTemplate impostato (vedere le note sulla versione 2.9 - 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).

Nell'API, creare i modelli coSpaceTemplate, quindi creare uno o più modelli accessMethodTemplate e assegnare il modello coSpaceTemplate a IdapUserCoSpaceTemplateSources. In alternativa, è possibile assegnare manualmente un modello coSpaceTemplate a un utente in api/v1/users.

È possibile creare e assegnare più modelli CoSpace e accessMethodsTemplates. Per ulteriori informazioni, vedere la guida all'API CMS (<https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html>)

The screenshot displays the API interface for managing CoSpaceTemplates. It shows the configuration for a specific CoSpaceTemplate and a list of its associated accessMethodTemplates.

CoSpaceTemplate Configuration:

Object configuration	
name	First CoSpaceTemplate
callProfile	008e1aa7-0079-4d65-b6ae-fb218bd2e6b4
callLegProfile	ef582b0e-a6fe-49cf-bece-b557332a76bf
numAccessMethodTemplates	2

AccessMethodTemplate Configuration:

Field	Value	Required
name	First CoSpaceTemplate	present
description		
callProfile	008e1aa7-0079-4d65-b6ae-fb218bd2e6b4	present
callLegProfile	ef582b0e-a6fe-49cf-bece-b557332a76bf	present
dialInSecurityProfile		

The interface also shows a form for creating a new accessMethodTemplate with fields for name, uriGenerator, callLegProfile, generateUniqueCallId, and dialInSecurityProfile.

CoSpaceTemplate (configurazione API)

Nome: il nome che si desidera assegnare a coSpaceTemplate.

Descrizione: Breve descrizione, se desiderato.

callProfile: CallProfile bianco. Utilizzare gli spazi creati con questo modello? Se non viene fornito, utilizza ciò che è impostato a livello di sistema/profilo.

calllegProfile: specificare calllegProfile da utilizzare per gli spazi creati con questo modello. Se non viene fornito, utilizza ciò che è impostato a livello di sistema/profilo.

dialInSecurityProfile: specificare quale dialInSecurityProfile utilizzare per gli spazi creati con

questo modello. Se non viene fornito, utilizza ciò che è impostato a livello di sistema/profilo.

AccessMethodTemplate (configurazione API)

Nome: il nome che si desidera assegnare a coSpaceTemplate.

uriGenerator: espressione da utilizzare per generare i valori URI per questo modello di metodo di accesso. Il set di caratteri consentito è compreso tra 'a' e 'z', tra 'A' e 'Z', tra '0' e '9', '.', '-', '_' e '\$'. Se non è vuoto, deve contenere esattamente un carattere '\$'. L'esempio è \$.space che utilizza il nome fornito dall'utente durante la creazione dello spazio e vi aggiunge ".space". "Riunione team" crea l'URL 'Team.Meeting.space@domain'.

callLegProfile: specificare callLegProfile da utilizzare per gli accessMethods creati con questo modello. Se non specificato, utilizza il livello impostato di CoSpaceTemplate e, se non è presente, utilizza il livello impostato a livello di sistema/profilo.

generateUniqueCallId: indica se generare un ID numerico univoco per questo metodo di accesso che sostituisce quello globale per il cospazio.

dialInSecurityProfile: specificare quale dialInSecurityProfile utilizzare per i metodi di accesso creati con questo modello. Se non specificato, utilizza il livello impostato di CoSpaceTemplate e, se non è presente, utilizza il livello impostato a livello di sistema/profilo.

Funzione Chat

CMS 3.0 ha rimosso la funzione di chat persistente, ma in CMS 3.2 è stata restituita la chat non persistente all'interno degli spazi. La chat è disponibile per gli utenti dell'app Web e non viene archiviata da nessuna parte. Una volta installato CMS 3.2, gli utenti dell'app Web possono per impostazione predefinita scambiarsi messaggi durante le riunioni. Questi messaggi sono disponibili solo durante la riunione e vengono visualizzati solo i messaggi scambiati dopo la partecipazione. Non puoi partecipare in ritardo e scorrere indietro per vedere i messaggi precedenti.

Chiamate point-to-point WebRTC

Su CMS 2.9.x, i partecipanti WebRTC sono stati in grado di comporre dal loro client direttamente ad altri contatti. A partire da CMS 3.0, questo non è più possibile. Ora gli utenti devono accedere e unirsi a uno spazio. Da qui, se dispongono dell'autorizzazione nel parametro callLegProfile (addParticipants impostato su True), possono aggiungere altri contatti. In questo modo, il CMS chiama il partecipante e questi si incontrano in uno spazio nel CMS.

Modifiche alle impostazioni di webBridge di rilievo

CMS 3.0 e 3.1 ha rimosso o riposizionato alcune delle impostazioni di webbridge dalla GUI e devono essere configurate nell'API per garantire un'esperienza coerente agli utenti. Nella versione 3.x, utilizzare api/v1/webBridge e api/v1/webBridgeProfiles.

Verificare la configurazione corrente. Quando si esegue l'aggiornamento alla versione 3.0, è

possibile configurare i profili webbridge e webbridge nell'API di conseguenza.

The image displays three screenshots of CMS configuration pages, each with a red box highlighting specific sections:

- CMS 2.9.x:** The 'Web bridge settings' section is highlighted, containing fields for 'Guest account client URI', 'Guest account JID domain' (tp1ab2.local), 'Guest access via ID and passcode' (secure: require passcode to be supplied with ID), 'Guest access via hyperlinks' (allowed), 'User sign in' (allowed), and 'Joining scheduled Lync conferences by ID' (not allowed). Below it is the 'IVR' section with 'IVR numeric ID' (7772) and 'Joining scheduled Lync conferences by ID' (not allowed). The 'External access' section is also highlighted, containing 'Web Bridge URI' (https://14.49.25.94) and 'IVR telephone number'. A 'Submit' button is at the bottom.
- CMS 3.0:** The 'External access' section is highlighted, containing 'Web Bridge URI' (https://14.49.25.94) and 'IVR telephone number'. A 'Submit' button is at the bottom.
- CMS 3.1:** The 'External access' section is highlighted, containing 'Web Bridge URI' (https://14.49.25.94) and 'IVR telephone number'. A 'Submit' button is at the bottom.

Nella versione 3.0, le impostazioni del web bridge sono state rimosse dalla GUI, quindi in CMS 3.1 sono stati rimossi anche i campi di accesso esterno.

Impostazioni bridge Web nella GUI

- URI client account Guest - utilizzato da callBridge per trovare webBridge. Se nella distribuzione per WebRTC sono presenti più WebBridge, questo campo deve essere già vuoto ed è necessario disporre di URL univoci in api/v1/webbridge per ogni WebBridge a cui deve connettersi callBridge. Eliminare qualsiasi elemento in questo campo e assicurarsi che i WebBridge siano configurati nell'API.
- Dominio Jid account guest - non viene più utilizzato in CMS 3.0 ed è possibile eliminarlo.

- Accesso guest tramite ID e passcode - rimosso e non sostituito in CMS 3.0.
- Accesso guest tramite collegamenti Hyper - ora configurabile in webBridgeProfiles nell'API nell'impostazione "AllowSecrets".

The image shows two screenshots of the API configuration interface for webBridges. The top screenshot is for CMS 2.9.x and shows fields for url, resourceArchive, tenant, tenantGroup, idEntryMode, allowWeblinkAccess, showSignIn, resolveCoSpaceCallIds, resolveLyncConferenceIds, callBridge, and callBridgeGroup. The bottom screenshot is for CMS 3.0 and shows fields for url, tenant, tenantGroup, callBridge, callBridgeGroup, and webBridgeProfile. Both screenshots have a 'Create' button at the bottom.

Si noti che in CMS 3.0 i campi seriali sono stati rimossi da api/v1/webBridges.

- resourceArchive - ora in webbridgeProfiles.
- idEntryMode - ora deprecato.
- allowWeblinkAccess - ora in webBridgeProfiles come allowSecrets.
- showSignIn: ora in webBridgeProfiles come userPortalEnabled.
- resolveCoSpaceCallIds: ora in webbridgeProfiles.
- resolveLyncConferenceIDs - ora in webbridgeProfiles.

The image shows a screenshot of the API configuration interface for webBridgeProfiles in CMS 3.0 onward. It shows fields for name, resourceArchive, allowPasscodes, allowSecrets, userPortalEnabled, allowUnauthenticatedGuests, resolveCoSpaceCallIds, and resolveCoSpaceUris. A 'Create' button is at the bottom.

ProfiloWebBridge

- resourceArchive: se si utilizzano sfondi personalizzati e l'archivio delle risorse è memorizzato su un server Web, immettere l'URL qui.

- allowPasscodes: se false, gli utenti non hanno l'opzione di partecipare alle riunioni come ospiti. Possono solo accedere o utilizzare un URL contenente le informazioni sullo spazio e il segreto
- allowSecrets: se è impostato su false, gli utenti non possono unirsi agli spazi utilizzando un URL come https://meet.company.com/meeting/040478?secret=gPDnucF8is4W1cS87_l.zw. Gli utenti devono utilizzare <https://meet.company.com> e immettere l'ID chiamata/ID riunione/URI e il PIN/passcode se ne è stato configurato uno.
- userPortalEnabled: se è impostata su false, la pagina iniziale del portale dell'app Web non visualizza l'opzione di accesso. Vengono visualizzati solo i campi per l'immissione di ID chiamata/ID riunione/URI e PIN/passcode, se configurati.
- allowUnauthenticatedGuests: se impostato su False, gli ospiti non possono partecipare ad alcuna riunione, anche con l'URL completo che contiene l'ID riunione e il segreto. Se è False, solo gli utenti che possono accedere possono partecipare alle riunioni. Esempio. L'utente 2 sta tentando di utilizzare l'URL per la riunione dell'utente 1. Dopo aver immesso l'URL, l'utente 2 deve accedere per continuare con la riunione dell'utente 1.
- resolveCoSpaceCallIds: se impostato su False, gli ospiti possono partecipare alle riunioni solo immettendo l'URI e il PIN/passcode, se utilizzati. ID chiamata/ID riunione/ID numerico non accettati.
- resolveCoSpaceUris: 3 possibili impostazioni: off, domainSuggestionDisabled e domainSuggestionEnabled. Se questo webBridge accetta o meno gli URI SIP coSpace e coSpace accessMethod allo scopo di consentire ai visitatori di partecipare alle riunioni cospace.

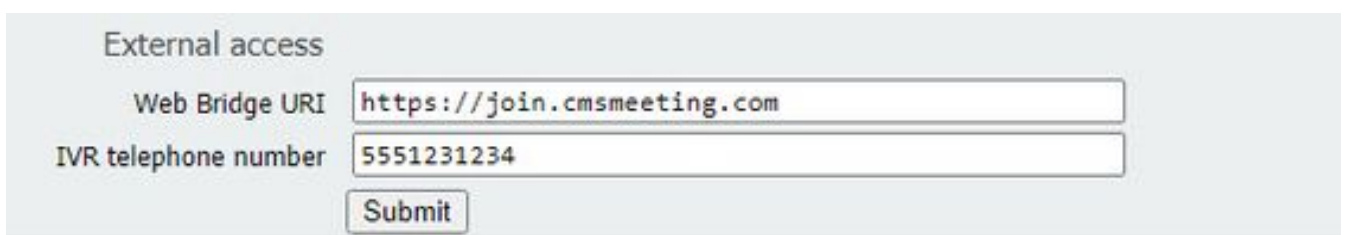
- Se impostato su 'off' join da URI è disabilitato.

- Se impostato su 'domainSuggestionDisabled', l'aggiunta tramite URI è abilitata, ma il dominio dell'URI non viene completato automaticamente o verificato su webBridges utilizzando questo webBridgeProfile.

- Se impostato su 'domainSuggestionEnabled', l'aggiunta tramite URI è abilitata e il dominio dell'URI può essere completato e verificato automaticamente su webBridges utilizzando questo webBridgeProfile.

Sezione Accesso esterno rimossa dalla GUI Web

In CMS 3.1, la sezione Accesso esterno è stata rimossa dalla GUI Web. Se queste sono state configurate prima dell'aggiornamento, è necessario riconfigurarle nell'API in webbridgeProfiles.



External access	
Web Bridge URI	<input type="text" value="https://join.cmsmeeting.com"/>
IVR telephone number	<input type="text" value="5551231234"/>
<input type="button" value="Submit"/>	

Innanzitutto, è necessario creare un profilo webbridge come descritto nella sezione precedente. Una volta creato un webbridgeProfile, è possibile creare un numero IVR e/o un URI di Web Bridge

tramite i collegamenti disponibili nell'API sotto il nuovo webBridgeProfile creato.



È possibile creare fino a 32 numeri IVR o 32 indirizzi webbridge per profilo WebBridge

Registrazione o streaming

Il componente di registrazione e streaming su CMS 2.9.x e versioni precedenti erano client XMPP e da CMS 3.0 sono basati su SIP. In questo modo è possibile modificare i layout per le registrazioni e lo streaming utilizzando il layout predefinito nell'API. Inoltre, nella sessione di registrazione/streaming sono visualizzate le etichette dei nomi. Per ulteriori informazioni sulle funzioni di registrazione/streaming, consultare le note di rilascio di CMS 3.0 - 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.

Se il registratore o il streamer è stato configurato nella versione 2.9.x, è necessario riconfigurare le impostazioni in MMP e API in modo che continuino a funzionare dopo l'aggiornamento.

Prima di eseguire l'aggiornamento a CMS 3.0, è consigliabile eseguire un backup utilizzando 'backup snapshot <servername_date>' e quindi accedere alla pagina webadmin nei nodi callbridge per rimuovere tutte le impostazioni XMPP. Quindi, collegarsi al pannello di gestione dei server ed eseguire la procedura seguente su tutti i server Core dotati di xmpp su una connessione SSH:

1. xmpp disable
2. reimpostazione xmpp
3. certificati xmpp nessuno
4. dominio xmpp nessuno

Registratore

MMP

Le figure mostrano un esempio delle configurazioni viste su CMS 2.9.1 quando il registratore è stato configurato, e come appare subito dopo l'aggiornamento alla versione 3.0.

```
CMSRecorder> recorder
Enabled                : true
Interface whitelist   : a:443
Key file               : recorder.key
Certificate file      : recorder.cer
CA Bundle file        : rootca.cer
Trust bundle          : onecert.cer
NFS domain name       : 14.49.25.22
NFS directory         : E/Shares/Recordershare
Resolution            : 720p
CMSRecorder> █

CMSRecorder> recorder
Enabled                : false
SIP interfaces        : none
SIP key file          : none
SIP certificate file  : none
SIP traffic trace     : Disabled
NFS domain name       : 14.49.25.22
NFS directory         : E/Shares/Recordershare
Resolution            : 720p
Call Limit            : none
CMSRecorder> █
```

CMS 2.9.x

CMS 3.x

Al termine dell'aggiornamento, è necessario riconfigurare il registratore:

Passaggio 1. Configurare l'interfaccia di ascolto SIP.

registrator sip ascolto a 5060 5061 (l'interfaccia e le porte su cui il registratore SIP è configurato per l'ascolto per TCP e TLS, rispettivamente. Se non si desidera utilizzare TLS, è possibile utilizzare 'recorder sip Listen a 5060 none')

Passaggio 2. Configurare i certificati utilizzati dal registratore se si utilizza una connessione TLS.

recorder sip certs <key-file> <crt-file> [crt-bundle] (senza questi certificati, il servizio tls non si avvia sul registratore. Il registratore utilizza il pacchetto crt per verificare il certificato callBridge.)

Passaggio 3. Configurare il limite di chiamate.

recorder limit <0-500|none> (imposta il limite per il numero di registrazioni simultanee che il server può eseguire). Questa tabella è inclusa nella documentazione e il limite del registratore deve essere allineato alle risorse del 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

Su `api/v1/callProfiles`, è necessario configurare `sipRecorderUri`. URI composto da `callBridge` quando deve avviare una registrazione. Il dominio di questo URI deve essere aggiunto alla tabella delle regole in uscita e puntare al registratore (o controllo delle chiamate) come proxy SIP da utilizzare.

Object configuration	
<code>recordingMode</code>	<code>automatic</code>
<code>sipRecorderUri</code>	<code>recorder@recorder.com</code>

Nella figura viene mostrato un collegamento diretto al componente recorder nelle regole in uscita trovate in Configurazione > Chiamate in uscita.

Outbound calls

Filter: Submit


Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption
<input type="checkbox"/> recorder.com	14.49.17.246-5061	Recorder	<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/> streamer.com	14.49.17.246-6001		<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/> recorder.com	14.49.17.246	Streamer	<use local contact domain>	Standard SIP	Stop	0	Auto
<input type="checkbox"/> streamer.com	14.49.17.246-6000		<use local contact domain>	Standard SIP	Stop	0	Auto


Nella Figura viene illustrata una chiamata al componente del registratore tramite un controllo di chiamata, ad esempio Cisco Unified Communications Manager (CUCM) o Expressway.

Outbound calls

Filter: Submit

Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption
<input type="checkbox"/> recorder.com	14.49.17.229	CUCM	<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/> streamer.com	14.49.17.229		<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/> recorder.com	14.49.17.252	Expressway	<use local contact domain>	Standard SIP	Stop	0	Auto
<input type="checkbox"/> streamer.com	14.49.17.252		<use local contact domain>	Standard SIP	Stop	0	Auto

 Nota: se il registratore è stato configurato per l'utilizzo di TLS SIP e le chiamate non riescono, controllare il nodo `callBridge` in MMP per verificare se è abilitata la verifica SIP TLS. Il comando MMP è `'tls sip'`. Le chiamate potrebbero non riuscire perché il certificato

 del registratore non è considerato attendibile da callBridge. È possibile verificarlo disattivandolo su callBridge utilizzando 'tls sip verify disable'.

Più registratori?

Configurare ciascuno di essi come descritto e modificare le regole in uscita di conseguenza. Se si utilizza un metodo diretto al registratore, modificare la regola esistente in uscita nel registratore impostandola sul comportamento "Continua" e aggiungere una nuova regola in uscita al di sotto di quella precedente con la priorità meno la prima. Quando il primo registratore ha raggiunto il limite di chiamate, invia un messaggio di errore 488 Inaccettabile a callBridge e callBridge passa alla regola successiva.

Se si desidera bilanciare il carico dei registratori, utilizzare un controllo delle chiamate e regolare il routing del controllo delle chiamate in modo che sia in grado di effettuare chiamate a più registratori.

Streamer

MMP

Dopo l'aggiornamento da 2.9.x a 3.0, è necessario riconfigurare streamer.

Passaggio 1. Configurare l'interfaccia di ascolto SIP.

streamer sip ascolta un 6000 6001 (l'interfaccia e le porte su cui SIP streamer è configurato per l'ascolto per TCP e TLS, rispettivamente. Se non si desidera utilizzare TLS, è possibile utilizzare 'streamer sip Listen a 6000 none')

Passaggio 2. Configurare i certificati utilizzati dallo streamer se si utilizza una connessione TLS.

streamer sip certs <file-chiave> <file-crt> [bundle-crt] (senza questi certificati, il servizio tls non viene avviato sul streamer. Lo streamer utilizza il crt-bundle per verificare il certificato callBridge.)

Passaggio 3. Configurare il limite di chiamate

streamer limit <0-500|none> (imposta il limite per il numero di flussi simultanei che il server può gestire. Questa tabella è inclusa nella documentazione e il limite del streamer deve essere allineato alle risorse del 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

Su `/api/v1/callProfiles`, è necessario configurare `sipStreamUri`. URI composto da `callBridge` quando deve avviare il flusso. Il dominio di questo URI deve essere aggiunto alla tabella delle regole in uscita e puntare allo streamer (o controllo delle chiamate) come proxy SIP da utilizzare.

`/api/v1/callProfiles/a7f80cbd-5c0b-4888-b3cb-5109408a1dec`

Related objects: </api/v1/callProfiles>

Table view XML view

Object configuration	
<code>streamingMode</code>	<code>automatic</code>
<code>sipStreamUri</code>	<code>stream@streamer.com</code>

Nella figura viene mostrato un collegamento diretto al componente Streamer nelle regole in uscita trovate in Configurazione > Chiamate in uscita.

Outbound calls

Filter Submit

	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption
<input type="checkbox"/>	recorder.com	14.49.17.246:5061	Recorder	<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/>	streamer.com	14.49.17.246:5001		<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/>	recorder.com	14.49.17.246		<use local contact domain>	Standard SIP	Stop	0	Auto
<input type="checkbox"/>	streamer.com	14.49.17.246:6000	Streamer	<use local contact domain>	Standard SIP	Stop	0	Auto
					Standard SIP	Stop	0	Auto


Nella Figura viene illustrata una chiamata al componente del registratore tramite un controllo di chiamata, ad esempio Cisco Unified Communications Manager (CUCM) o Expressway.

Outbound calls

Filter Submit

	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption
<input type="checkbox"/>	recorder.com	14.49.17.229		<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/>	streamer.com	14.49.17.229		<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/>	recorder.com	14.49.17.252		<use local contact domain>	Standard SIP	Stop	0	Auto
<input type="checkbox"/>	streamer.com	14.49.17.252		<use local contact domain>	Standard SIP	Stop	0	Auto
					Standard SIP	Stop	0	Auto

Annotations: A green arrow points from the 'SIP proxy to use' column to the '14.49.17.229' value. A red arrow points from the 'SIP proxy to use' column to the '14.49.17.252' value. A blue 'CUCM' label is placed above the 'Local contact domain' column. A red 'Expressway' label is placed above the 'Local from domain' column.

 Nota: se lo streamer è stato configurato per l'utilizzo di TLS SIP e le chiamate non riescono, controllare il nodo callBridge in MMP per verificare se è abilitata la verifica SIP TLS. Il comando MMP è 'tls sip'. Le chiamate potrebbero non riuscire perché il certificato del gestore di flusso non è considerato attendibile da callBridge. È possibile verificarlo disattivandolo su callBridge utilizzando 'tls sip verify disable'.

Più Streamer?

Configurare ciascuno di essi come descritto e modificare le regole in uscita di conseguenza. Se si utilizza un metodo direct to streamer, modificare la regola esistente outbound to recorder impostandola sul comportamento "Continua" e aggiungere una nuova regola outbound al di sotto della precedente con la priorità meno la prima. Quando il primo streamer ha raggiunto il limite di chiamate, invia un messaggio di errore 488 Inaccettabile a callBridge e callBridge passa alla regola successiva.

Se si desidera bilanciare il carico dei flussi, utilizzare un controllo delle chiamate e regolare il routing del controllo delle chiamate in modo che sia in grado di effettuare chiamate a più flussi.

Considerazioni su Expressway

Se si utilizza Cisco Expressway per il proxy Web, è necessario verificare che Expressway esegua almeno X12.6 prima dell'aggiornamento del CMS. Questo è richiesto da CMS 3.0 per il funzionamento e il supporto del proxy Web.

La capacità dei partecipanti alle app Web è aumentata rispetto a Expressways se utilizzata con CMS 3.0. Per una grande superstrada OAV, la capacità prevista è di 150 chiamate Full HD (1080p30) o 200 chiamate di altro tipo (ad esempio 720p30). È possibile aumentare questa capacità raggruppando Expressway, fino a 6 nodi (dove 4 viene utilizzato per la scalabilità e 2 per la ridondanza, quindi fino a un massimo di 600 chiamate Full HD o 800 chiamate di altro 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

CMS Edge viene reintrodotta in CMS 3.1 in quanto offre capacità superiori rispetto a Expressway per le sessioni di app Web esterne. Si consigliano due configurazioni.

Specifiche dei bordi piccoli

4 GB di RAM, 4 vCPU, interfaccia di rete a 1 Gb/s

Questa specifica di VM Edge ha una potenza sufficiente per coprire una singola capacità di carico audio e video CMS1000 pari a 48 x 1080p, 96 x 720p, 192 x 480p e 1000 chiamate audio.

Per l'installazione, si consiglia di disporre di un server di piccole dimensioni per CMS1000 o di quattro server di piccole dimensioni per CMS2000.

Specifiche dei bordi grandi

8 GB di RAM, 16 vCPU, interfaccia di rete a 10 Gbps

Questa specifica di VM Edge dispone di alimentazione sufficiente per coprire una singola chiamata audio e video CMS2000, ovvero 350 x 1080p, 700 x 720p, 1000 x 480p e 3000 x.

Per l'installazione è consigliabile disporre di un server perimetrale di grandi dimensioni per CMS2000 o per 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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).