Cisco Meeting Server 2.9에서 3.0 이상으로의 원활한 업그레이드를 위한 지침

목차

소개

이 문서에서는 버전 2.9(또는 이전)를 실행하는 Cisco Meeting Server 구축을 3.0(또는 이후)으로 업그레이드하는 문제와 원활한 업그레이드 프로세스를 위해 이러한 문제를 처리하는 방법에 대해 설명합니다.

제거된 기능: XMPP가 제거됨(WebRTC에 영향을 미침), 트렁크/로드 밸런서, webbridge

변경된 기능: 이제 레코더와 스트리머가 SIP가 되고 webbridge가 webbridge3로 교체됩니다.

이 문서에서는 업그레이드하기 전에 고려해야 하는 항목만 다룹니다. 3.X에서 사용할 수 있는 모든 새로운 기능을 다루지는 않습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CMS 관리
- CMS 업그레이드
- 인증서 생성 및 서명

여기에 언급된 모든 내용은 다양한 문서에 요약되어 있습니다. 기능에 대한 추가 설명이 필요한 경우 제품 릴리스 정보를 읽고 프로그래밍 가이드 및 배포 가이드를 참조하는 것이 좋습니다. CMS 설치 및 구성 가이드와 CMS 제품 릴리스 정보.

사용되는 구성 요소

이 문서의 정보는 Cisco Meeting Server를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서는 단일 통합 또는 복원력 여부에 관계없이 이미 CMS 2.9.x(또는 이전) 구축을 완료했고 CMS 3.0으로 업그레이드할 계획이 있는 경우 이에 대한 지침입니다. 이 문서의 정보는 모든 CMS 모델과 관련이 있습니다.

> **참고:** X-Series를 CMS 3.0으로 업그레이드할 수 없습니다. 가능한 한 빨리 X-Series 서버를 교체해야 합니다.

업그레이드에 대한 중요 정보

CMS 업그레이드에 지원되는 유일한 방법은 단계별 업그레이드입니다. 이 글을 쓸 당시 CMS 3.5가 출시된 바 있다. CMS 2.9를 사용하는 경우 단계적으로 업그레이드해야 합니다(2.9 —> 3.0 —> 3.1 —> 3.2 —> 3.3 —> 3.4 —> 3.5(CMS 3.5부터 업그레이드 프로세스가 변경되었으므로 릴리스 정보를 주의 깊게 읽으십시오!!).

단계별 업그레이드를 수행하지 않고 비정상적인 동작이 발생하는 경우 TAC에서 다운그레이드 및 재시작을 요청할 수 있습니다.

또한 CMS 3.4부터 CMS는 스마트 라이센싱을 사용해야 합니다. CMS 3.4 이상으로 업그레이드할 수 없으며 기존 라이센스는 계속 사용할 수 있습니다. Smart Licensing을 설정하지 않은 경우 CMS

3.4 이상으로 업그레이드하지 마십시오.

고려할 사항 요약

이 질문을 사용하여 자신의 상황과 관련된 섹션으로 이동합니다. 각 고려 사항에는 이 문서에 제시된 보다 자세한 설명으로 연결되는 하이퍼링크가 포함됩니다.

라이센스

업그레이드하기 전에 서버에 PMP(Personal MultiParty)/SMP(Shared MultiParty) 라이센스가 충분히 있습니까?

3.0에서는 사용자가 로그인하지 않은 경우에도 PMP 라이센스가 할당됩니다. 예를 들어, LDAP를 통해 10000 사용자를 가져왔지만 PMP 라이센스가 100개뿐인 경우 3.0으로 업그레이드하는 즉시 규정 위반이 됩니다. 이 활용 사례에서는 userProfile이 설정된 테넌트 및/또는 시스템/프로필을 확인하여 값이 true인 userProfile이 설정되어 있는지 확인하십시오.

API에서 userProfile을 확인하고 hasLicense=true set(PMP 라이센스 사용자를 의미)이 있는지 확인하는 방법은 이 섹션에서 자세히 다룹니다.

현재 cms.lic 파일에 PMP/SMP 라이센스가 있습니까?

3.0 이후의 라이센스 동작 변경으로 인해 업그레이드를 수행하기 전에 PMP/SMP 라이센스가 충분한지 확인해야 합니다. 이에 대해서는 이 섹션에서 자세히 **설명합니다.**

CMM(Cisco Meeting Manager)을 구축했습니까?

라이센스 처리 방식이 변경되어 CMS 3.0에는 CMM 3.0이 필요합니다. 90일 보고서에서 지난 90일 동안의 라이센스 사용량을 확인할 수 있으므로 환경을 3.0으로 업그레이드하기 전에 CMM 2.9를 구축하는 것이 좋습니다. 이에 대해서는 이 섹션에서 자세히 **설명합니다**.

Smart Licensing을 보유하고 있습니까?

라이센스 처리 방식이 변경되어 CMS 3.0에는 CMM 3.0이 필요합니다. 따라서 CMM을 통해 Smart Licensing을 이미 사용 중인 경우 클러스터에 PMP 및 SMP 라이센스가 연결되어 있는지 확인합니다.

Webbridge(WebRTC 및 CMA 클라이언트)

CMS 2.9에서 WebRTC를 사용하십니까?

Webbridge는 CMS 3.0에서 크게 변경되었습니다. webbridge2에서 webbridge3로의 마이그레이션 및 웹 앱 사용에 대한 지침은 이 섹션에 있습니다.

사용자가 CMA 씩 클라이언트를 사용합니까?

이러한 클라이언트는 XMPP 기반이므로 업그레이드 후 XMPP 서버가 제거되었으므로 더 이상 이러한 클라이언트를 사용할 수 없습니다. 사용 사례에 해당하는 경우 이 섹션에서 자세한 내용을 확인할 수 있습니다.

WebRTC에서 채팅을 사용하십니까?

3.0에서는 웹 앱에서 채팅 기능이 제거됩니다. CMS 3.2에서는 채팅이 다시 도입되지만 지속적이지 않습니다. 이 기능에 대한 자세한 내용은 이 섹션에서 확인할 수 있습니다.

사용자가 WebRTC에서 디바이스로 포인트투포인트 통화를 수행합니까?

CMS 3.0에서는 웹 앱 사용자가 더 이상 다른 디바이스로 직접 전화를 걸 수 없습니다. 이제 미팅 공간에 참가하고, 참가자를 미팅에 추가하여 동일한 작업을 수행할 수 있는 권한이 있어야 합니다. 이 부분에 대한 자세한 내용은 이 섹션에서 확인할 수 있습니다.

사용자가 WebRTC에서 자체 coSpaces를 생성합니까?

3.0에서 웹 앱 사용자가 클라이언트에서 스페이스를 직접 만들 수 있으려면 coSpaceTemplate을 API에서 만들어 사용자에게 할당해야 합니다. 이는 LDAP 가져오기 중에 수동 또는 자동이 될 수 있습니다. CanCreateCoSpaces가 UserProfile에서 제거되었습니다. 이 기능에 대한 자세한 내용은 이 섹션에서 확인할 수 있습니다.

웹 GUI 변경

웹 관리 GUI에 webBridge 설정이 구성되어 있습니까?

3.0에서는 webBridge 설정이 GUI에서 제거되므로 API에서 웹 브리지를 구성하고 현재 설정이 GUI에 있는지 기록해야 API에서 webBridgeProfiles를 적절히 구성할 수 있습니다. 이 변경 사항에 대한 자세한 내용은 이 섹션에서 확인할 수 있습니다.

웹 관리 GUI에 외부 설정이 구성되어 있습니까?

CMS 3.1의 GUI에서 외부 설정이 제거되었습니다. CMS 3.0 또는 이전 웹 관리 GUI(컨피그레이션 —> 일반 —> 외부 설정)에서 Webbridge URL 또는 IVR을 구성한 경우 이러한 URL은 웹 페이지에서 제거되었으므로 API에서 구성해야 합니다. 3.1로 업그레이드하기 전의 이전 설정은 API에 추가되지 않으며 수동으로 수행해야 합니다. 이 변경 사항에 대한 자세한 내용은 이 섹션에서 확인할 수 있습니다.

리코더 / 스트리머

현재 CMS 레코더 및/또는 스트리머를 사용하고 계십니까?

이제 CMS 레코더 및 스트리머 구성 요소는 XMPP 기반이 아니라 SIP 기반입니다. 따라서 XMPP를 제거하는 중이므로 업그레이드 후 이를 수정해야 합니다. 이 변경 사항에 대한 자세한 내용은 이 섹션에서 확인할 수 있습니다.

Cisco Expressway 고려 사항

Expressway를 사용하여 WebRTC를 프록시하는 경우 현재 사용 중인 Cisco Expressway 버전은 무엇입니까?

CMS 3.0에는 Expressway 12.6 이상이 필요합니다. 이 섹션에서 이 WebRTC 프록시 기능에 대한 자세한 내용을 확인할 수 있습니다.

CMS 에지

현재 환경에 CMS Edge가 있습니까?

CMS Edge는 CMS 3.1에 다시 도입되었으며 외부 연결을 위한 확장성이 더욱 향상되었습니다. 이 부분에 대한 자세한 내용은 이 섹션에서 확인할 수 있습니다.

CMS(Acano) X-Series

현재 환경에 x-series 서버가 있습니까?

이 서버는 CMS 3.0으로 업그레이드할 수 없으며 곧 교체해야 합니다(3.0으로 업그레이드하기 전에 가상 머신 또는 CMS 어플라이언스로 이동). 이 링크에서 이러한 서버에 대한 단종 알림을 찾을 수 있습니다.

SIP 에지

현재 환경에서 SIP Edge를 사용하고 계십니까?

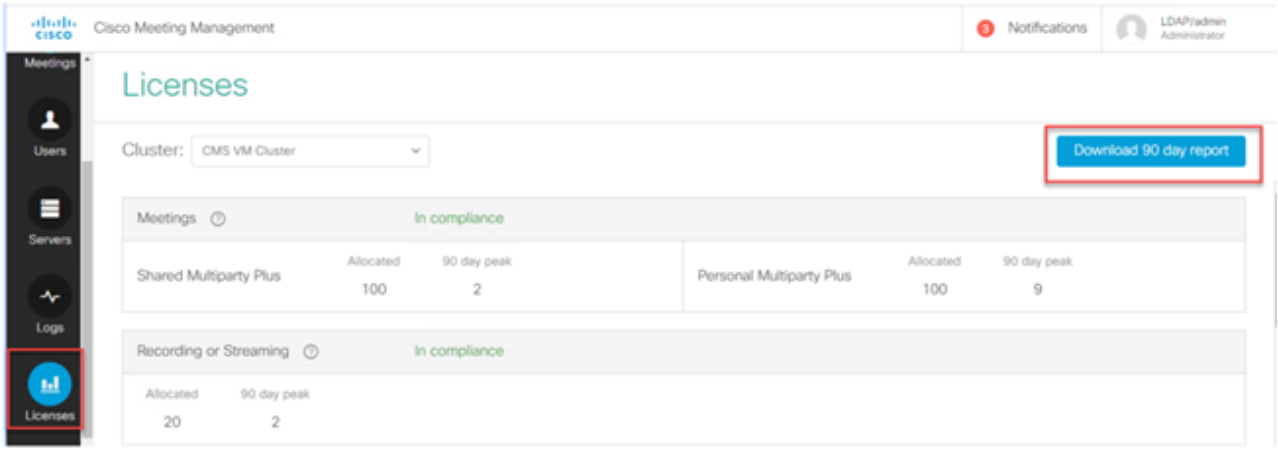
Sip Edge는 CMS 3.0부터 완전히 사용이 중단되었습니다. Cisco Expressway를 사용하여 CMS에 SIP 통화를 연결해야 합니다. Expressway를 조직에서 구입하는 방법은 Cisco 어카운트 담당자에게 문의하십시오.

추가 정보

라이센스 - 업그레이드 전에 라이센스 확인

규정 준수 위반 라이센스 상태는 2.x 버전에서 3.0 이상으로 업그레이드할 때 가장 큰 영향을 미치는 문제입니다. 이 섹션에서는 원활한 업그레이드를 위해 필요한 PMP/SMP 라이센스의 양을 결정하는 방법에 대해 설명합니다.

구축을 3.0으로 업그레이드하기 전에 CMM 2.9를 구축하고 Licenses(라이센스) 탭에서 **90일 보고서**를 확인하여 라이센스 사용량이 CMS 노드에서 현재 할당된 라이센스 금액 이하에 머물렀는지 확인합니다.

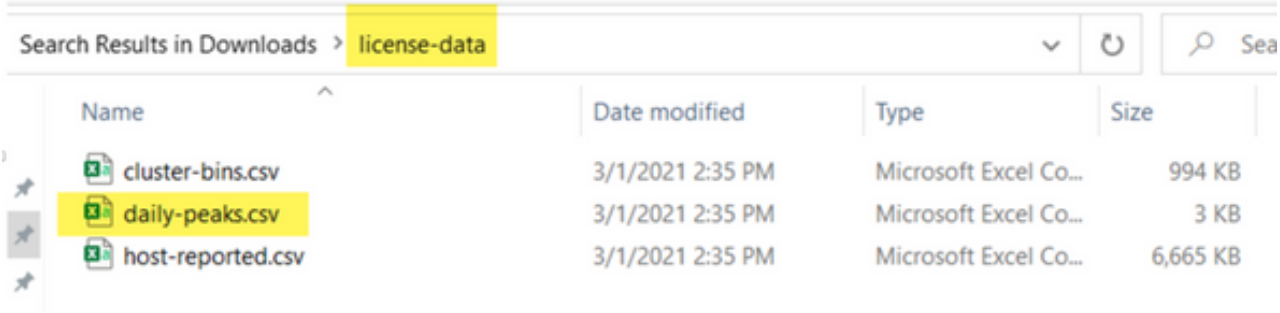


기존 라이센스(cms.lic 파일은 CMS 노드에 로컬로 설치됨)를 사용할 경우 CMS 라이센스 파일에서 각 CMS 노드의 개인 및 공유 라이센스 수량(여기 이미지에 따라 100/100)을 확인합니다(각 callBridge 노드에서 WinSCP를 통해 다운로드).

```
],
"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",
```


Smart Licensing을 이미 사용하고 있는 경우, CMS 서버용 Cisco Software Smart 포털에서 할당된 PMP/SMP 라이센스의 수를 확인합니다.

90일 보고서(Zip 파일의 이름은 *license-data.zip*)를 열고 *daily-picks.csv*라는 *파일을 엽니다*.



Excel에서 PMP 열을 Z에서 A로 정렬하여 높은 값을 맨 위로 가져온 다음 SMP 열에 대해 동일한 작업을 수행합니다. 이 파일에 표시된 값이 CMS 라이센스 파일에서 사용할 수 있는 라이센스보다 낮

습니까? 대답이 "예"인 경우, 당신은 괜찮고 완벽하게 규정을 준수합니다. 그렇지 않은 경우 그림 6의 CMS 구축 가이드 섹션 1.7.3에서 경고 및/또는 오류를 생성합니다. 이에 대한 자세한 내용은 섹션 1.7.4를 참조하십시오.

예를 들어 이미지에 따르면 지난 90일 동안 2.1667개의 SMP 라이센스가 사용되었으며 PMP 라이센스는 정점에 따라 사용되지 않았습니다. cms.lic 파일에 각 라이센스 유형의 단위가 100개로 표시되어 이 설정이 완전히 준수됩니다. 따라서 이 설치 프로그램을 CMS 3.0으로 업그레이드할 때는 라이센스 관련 문제가 발생하지 않습니다. 그러나 설치 시 LDAP를 통해 10,000명의 사용자를 가져왔을 때 문제가 발생할 수 있습니다. 그러면 PMP 라이센스는 100개만 있지만, 10000(hasLicense가 True로 설정된 userProfile)을 할당하므로 이 경우 3.0으로 업그레이드하자마자 컴플라이언스를 위반하게 됩니다. 이에 대한 자세한 내용은 다음 섹션을 참조하십시오.

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

업그레이드한 후 PMP 라이센스가 할당된 사용자 수 결정

가져오고 hasLicense=true인 userProfile을 **사용하**는 모든 **사용자**는 CMS 3.0에서 PMP 라이센스가 자동으로 할당됩니다.

API에서 보유하고 있는 userProfiles의 수를 확인하고 그중 하나라도 "hasLicense=true"가 설정되어 있는지 확인합니다. 사용자 프로파일이 할당된 위치를 확인해야 합니다.

사용자 프로필은 다음 레벨 중 하나에서 할당할 수 있습니다.

1. Ldap소스
2. 테넌트
3. 시스템/프로필

assigned userProfiles(할당된 사용자 프로필)의 3개 위치 모두에서 assignLicense=true를 선택합니다.

1. Ldap소스/테넌트

테넌트 또는 userProfile을 사용하는 각 ldapSource에 대해, hasLicense 매개변수가 True로 설정된 경우 해당 ldapSource로 가져온 사용자에게 PMP 라이센스가 할당됩니다. 테넌트가 있는 경우 테넌트 ID를 클릭하여 userProfile이 할당되었는지 확인한 다음 해당 userProfile이 'hasLicense=true'로 구성되어 있는지 확인해야 합니다. 테넌트가 없지만 userProfile 집합이 있는 경우 이를 클릭하여 'hasLicense=true'가 있는지 확인합니다. 어느 쪽이든 'hasLicense=true'인 경우 'api/v1/users'에 대해 GET을 수행하고 ldapSource에 연결된 ldapmapping에서 jidMapping에 사용된 도메인에 대해 필터링하여 가져온 사용자 수를 확인할 수 있습니다.

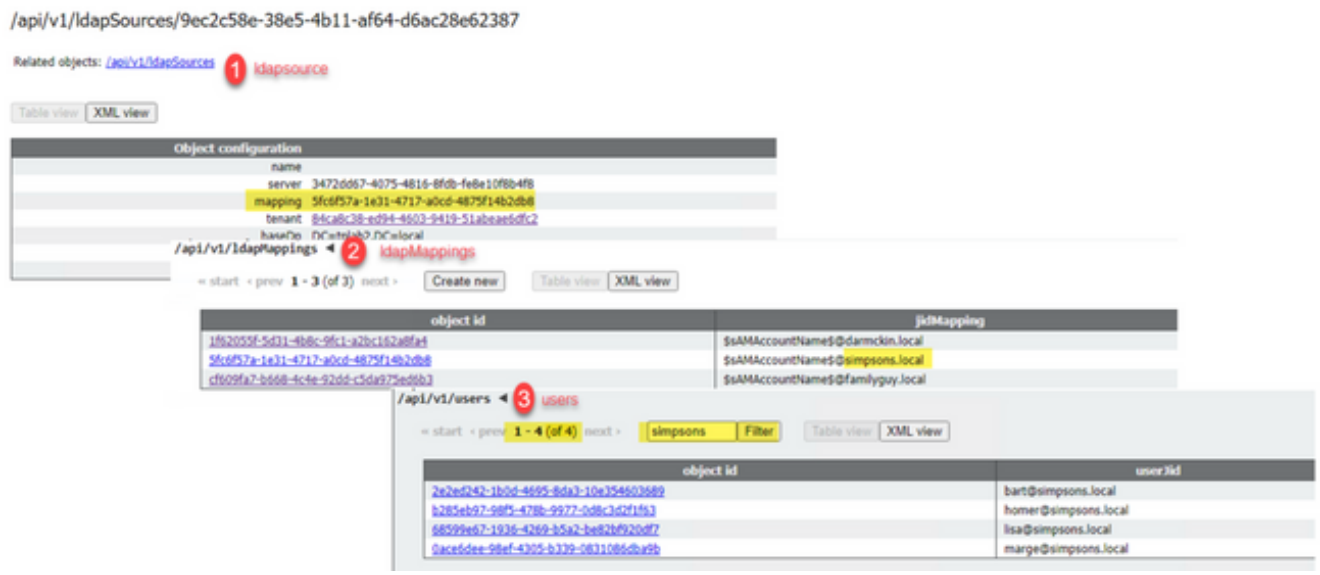
> **참고:** 이는 사용자가 생성한 ActiveDirectory 매핑 및 필터를 사용하여 이를 확인해야 하는 다른 상황에서는 더 복잡할 수 있습니다.

1단계. ldapSource에서 매핑 ID를 찾습니다.

2단계. ldapMappings를 검색하여 jidMapping을 찾습니다.

3단계. api/v1/users에서 jidMapping에 사용된 도메인을 검색합니다.

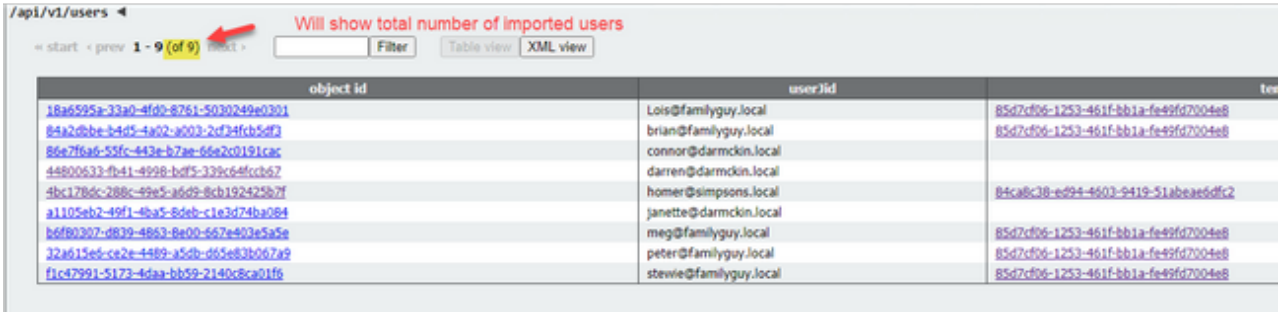
4단계. 각 ldapSource에서 찾은 사용자를 추가합니다. 가져온 LDAP 사용자 중 PMP 라이센스가 필요한 사용자 수입니다.



2. 시스템/프로필

userProfile이 시스템/프로필 수준으로 설정되어 있고 해당 userProfile에 "hasLicense=true"가 있으면 서버를 업그레이드할 때 CMS로 가져온 모든 사용자에게 PMP 라이센스가 할당됩니다. 10,000명의 사용자를 가져왔지만 PMP가 100개뿐인 경우, CMS 3.0으로 업그레이드할 때 규정을 준수하지 못하게 되며 통화가 시작될 때 화면에 30초 메시지가 표시되고 오디오 프롬프트가 표시될 수 있습니다.

시스템 레벨의 userProfile에서 사용자가 PMP를 가져와야 한다고 표시하는 경우 api/v1/users로 이동하여 총 사용자 수를 확인합니다.



이전에 ldap에서 모든 사용자를 가져왔지만 해당 목록의 특정 하위 집합만 필요하다는 것을 깨달은 경우 ldapSource에서 더 나은 필터를 생성하여 PMP 라이센스를 할당할 사용자만 가져오도록 합니다. ldapSource에서 필터를 수정한 다음 api/v1/ldapsync에서 새 LDAP 동기화를 수행합니다. 이렇게 하면 원하는 사용자만 가져오고, 이 이전 가져오기의 다른 모든 사용자는 제거됩니다.

> **참고:** 이 작업을 올바르게 수행하고 새 가져오기를 통해 원치 않는 사용자만 제거할 경우 나머지 사용자 coSpace CallID 및 암호는 변경되지 않지만, 실수로 인해 모든 callId 및 암호가 변경될 수 있습니다. 이 문제가 우려되는 경우 시도하기 전에 데이터베이스 노드를 백업하십시오!

SMP 라이센스가 충분합니까?

CMM 90 Day Report(CMM 90일 보고서)에서 일일 피크 시간을 확인했을 때, 최대 피크 시간에 맞출 수 있는 SMP 라이센스가 이미 충분합니까? SMP 라이센스는 미팅 소유자에게 PMP 라이센스가 할당되지 않은 경우 사용됩니다(coSpace 소유자/임시 미팅/TMS 예약 미팅). SMP를 의도적으로 사용하고 피크 시간을 충분히 감당할 수 있다면 이 방법도 괜찮습니다. SMP에 대한 90일 피크를 확인하고 이것이 왜 소비되는지 불분명하다면, 몇 가지 확인할 사항이 있다.

1. 병합에 사용된 장치가 userProfile을 통해 CMS에서 PMP 라이센스를 할당받은 사용자와 연결되지 않은 경우 CUCM에서 에스컬레이션된 임시 통화에서 SMP 라이센스를 사용합니다. CUCM은 회의를 에스컬레이션하는 사용자의 GUID를 제공합니다. 해당 GUID가 할당된 PMP 라이센스가 있는 가져온 Meeting Server LDAP 사용자에 해당하는 경우 해당 사용자의 라이센스가 사용됩니다.

2. CoSpace 소유자에게 PMP 라이센스가 할당되지 않은 경우 특정 CoSpace에 대한 통화는 SMP 라이센스를 사용합니다.

3. 미팅이 TMS 버전 15.6 이상에서 예약되어 있는 경우, 회의 소유자는 CMS로 전송되며, 사용자에게 PMP 라이센스가 할당되지 않은 경우 해당 미팅은 SMP 라이센스를 사용합니다.

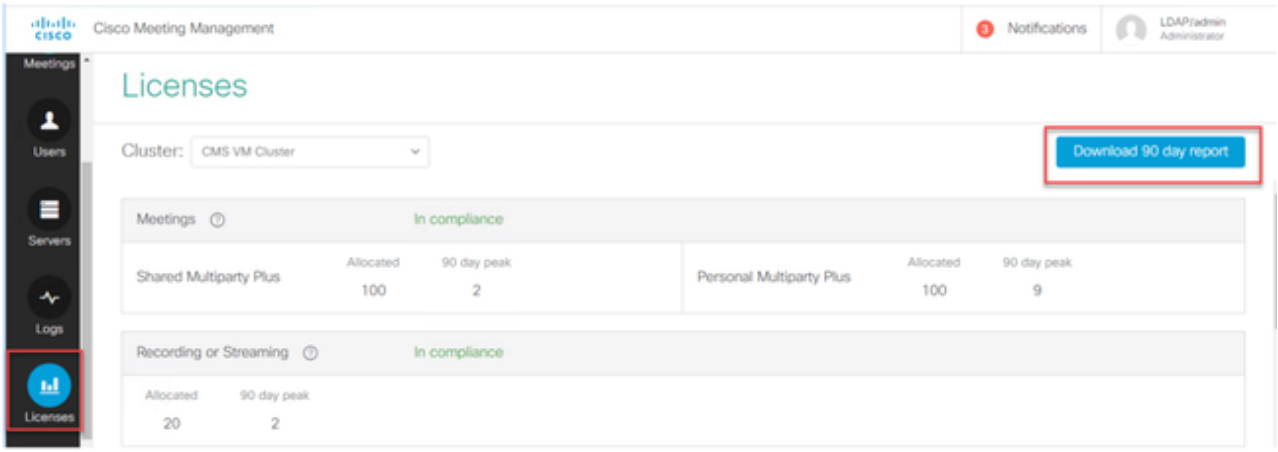
CMM 구성

CMS가 제대로 작동하려면 CMS 3.0과 마찬가지로 CMM 3.0이 필요합니다. CMM은 CMS 라이센스를 담당하므로 CMS를 3.0으로 업그레이드하려는 경우 CMM 서버가 있어야 합니다. CMS 2.9를 사용하는 동안에는 CMM 2.9를 구축하는 것이 좋습니다. 그러면 업그레이드하기 전에 라이센스 사용량을 확인할 수 있습니다.

CMM은 추가된 모든 callBridge에서 SMP 및 PMP 라이센스와 callBridge 라이센스를 확인합니다. 클러스터 내의 여러 디바이스 전체에서 가장 높은 번호를 사용합니다.

예를 들어 기존 라이센스에서 CMS1에 PMP 라이센스가 20개, SMP 라이센스가 10개 있고 CMS2에 PMP 라이센스가 40개, SMP 라이센스가 5개 있는 경우 CMM은 사용할 PMP 라이센스가 40개, SMP 라이센스가 10개라고 보고합니다.

PMP 라이센스가 가져온 사용자보다 많은 경우 PMP(또는 SMP) 라이센스와 관련된 문제는 없지만, 90일 정점을 확인하고 사용 가능한 것보다 더 많이 사용한 것을 발견하더라도 CMS 3.0으로 업그레이드하고 CMM에서 90일 평가판 라이센스를 사용하여 라이센스로 문제를 정리하거나 업그레이드 전에 조치를 취할 수 있습니다.



Webbridge 구성(WebRTC 및 CMA 클라이언트)

CMS 3.0은 XMPP 서버 구성 요소를 제거하므로 webBridge와 CMA 씩 클라이언트를 사용하는 기능이 제거됩니다. WebBridge3은 브라우저를 사용하여 웹 앱 사용자(이전의 WebRTC 사용자)를 미팅에 연결하는 데 사용됩니다. 3.0으로 업그레이드할 경우 webbridge3를 구성해야 합니다.

> **참고:** CMS 3.0으로 업그레이드한 후 CMA 씩 클라이언트는 작동하지 않습니다!

이 비디오에서는 webbridge 3 인증서를 생성하는 프로세스를 안내합니다.

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

3.0으로 업그레이드하기 전에 고객은 Webbridge3 구성 방법을 계획해야 합니다. 가장 중요한 단계는 여기에 강조 표시되어 있습니다.

1. webbridge3에 대한 키 및 인증서 체인이 필요합니다. 인증서가 webbridge3를 실행 중인 SAN(주체 대체 이름)/CN(공용 이름)으로서 모든 CMS 서버 FQDN 또는 IP 주소를 포함하고 있고 다음 중 하나가 충족되는 경우 이전 webbridge 인증서를 사용할 수 있습니다.

a. 인증서에 고급 키 사용이 없습니다(클라이언트 또는 서버로 사용할 수 있음).

b. 인증서에는 클라이언트 및 서버 인증이 모두 있습니다. HTTPs 인증서는 서버 인증만 필요하지만 C2W 인증서에는 서버와 클라이언트가 모두 필요합니다.)

2. "webbridge**3 https**" 인증서에 대한 새 인증서를 만들려면 (웹 앱을 사용할 때 클라이언트에서 인증서 경고를 피하기 위해) 공개 서명하는 것이 좋습니다. 이 동일한 인증서를 "webbridge3 c2w cert"에 사용할 수 있으며, 인증서에는 SAN/CN에 있는 webbridge 서버의 FQDN이 있어야 합니다.

3. CallBridge는 webbridge3 **c2w listen** 명령에서 구성된 포트를 사용하여 새 webbridge**3과 통신해야** 합니다. 449와 같이 사용 가능한 모든 포트가 될 수 있습니다. 사용자는 callbridge가 이 포트의 webbridge3와 통신할 수 있는지 확인하고, 필요한 경우 미리 방화벽을 변경해야 합니다. "webbridge https"에서 수신 대기하는 데 사용하는 포트와 같을 수 없습니다.

CMS를 3.0으로 업그레이드하기 전에 '백업 스냅샷 <servername_date>'를 사용하여 백업을 수행한 다음 callbridge 노드의 webadmin 페이지에 로그인하여 모든 XMPP 설정 및 Webbridge 설정을 제거하는 것이 좋습니다. 그런 다음 서버의 MMP에 연결하고 SSH 연결을 통해 xmpp 및 webbridge가 있는 모든 코어 서버에서 다음 단계를 수행합니다.

1. **xmpp 비활성화**
2. **xmpp 재설정**
3. **xmpp certs none**
4. **xmpp 도메인 없음**
5. **webbridge 비활성화**
6. **webbridge 수신 대기 없음**
7. **webbridge certs 없음**
8. **webbridge 트러스트 없음**

3.0으로 업그레이드한 후에는 이전에 webbridge를 실행한 모든 서버에서 webbridge3를 구성하여 시작합니다. 이러한 서버를 가리키는 DNS 레코드가 이미 있기 때문에 이 작업을 수행해야 합니다. 따라서 사용자가 webbridge3로 전송될 경우 요청을 처리할 준비가 되었는지 확인합니다.

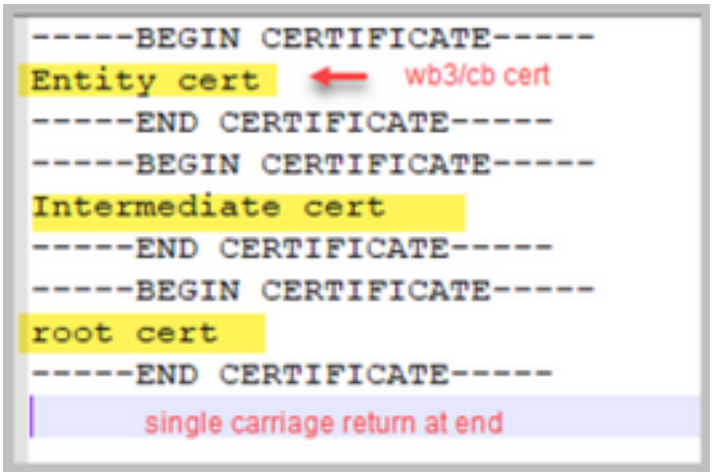
Webbridge3 컨피그레이션(모두 SSH 연결을 통해)

1단계. webbridge3 http 수신 대기 포트를 구성합니다.

Webbridge3 https 수신 대기 a:443

2단계. 브라우저 연결을 위해 webbridge3용 인증서를 구성합니다. 이 인증서는 브라우저에 전송되며 공용 CA(Certificate Authority)에서 서명해야 하며 브라우저에서 연결을 신뢰하도록 브라우저에서 사용하는 FQDN을 포함해야 합니다.

Webbridge3 https certs wb3.key wb3trust.cer(이것은 신뢰 체인이어야 합니다. 맨 위에 끝 엔티티가 있고 그 뒤에 중간 CA가 순서대로 있는 신뢰 인증서를 만들고 RootCA로 마무리합니다.



3단계. c2w(callBridge to webbridge) 연결을 수신하는 데 사용할 포트를 구성합니다. 443은 webbridge3 https 수신 대기 포트에 사용되므로 이 구성은 449와 같이 다른 사용 가능한 포트여야 합니다.

Webbridge3 c2w 수신 대기 a:449

4. webbridge가 c2w 트러스트를 위해 callbridge에 보내는 인증서를 구성합니다

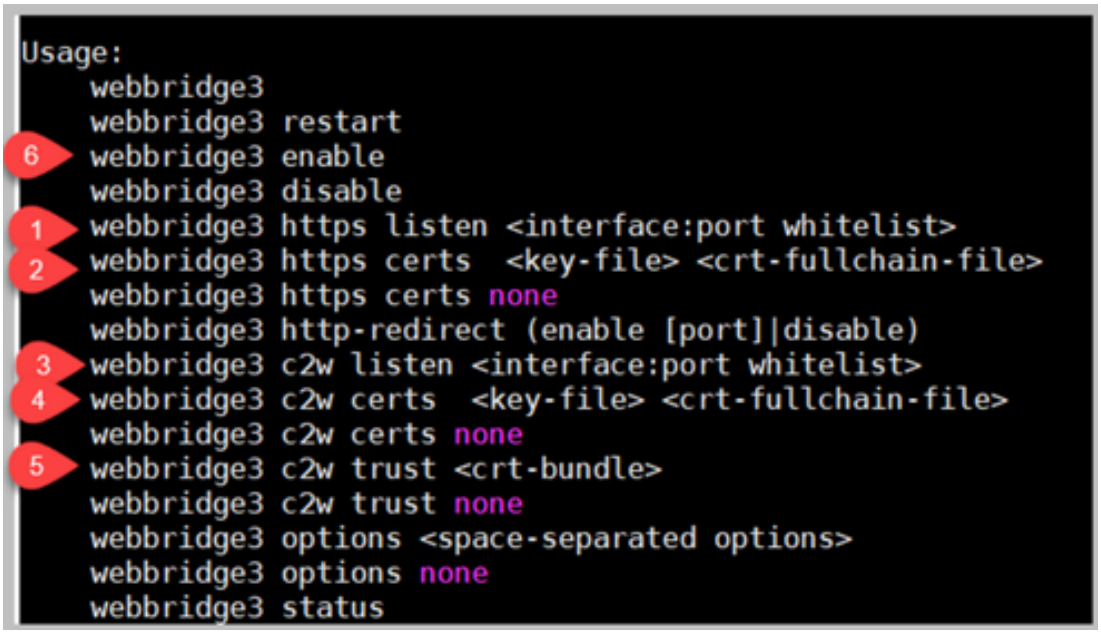
Webbridge3 c2w certs wb3.key wb3trust.cer

5. WB3에서 callBridge 인증서를 신뢰하는 데 사용하는 트러스트 저장소를 구성합니다. 이 값은 callbridge CA 번들에서 사용된 인증서와 동일해야 합니다(맨 위에 중간 인증서 번들이 있고 맨 끝에 루트 CA가 있고 단일 캐리지 리턴이 있어야 함).

Webbridge3 c2w 트러스트 rootca.cer

6. webbridge3 활성화

Webbridge3 활성화



CallBridge 컨피그레이션 변경(모두 SSH 연결을 통해)

1단계. webbridge3 c2w 인증서에 서명한 CA 인증서/번들로 callBridge 트러스트를 구성합니다.

Callbridge 트러스트 c2w rootca.cer

2단계. callBridge를 다시 시작하여 새 트러스트를 적용합니다. 이렇게 하면 이 특정 callBridge의 모든 통화가 중단되므로 이 작업을 신중하게 사용하십시오.

Callbridge 다시 시작

webBridge3에 연결하기 위한 callBridge의 API 컨피그레이션

1. API에서 POST를 사용하여 새 webBridge 개체를 만들고 webbridge c2w 인터페이스 화이트리스트에 구성된 FQDN 및 포트를 사용하여 URL 값을 제공합니다(webbridge3 구성의 3단계).

c2w://webbridge.darmckin.local:449

이때 Webbridge3는 다시 작동하며 스페이스를 게스트로 조인할 수도 있고, 이전에 가져온 사용자가 있으면 해당 사용자가 로그인할 수 있어야 합니다.

웹 앱 사용자 공간 만들기 권한

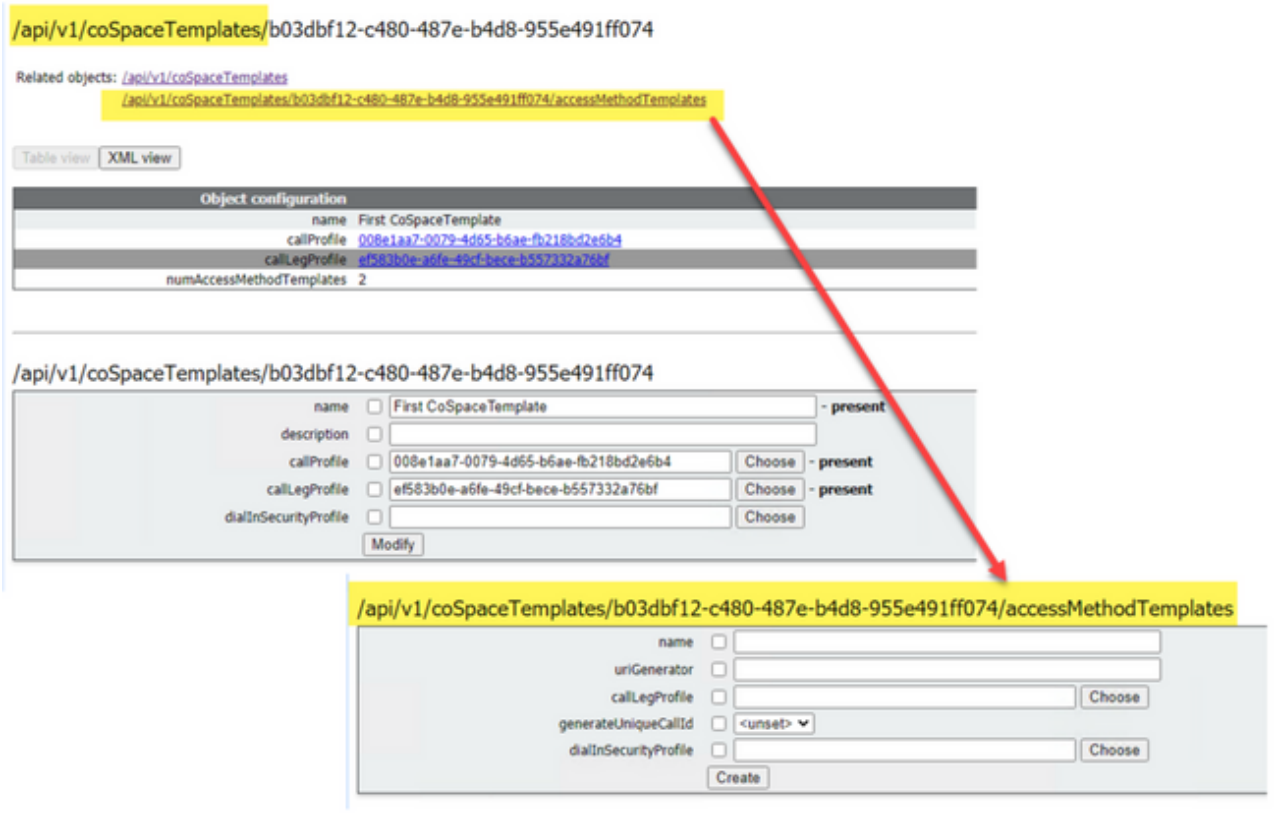
사용자가 WebRTC에서 스페이스를 직접 만들 수 있는 데 익숙합니까? CMS 3.0부터 웹 앱 사용자는 자신에게 할당된 cospace 템플릿이 없으면 자신의 coSpaces를 만들 수 없습니다.

coSpaceTemplate이 할당된 경우에도 다른 사용자가 다이얼할 수 있는 공간을 만들지 않습니다(URI 없음, 통화 ID 또는 암호 없음). 그러나 coSpace에 'addParticipantAllowed'가 있는 callLegProfile이 있는 경우 해당 사용자는 공간에서 다이얼아웃할 수 있습니다.

새 스페이스로 전화를 거는 데 사용할 수 있는 다이얼 문자열을 사용하려면 coSpaceTemplate에 accessMethodTemplate 설정이 있어야 합니다(2.9 릴리스 정보 - 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 참조).

API에서 coSpaceTemplate을 만든 다음 accessMethodTemplate을 만들고 ldapUserCoSpaceTemplateSources에 coSpaceTemplate을 할당하거나, api/v1/users의 사용자에게 coSpaceTemplate을 수동으로 할당할 수 있습니다.

여러 CoSpaceTemplates 및 accessMethodsTemplates를 만들고 할당할 수 있습니다. 자세한 내용은 CMS API 설명서(https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html)를 참조하십시오.



CoSpaceTemplate(API 구성)

이름: coSpaceTemplate에 지정할 이름입니다.

설명: 필요한 경우 간단한 설명

통화 프로필: White callProfile 이 템플릿으로 생성된 공백을 사용하시겠습니까? 제공되지 않을 경우 시스템/프로파일 레벨에서 설정된 것을 사용합니다.

calllegProfile: 이 템플릿으로 만든 공백을 사용할 calllegProfile을 선택하십시오. 제공되지 않을 경우 시스템/프로파일 레벨에서 설정된 것을 사용합니다.

dialIn보안 프로파일: 이 템플릿으로 만든 공백을 어떤 dialInSecurityProfile에서 사용하시겠습니까? 제공되지 않을 경우 시스템/프로파일 레벨에서 설정된 것을 사용합니다.

AccessMethodTemplate(API 구성)

이름: coSpaceTemplate에 지정할 이름입니다.

uriGenerator: 이 액세스 메서드 템플릿에 대한 URI 값을 생성하는 데 사용되는 식입니다. 허용되는 문자 집합은 'a'에서 'z', 'A'에서 'Z', '0'에서 '9', '.', '-', '_' 및 '$'입니다. 비어 있지 않으면 정확히 하나의 '$' 문자를 포함해야 합니다. 예를 들면 공간을 만들 때 사용자가 제공한 이름을 사용하고 ".space"를 추가하는 $.space가 있습니다. "팀 모임"은 url 'Team.Meeting.space@domain'을 만듭니다.

callLegProfile: 이 템플릿으로 만든 accessMethod에서 사용할 callIegProfile을 선택하십시오. 제공하지 않으면 설정된 CoSpaceTemplate 레벨을 사용하고, CoSpaceTemplate 레벨이 없으면 시스템/프로파일 레벨에 있는 것을 사용합니다.

generateUniqueCallId: cospace에 대한 전역 ID를 재정의하는 이 액세스 메서드에 대해 고유한 숫자 ID를 생성할지 여부를 지정합니다.

dialIn보안 프로파일: 어떤 dialInSecurityProfile에서 이 템플릿으로 만든 액세스 메서드를 사용하시겠습니까? 제공하지 않으면 설정된 CoSpaceTemplate 레벨을 사용하고, CoSpaceTemplate 레벨이 없으면 시스템/프로파일 레벨에 있는 것을 사용합니다.

채팅 기능

CMS 3.0에서 Persistent Chat 기능을 제거했지만 CMS 3.2에서는 공간 내 비Persistent Chat 기능이 반환되었습니다. 채팅은 웹 앱 사용자가 사용할 수 있으며 어디에도 저장되지 않습니다. CMS 3.2가 설치되면 웹 앱 사용자는 기본적으로 모임 중에 서로 메시지를 주고받을 수 있습니다. 이러한 메시지는 회의 중에만 사용할 수 있으며, 참가 후 교환된 메시지만 표시됩니다. 나중에 참가하고 다시 스크롤하여 이전 메시지를 볼 수 없습니다.

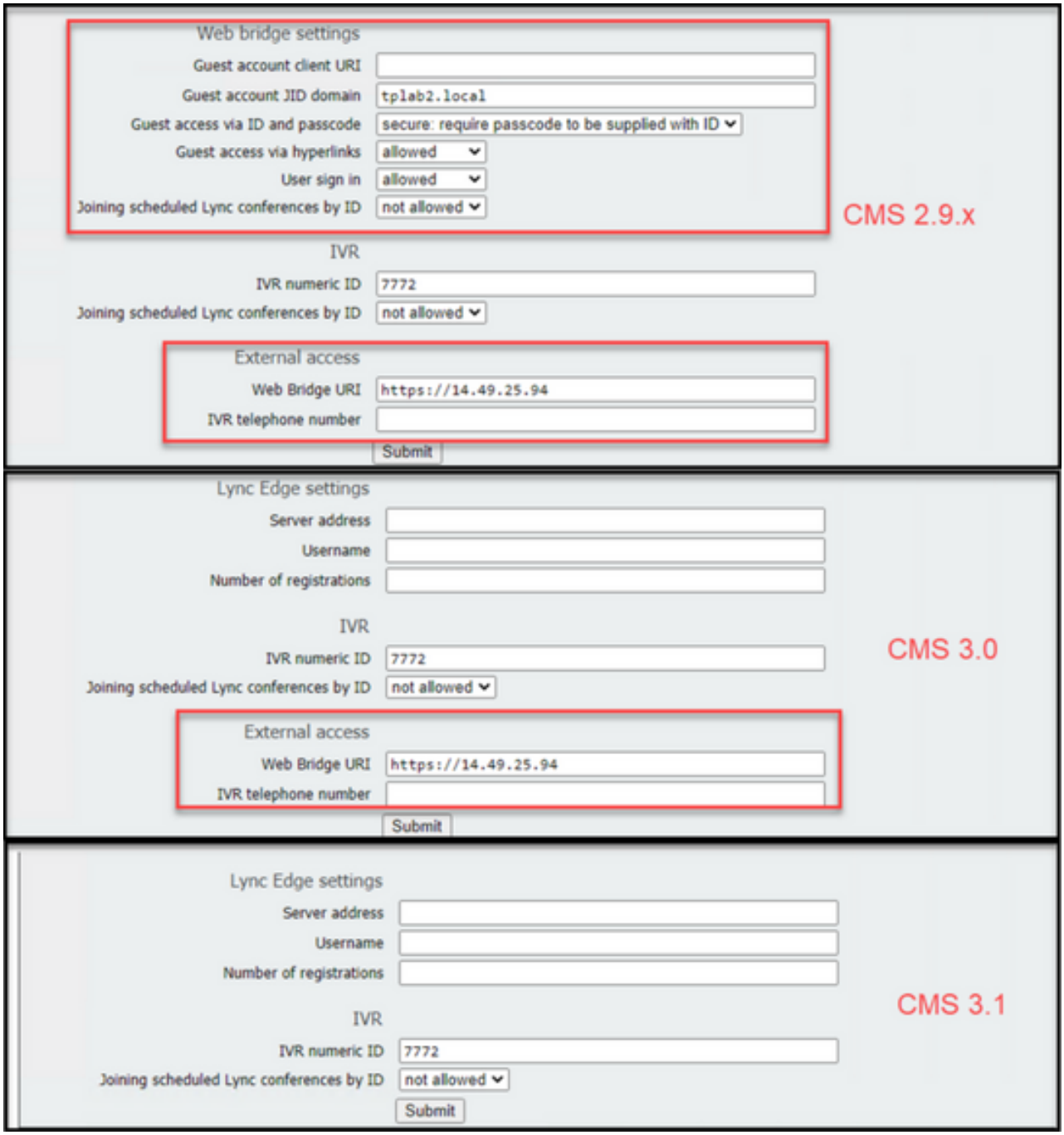
WebRTC 지점 간 통화

CMS 2.9.x에서 WebRTC 참가자는 자신의 클라이언트에서 직접 다른 연락처로 전화를 걸 수 있었습니다. CMS 3.0부터는 더 이상 불가능합니다. 이제 사용자가 로그인하고 스페이스에 가입해야 합니다. 여기에서 callLegProfile에 권한이 있는 경우(addParticipants 매개 변수가 True로 설정된 경우) 다른 연락처를 추가할 수 있습니다. 그러면 CMS에서 참가자에게 전화를 걸어 CMS의 한 공간에서 만나게 됩니다.

주목할 만한 webBridge 설정 변경

CMS 3.0 및 3.1은 GUI에서 일부 webbridge 설정을 제거했거나 재배치했으며 API에서 이를 구성하여 사용자의 일관된 환경을 유지해야 합니다. 3.x에서는 **api/v1/webBridges** 및 **api/v1/webBridgeProfiles를 사용합니다**.

3.0으로 업그레이드할 때 API에서 webbridge 및 webbridge 프로파일을 적절히 구성할 수 있도록 현재 구성한 내용을 확인합니다.

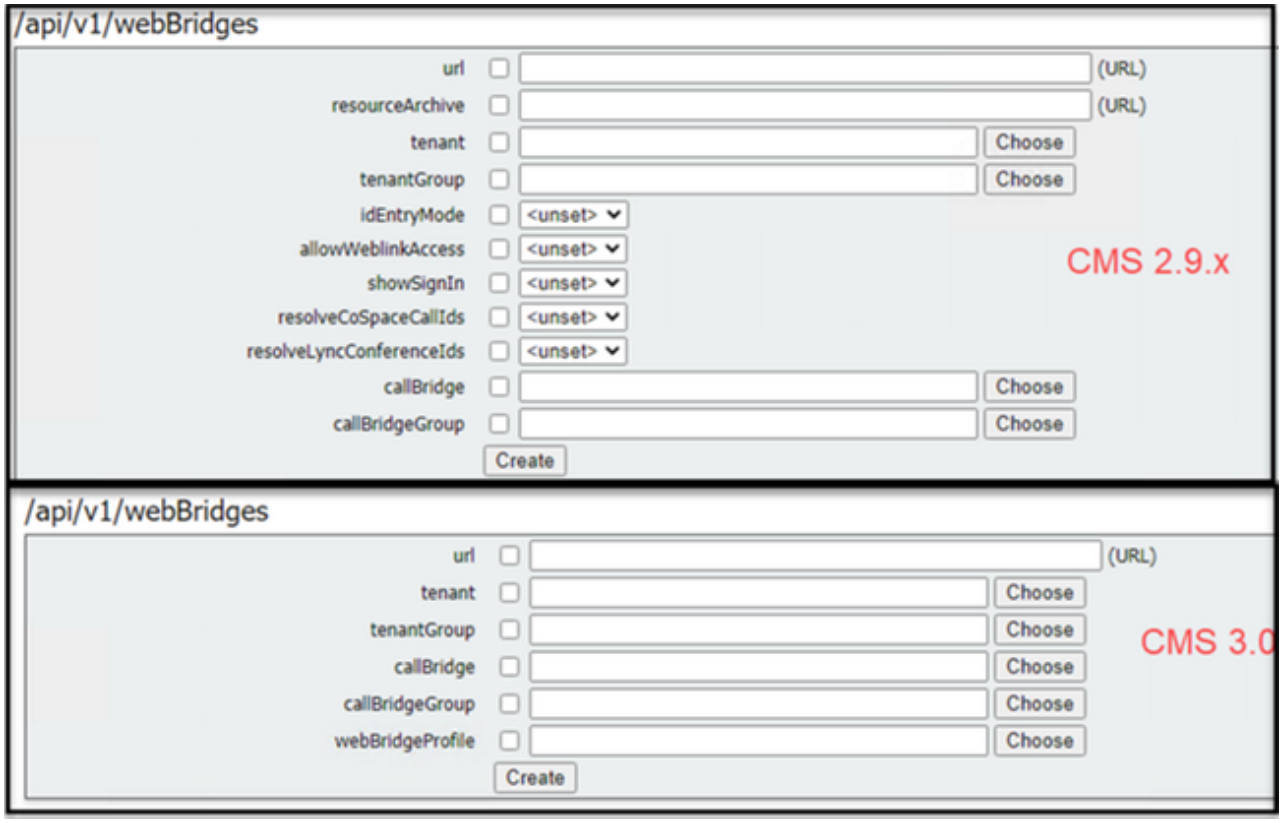


3.0에서는 GUI에서 **웹 브리지 설정**이 제거되고 CMS 3.1에서는 **외부 액세스** 필드도 제거되었습니다.

GUI의 웹 브리지 설정

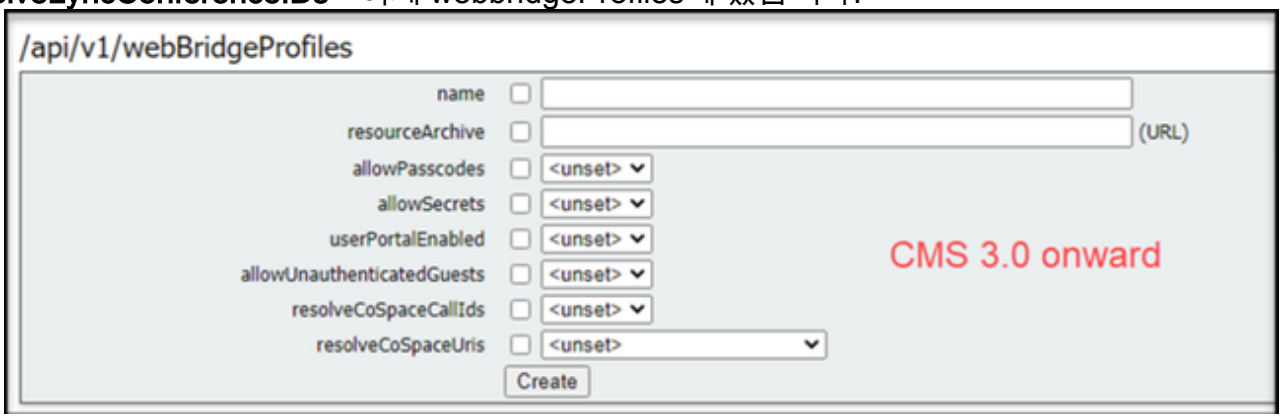
- **게스트 계정 클라이언트 URI** - 이 URI는 callBridge에서 webBridge를 찾는 데 사용되었습니다. WebRTC용 배포에 여러 개의 webBridge가 있는 경우 이 필드는 이미 비어 있어야 하며 callBridge가 연결해야 하는 각 webBridge에 대해 api/v1/webbridge에 고유한 URL이 있어야 합니다. 이 필드의 내용을 삭제하고 API에 webBridge가 구성되어 있는지 확인하십시오.

- **게스트 어카운트 Jid 도메인** - CMS 3.0에서는 더 이상 사용되지 않으며 이를 삭제할 수 있습니다.
- **ID 및 패스코드를 통한 게스트 액세스** - CMS 3.0에서 제거되었거나 교체되지 않았습니다.
- **Hyper Links를 통한 게스트 액세스** - 이제 "AllowSecrets" 설정의 API의 webBridgeProfiles에서 구성할 수 있습니다.



CMS 3.0에서는 api/v1/webBridges에서 서버 필드가 제거되었습니다.

- **resourceArchive** - webbridgeProfiles에 있습니다.
- **idEntryMode** - 더 이상 사용되지 않습니다.
- **allowWeblinkAccess** - 이제 webBridgeProfiles에서 allowSecrets로 지정됩니다.
- **showSignin** - 이제 webBridgeProfiles에서 userPortalEnabled로 표시됩니다.
- **resolveCoSpaceCallIds** - 이제 webbridgeProfiles에 있습니다.
- **resolveLyncConferenceIDs** - 이제 webbridgeProfiles에 있습니다.



WebBridge프로파일

- **resourceArchive** - 사용자 지정 배경을 사용하고 리소스 아카이브가 웹 서버에 저장되어 있는 경우 여기에 URL을 입력합니다.
- **allowPasscodes** - false인 경우 사용자가 게스트로 회의에 참가할 수 있는 옵션이 없습니다. 스페이스 정보 및 암호가 포함된 URL만 로그인하거나 사용할 수 있습니다
- **allowSecrets** - false로 설정하면 https://meet.company.com/meeting/040478?secret=gPDnucF8is4W1cS87_l.zw과 같은 URL을 사용하여 스페이스에 참가할 수 없습니다. 사용자는 https://meet.company.com을 사용하고 통화 ID/모임 ID/URI 및 PIN/암호(구성된 경우)를 입력해야 합니다.

- **userPortalEnabled** - false로 설정된 경우 웹 앱 포털 랜딩 페이지에 로그인 옵션이 표시되지 않습니다. 통화 ID/회의 ID/URI 및 PIN/암호(구성된 경우)를 입력하는 필드만 표시됩니다.
- **allowUnauthenticatedGuests** - False로 설정된 경우 모임 ID와 암호가 포함된 전체 URL을 사용하더라도 게스트는 어떤 모임에도 참가할 수 없습니다. False인 경우 로그인할 수 있는 사용자만 미팅에 참가할 수 있습니다. 예. 사용자2가 사용자1의 모임에 대한 URL을 사용하려고 합니다. URL을 입력한 후 User2가 로그인해야 User1의 미팅이 진행됩니다.
- **resolveCoSpaceCallIds** - False(거짓)로 설정된 경우 게스트는 URI 및 PIN/패스코드를 입력해야만 미팅에 참가할 수 있습니다(사용되는 경우). 통화 ID/회의 ID/숫자 ID는 허용되지 않습니다.
- **resolveCoSpaceUris** - 3가지 가능한 설정: off, domainSuggestionDisabled 및 domainSuggestionEnabled입니다. 이 webBridge에서 방문자가 cospace 모임에 참가할 수 있도록 coSpace 및 coSpace accessMethod SIP URI를 허용할지 여부를 지정합니다.

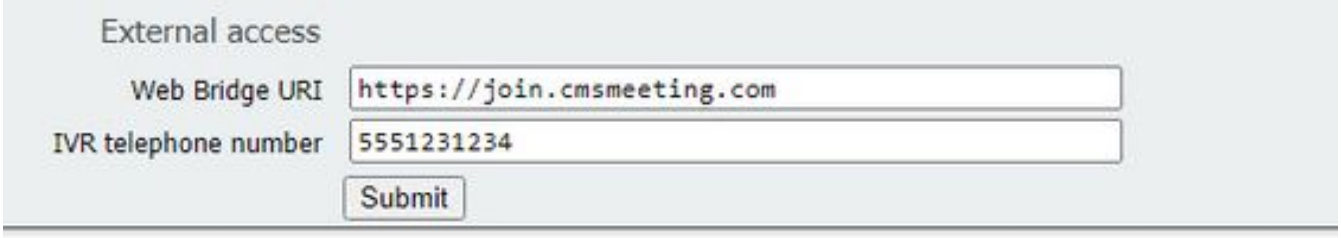
- '*off*'로 설정된 경우 URI로 가입할 수 없습니다.

- 'domainSuggestionDisabled'로 설정하면 URI에 의한 조인이 활성화되지만 이 webBridgeProfile을 사용하는 webBridges에서 URI의 도메인이 자동으로 완료되거나 확인되지 않습니다.

- 'domainSuggestionEnabled'로 설정된 경우 URI에 의한 조인이 활성화되며 이 webBridgeProfile을 사용하여 웹 브리지에서 URI의 도메인을 자동 완성하고 확인할 수 있습니다.

웹 GUI에서 외부 액세스 섹션 제거

CMS 3.1에서는 웹 GUI에서 외부 액세스 섹션이 제거되었습니다. 업그레이드 전에 이러한 구성을 구성한 경우 webbridgeProfiles 아래의 API에서 다시 구성해야 합니다.



먼저 이전 섹션에서 설명한 대로 webbridgeProfile을 만들어야 합니다. webbridgeProfile을 만든 후에는 새로 만든 webBridgeProfile 아래의 API에서 사용 가능한 링크를 통해 IVR 번호 및/또는 웹 브리지 URI를 만들 수 있습니다.

webBridgeProfile당 최대 32개의 IVR 번호 또는 32개의 webbridgeAddresses를 만들 수 있습니다

녹음 또는 스트리밍

CMS 2.9.x 이전 버전의 레코더 및 스트리머 구성 요소는 XMPP 클라이언트였으며 CMS 3.0에서는

SIP 기반입니다. 이제 API의 기본 레이아웃을 사용하여 녹음 및 스트리밍의 레이아웃을 변경할 수 있습니다. 또한 이제 녹음/스트리밍 세션에 이름 레이블이 표시됩니다. 레코더/스트리밍 기능에 대한 자세한 내용은 CMS 3.0 릴리스 정보 (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)를 참조하십시오.

2.9.x에서 레코더 또는 스트리머를 구성한 경우 MMP 및 API의 설정을 재구성하여 업그레이드 후에도 이 설정이 계속 작동하도록 해야 합니다.

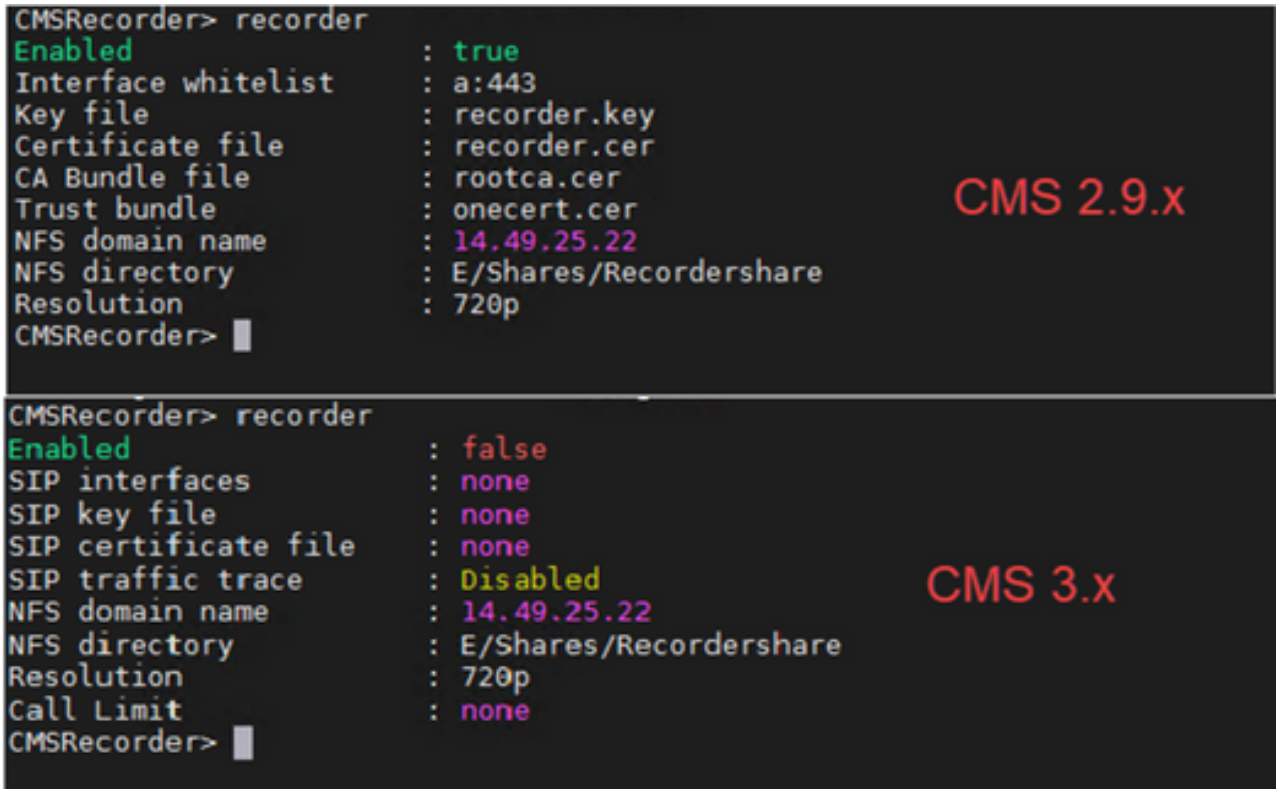
CMS를 3.0으로 업그레이드하기 전에 '백업 스냅샷 <servername_date>'를 사용하여 백업을 수행한 다음 callbridge 노드의 webadmin 페이지에 로그인하여 모든 XMPP 설정을 제거하는 것이 좋습니다. 그런 다음 서버의 MMP에 연결하고 SSH 연결을 통해 xmpp가 있는 모든 코어 서버에서 다음 단계를 수행합니다.

1. **xmpp 비활성화**
2. **xmpp 재설정**
3. **xmpp certs none**
4. **xmpp 도메인 없음**

레코더

MMP

이 그림에는 레코더를 구성할 때 CMS 2.9.1에서 볼 수 있는 구성의 예가 나와 있으며 3.0으로 업그레이드한 직후에 어떻게 보일지 나와 있습니다.



업그레이드 후 레코더를 재구성해야 합니다.

1단계. SIP 수신 대기 인터페이스를 구성합니다.

레코더 sip listen a 5060 5061(SIP 레코더가 TCP 및 TLS를 수신 대기하도록 설정한 인터페이스 및

포트) TLS를 사용하지 않으려면 '**레코더 sip listen a 5060 none**'을 사용할 수 있습니다.

2단계. TLS 연결을 사용하는 경우 레코더가 사용하는 인증서를 구성합니다.

레코더 sip 인증서 <key-file> <crt-file> [crt-bundle] (이러한 인증서가 없으면 레코더에서 tls 서비스가 시작되지 않습니다. 레코더는 crt 번들을 사용하여 callBridge 인증서를 확인합니다.

3단계. 통화 제한을 구성합니다.

recorder limit <0-500|none> (서버가 제공할 수 있는 동시 녹음 수의 제한을 설정합니다. 이 표는 설명서에 나와 있으며 레코더 제한은 서버의 리소스와 일치해야 합니다.)

Table 6: Internal SIP recorder performance and resource usage

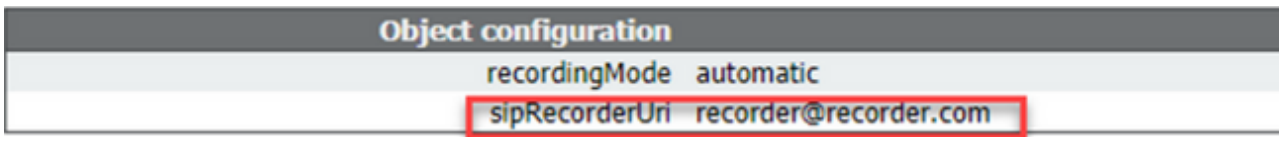
Recording Setting	Recordings per vCPU	RAM required per recording	Disk budget per hour	Maximum concurrent recording
720p	2	0.5GB	1GB	40
1080p	1	1GB	2GB	20
audio	16	100MB	150MB	100

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

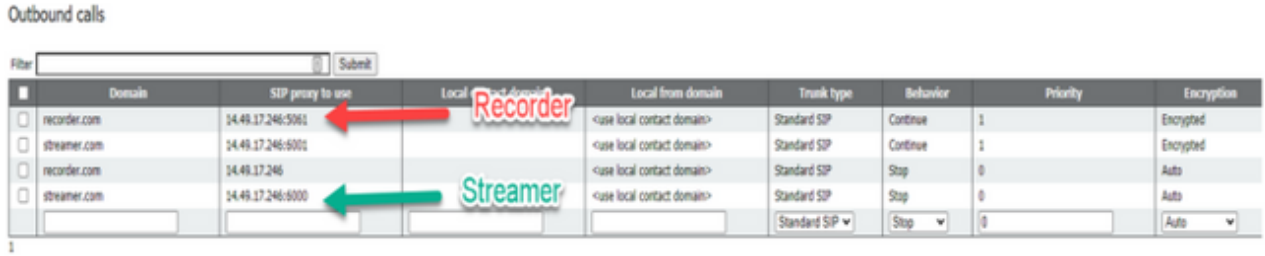
- Performance scales linearly adding vCPUs up to the number of host physical cores.

API

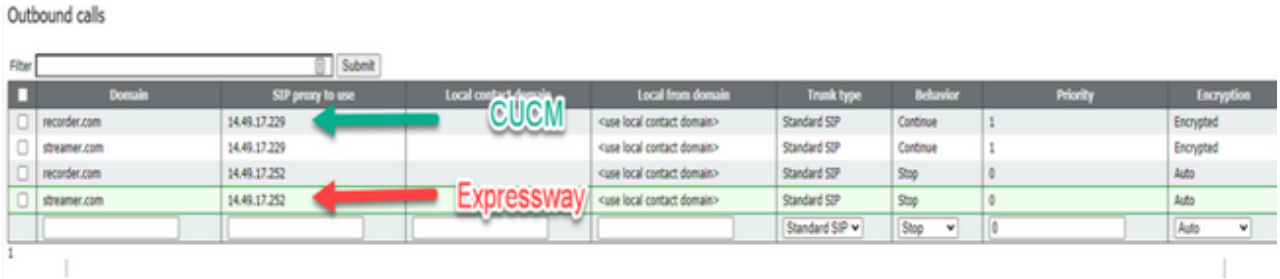
api/v1/callProfiles에서 sipRecorderUri를 **구성해야 합니다**. 녹음을 시작해야 할 때 callBridge에서 호출하는 URI입니다. 이 URI의 도메인을 아웃바운드 규칙 테이블에 추가하고 사용할 SIP 프록시로 레코더(또는 통화 제어)를 가리켜야 합니다.



이 그림에서는 Configuration(컨피그레이션) **> Outbound Calls(**아웃바운드 통화)에 있는 아웃바운드 규칙의 레코더 구성 요소에 대한 직접 **다이얼을 보여줍니다**.



이 그림에서는 통화 제어(예: Cisco Unified Communications Manager(CUCM) 또는 Expressway)를 통해 레코더 구성 요소에 대한 통화를 보여 줍니다.



참고: SIP TLS를 사용하도록 레코더를 구성한 경우 통화가 실패하는 경우 MMP의 callBridge 노드를 확인하여 TLS SIP 확인이 활성화되었는지 확인합니다. MMP 명령은 'tls **sip**'입니다. CallBridge에서 레코더 인증서를 신뢰하지 않으므로 통화가 실패할 수 있습니다. 'tls sip verify disable'을 사용하여 callBridge에서 이 기능을 비활성화하여 이 **기능을** 테스트할 **수** 있습니다.

여러 개의 녹음기?

설명한 대로 각각을 구성하고 그에 따라 아웃바운드 규칙을 조정합니다. Direct to Recorder 메서드를 사용하는 경우 기존 아웃바운드 to Recorder 규칙을 동작 "Continue(계속)"로 변경하고 이전 아웃바운드 규칙 아래에 첫 번째 아웃바운드 규칙보다 우선순위가 낮은 새 아웃바운드 규칙을 추가합니다. 첫 번째 레코더가 통화 제한에 도달하면 여기서 488 Unacceptable을 다시 callBridge로 보내고 callBridge를 다음 규칙으로 이동합니다.

녹음기의 로드 밸런싱을 수행하려면 통화 제어를 사용하고 여러 녹음기에 전화를 걸 수 있도록 통화 제어 라우팅을 조정합니다.

기드림

MMP

2.9.x에서 3.0으로 업그레이드한 후에는 더 간소하게 재구성해야 합니다.

1단계. SIP 수신 대기 인터페이스를 구성합니다.

streamer sip listen a 6000 6001(SIP streamer가 TCP 및 TLS를 수신 대기하도록 설정한 인터페이스 및 포트. TLS를 사용하지 않으려면 'streamer sip listen a **6000 none'을** 사용할 수 있습니다.

2단계. TLS 연결을 사용하는 경우 스트리머가 사용하는 인증서를 구성합니다.

streamer sip certs <key-file> <crt-file> [crt-bundle] (이러한 인증서가 없으면 tls 서비스가 streamer에서 시작되지 않습니다. 스트리머는 crt-bundle을 사용하여 callBridge 인증서를 확인합니다.

3단계. 통화 제한을 구성합니다

streamer limit <0-500|none> (서버가 제공할 수 있는 동시 스트림 수의 제한을 설정합니다. 이 표는 설명서에 나와 있으며 서버 리소스와 함께 스트리머 제한이 일치해야 합니다.)

Table 7: Internal SIP streamer recommended specifications

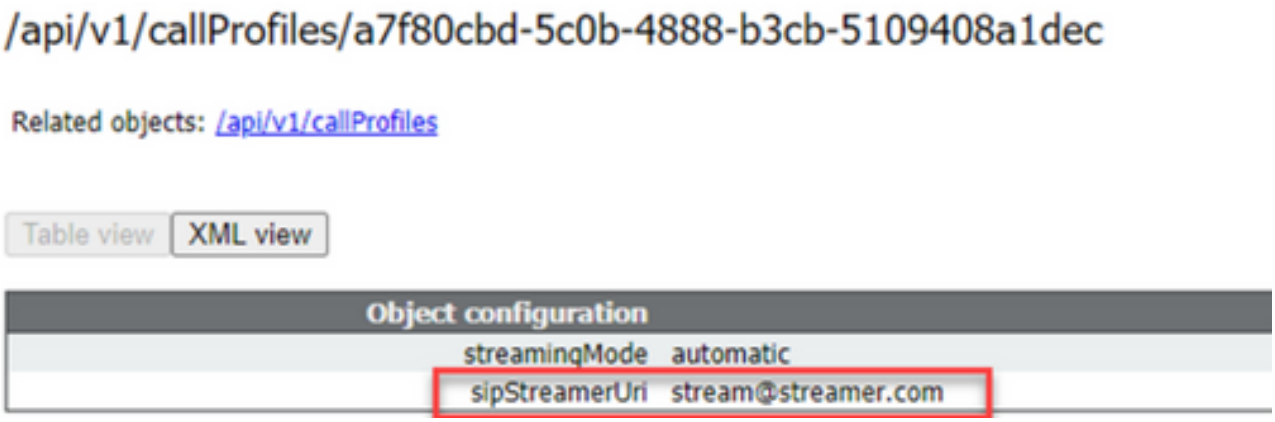
Number of vCPUs	RAM	Number of 720p streams	Number of 1080p streams	Number of audio-only streams
4	4GB	50	37	100
4	8GB	100	75	200
8	8GB	200	150	200

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

api/v1/callProfiles에서 sipStreamUri를 **구성해야 합니다**. 스트리밍을 시작해야 할 때 callBridge에서 호출하는 URI입니다. 이 URI의 도메인은 아웃바운드 규칙 테이블에 추가되어야 하며 사용할 SIP 프록시로 스트리머(또는 통화 제어)를 가리켜야 합니다.



이 그림에서는 Configuration(컨피그레이션) **> Outbound Calls(**아웃바운드 통화)에 있는 아웃바운드 규칙의 스트리머 구성 요소에 **대한** 직접 **다이얼을 보여줍니다**.

이 그림에서는 통화 제어(예: Cisco Unified Communications Manager(CUCM) 또는 Expressway)를 통해 레코더 구성 요소에 대한 통화를 보여 줍니다.

참고: SIP TLS를 사용하도록 스트리머를 구성한 경우 통화가 실패하는 경우 MMP의 callBridge 노드를 확인하여 TLS SIP 확인이 활성화되었는지 확인합니다. MMP 명령은 'tls **sip**'입니다. streamer 인증서가 callBridge에서 신뢰하지 않으므로 통화가 실패할 수 있습니다. 'tls sip verify disable'을 사용하여 callBridge에서 이 기능을 비활성화하여 이 **기능을** 테스트할 **수** 있습니다.

다중 스트리머?

설명한 대로 각각을 구성하고 그에 따라 아웃바운드 규칙을 조정합니다. Direct to streamer 메서드를 사용하는 경우 기존 아웃바운드 to 레코더 규칙을 동작 "Continue(계속)"로 변경하고 이전 아웃바운드 규칙 아래에 첫 번째 아웃바운드 규칙보다 우선순위가 낮은 새 아웃바운드 규칙을 추가합니다. 첫 번째 스트리머가 통화 제한에 도달하면 여기서 488 Unacceptable을 callBridge로 다시 보내고 callBridge를 다음 규칙으로 이동합니다.

스트리머의 로드 밸런싱을 수행하려면 통화 제어를 사용하고 여러 스트리머에게 전화를 걸 수 있도록 통화 제어 라우팅을 조정하십시오.

Expressway 고려 사항

Cisco Expressway for Web Proxy를 사용하는 경우 CMS를 업그레이드하기 전에 Expressway가 X12.6 이상 실행 중인지 확인해야 합니다. CMS 3.0에서 웹 프록시가 작동하고 지원되려면 이 기능이 필요합니다.

CMS 3.0과 함께 사용할 경우 Expressway에 비해 웹 앱 참가자 용량이 증가했습니다. 대형 OVA Expressway의 경우 예상되는 용량은 150개의 Full HD 통화(1080p30) 또는 200개의 Other 유형 통화(예: 720p30)입니다. Expressway를 클러스터링하여 이 용량을 늘릴 수 있습니다. 최대 6개의 노드를 클러스터링합니다(이 경우 4개는 확장에 사용되고 2개는 이중화에 사용되므로 최대 600개의 풀 HD 통화 또는 800개의 기타 유형 통화가 가능합니다).

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 에지

CMS Edge는 CMS 3.1에서 외부 웹 앱 세션에 대해 Expressway보다 높은 용량을 제공하는 것으로 다시 도입되었습니다. 권장 컨피그레이션에는 두 가지가 있습니다.

소규모 엣지 사양

4GB RAM, 4개의 vCPU, **1Gbps** 네트워크 인터페이스

이 VM Edge 사양은 48 x 1080p, 96 x 720p, 192 x 480p 및 1000 오디오 통화인 단일 CMS1000 오디오 및 비디오 로드 용량을 지원할 수 있는 충분한 전력을 보유하고 있습니다.

구축의 경우 CMS1000당 소규모 에지 서버 1개 또는 CMS2000당 소규모 에지 서버 4개를 보유하는 것이 좋습니다.

대형 에지 사양

8GB RAM, vCPU 16개, **10Gbps** 네트워크 인터페이스

이 VM Edge 사양은 350 x 1080p, 700 x 720p, 1000 x 480p 및 3000 x 오디오 통화인 단일 CMS2000 오디오 및 비디오 용량을 지원할 수 있는 충분한 전력을 보유하고 있습니다.

구축의 경우 CMS2000당 또는 CMS1000당 대형 에지 서버 1대를 보유하는 것이 좋습니다.

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.